CYBER SECURITY

The complete guide to cyber threats and protection Second edition

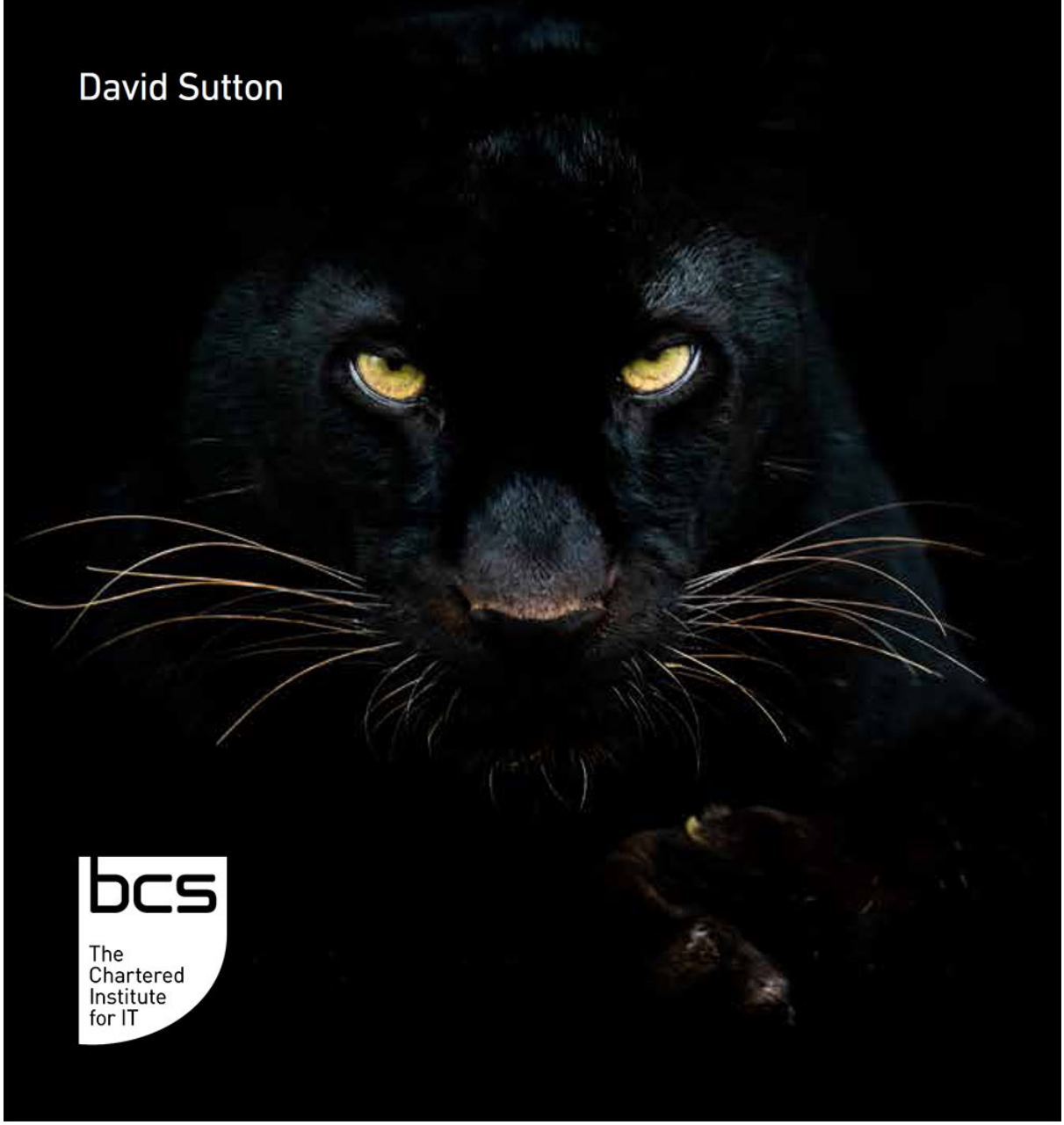
David Sutton

bcs
The Chartered Institute for IT

CYBER SECURITY

The complete guide to cyber threats and protection Second edition

David Sutton



bcs
The Chartered Institute for IT

David Sutton’s book provides a well researched, comprehensive guide to the multifaceted, rapidly growing cyber domain. It serves as a valuable guide to both current professionals and those wishing to embark on a cyber security profession. An excellent read.

***Colonel John S Doody FBCS FCMI CITP ACISP MIOD**, Director, Interlocutor Services Limited*

A very comprehensive primer on cyber security covering issues, solutions and suggestions for further action. After reading this book anyone that worries about cyber security without necessarily wanting to become an expert will find themself much better informed and quite probably much more interested.

***Susan Perriam MBA MSc CMgr MBCS CISSP**, Cyber Security Consultant*

This book manages to strike a perfect balance between technical breadth and depth. It includes enough detail to understand the broad range of concepts and techniques found in a complex industry, along with practical and real-life examples. This latest revision is packed with recent examples, scenarios, tools, and techniques that make it a fascinating read for both industry veterans and recent joiners alike. Highly recommended.

***Martin King FBCS CITP CISSP**, Chief Technology Officer, IT Transformed*

This book describes the eco system of cyber security and provides excellent go-to guides and considerations for people/teams dealing with both technical and non-technical security. Awareness and training are at the very heart of the book, successfully paralleled by descriptions of how our day-to-day information sharing and

protection should take place safely. A useful and insightful read and highly recommended.

***Lesley-Anne Turner**, Cyber Compliance, CDDO, Cabinet Office*

The style and structure makes it an ideal book for students as it covers all the important topics, from the fundamentals of information security such as the CIA model, through to organisational issues (policies and disaster recovery), legal requirements and security standards. Terminology is clearly explained and supported with current, real-world examples. It is a most valuable resource.

***Richard Hind MSc MBCS FHEA**, Tutor of Digital Technologies, York College*

This book gives a good insight into cyber security, with modern day examples and practical guidance on how to proactively mitigate against risks. This will definitely be a book I refer to frequently.

***Bianca Christian**, Business Analyst, Young Business Analysts (YBA)*

On first reading this book, the biggest impression that greets the reader is that it’s NOT a technical reference book and is widely focused on the wider impact of cyber security on society as a whole. It is not just for technologists and treats a complex subject with just the right level of both technical and socioeconomic balance. Highly recommended.

***Adrian Winckles MBCS CITP CEng**, Chair of BCS Cybercrime Forensics SG and OWASP Education Committee*

Cyber Security 2e is a rich technical guide on cyber threats. Leaving no stone unturned, the first half touches on key examples and paints

a clear picture of the current threat landscape that both individuals and organisations face, and the second half contains solutions. Sutton aptly spotlights a number of actions that anyone could be encouraged to practice for good personal and corporate security.

***Ester Masoapatali MBCS**, Information Security Specialist, Partnerships Manager, CybSafe*

This book is a fantastic resource for those breaking into the industry, or for non-security leaders who want to know more about the risks faced by their business. Written in an accessible manner, this second edition gives readers updated information and current examples showing the changing trends and tactics of attackers.

***Jim Wright**, Managing Director, Principle Defence*

This book is for anyone who wants to understand and learn more about cybersecurity. It provides a foundation of cybersecurity knowledge as well as essential practical skills and techniques for entry and junior-level cybersecurity roles. It is also designed to help learners in building a promising and rewarding career pathway in the cybersecurity field.

***Dr Sherif El-Gendy FBCS**, Information Security Expert*

This highly accessible second edition provides a thorough update to the world of cyber security in a non-technical manner; firstly clarifying cyber security issues and then focusing on cyber security solutions. If you are looking for a go-to reference that explains cyber security in plain language, this book is for you.

***Tim Clements FBCS CITP FIP CIPP/E CIPM CIPT**, Purpose and Means*

This book demystifies what can, to many, be a rather bewildering topic, and it sets clear context and eloquently describes the

landscape of threats and issues, and provides clear, actionable advice across key topics. A handy and well-written reference guide, and highly recommended reading!

***Paul Watts MBCS CITP FCIIS CISSP CISM**, former CISO and Distinguished Analyst, Information Security Forum*

A thought-provoking and excellent read. Essential for cybersecurity practitioners working across numerous specialisations and at all levels of management. This blended use of theory and practical applications sets this book apart, complements industry-leading certifications and make it a must-read for anyone working within cyber.

***Gary Cocklin CITP CISSP**, Senior Cyber Security Practitioner, UK Royal Air Force (RAF)*

This book is not just for cyber professionals, it's for everyone. This book is easy to follow and clearly articulates what cyber is and why it matters. It provides insights into why cyber-attacks occur and offers practical and technical guidance for individuals and businesses to protect themselves. This will be my go-to resource for cyber security.

***Thando Jacobs**, Business Analyst, Senior Leadership Team, Young Business Analysts (YBA)*

This book delivers a comprehensive overview of cyber security and is packed with numerous interesting, relevant examples to illustrate key points. Readers will gain insights on why they might be attacked and measures to protect against ever increasing cyber threats. Therefore I highly recommend this publication for individuals and organisations alike.

***Olu Odeniyi**, Cyber Security, Information Security and Digital Transformation Advisor, Thought Leader and*

Speaker

CYBER SECURITY

BCS, THE CHARTERED INSTITUTE FOR IT

BCS, The Chartered Institute for IT, is committed to making IT good for society. We use the power of our network to bring about positive, tangible change. We champion the global IT profession and the interests of individuals, engaged in that profession, for the benefit of all.

Exchanging IT expertise and knowledge

The Institute fosters links between experts from industry, academia and business to promote new thinking, education and knowledge sharing.

Supporting practitioners

Through continuing professional development and a series of respected IT qualifications, the Institute seeks to promote professional practice tuned to the demands of business. It provides practical support and information services to its members and volunteer communities around the world.

Setting standards and frameworks

The Institute collaborates with government, industry and relevant bodies to establish good working practices, codes of conduct, skills frameworks and common standards. It also offers a range of consultancy services to employers to help them adopt best practice.

Become a member

Over 70,000 people including students, teachers, professionals and practitioners enjoy the benefits of BCS membership. These include access to an international community, invitations to a roster of local

and national events, career development tools and a quarterly thought-leadership magazine. Visit www.bcs.org/membership to find out more.

Further information

BCS, The Chartered Institute for IT,
3 Newbridge Square,
Swindon, SN1 1BY, United Kingdom.
T +44 (0) 1793 417 417
(Monday to Friday, 09:00 to 17:00 UK time)
www.bcs.org/contact
http://shop.bcs.org/

CYBER SECURITY

The complete guide to cyber threats and protection
Second edition

David Sutton

bcs
The Chartered Institute for IT

Published by BCS Learning and Development Ltd, a wholly owned subsidiary of BCS, The Chartered Institute for IT, 3 Newbridge Square, Swindon, SN1 1BY, UK.
www.bcs.org

Paperback ISBN: 978-1-78017-5959
PDF ISBN: 978-1-78017-5966
ePUB ISBN: 978-1-78017-5973

British Cataloguing in Publication Data.
A CIP catalogue record for this book is available at the British Library.

such information or any instructions or advice contained within this publication or by any of the aforementioned.

All URLs were correct at the time of publication.

Publisher's acknowledgements
Reviewers: Debbie Evans, Steven Sands, Angus McIlwraith
Publisher: Ian Borthwick
Commissioning editors: Rebecca Youé/Heather Wood
Production manager: Florence Leroy
Project manager: Sunrise Setting Ltd
Copy-editor: Cathy Tingle
Proofreader: Barbara Eastman
Indexer: Matthew Gale
Cover design: Alex Wright
Cover image: shutterstock_1543677161_AB Photographie
Typeset by Lapiz Digital Services, Chennai, India

In October 2021 a third planned family holiday was spoiled (Covid lockdowns spoiled the first two attempts) when I was admitted to University Hospitals Sussex, where I spent three weeks. I returned home in considerably better health.

This book is dedicated to all the truly amazing NHS staff in both the Chichester and Worthing hospitals, who work relentlessly to care for their patients, often under great physical and emotional stress. They deserve far more than mere applause.

CONTENTS

LIST OF FIGURES AND TABLES

AUTHOR

David Sutton’s career spans more than 55 years and includes radio transmission, international telephone switching, computing, voice and data networking, structured cabling systems, information security and critical information infrastructure protection.

He joined Cellnet (now Telefónica UK) in 1993, where he was latterly responsible for ensuring the continuity and restoration of the core cellular networks and represented the company in the electronic communications industry’s national resilience forum. In December 2005 he gave evidence to the Greater London Authority review into the mobile telecoms impact of the London bombings.

David has been a member of the BCS Professional Certification Information Security Panel since 2005 and delivered lectures on information risk management and business continuity at the Royal Holloway, University of London, from which he holds an MSc in Information Security.

He is a Chartered Fellow of BCS, the Chartered Institute for IT, a member of the Chartered Institute for Information Security (CIISec),

a Freeman of the Worshipful Company of Information Technologists and a Freeman of the City of London.

Other books by the author

Business Continuity in a Cyber World: Surviving Cyberattacks. New York: Business Expert Press, 2018. ISBN 978-1-94744-146-0

Information Security Management Principles. Third edition (co-author). Swindon: BCS, 2020. ISBN 978-1-78017-518-8

Information Risk Management: A Practitioner's Guide. Second edition. Swindon: BCS, 2021. ISBN 978-1-78017-572-0

ACKNOWLEDGEMENTS

I would like to express my thanks to BCS for kindly inviting me to produce a second edition of this book, and to my wife Sharon for yet again putting up with my grumpier moments and for her unceasing encouragement.

While I have referenced many (hopefully) reliable sources and included most of the suggestions from the book's excellent peer reviewers, the views I have expressed are my own, as are any errors and omissions.

PREFACE

While conducting my research for this (and the first edition of this) book, I have noted literally hundreds of cyber security incidents – some relatively trivial, some rather more serious. What has never ceased to amaze me is not that they keep happening, but that the same kinds of incident keep happening, and that some people do not appear to learn the lessons of others' mistakes and occasionally even of their own.

In the 21st century, we are almost totally reliant upon information technology, and in particular the interconnectedness that allows us to conduct our lives more efficiently. We now regard access to the connected world as a basic utility along with gas, electricity and water. As business, commerce and government continue to place their services online, we have become increasingly dependent upon something that few people truly understand, and to which some for whatever reason are denied access.

It is an unfortunate fact that when the internet was developed (originally as the ARPANET[1]), its main purpose was to enable information to be shared freely between institutions conducting

research for the US Department of Defense (DoD), and because it was essentially a closed network, security within it was not even considered as a requirement. A consequence of this is that many of the protocols used over the internet are completely insecure, and until recently there has been a general reluctance among the software development community to build security into the protocols and applications that make use of it.

That aside, many of the underlying security issues in cyberspace are often caused by a lack of understanding of the risks of using cyberspace; by people who have not been adequately trained to do their job; who have not done it correctly; or who were simply unaware that there was anything for them to do in the first place. These issues affect everybody who uses cyberspace – in their personal as well as professional lives – at home, while travelling and at work.

When electronic equipment became a commodity product in the late 1960s and early 1970s, enthusiasts began to experiment with modifications – both to hardware and software – and they became known as ‘hackers’. Hacking then was a benign activity, intended to encourage learning and to find ways of improving the performance of electronic equipment, but as time progressed the term began to be used in a derogatory way for those who broke into other people’s computer resources.[2]

While there are laws, regulations and rules regarding the protection of physical and information assets, there are fewer that apply to virtual assets within cyberspace. However, in the realm of cyber security, there are some clear objectives:

- to protect the overall security of our activities in cyberspace;

- to plan for responding to disruptive incidents and to exercise those plans;
- to improve the awareness of cyberspace users;
- to share threat and vulnerability information relating to cyberspace;
- to recommend controls appropriate to the risks encountered;
- to address critical interdependencies within cyberspace.

Much of this work is already underway, but there is considerably more to do, and it is an ongoing exercise. In 2020, the UK's National Crime Agency reported that there were an estimated 3.8 million cases of online fraud in the previous year – with the losses due to investment fraud totalling £338 million.[3]

The lesson – as many a security professional will tell you – is that if a well-resourced attacker really wants to break into your computer, read, steal or change your information, then they will almost certainly find a way of doing so. It may not be cheap or easy, it may involve using a mix of technology and human agents, but if they think it is worth it, you will find it very, very hard to stop them.

In 2014, FBI Director James Comey said, 'There are those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese.'[4]

We frequently take things at face value, especially in the online world. Why?

If a stranger approached you in a street and said, 'I can do you a really good deal', you would naturally be suspicious, but put the

same words online, and people are falling over themselves to take up the offers.

The expression, ‘If it sounds too good to be true, it probably is’, is frequently quoted in the online world, but it’s amazing how many people cannot bear the thought of missing out on the possibility of getting something for nothing and end up either getting nothing or losing everything.

Criminals have always preyed upon human frailty and greed and will doubtless continue to do so until the end of time, but there are simple steps we can take to reduce the chance of becoming their victims, and to make their lives so difficult that they go hunting elsewhere.

Criminality does not respect national borders or trade barriers. It is still perhaps too early to tell whether the UK’s referendum vote to leave the European Union (EU) has resulted in negative impacts for the cyber security community, but we can say for sure that new vulnerabilities will surface at frequent intervals, new threats will arise, and that the world of cyberspace will continue to be populated by the good, the bad and the downright ugly.

We don’t really need to know in detail how the connected world works, no more than the driver of a car needs to understand the workings of the internal combustion engine, but hopefully this book will help to make its readers into better drivers.

Shortly before I began to update this book, Russia invaded Ukraine, and within days, members of the loosely coupled hacking group ‘Anonymous’ declared their intention to attack Russian government

and military cyber assets, which they achieved with some degree of success.

This has given the cyber security community something of a dichotomy. While most of us would agree that the invasion was a bad thing, and that Anonymous might be able to influence matters in Ukraine's favour, we should be conscious that attacks on a nation state's government and military infrastructure would constitute an offence in (almost) any jurisdiction, unless of course the attack was undertaken as an act of aggression by one nation state against another.

It is therefore for the individual reader to decide for themselves whether this illegal/unlawful intervention represents well-intentioned ethical behaviour, or whether it is simply a group of cyber terrorists attempting to change the balance of power in the hope that their less respectable endeavours will pass unnoticed.

In March 2020, the UK government introduced a lockdown in an attempt to reduce the spread of Coronavirus, and this resulted in many organisations, not only in the UK but around the world, having to suddenly re-equip their information infrastructures to cope with significantly greater quantities of remote working than they might previously have undertaken.

Those organisations that already had experience of remote working were obliged not only to increase their internal network capacity, but also to ensure that those new to remote working were equipped with a suitable access mechanism, and that telephone calls could be re-routed to them. For those organisations that had never previously engaged in remote working, there was a very steep learning curve, coupled with the need to procure the required infrastructure from

scratch, resulting in shortages of equipment and heavy demands on broadband providers (both at the organisation's central network level and at the customers' end points).

For both types of organisation, this placed increased pressure upon their cyber security capabilities, and in many cases meant that the cyber security infrastructure itself had to be managed remotely.

WHO SHOULD READ THIS BOOK?

The obvious answer to this is probably 'anyone who has an interest in or concerns about cyber security'. It is aimed at both the public and private sectors and should have appeal to home users; students studying information security, computer science and other information technology-related subjects; and information security practitioners and their line managers, whether technical or not.

The aim is to inform the reader about the realities of cyber security, detailing the issues faced by both individuals and organisations, the likely targets of cyber-attacks, the vulnerabilities exhibited by an individual's or an organisation's assets and the impacts these attacks may cause; the kinds of threat we face; and how to go about protecting an individual's or organisation's assets against cyber-attacks.

WHAT EXACTLY DO WE MEAN BY CYBER?

Since this book deals with cyber security issues, we should begin by trying to define 'cyber'.

The science fiction author William Gibson coined the term 'cyberspace' in a short story entitled *Burning Chrome*[5] in 1982, but

did not define it until two years later in his book *Neuromancer*,[6] in which he describes it thus:

> Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation … a graphic representation of data from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters, and constellations of data.

Bearing in mind that this predates the development in 1990 of the World Wide Web by Sir Tim Berners-Lee at the European Organization for Nuclear Research (CERN) by some six years, it is quite a startling piece of insight.

The UK National Security Strategy 2022[7] offers this definition:

> To many of us, cyberspace is the virtual world we experience when we go online to communicate, work and conduct everyday tasks. In technical terms, cyberspace is the interdependent network of information technology that includes the internet, telecommunications networks, computer systems and internet-connected devices. For the military, and when considering our efforts to counter threats in cyberspace, it is an operational domain, along with land, sea, air and space.

Perhaps the most meaningful definition can be found in the present-day definition of cyberspace from the International Organization for Standardization (ISO) of:

> A complex environment resulting from the interaction of people, software, and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.[8]

Cyber security therefore refers specifically to information security as applied to cyberspace, and in this respect it is slightly different from the wider concept of information security, which includes non-electronic information as well. It is sometimes also referred to as computer security or IT security. Again, the ISO standard has a

simple definition for cyber security – ‘preservation of confidentiality, integrity and availability of information in the Cyberspace.’

It notes: ‘In addition, other properties, such as authenticity, accountability, non- repudiation, and reliability can also be involved.’[9]

Finally, the standard defines cybercrime as:

> criminal activity where services or applications in the Cyberspace are used for or are the target of a crime, or where the Cyberspace is the source, tool, target, or place of a crime.[10]

While the first edition of this book was in its latter stages of production in mid-May 2017, the ‘WannaCry’ virus made an unwelcome appearance. News of the attack was not a great surprise, but the scale of it was – I, and many others, had expected it to have a considerably wider impact, and it is to the credit of the IT and security specialists around the world that its spread was limited and dealt with so quickly, although a great many people had a thoroughly frustrating and exhausting weekend. Threats such as viruses and ransomware are covered in detail in Chapter 5 of this book, and methods of preventing and/or dealing with them are covered in Chapters 8 and 9.

Let us hope that the lessons have been learned from ‘WannaCry’: that out-of-support software is replaced, patches are applied and the recommendations in this book are followed. It is not a question of if another attack occurs, but when; and when it does, it may well be far more aggressive.

OVERVIEW OF THIS BOOK

While there is a logical (I hope) layout to this book, although this may be helpful it is not necessary to read through it sequentially – the reader should feel free to dip in and out of chapters in any order they wish.

The chapters are organised as follows:

Part I – Cyber security issues

Chapter 1 – Introduction – what cyber security is all about, and a summary of the expectations of individuals and organisations who would be affected by a cyber-attack.

Chapter 2 – The big issues, including privacy and security (and privacy versus security), confidentiality, integrity, availability, non-repudiation, big data and data aggregation and the likely vulnerabilities that could allow an attack to be successfully conducted.

Chapter 3 – Cyber targets, including finance organisations, commercial businesses, critical infrastructure, manufacturing, academia and research organisations, industrial control systems and government and military targets.

Chapter 4 – Cyber vulnerabilities and impacts, including policy, process and procedure vulnerabilities, technical vulnerabilities, people-related vulnerabilities, physical and environmental vulnerabilities; personal impacts and organisational impacts.

Chapter 5 – Cyber threats, including types of attacker, types of attack, the motivations for and the benefits of launching an attack, the risks involved in doing so, and how attacks typically are conducted.

Part II – Cyber security solutions

Chapter 6 – A brief overview of information risk management, including identifying assets, risk identification, analysis and evaluation, and options for risk treatment.

Chapter 7 – The benefits of business continuity and disaster recovery.

Chapter 8 – Steps that can be taken by both individuals and corporate users to improve their cyber security.

Chapter 9 – Additional steps that can be taken by organisations, including cyber security policies and operational actions.

Chapter 10 – How users can be made aware of cyber security risks, and how training may be required for those more closely involved in securing the organisation.

Chapter 11 – Information sharing, including the information available to assist in the management of cyber security issues.

Appendices

Appendix A – Standards

- ISO/IEC 27000 series standards
- Other relevant ISO standards
- Business continuity standards
- National Institute of Standards and Technology (NIST) standards

Appendix B – Good practice guidelines

- General cyber security advice

- UK government cyber security advice

Appendix C – Cyber security law

- UK law
- EU directives and regulations

Appendix D – Training and qualifications

Appendix E – Links to other useful organisations

Appendix F – Further reading

Appendix G – Abbreviations and glossary

---

1. For an excellent description of how the ARPANET/internet began, read *Where Wizards Stay Up Late* by Katie Hafner and Matthew Lyon (New York: Touchstone, 1998). An Audible version was available at the time of writing.
2. An early example of this can be found in *The Cuckoo's Egg* by Clifford Stoll (London: Pan Books, 1991). Note: this may be out of print, but an Audible version was available at the time of writing.
3. See www.nationalcrimeagency.gov.uk/who-we-are/publications/437-national-strategic-assessment-of-serious-and-organised-crime-2020/file
4. See https://www.businessinsider.com/fbi-director-china-has-hacked-every-big-us-company-2014-10?r=US&IR=T
5. William Gibson (1995) *Burning Chrome*. New York: Harper Voyager, New edition.
6. William Gibson (2015) *Neuromancer*. New York: Harper Voyager, New edition.
7. See National Cyber Strategy 2022 (HTML) – https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022
8. See ISO/IEC 27032:2012 p. 4.
9. Ibid.
10. Ibid.

PART I
CYBER SECURITY ISSUES

1 INTRODUCTION

In this chapter, we will examine the fundamentals of data and information since these lie at the very heart of cyber security. Although the two terms are frequently used interchangeably, it is important to understand the essential difference between them. We shall also consider the wider context of cyber security and provide an overview of the remainder of the book.

BACKGROUND

Anyone born after the late 1980s will have little or no concept of life before mobile phones and the internet. They have grown up accustomed to searching the World Wide Web for resources; sending emails; shopping without leaving the house; listening to music and watching films online; keeping in touch with friends using social media; and a hundred and one other things. If we took away their smartphones and computers, they would find it almost impossible to conduct what some of us will remember as a ‘normal’ life.

While many of us may have experienced difficulty with the transition from writing letters, visiting the library, going to the cinema and buying records, the connected world remains a fact of life and is accepted as such – and it's going to become even more widespread. Services will increase in capability while becoming more intuitive, and they will become faster and cheaper – the newer generations are already considering ubiquitous connectivity and availability of information as the norm.

In recent years, it has become increasingly apparent that many of these services and applications are completely insecure, and, whether by accident or design, can often leak our personal information, location and credentials.

This has resulted in a paradigm shift in the criminal world. The American serial bank robber Willie Sutton (no relation) was once quoted as saying that he robbed banks 'because that's where the money is'. While this may still be true, it is much less risky for a thief to steal money from a computer on the other side of the world than to break into a bank or hold up staff with a shotgun. As we shall see later in this book, it can also be much more lucrative.

We worry about privacy, yet we willingly give out our home address, email address and credit card information to a company we have never heard of in anticipation of getting a bargain. Most of the time we are lucky: the company turns out to be genuine and we get what we paid for. But sometimes we might not be so lucky – either the offer might be a scam, or, rather more seriously, the company's records might be stolen, including the personal information we have provided, and now an unknown third party has this, and can use it, abuse it or sell it on.

When we hear of a new Act of Parliament in which the law appears to give the police and security services the unconditional right to snoop into our private lives, we feel threatened; when we hear that the security services have used the same legislation to intercept communications between terrorists and have prevented an attack, we are encouraged. We understand that there must be such surveillance, but we don't want it to apply to us – after all, as far as we are concerned, we have done nothing wrong. This is something we're going to have to live with, but there is no reason why we should not take measures to protect ourselves from unwarranted intrusion – just as we lock our doors and windows to protect us from intruders.

In a 2019 report on the financial cost of fraud in the UK between April 2018 and March 2019 there were 741,123 crimes reported to Action Fraud, with an estimated £2.2 billion lost by victims; 65 per cent of reports were from businesses and 35 per cent from individuals.[1] The upshot of this is that most people in the UK are now far more likely to be the victims of cybercrime than plain old-fashioned burglary. These figures may not include cases of intellectual property (IP) theft, which is dealt with in later chapters.

When we purchase goods on the internet, especially software for our smartphones and computers, we have to accept the terms and conditions dictated by the seller, but do we ever read them before clicking 'Agree'? In 2014, F-Secure, a provider of security software, arranged for a free Wi-Fi network to be deployed in the Docklands area of London.

> Anybody wishing to use the network had to accept the terms and conditions, and a number of people did so, being completely unaware that they had committed themselves to ‘assign their first-born child to us for the duration of eternity’.

This Herod clause was inserted as a light-hearted way of establishing whether or not anyone had actually read the terms and conditions, and later an F-Secure spokesperson said, ‘We have yet to enforce our rights under the terms and conditions but, as this is an experiment, we will be returning the children to their parents.’

We assume – often wrongly – that terms and conditions will be fair and will comply with legitimate and reasonable trading standards, but often they are so lengthy and written in legalese that even if we begin to read them, we soon lose interest. Of course, if you don’t click ‘Agree’, you can’t use the facility or the software – or maybe can only use a heavily cut-down version of its functionality. We download ‘apps’ for our smartphones and tablet computers that are designed to make our lives more fulfilling, but many of these use the device’s location whether they need to or not, and this data can be collected, aggregated and sold on to others.

So, when things do go wrong, we must accept at least a part of the blame – after all, whether knowingly or unknowingly, we have given away information that can be used to identify us and the chance for someone else to take advantage of opportunities for gain at our expense.

The problem, however, is much wider than that of our own failings. Attackers will try to take advantage of insecure applications and web-based services to gather information about us, and in this case,

it is the organisation that hosts the service and holds the information rather than the consumer that must shoulder the responsibility.

While most organisations who suffer hacking attacks fix the problem (shutting the stable door after the horse has bolted), some change their terms and conditions in such a manner as to place the onus back on the consumer in the event that their website contains vulnerabilities. An example of this is the cyber-attack on the toy maker VTech in December 2015, following which the company made this addition among others to its terms and conditions:

> You acknowledge and agree that any information you send or receive during your use of the site may not be secure and may be intercepted or later acquired by unauthorised parties.[2]

We can all draw our own conclusions as to how secure we think their website is and whether or not we would use it again – that is if we had bothered to read the terms and conditions in the first place. However, their statement would no longer stand up in a court of law, since the General Data Protection Regulation (GDPR) principles for lawful and fair processing require that personal data is processed in a manner that ensures its appropriate security.

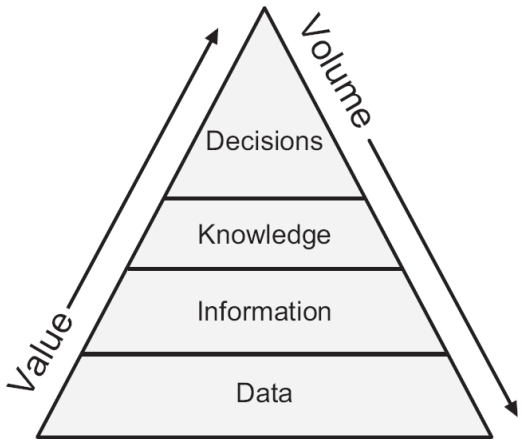
Although the law is evolving to place greater responsibility on companies offering services to safeguard individuals, failing to secure our computers, smartphones and tablets, and wilfully handing over our credentials to strangers is the cyber equivalent of leaving the house unlocked when we go on holiday, with the keys left in the car on the driveway, and we wouldn’t dream of doing that, would we?

The knowledge hierarchy

As a first step towards understanding the knowledge hierarchy, we begin the journey by collecting *data* – facts and figures, as shown in Figure 1.1. We then combine these to construct meaningful *information* that informs us and provides *knowledge*. Using this knowledge, we can make inferences and deductions, predictions and recommendations, resulting in meaningful decisions.

At the data level, volumes are high, but the value of each individual item of data is low. As we move up the scale, through information and knowledge to decision-making, the volumes are greatly reduced, but the value increases dramatically.

Figure 1.1 The journey of data



Examples of the sources of data

There are so many sources of data that it would be difficult to list them all, but let's look at some examples of those that would affect us in our everyday lives in the context of cyber security:

- call data records from our mobile phones that itemise who we have called, the make and model of mobile phone we are using,

when the call was made, from where, and how long the call lasted. The same information will also apply to incoming calls;

- social networks – text and photographs from the likes of Facebook, Twitter, Instagram, TikTok and LinkedIn;
- Global Positioning System (GPS) location recovered from mobile phones and photographs we have posted;
- travel cards, such as the Oyster card used in London and the surrounding areas;
- fitness tracking data from running shoes and body monitors;
- number plate recognition data including data from congestion charge cameras;
- PayPal, credit and debit card transactions;
- withdrawals from automatic teller machines (ATMs);
- airline passenger name records and loyalty cards;
- company ID cards, especially where used for physical access control;
- computer device media access control (MAC) addresses and Internet Protocol (IP) addresses;
- Bluetooth and wireless network (Wi-Fi) identifiers;
- passport scanners;
- store loyalty cards;
- user identification names and associated passwords.

You may be able to add considerably to this list, but just think – if someone could gain access to all or even a large proportion of this information, they would know a great deal about you, your movements, your relationships, both business and personal, your

spending habits, your religion, sexual orientation and/or gender, political views and general health.

They could also increase their store of knowledge by comparing some of your data with that of other people – your Facebook friends, for example.

This information has value – not only to you, but also to those who might wish to make use of it, whether for legitimate purposes or otherwise. When we sign up for a ‘free’ service, it is anything but free. We are trading some of our personal information in exchange for that service, and once we have given it away, we have completely lost control over it, since although data protection law is intended to provide safeguards to personal data, the sad reality is that these rights are not always respected.

The critical information security concepts

When we consider the security of information (including the requirements of cyber security), there are some fundamental terms that should be understood. These begin with what is often referred to as the information security triad – confidentiality, integrity and availability. However, there are two additional terms – authentication and non-repudiation – which are rapidly becoming increasingly important.

Confidentiality

Confidentiality is concerned with ensuring that information is neither disclosed nor made available to those who are not authorised to have access to it. Loss of confidentiality can either be considered as an end in its own right, as in the case of the formula for a new drug, for example, or as a means to an end, as in the example of a

password or personal identification number (PIN) that gives someone access to a bank account.

In either case, the loss of confidentiality can have a profound impact on the person or organisation that suffers a cyber-attack.

Integrity

Integrity is concerned with securing the accuracy and trustworthiness of information, however it's stored or transmitted. Integrity involves ensuring that only authorised people can create, change or delete information, and is very closely linked with confidentiality, since it is usually people who have, whether authorised or not, access to information that will also cause integrity issues.

Integrity failures can also have a profound effect, for example the unauthorised changing of a student's grades from a 'fail' to a 'pass', or a user's access level from 'guest' to 'administrator'; changing a criminal sentence from a custodial sentence to a fine; altering a mortgage applicant's credit rating; or removing details of previous illness from someone's medical records.

Availability

Availability is concerned with ensuring that systems and the information stored on them is available for use when required, and by whatever means have been agreed. For example, a bank's customers would reasonably expect to be able to access their accounts, either online or via telephone banking, at any time of the day or night.

Failures of availability almost invariably result in inconvenience, such as the 2012 failures of the Royal Bank of Scotland systems that left customers without access to their accounts and prevented many

inter-bank transfers; but in extreme cases they could be instrumental in life-or-death situations, for example in the case of access to a hospital database containing details of an unconscious patient's allergies.

Authentication

Enabling a system to identify users with a high degree of confidence is rapidly becoming the norm. In recent years, financial and commercial organisations have introduced additional authentication mechanisms. The old-style username and password have long been considered to be insufficient to make a positive identification, so additional methods have been introduced – one such is two-factor authentication, in which the usual username and password (something you know) are supplemented by another form of identification, such as a token or smartphone app that generates a time-dependent one-time random number (something you have), or a biometric factor such as a fingerprint or iris scan (something you are), as seen on the more recent versions of smartphones and laptop computers.

Non-repudiation

Despite the fact that someone has authorised access to a system or information, in the case of a breach of confidentiality, integrity or availability they can deny having taken the action that resulted in the problem occurring.

Non-repudiation is concerned with ensuring that authenticated users cannot deny having carried out a particular action. This invariably means that a precise audit trail is kept of every action that the user undertakes.

It is also worth taking a little time to explain some of the more common terms that we frequently take for granted.

Security

Security is a term generally used to include both confidentiality and integrity, and to a somewhat lesser extent, availability. It implies quite simply that something is protected from unauthorised access or harm, but the definition really goes no further.

We feel that we and our property are secure when protected against unwanted intrusion, whether by the use of physical locks or by some purely electronic mechanism that forbids entry to those without the right keys.

Security is not only a mechanical or physical condition, but also a state of mind – an emotional condition.

Privacy

Privacy, on the other hand, has a slightly different meaning. While the same considerations as security apply, privacy brings in a more personal view, in that the subject matter, rather than being general in scope, is much more personal to us. For example, someone living under a repressive regime might highly value the privacy of their political opinions.

On face value, we may think that security and privacy are very similar, and in some instances they are. However, there is also a tension between the two – for example, we rely on the government to keep us secure, both individually and as a nation, but in order to do this we may feel that they have invaded our privacy by intercepting our internet transactions and emails. Security can come at the cost of privacy.

While safety represents the safeguarding of data, privacy represents the safeguarding of a user's identity.

This conflict of ideals is covered in the next chapter under 'Surveillance'.

Trust

The Oxford online dictionary definition is that trust is 'the firm belief in the reliability, truth or ability of someone or something'.

Trust is rather like a raw egg. It is extremely easy to break and almost impossible to rebuild. We place our trust in people, organisations and systems, sometimes without thinking or pondering the possible consequences.

Sometimes, when trust is broken, the party responsible suffers irreparable reputational or financial damage, for example when an online trader 'loses' our credit card details along with those of thousands of other customers. However, on some occasions the share price eventually recovers to normal or near-normal levels.

Trust may not be simply a two-way thing. For example, if Alice and Bob trust each other, and Bob and Charles also trust each other, then there may be good reason for Alice also to trust Charles.

Trust can also be widened to larger groups of people and organisations – for example in information sharing, where one individual or organisation shares often sensitive information with the wider group, knowing that it will remain within that group and not be distributed outside it. Information sharing is discussed in greater detail in Chapter 11.

Some critical information security concerns

Big data and data mining

We have heard increasing reports about big data in recent years. The term itself is not particularly informative, since it simply suggests large volumes of data. In fact, it refers not only to large volumes, but also to multiple data sources and their aggregation, and implies both an ability and a will to sift through the records and establish trends – turning information into knowledge.

For example, one could imagine that a major supermarket chain holds big data – its databases contain the registration and payment details for millions of customers; tens of thousands of products; the combination of which customers have bought which products; and when, where and how much they paid, and how.

The value of that data to the supermarket is immense, but it is only its ability to make sound business use of it that will determine its eventual value to both the supermarket and the consumer.

Data aggregation

Data aggregation describes the way in which big data is acquired. Some big data (as in the example above) has just one source, but other uses will require additional data sets to be included. These may be acquired directly by the organisation requiring the data, or if they are not available from within the organisation they may be brought in from outside.

If carried out properly, data aggregation can be a very powerful tool in combining seemingly unrelated data sets into one that can be used to provide a detailed profile of a subject. However, data aggregation is much more than simply a means of acquiring big data. It creates a whole set of challenges in the world of security – for example, combining seemingly unimportant and unconnected

data sources can result in a goldmine of personally identifiable information (PII), which includes:

- name and surname;
- email address;
- phone number;
- home address;
- date of birth;
- race;
- gender;
- credit card numbers;
- data held by a hospital or doctor;
- photograph where an individual is identifiable;
- identification card number;
- a cookie ID;
- IP address;
- location data (for example, the location data from a mobile phone);
- the advertising identifier of your phone.

Further, there is the concept of sensitive personal data, which includes:

- ethnic or racial origin;
- political opinions;
- cultural or social identity;
- philosophical or religious beliefs;
- trade union memberships;

- genetic data;
- biometric data (that can be used to uniquely identify someone).

THE EXPECTATIONS OF USERS AND ORGANISATIONS

Individual users, as well as those who work for organisations, together with the organisations for whom they work, all have an implicit expectation that they will not be impacted by the concepts nor the concerns described above. For example, people have a right to expect that an organisation handling information about them will treat it in confidence, with respect and in accordance with the appropriate legislation such as the Data Protection Act (DPA) and GDPR, and will not allow it to be made available to those who have no entitlement to see it.

This includes the 'selling on' of users' information, much of which is completely illegal. In January 2017, the UK's consumer magazine *Which?* published an article in which it claimed to have been in a position to purchase personal details including names, addresses and credit card details from 10 legitimate 'list broker' firms for as little as £0.04 per unit.[3] People have not only an expectation but also a right to know that their personal details will not be sold on in this way.

People also have a perfectly reasonable expectation that information they access will be correct (integrity), and available to them when they require it (availability). In 2017, a major retail company that operates its own credit card upgraded its systems over a weekend at the end of a month. The upgrade was fraught with problems, and customers were unable not only to access their account details but also to contact the company's customer service operation due to the

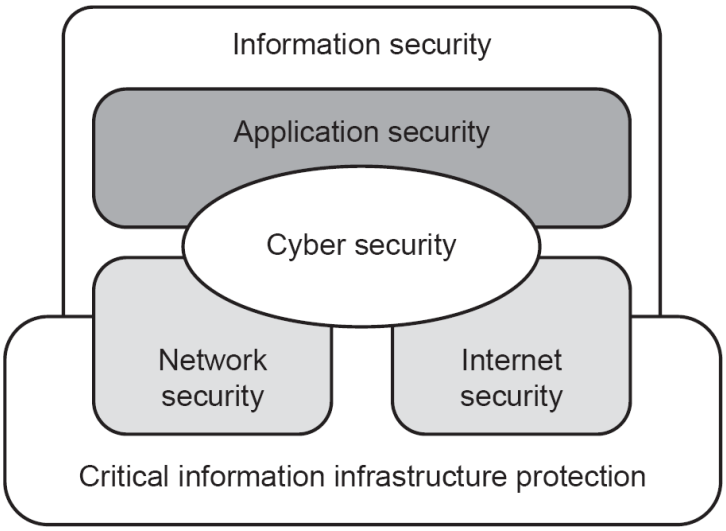
high level of calls. And all this at a time when many of the credit card customers were trying to pay their account.

CYBER SECURITY IN THE WIDER CONTEXT

Cyber security overlaps with several other aspects of security, and Figure 1.2 shows these relationships pictorially:

- Information security, which is concerned with the protection of confidentiality, integrity and availability in all areas of information, not just that which exists in cyberspace.
- Application security, which is concerned with the introduction of controls and measurements to an organisation's applications, whether software, hardware or information.
- Network security, which is concerned with ensuring the protection of an organisation's networks, within the organisation, between organisations and between the organisation and its users. Network security can also include server operating systems (OSs) and increasingly the virtualisation layer and associated management systems in cloud services.
- Internet security, which is concerned with protecting the availability and reliability of an organisation's internet-based services and protecting individual users both at work and in their home environment.
- Critical information infrastructure protection, which covers the cyber security aspects of elements of a country's critical information infrastructure (CII) elements, as discussed in greater detail in Chapter 3.

Figure 1.2 Relationship between security domains



1. See https://www.crowe.com/uk/croweuk/-/media/Crowe/Firms/Europe/uk/CroweUK/PDF-publications/The-Financial-Cost-of-Fraud-2019.pdf
2. See https://www.telegraph.co.uk/technology/2016/02/10/vtech-says-it-is-not-responsible-for-security-after-hack-exposed/
3. *Which? Magazine*. January 2017. London: The Consumer's Association.

2 THE BIG ISSUES

In this chapter, we will examine the key cyber security issues that concern us, both as individuals and organisations, regardless of the inherent threats and vulnerabilities or the actual impacts and consequences. These will be discussed in later chapters.

SOME THOUGHTS ON SOCIAL, POLITICAL AND OTHER ISSUES

The Industrial Revolution began in Great Britain around 1760, and during this period there were many technical developments, beginning with the move from stone and wood-based construction to the use of iron and steel, and the move from water, man- and horsepower to the use of steam engines to drive the new machinery such as powered looms. This enabled increased and more efficient production of goods and food.

Not everybody welcomed these developments (for example the Luddites), since they resulted, in many cases, in people losing their jobs, but by the mid-19th century there was no going back to the ‘old’

ways, with the exception of small artisan specialists who were able to continue (and to a certain extent, still are) without recourse to the latest technology.

This revolution resulted in wide-ranging changes to both the social and economic structure of the country – people gradually became wealthier, lived longer and enjoyed a less physically demanding lifestyle. Manufacturing companies enjoyed greatly increased demand for their products, and the resulting increase in profits made many of their owners extremely wealthy.

Fearing that the spread of these new technologies to other countries would potentially damage Britain's position in the world, the government at the time banned the export of machinery and production techniques, and forbade skilled workers to travel abroad.

By the mid-19th century, however, this position was untenable, and over the next few decades equipment, techniques and skills spread across most of the western world.

As technology developed over the 19th and 20th centuries, standards of living generally increased, and political differences became focused mainly on economic stability, while new developments in weaponry and warfare technology gradually enabled conflicts to be resolved with (usually, but not always) reduced loss of life.

Now in the 21st century we are witnessing the next stage of industrial revolution following the development of the internet; the physical world is fast being superseded by the digital world, whose advent has brought us many benefits, allowing almost instant (and

virtually free) worldwide communication and the sharing of information, whether for good or evil.

However, as with the original Industrial Revolution, not everybody is able to take advantage of the facilities we are now offered. There is a risk that those who do not have access to the online world may not only be disconnected from it but may also suffer some form of deprivation as a direct result (digital poverty), while those who are uncomfortable with using online services, or who are nervous of the technology needed to do so, are also cut off from it.

While much of this book describes technology issues, it is clear that they are just the surface layer, and that there exist many social, economic and political issues below them.

From an economic perspective, matters depend on which side of the law you stand. On one side, there is money to be made quite legally, selling legitimate goods and services online and permitting customers to access their bank accounts. Viewed from the other side, there is also money to be made – by selling fake or illegal goods, stealing people's banking credentials and stealing their money, or simply scamming people out of their hard-earned savings. This, however, also requires a lack of awareness on the part of the victims.

From the social perspective, online access allows cheap or (more often) free communications by voice, text or video with anyone else – the cost frequently being covered by advertising revenue. Collaborative working has become increasingly effective without the need to meet physically, saving time, effort, needless travel expenditure and carbon emissions, with social media applications allowing the sharing of information, photographs and videos. Both of

these attributes have been of enormous benefit during the pandemic lockdowns in 2020 and 2021, relieving to some extent the stress of being unable to meet in person or in groups.

The negative side of the social aspect has made the distribution of inaccurate, offensive, inflammatory and libellous information immensely easy, and has reputedly poisoned the normal processes of elections of governments. It should be noted here that this also requires some of the recipients of this misinformation to be sufficiently taken in to believe it.

> For example, there is some evidence that in the lead-up to the UK referendum on leaving the EU, Cambridge Analytica (described by a former employee as a ‘psychological warfare company’) was hired to disseminate false information in order to influence the outcome of the referendum.[1]

Unfortunately, disseminating false information (disinformation) of this kind is not currently a crime, although it can be extremely harmful. Were it an offence on the statute books, several UK newspapers would already be in the firing line. However, the UK government has proposed to introduce legislation into the online safety bill,[2] which would (in theory at least) protect us from state-backed disinformation. It remains to be seen whether this actually takes place, and if so, whether or not it has any effect.

From a political perspective, too, the digital world has good and bad points. On the positive side, it permits governments to engage in cyber espionage – which seen from the viewpoint of other countries is a negative aspect – and where and when they feel so minded they can conduct more intrusive activities. They also have the freedom to make use of the World Wide Web to promulgate their views (whether truthful or otherwise), and especially to direct the content of the media when newspapers and radio and television stations support their views, and where possible suppress dissenting views.

On the negative side, many governments fear the ability of their populations to share their opinions, and at the same time they need to take precautions to detect and foil cyber-attacks, whether by terrorist organisations or by unfriendly (or supposedly friendly) governments.

Clearly, the technology that provides the internet and the World Wide Web is not truly to blame for all the negative aspects – these require the full involvement of the offenders who, if the infrastructure was not there, would still find ways to undertake their nefarious activities. These might take longer, carry a greater risk in their undertaking, and not result in such generous results, but they would still happen in one form or another.

The tech companies who provide social media services, such as Twitter, Facebook (now known as Meta) and so on must shoulder some degree of responsibility for policing their services' content. Banks and online retailers must ensure that their services are fully secured, and that the personal and financial details of their customers are protected against unauthorised access.

Governments should also ensure that suitable legislation (supported by appropriate, and enforced, penalties) is enacted to protect individuals, businesses and itself against cyber-attacks, while at the same time allowing freedom of expression and protest to continue.

At the same time, banks, retail organisations and central government should remember that for many years to come there will be people who either cannot or are unwilling to become members of the online community, and will still require access to banking, retail and government services, and must make suitable provision to include their needs.

> My 96-year-old neighbour falls into this category, and because his bank refuses to give him a telephone number to call his branch, I drive him into town, try to park – using his Blue Badge – near the bank and wait while he queues to have a two-minute conversation with one of the staff. Quite ridiculous.

However, much, in the end, comes down to the individual users and organisations who make use of the online environment. If they are to gain the most out of the online benefits, and outwit and survive the ‘bad guys’, they need to familiarise themselves with the threats, understand the potential consequences, assess the risks, and, using the available information and technology, enact suitable measures to protect themselves.

When you look at all the issues, they tend to resolve themselves into one of four areas of cyber security:

- cybercrime;
- cyber harassment or cyber bullying;
- cyber warfare;
- cyber surveillance.

CYBERCRIME

The first big issue we will examine is that of cybercrime. Many cybercrimes will also be recognisable as ‘ordinary’ crimes, but each of these will have a cyber element to it – either as a means, using cyber systems or networks to achieve an end, or where cyber systems or networks are the means, the method and the target.

Cybercrime can affect anybody, regardless of whether or not they are online. Once a criminal acquires your bank or credit card details, they can spend your money, even if you have never used a computer.

Financial theft

Financial theft is the most widespread type of cybercrime. Unlike a conventional bank robbery, where hard cash is stolen, this type of crime requires little or no risk to the thief – no guns, masks or getaway cars – and can deliver a significantly greater reward.

One downside to the criminal of financial theft by cyber means is that there may well be an audit trail, indicating where the money came from and where it was transferred to. Cyber thieves have tried to address this weakness in their plan by money laundering,[3] and also by distancing themselves from the criminal act itself by using

intermediaries. This increasingly makes use of cryptocurrency as a means of undertaking money laundering.

Increasingly, cyber criminals are taking less interest in acquiring individual personal details in order to commit the crime – not that we should be complacent about this – but are looking to acquire thousands or millions of individuals' personal details so that they can maximise their return on investment, since each item of information will have potential value.

They often achieve this by selling the data to larger criminal gangs whose resources make them better placed to use the information in wide spam campaigns such as those that purport to sell high-end watches and mobile phones.

Alternatively, criminal gangs are targeting specific groups of individuals by advertising on legitimate websites non-existent vehicles for sale. After agreeing to purchase the vehicle via email with the fraudsters, buyers then receive an email purporting to be from an organisation such as Amazon stating that their money will be held in an escrow account, and that once the buyer has confirmed that they agree with the arrangement, the money will be released to the seller, therefore offering 'buyer protection'. In reality, of course, once the money has been transferred by the buyer into the 'escrow account', the transaction ends with no vehicle in sight.

Hacking

The term 'hacker' originally referred to someone who was inquisitive about how things worked, took them apart to understand them and frequently put them back together again in a way that made them work better.

A later definition of a hacker was someone who wrote software that would perform a useful action in an elegant manner. When computer memory was an incredibly expensive commodity,[4] a piece of code that was reduced to run in a very small memory space was considered to be ‘a great hack’.

Some of the greatest inventions have come through this benign activity, but sadly the term ‘hacking’ has mutated to become something rather uglier in recent times, referring to those who have less honourable intentions and break into other people’s computers for fun, revenge or to make a statement of some form – often on political, ethical or environmental matters.

Website defacement

Some hackers will simply deface an organisation’s website (usually its ‘landing’ page) in order to make their point, usually by making derogatory statements about the organisation, or showing offensive images. Others will alter the code behind the landing page to divert users to other websites – sometimes malicious – in order to extract money or plant a virus of some kind.

Planting the flag

Some hackers will simply break into a system ‘because it’s there’, and ‘because they can’. There is little merit in this, other than to demonstrate how clever they are and how poor the target’s security is. This intrusion, sometimes called ‘planting the flag’, is to show they have been successful, and will (they hope) gain them the admiration of their peers.

On occasion, this form of hacking is relatively benign, and can result in defacement of website pages. Hackers of this type are often script kiddies, who take advantage of software and techniques they have

discovered in the darker areas of the World Wide Web. Although they may mean no real harm, serious damage can easily result since their knowledge and ability to use the software and tools may be very limited.

However, script kiddies can graduate into full-blown cyber criminals if they are encouraged and able to develop their skills, and this can cause a great deal of damage.

> Many organisations affected by this type of hacking accept they have been less than careful about their cyber security and respond by tightening their security practices, while others may press for arrest, prosecution and even deportation, as in the case of Gary McKinnon, who was accused of hacking into almost 100 NASA and US military computers over a 13-month period in 2001 and 2002.[5]

Exploitation

Exploitation takes intrusion to another level entirely. A hacker who exploits a system they have penetrated may well exfiltrate, delete or corrupt information, and the impact of this can be extremely serious, not only for the target organisation, but potentially for its customers and system users.

In 2013, the American chain store Target was hacked and the personal details, including credit card details, of 40 million customers were stolen.[6] The hackers almost certainly gained access by using the stolen credentials of a maintenance supplier before planting the malware in the cashiers' terminals. Technical security measures (intrusion detection software) spotted the attack, but failure to follow processes and procedures resulted in nothing being done to prevent the information from being stolen. The cyber-attackers were to blame for the original crime, but the company was equally culpable for failing to act and protect its customers' data.

In a more recent example from 2022, attackers were able to use social engineering (see Chapter 5) to gain access to an employee's computer in the Marriott Hotel in Baltimore-Washington and extract 20 GB of data that allegedly included credit card details of guests. Although the attackers stated that they did not ask for payment on this occasion, claiming that they were simply highlighting the company's lack of security, the hotel chain's version of events is somewhat different. In 2018 and 2020 Marriott had been successfully attacked, with the loss of millions of unencrypted passport numbers and hundreds of millions of guest booking records.[7]

Denial of service (DoS) and distributed denial of service (DDoS)

Although they can be used for other purposes, DoS attacks are usually mounted in order to prevent legitimate users from accessing an organisation's website. The reasons for this will vary – some will be used as a weapon of blackmail ('pay us money and we'll stop');

some will be due to political or other activism (usually known as hacktivism) and will simply be to cause financial loss and/or public embarrassment; while others will be in revenge for some action, real or perceived.

Some DoS attacks are designed to crash a website by overloading it to a point at which it can no longer function at all, whereas others will simply block legitimate access, leaving the supporting applications unable to receive and process requests for service. Either way, the end result is that response from the website will slow dramatically and will usually stop completely.

DoS attacks can also target an organisation's email service, causing the exchange server to overload and stop handling valid email traffic. Such an attack can be mounted by a disgruntled employee.

Nowadays, the most seen kinds of DoS attack are the distributed (DDoS) attacks,[8] in which multiple computers work together to overload the target website. Attackers frequently use botnets (discussed in Chapter 5) in order to assemble sufficient capability, since very few stand-alone systems are capable of successful attacks against very large websites.

A recent example of a major DDoS attack was in February 2020, when Amazon Web Services suffered an attack that lasted for three days. Amazon claimed that its AWS Shield system was able to defend the organisation from the attack, the motivation for which is unclear.[9]

Copyright violation and intellectual property (IP) theft

Copyright violation is a major industry, but often brings little direct reward, other than ‘free’ goods for the recipient. Copyright infringement can occur with materials including music, films, books, photographs and computer software.

While the copyright holder normally still retains ownership of the material, illegal copies are made, and the owner therefore is deprived of the benefit they may have earned from it.

Copyrighted material is often distributed using file sharing websites, such as the Pirate Bay, using torrent files that link users back to the particular file or files to be downloaded. As more users join the sharing process, the downloaded material becomes shared between them, and distribution is on a peer-to-peer basis. This also makes it impossible to identify the individual who originally hosted the material, since many copies will have been made in a very short space of time.

While exchanging files by torrent is not illegal, the content may well be, especially if it is someone else’s copyright and they have not agreed to its being shared in this way. Losses to various industries are estimated to be in excess of US $50 billion per annum.

Various organisations exist to protect copyright[10] – these include:

- the Copyright Licensing Agency;
- the UK Copyright Service;
- the Performing Rights Society;
- the British Association of Picture Libraries and Agencies;
- the Intellectual Property Office;

- the Motion Picture Licensing Corporation;
- the Design and Artists Copyright Society;
- the Federation Against Software Theft.

While the theft of intellectual property is similar in many respects, its subsequent sale or distribution is usually not. Whereas copyright violation generally allows a wide audience to benefit from free software, music or video material for example, IP theft is more generally carried out to order for one or a few select customers, and rarely becomes more widely distributed. In the past, this would have commonly been referred to as ‘industrial espionage’.

At the other end of the scale, however, some IP theft can reap rich rewards. For example, if an attacker can steal the formula for a rare and potentially expensive medication and is able to replicate it, there are potentially many millions (in any currency) to be made. If the people who purchase the medication are lucky, it will be safe and reliable. If they are unlucky, the consequences could be fatal. The consequential financial loss to the IP owner can be disastrous, having invested extremely large sums of money into research and development of the drug, only to lose its formula to a competitor who can then sell it with merely the production, packaging, marketing and distribution costs.

Use of dark patterns[11]

The use of dark patterns, while not actually a crime, does tend to come very close to the line between fairness and dishonesty.

Occasionally when you access a website you will find that because the text on web pages was unclear, you have agreed to download software or accepted an offer when you did not intend to do so.

Sometimes, web page designers deliberately place selection boxes in unusual places or make the choices complex so that you are driven to making their choice rather than yours.

Entire businesses exist that use psychological analysis to identify the shapes, sizes and colours of buttons, click boxes and text that a user is most likely to click on – and those that they are least likely to – when accessing a web page. The results are sold to organisations developing new websites or upgrading existing ones with the intention of encouraging users to select the organisation's choice rather than making their own.

In extreme cases, items you did not request might be added to your online shopping basket, and if you aren't sufficiently aware, you may inadvertently purchase something you simply don't want as well as the items that you do.

This process of making web pages confusing is referred to as dark patterning, and the techniques are extremely subtle, relying on known aspects of human behaviour. For instance, if you are trying to book a flight, you may find that the airline or travel agency offers to sell you travel insurance, and that unless you deliberately opt out of the offer, as opposed to opting in, you will discover that you have bought it and may have some difficulty in obtaining a refund.

There is nothing technically illegal about these dark patterns, but to many people's minds they represent sharp practice. Pressure groups are now developing that try to combat such practice by setting out a code of conduct for web developers. However, it is possible that only legislation will fully resolve the issue, since the sales and marketing policies of the offending organisations are likely to drive the use of

dark patterns for the foreseeable future – especially where it increases that organisation's revenue.

In the EU, the Digital Services Act will go some way towards preventing the use of dark patterns, but it remains to be seen whether the UK will either adopt a British version or develop its own legislation.

On a positive note, however, while the author was finalising this version of the book, Amazon announced that it will shortly make changes to its Prime account so that a subscriber can opt out with just two mouse clicks, instead of the rather convoluted process in place currently.

CYBER HARASSMENT OR CYBER BULLYING

Cyber harassment or bullying is simply the act of harassing or bullying a person or group of people using cyber-based methods such as social media, text messaging and the like. I have chosen to separate this from cybercrime, since although cyber bullying is actually an offence under criminal law, it does not generally relate to financial crime but does represent a major issue in today's society. However, some jurisdictions have introduced legislation that extends the offences of conventional harassment to include cyber harassment as well. The difference between cyber harassment and cyber bullying is usually that with cyber harassment, anyone or any organisation can be the victim, whereas cyber bullying generally refers to children and young adults as being the victims.

Cyber harassment or bullying can begin in the same way as conventional harassment or bullying, where one person makes a negative comment about another, causing offence. The bully

(someone who has control issues) seizes upon this effect and continues to exploit it, often encouraging others to join in. The results can be devastating, and some people who have been persistently harassed or bullied have been driven to take their own lives. Cyber harassment or bullying is no less aggressive and dangerous, and it may take a number of forms.

Cyber harassment is intended to make the victim aware that something very specific might happen to them. The person making the threats might be known to the victim, or they may be unknown, and targets can include organisations that the person making the threats feels have caused some injustice to them or to someone else.

Cyber stalking

As with conventional stalkers, cyber stalkers operate in two slightly different ways. First, they can follow the movements and activities of their victim by stealth, and not alert them to the fact that someone is following them. Second, they can still follow the movements and activities of their victim, but this time rather more openly, with the victim being aware they are being stalked, but usually without knowing the identity of the stalker.

Sometimes the victim will be a person known to the stalker – a relative, former partner or neighbour; but on other occasions the victim will be completely unknown to the stalker – as in the example of a celebrity, the chief executive officer (CEO) of an organisation or a politician. Whoever is the target of cyber stalking, its main objective is usually to cause distress, and unless stopped it is frequently successful.

Cyber stalking is sometimes concerned with intimidation of the victim by letting them know that the stalker is watching them, but that is normally where it stops.

Cyber trolling

The activity of cyber trolling is a form of verbal abuse designed to intimidate or offend the victim in some way. Cyber trolls make confrontational or abusive statements online and differ from cyber stalkers in that cyber trolls rarely make much effort to hide their identity. Cyber trolling also differs from cyber bullying or harassment in that it is carried out quite openly, possibly in the hope that others will support the cyber troll's point of view, and is designed to cause distress or embarrassment to the victim.

Cyber trolling also differs from free and intelligent discussion since it neither provides nor invites a rational interchange of views, and focuses purely on the cyber troll's negative and usually strongly expressed and frequently irrational opinions.

Cyber trolls will often use social media or online discussion forums to post inflammatory comments, designed to provoke a reaction or response from the victim, which will invariably seed the troll with further opportunities for posting comments, and this can easily escalate into a full-blown online fight.

Current wisdom suggests that ignoring comments posted by cyber trolls is by far the best way of dealing with them, since their activities will soon peter out if there is no reaction, response or exchange. Alternatively, on many discussion forums, offensive users can be blocked so that victims of trolling no longer see their comments.

Cyber trolls can also be reported to the forum administrator and may have their accounts deleted as a result.

Account blocking can also extend to individuals who post fake news or generally offensive comments as opposed to targeting an individual person or organisation.

> An excellent example of this is the blocking of Donald Trump's Twitter account in January 2021.

CYBER WARFARE

The term 'cyber warfare' describes the process by which one nation state or politically motivated group conducts an attack against some aspect of another – possibly its critical infrastructure (CI), its government's political process or indeed the offensive or defensive capability of its armed forces.

Until recently, warfare was a relatively straightforward affair. One nation state picked a fight with another nation state, and their two sets of armed forces attacked each other with gusto until one nation state capitulated and the war was over. This was only ever really complicated when more nation states joined in on either side, but the net result was usually the same. This kind of warfare is often referred to as symmetric warfare since both 'sides' are usually evenly matched.

With the rise of terrorism, however, the boundaries became less clear. A militant group could declare war on many nations – frequently being quite indiscriminating about whether some of those nations supported the same religious or ideological concepts. Since terrorist groups rarely have the same purchasing power as nation states, the weapons they use are often home-made – improvised explosive devices (IEDs), for example – but since they can be used in unconventional ways – not in a straight battle – they tend to be deployed as roadside devices or detonated by suicide bombers.

This kind of warfare is termed asymmetric warfare, since one side may be extremely small in numbers in comparison to their opposition but can still deliver devastating results.

However, a cyber-attack or cyber incursion by one nation state against another does not technically mean that they are actually at war, and the attack could simply be seen as an act of aggression as opposed to a full declaration of hostilities.

Cyber warfare adopts both symmetric and asymmetric methods, since it can be used by one nation state against another, or by small groups – even by individuals – against a significantly larger adversary. Cyber warfare can be conducted just as easily from an armchair, a stool in a cybercafé or an office chair in a government building, and carries few of the dangers of conventional warfare, unless the other side can locate the attacker and direct a drone to deliver lethal ordnance.

If they work for the government or military, or are a highly skilled and experienced individual, once a ‘cyber warrior’ has completed their daily or nightly shift, they can walk home safe in the knowledge that

they are unlikely to be shot at, despite possibly having caused their adversary significant cyber havoc.

Espionage

Espionage is the capability to obtain secret information without either the permission or the knowledge of its owner. Governments routinely spy on one another. They have done so for centuries and will doubtless continue to do so for many more. Sometimes, the espionage is concerned with finding out what another government has – for example, its nuclear missile capability – while at other times it is concerned with another government's intentions, which may be more difficult to discover, but which might be deduced, given sufficient data.

> In July 2022, *The Guardian* reported[12] that the UK Security Service (MI5) had revealed that 50 Chinese students had left the UK in the past three years as part of a crackdown on the threat of espionage posed by Beijing, the main targets being UK university research departments.

Cyber espionage is no different, but whereas conventional espionage involves agents who place themselves in some danger by operating in enemy territory, cyber espionage can be safely conducted from a comfortable office with no risk whatsoever to the agent.

If a field agent is captured and exposed as a spy from another nation state, the diplomatic repercussions can last for months or years, but because the cyber espionage departments of nation states take great care to conceal their identities, and frequently disguise the attack as originating from somewhere else, it is difficult, if not impossible, to prove absolutely who carried out an attack, and assumptions, even if correct, do not constitute sufficient evidence.

Surveillance

Surveillance is slightly different from espionage – perhaps not in the way it is carried out, but in its aims and objectives. Surveillance focuses on keeping track of people's activities, communications and contacts, and in cyber warfare terms could be described as being more akin to investigations into terrorism, or attempting to understand another nation's capabilities and intentions.

This is where there is a particular crossover in the techniques used by security agencies and the military, since both need to co-operate in order to track down suspected terrorists.

Surveillance has played a key role in identifying and locating individuals and groups who have clear intentions to carry out acts of terrorism. Although the details remain secret, the UK government has made it clear that a number of potentially lethal attacks have been prevented by careful surveillance, and they are using this argument to make the case for legislation that makes it less demanding for the security services to be able to monitor the activities of the population – that unsteady balance between security and privacy we mentioned earlier.

Non-military surveillance is also discussed in greater detail in the section on cyber surveillance later in this chapter.

Infiltration

Although governments and security services do not publicly discuss this area of cyber warfare, one of the best (but risky) methods of conventional surveillance has been through infiltration of activist groups, allowing agents to identify possible targets and the leaders of these groups.

Cyber infiltration is no different in terms of its objectives, and agents must be able to infiltrate online groups just as easily. Because of agents' physical separation from the rest of the group they are much less at risk if their activities are identified and there is the possibility of their being 'outed'.

Sabotage

When we consider sabotage, we often think of war films in which a small group of saboteurs destroy something the enemy holds dear. Usually, one or more meet a grisly end or are captured and interrogated, but usually the film ends with success.

Cyber sabotage is again much less risky for its teams of saboteurs. Operating remotely, they will identify and surveil their target from afar, and by one of the methods of attack we have already described will carefully position their weapon, which will then wreck the enemy's infrastructure.

By far the best example of this is the Stuxnet attack on the Iranian nuclear research programme. It was believed to have been conducted by a joint US–Israeli team,[13] who developed software that would identify a very specific laboratory – Natanz in Iran – which used Siemens SCADA[14] systems to control the centrifuges. The malware they were able to deploy caused the control system to repeatedly speed up then slow down the rotation of the centrifuges, while hiding the fact from the monitoring systems, resulting in destruction of the machinery.

While it was not 100 per cent successful, the action did at least temporarily slow down Iran's nuclear programme.

It has also been shown to be possible to commit sabotage on elements of critical infrastructure.

The Idaho National Laboratory in the USA ran a test in 2007 in which it repeatedly opened and closed the circuit breakers connecting a 50 MW generator to the grid out of synchronisation, causing the generator to shake itself to pieces.[15] On a larger scale, the impact on a major power station generating hundreds of megawatts of power could seriously impact the country's economy.

Psychological cyber warfare

Psychological cyber warfare only differs from cyber harassment or bullying in one key aspect – that of scale. Whereas cyber bullies are generally individuals or small groups, psychological cyber warfare is conducted by much larger groups, for example terrorist organisations, and by nation states.

Psychological cyber warfare generally has one of two main objectives. First, it is used by one organisation or government to demoralise the population of another country, with the ultimate objective of them withholding their support for the current regime.

> During World War II, both the Allies and the Axis forces used psychological warfare radio broadcasts in attempts to cause antagonism towards the opposing governments. In this respect, psychological cyber warfare simply takes the medium from broadcast radio to the internet.

The alternative objective is subjugation and repression of the population by its government – often an oppressive regime – which can use cyber techniques to deter the population from standing up to it and to spread the fear of the possible penalties for doing so.

As well as using the internet as a weapon in this way, such regimes frequently also control how the population can use the internet by preventing access to websites that do not support the regime or that actively oppose it, as in the case of the Great Firewall of China.

Negative news stories in the foreign press about a regime can be suppressed, and glowing accounts of its leadership and their achievements can be substituted – all while the population lacks the basic amenities that less repressed societies enjoy, as in the case of North Korea, for example.

Deception

Declarations of war are very public. When one nation state actively and openly declares war on another, the event is fairly obvious; the outcome can be witnessed by everybody; the participants are easily identified; and an open attack by one nation state against another may be the trigger for war to be declared. However, in asymmetric warfare, the question of ‘sides’ is less easy to visualise, and many nation states may be targets, while a few individuals who could be based anywhere in the world may be waging the war.

Does then a cyber-attack by one nation state against another nation state or its infrastructure qualify as an act of war? It is often very difficult to establish and prove exactly which nation state or which terrorist group has initiated the attack, and although it may appear obvious on the surface, things are not always as they seem.

One nation state may obscure the origin of a cyber-attack against another by planting ‘evidence’ in the attack vector that would lead one to infer its origin, but who is to say that it is not the work of yet another nation state that wishes to take advantage of a possible breakdown in diplomatic relations?

Whatever the reason, establishing the source of an attack will always remain an extremely difficult challenge, and for that reason, the term ‘cyber war’ is perhaps somewhat misused.

CYBER SURVEILLANCE

Whether or not we are conscious of the fact, we are continually under surveillance. There are two quite distinct types of cyber surveillance. The first that readily springs to mind is that of intrusive or invasive snooping, which particularly since the Snowden revelations[16] is usually associated with surveillance by the security services. The second, which on the surface is much less intrusive, is the collection and use of data about us by organisations with whom we interact on a daily basis.

Targeted surveillance

This will usually be because the subject has come to the attention of the authorities, who are taking an active interest in his or her activities. Such people are normally (but not always) criminals or terrorists, and we are content to know that the appropriate police or security services are giving them their full attention.

However, if we gain the impression that we are being snooped upon we tend to take a rather different view, and at this point we are conscious of the problem that the police and security services constantly experience when they do not have a definite target – they have to collect far more data than they need and then (in theory) throw away any that is not relevant and which they don't need to retain.

Because the cost of storage media is continuing to fall rapidly, data collection and storage is costing less as time goes on, and therefore organisations will collect and store as much as they can and keep it until they can understand how best it can be used, provided that they adhere to the principle of minimisation under data protection law.

Catch-all surveillance

In the aftermath of the Snowden leaks, we have heard that the security services on both sides of the Atlantic are monitoring telephone calls, emails, internet searches and transactions without necessarily having the legal right to do so, which gives us serious cause for concern since we have almost no control over this.

The National Security Agency (NSA) has its own interpretation of the word ‘collect’ as applied to data. We might think of collection as simply involving monitoring, interception and storage of data, but the NSA considers that it also includes analysis of data.

It is also worth noting that the USA does not currently have any general federal data protection legislation, although there are several instances of very specific legislation, such as the Children’s Online Privacy Protection Act (COPPA). A number of states do have varying levels of data protection legislation, but the upshot is that should your personally identifiable information be hosted there (for example on Facebook/Meta) you may have no control whatsoever over it.

Alarmed by a spate of requests by the American security services for operators to hand over personal correspondence, and following the unsuccessful attempt by the FBI to force Apple to weaken the security settings of an iPhone, in April 2016 the authors of WhatsApp introduced end-to-end encryption[17] of users’ messages so that they can only be decrypted by the recipient.

However, in January 2017, it came to light that the WhatsApp service may not be as secure as claimed, since the company has the ability to reset the encryption key, and in certain circumstances attackers can pose as the recipient of a message and force WhatsApp to reissue keys. Sophisticated manipulation of this system would let attackers intercept and read messages, and unless the sender has selected the 'Show Security Notifications' option, they might never know that a new key had been generated.

Apple refused to comply with the FBI's request,[18] and the FBI later withdrew it, claiming that they had been able to successfully break the security of the iPhone in question, possibly with the assistance of the Israeli security company Cellebrite.

We shall deal with the state aspects of surveillance in Chapter 5 under 'Whistleblowing', but for now let us consider the theoretically more benign aspect of surveillance undertaken by organisations with whom we interact on a day-to-day basis making use of the data they collect when that interaction takes place. For example, whenever we make an internet search, along with our anticipated search results the search engine will deliver advertising material that matches either our current or previous searches in order to help us make informed decisions. Well, that's their story anyway.

Referring back to the Cambridge Analytica issue mentioned in the first section of this chapter, their activity demonstrated a level of investment that might be used by a nation state, but in this case by a non-nation state actor.

In practice, of course, the operators of the search engines are not completely altruistic. They earn revenue from advertisers and the more often they can place an advert in front of a potential customer, regardless of whether or not it is actually read, the more revenue they are likely to earn.

> In August 2022, it was revealed that Amazon had signed a deal to purchase iRobot – the makers of the Roomba vacuum-cleaning robot.[19] It is reasonable to assume that the Roomba, having mapped the rooms in your house so that it can clean them, would store that information. If that is the case, and the manufacturers could upload the data the Roomba has collected, this would essentially provide Amazon with floor plans of your house.

It's all about someone else making money on information that they acquire (legally or otherwise) about you or your preferences, and usually without your knowledge or active consent.[20]

Internet search

When you search for something on the internet, how much personal information are you giving away freely? Probably more than you think. Let's just take Amazon as an example. They keep an accurate record of everything you've bought from them, so that if you need the same thing again, with a couple of clicks you can order more and not have to try to remember who supplied it.

They also keep a record of every item you've searched for in the recent past, so in spite of the fact that you're trying to locate a mint vinyl copy of *Dark Side of the Moon*, you will still see 'recommendations' below your search results for the camera lens you looked at last week, a book you thought about buying a month ago and a DVD similar to the one you bought for your partner at Christmas.

They know what interests you and they want to sell you more. They know how often you actually buy compared with simply browsing; they know that if you look at an item more than a number of times, you will probably buy it; they know how you like to pay; and they know whether you will save up items so that you get free delivery.

When you use an internet search engine, your search request is stored. The links that you subsequently click on are stored. The search engine stores details of every website you search on regularly and automatically makes it a 'favourite'.

In December 2016, the UK's Investigatory Powers Act obtained Royal Assent and became law. One of its more controversial aspects is that the records of any website and messaging service visited by UK-based citizens from any device must now be retained by the communications company providing the service.

It has been reported that a total of 48 government departments[21] will be able to view this data, and while many, including the police and security agencies, would appear to have a legitimate need to do so, it is difficult to imagine why the Foods Standards Agency might.

Apart from the increased invasion of privacy that this introduces, one of the chief concerns, voiced by the chairman of the Internet Service

Providers' Association,[22] is that 'it only takes one bad actor to go in there and get the entire database'.

Cookies

It's not only searches that leave a digital trail – whenever you visit a website, it can leave one or more small files on your computer known as 'cookies'. Many cookies are essential to being able to use the website – for example, when you are shopping online, the store needs to be able to link your shopping basket with your computer so that you buy what you actually want. Other cookies are less helpful to you, and may record which pages you have opened, which flights you've examined or which camera you've investigated.

Cookies continue to frustrate me. Every so often, a website asks me to confirm my choices of their cookies, and I have no option but to do so. I believe I am extremely unlikely to change the settings – do they think that I am suddenly going to elect to agree to receiving their advertising or that of other organisations in whom I have no interest? I think not.

Some cookies may not seem to be particularly awful, but when you next visit a website selling airline tickets, it may just use the fact that you've been there before to hike the ticket price or advise you that the cheaper flight is full and that you must choose another more expensive one. This form of surveillance – and subsequent manipulation – is very subtle, and we are not usually aware of it.

Other cookies record these things so that advertisers can place their adverts in prominent parts of the screen. If you use one of the main search engines or shopping websites and subsequently examine a particular type of camera, when you revisit the site you will almost

certainly see an offer from one of the photographic suppliers for that very camera. Again, this is relatively benign in its own right, but remember that the search engine or website may well have recorded every single item you've looked for. This kind of information enables advertisers to build a very accurate profile of you as an individual, and (in theory) to deliver highly relevant advertising to you. In practice, of course, the advertiser will be advertising what they want to sell you, not necessarily what you might want to buy.

In 2011, an EU directive required owners of websites to obtain consent from users before placing cookies on their computer. However, although this seems at first like a great idea, there are two fundamental flaws.

Some websites do not allow you to say 'No' to cookies. They frequently allow you to click on 'I understand' or something similar, click on 'Tell me more', or simply ignore the message.

Many websites operate a system of 'implied consent', which means that if you ignore the cookie message described above and continue to use the website, you have implicitly given your permission for the placement of cookies. This is actually a breach of GDPR, but not necessarily one that can be easily dealt with by the authorities.

However, the laws and regulations relating to cookies are continuously changing, and in most cases you can make an informed decision as to whether to accept or reject them. Also, some websites remind you of the status of cookies held on your web browser and ask you to either confirm your previous decisions or to change them.

Currently the Information Commissioner's Office in the UK issues guidance regarding the use of cookies to state that only those cookies that are strictly necessary should be turned on, and those that are optional should require the user's explicit consent.

Email

When you send or receive an email, a copy is stored by default on your provider's server in case you ever need to find it again. You can disable this, but how many of us actually take the trouble to do so?

At a corporate level, organisations should have a policy in place that sets out the arrangements for retention of emails, and this (working within the GDPR) should include how long emails are retained and how and when they will be deleted.

Analysis of emails, whether these are obtained by interception or by access to an internet service provider's (ISP's) servers, can provide a surveillance organisation with a wealth of information, since there may well be a complete archive of all emails in the 'conversation', and every email sent and received will contain details of the sender and recipients.

Email can be just as pernicious as website cookies. Unless you delete every copy of every email you have sent or received, including those that you have forwarded to other people, the message will still exist in some form somewhere, and emails can also reveal many facts about you, just as web searches can.

Unless you encrypt all your emails containing personal information (again, how many people actually do this?) they can be read just like a postcard, copied, printed, forwarded to others, and used in

evidence against you if they contain either something derogatory you have said or something that implicates you in a crime.

Email can be an extremely powerful tool in the cyber surveillance world. Not only can the content provide valuable information to the security services and law enforcement agencies, but also the ‘to’ and ‘from’ fields in an email can yield additional targets for surveillance.

Just think for a moment about those investigations that made the headlines about the activities of the former US President Donald Trump, and how phone call records, email and text messages featured in those news items.

Far from being a blessing, email can be a curse, and many of us will look at our inboxes and wonder how and why we have accumulated so much junk. This is similar to keeping all the letters, postcards, advertising material and free newspapers we receive in the post: we would drown in a sea of paper.

Email can also attract cyber-attacks through the receipt of spam, and this is perhaps the most tiresome aspect of this modern miracle.

Smartphones

Many people now have moved away from the conventional mobile phone. All it can do is make and receive calls and text messages. Along came the iPhone and changed all that. Now all the major mobile phone vendors have jumped on the smartphone bandwagon, and the amount of data they can collect from you is absolutely staggering.

The term ‘smartphone’ is probably a misnomer. The device is actually a very small computer that runs applications, takes

photographs and just happens to make and receive calls and text messages as well, so in those terms it is not too different from your laptop – just much smaller and often no less powerful, and nowadays the camera quality can easily equal or exceed that of expensive professional digital single-lens reflex (SLR) cameras.

Unless you have switched your phone off, your network operator always knows roughly where you are so that it can route calls and text messages to you. Unless you have ventured into the security settings on your smartphone, you will probably be relaying your GPS coordinates, and this will pinpoint your position to within a metre or two.

Every application on the smartphone that makes use of your location is now able to track your movements. This will be absolutely fine if you're using a mapping application, but are you as happy to have your location sent back to the application developer when you're playing a game or reading a book? Of course, the application developer is not particularly interested in where you are, but they might be selling your location along with those of thousands of others to a third party.

Have you taken a photograph on your smartphone? The location was recorded in the photograph's metadata, known as the exif data. When you upload that photograph to the internet, that exif data becomes available as well. The exif data will also contain details on when the photograph was taken and probably also the serial numbers of the camera and lens you used.

Facial recognition

Facial recognition permits the identification of individuals either live from a modern camera or smartphone, or from a previously taken photograph. The image is compared with those held in a central database, and sophisticated algorithms are used to match features such as the eyes, the mouth, the shape of the head and so on. Once a match has been made in this way, additional information about the individual may be acquired, either from the same database or from a wider search of the internet or other databases.

The police and security services must make considerable use of this in tracking down and monitoring suspected criminals and terrorists, but as individuals we must face the fact (no pun intended) that if someone's photograph is posted on the internet, they can be identified and possibly traced regardless of whether or not they have committed a crime.

However, if facial recognition is used as a means of authentication, it could be possible to falsify the matching process by wearing a mask, so this should not be used in isolation.

Consider, for example, someone who was photographed while taking part in a peaceful demonstration in a country where the government exercises total control over its population. By the security service combining surveillance and facial recognition using artificial intelligence (AI), the demonstrator might subsequently receive a visit from the secret police.

Terms and conditions

Terms and conditions are potentially a major issue, as we discussed in the introduction to this book. Few of us even glance at them. Due to their general length and complex 'legalese' wording, hardly

anyone will have read any of them from start to finish and will have simply clicked on the ‘Accept’ button, potentially committing themselves to signing away any control they might have had over their personal information or agreeing (albeit unwittingly) that they have committed themselves to some form of subscription, purchase or service. Of course, the software vendors give us no choice – there is no negotiation involved, and if we want the goods or software, we have to revoke all rights we may have had.

Additionally, and possibly more worryingly, by signing away our rights by accepting the terms and conditions, we may leave ourselves open to some form of surveillance, such as providing our location when using a smartphone.

When you first use an application on your smartphone or tablet computer, you will have had to accept the terms of use, which invariably will include that the application author’s organisation can store, use and sell on the details of what you have done. Not only that, because many of us don’t turn off the GPS facility in our smartphones, the application can contain the ability to track your location and report it back to the provider – sometimes even when you are not actually using the app.

Even if you do read the terms and conditions when you initially load an application or purchase goods on the internet, the seller may at some stage update them (their ability to do this without telling you may be enshrined in the original terms and conditions), so you may never know that they have changed. If the supplier does inform you there has been a change, the privacy bar may have been lowered, but will you read them this time?

Store loyalty schemes

Are you enrolled in a store loyalty scheme? Many of us are, and this allows the store to record the fine details of everything we buy there, how much we have paid for it, where and when. Store loyalty schemes are a wonderful invention. The deals the store subsequently offer us usually represent good value for money, and this often helps the store to dispose of goods it might not otherwise be able to sell. We might be able to enjoy a discount on some products; a free coffee and cake on our next visit; an invitation to the ‘special’ pre-Christmas shopping event; or jump the queue when a new product is announced. Some stores now produce a smartphone application that gives you access to their website, your account and many other things.

Do you collect Tesco points, Nectar points or Avios? Think of the volume of data they can collect based on your spending habits.

Have you ever received an email out of the blue from a company you have never dealt with online and wondered how you came to receive it? It is highly likely that when you signed up for a loyalty scheme, you failed to tick one of the opt-out boxes on the form – or was it an opt-in box? This is yet another failing within the context of GDPR.

Many companies use dark pattern methods (see ‘Use of dark patterns’) to trick you into making the wrong choice when completing such a form, and since you didn’t actually read the terms and conditions, you find that you have agreed to the store selling your contact details to a third party. Of course, you can try to change this, but often it is either too much trouble or the means of doing so are too difficult to find on the company’s website, so you just put up with it.

Is this a cyber security issue? Definitely, since now a third party has all your details as well as the store that offered you the loyalty scheme, and if the third party's network is hacked, those details could go anywhere.

Credit cards

What about credit and debit cards? In the UK, billions of pounds are spent annually using credit and debit cards rather than cheques or cash, and much of this spend is online. One of the consequences of the Coronavirus pandemic was the huge increase in online spending, as people were unable to go shopping in the normal way for many weeks. The UK Cards Association reported that in 2021 alone £250 billion was spent online including purchases on both credit and debit cards.[23] Credit cards allow us to make spontaneous purchases when we might not have sufficient funds in our bank account; as long as we pay off the outstanding balance each month there is no financial charge; and they even act as protection if something goes wrong when we make some purchases.

The same applies to newer forms of payment. mPay, ApplePay, Google Pay, AndroidPay and travel money cards such as Caxton all represent benefit to the provider as well as to the consumer, but with similar levels of risk.

Combine a credit card or debit card with a loyalty scheme and things begin to look very rosy indeed for the provider. Combine them yet again with their smartphone application you downloaded that tracks your movements and you could find that the next time you are shopping you receive a text message as you pass a particular supermarket aisle that offers you extra discount. Possible? Absolutely.

Combine them further where a retailer provides the SIM card for your mobile phone (and therefore knows your regular contacts and movements), and when you accepted the terms and conditions you may have agreed to allow the retailer to include the fact that their banking service is aware of all your current account financial transactions.

Travel cards

Do you travel in a major city like London? If you do, you will probably use an Oyster card or something similar. You load the card with money and use it whenever you need to – on the Underground, the buses, the river and even on some overground train services.

Again, the card provider knows exactly when you have travelled, your route, how long it took (except on buses, where you only use the card when you board and not when you leave) and where, how and how often you top up the card.

All this is seemingly quite harmless, since we benefit from much of the technology and services, but to go back to one of the original points of this section – if the security services wanted to build up a profile of you, it would be extremely easy to pull together the credit/debit cards, store cards, travel cards, email messages and internet searches and combine them with closed-circuit television (CCTV) facial recognition images.

Data aggregation and analytics

We have mentioned data aggregation in this book's introduction, but now we have had an opportunity to examine some of the types of data that organisations hold about us, and over which we have

absolutely no control, we can see that a data aggregator could build up a very detailed picture of our daily lives.

They would know where we lived; where we work, and possibly the kind of work we do; who our partners and friends are; when and where we shop; what and where we eat and drink; where we go on holiday; what music and films we like; what newspapers and magazines we read; what television shows we watch; what kind of car we drive and where we go in it; and what our hobbies are. In short, there's very little about our private lives that is actually private any more.

In August 2022, it was reported that Meta has been injecting code into its websites in order to track its users, which allegedly allows the organisation to send its users targeted advertising. However, there are concerns that Meta is also capturing additional information such as passwords, addresses and credit card details.[24]

Home entertainment systems

In recent years, home entertainment systems have become increasingly sophisticated. Televisions are able to connect to the internet, not only to allow the downloading of viewing material, but also to provide the manufacturers with statistics relating to viewing habits. In theory, this form of remote monitoring should only be carried out with the viewer's express permission, but there have been cases in which manufacturers have uploaded viewing information without the viewer being aware of it.

In March 2017, following a WikiLeaks publication, it was reported that the CIA was using software developed in-house to remotely enable the microphone on certain televisions, even when the viewer

believed that the set was switched off. The report stated that the programme ‘Weeping Angel’ also allowed audio to be recorded while the set was in standby mode, the recording being uploaded once the set was switched back on again.[25]

While this form of information gathering may be less common than others, it is considerably more intrusive, and suggests that George Orwell’s imagined world of *1984* has come a step nearer.

WHY WE SHOULD CARE

From a personal point of view, we should always be concerned that our personal information is being stored and used in a proper manner. When our credit card provider calls us to query a transaction that appears to fall outside our normal spending profile, we are delighted that they have taken the time to do so in order to protect us.

Proactively, therefore, we should take greater care over the information we give out to others – information that can be abused or misused for their gain and our loss; and reactively, if we detect abuse or misuse of our information or credentials, we should take immediate steps such as changing passwords and notifying financial institutions.

From a business perspective, there are four key reasons why we should take notice of cyber incidents, plan to defend ourselves and our organisations against cyber-attacks, and be prepared to respond to them if they occur.

- **Managing risk:** It is nothing less than good practice to manage risk, and that includes the risks of cyber-attacks, whether these

are accidental or deliberate, whether as individuals or businesses. Indeed, there are fiduciary responsibilities for corporates (and board members) to do this.

- **Customer expectations:** Customers have a right to expect organisations to safeguard their information when they provide it to them for whatever reason, and they need to trust that the organisations will not misuse or re-sell it – in other words, to expect robust adherence to data protection legislation. When the GDPR (described in greater detail in Appendix C) came into force in 2018, these expectations were considerably extended.
- **Legal compliance:** In highly regulated sectors, organisations may need to be able to demonstrate compliance with national or EU law; international standards, such as ISO/ International Electrotechnical Commission (IEC) 27001; and sector standards, such as the Payment Card Industry Data Security Standard (PCI DSS),[26] the US Health Insurance Portability and Accountability Act (HIPAA),[27] and the Sarbanes–Oxley Act.[28]
- **Good practice:** Organisations should be able to demonstrate good security practice as a means of achieving competitive advantage. Some larger organisations may make use of the ISO/IEC 27001 certification as a means of demonstrating this, while small-to-medium enterprises (SMEs) may ensure they remain within the law by adopting the Cyber Aware[29] or Cyber Essentials schemes promoted by the UK government.[30]

Under an EU ruling, C-131/12,[31] we now have the right to be forgotten should we choose to have information about us removed from websites, especially if we feel that it is no longer relevant. This is also enshrined in GDPR legislation, which the UK government has enacted regardless of Britain's exit from the EU.

We keep our memories in digital form now rather than exclusively on paper. Letters, postcards and photographs are all just another group of files on our computer, and when we compare information about us to footprints in the sand or the vapour trail of an aircraft, the digital footprint we constantly generate remains, possibly forever, while physical footprints are washed away by the tide and vapour trails evaporate.

In 2014, a group founded by Max Schrems, an Austrian privacy activist, launched a case in the Irish High Court, claiming that Facebook had handed personally identifiable information to the US NSA, and this had placed the company in breach of EU data protection law, since its European headquarters are in Ireland, and the data was supposedly protected by the 'Safe EU–US Privacy Shield' agreement.

In 2020, the European Court of Justice judged in a case known as 'Schrems II'[32] that the EU–US Privacy Shield was invalid, since US law has several shortcomings that impede the protection of personal data and thus violate the GDPR. The judgment essentially required organisations such as Facebook (now Meta) to assess the country's level of compliance with the GDPR, and to ensure adequate protection of personal data.

WHAT MAKES CYBER SECURITY DIFFICULT?

Unfortunately, life is not as simple as we would like it to be, and there are a number of inhibitors or barriers to our achieving our expectations about privacy and security, especially for individuals, smaller organisations or SMEs.

Cyber security knowledge and skills

Cyber security is often seen as a highly specialised subject, and many individuals and smaller organisations believe that they do not possess the necessary knowledge or skills to understand or undertake the necessary work to protect themselves from cyber-attack. This need not necessarily be the case, since it is really a cultural matter with often technical solutions, as we shall see in Chapter 8.

Organisations of all sizes frequently do not possess the suitably skilled people or resources they should allocate to this kind of work.

The organisation's senior management team may not fully understand the need for good cyber security and how it might be beneficial to their business, and also generally do not grasp that the data and thus the information held by the organisation belongs to them and not to the IT department.

When we examine the standards produced in the cyber security field, it appears that many of them are geared more towards larger organisations and multinationals. However, the UK Cyber Essentials scheme does address this for smaller organisations. Many SMEs

outsource their IT, and often the outsourced companies themselves are also SMEs and can lack good cyber security skills.

Cyber security capabilities

If an organisation is able to allocate resources to internal IT work, it is often assumed that those same members of staff will also take on the responsibility for cyber security. This is a major mistake since it may conflict with one of the main principles of cyber security – the segregation of duties.

The organisation must define the cyber security requirement because it owns the data, information and strategic direction. The IT function must use good security practice to turn the requirement into technical policies. The human resources (HR) function must then, in consultation with the IT function and the business function, develop staff training and education to support the requirement.

In cases where the IT function is outsourced, there is often a tendency to overlook or underplay the need for good cyber security in the outsourcing contract, since those undertaking the negotiation may not have sufficient understanding of the requirement, or they may remove it, since they see it as an unnecessary cost. If this aspect is omitted from such a contract, there may be no individual or department responsible or accountable for security failures.

When the security function is outsourced, it may very often have been a form of abrogation of responsibility rather than of delegation. The principle that must be applied is that while organisations can outsource the information security implementation and management, they cannot outsource the responsibility for ownership.

There will be additional financial burdens on the organisation in developing and implementing a cyber security framework that will be suitable to protect it, and obtaining capital or operational budget approval may prove a challenge.

The ability to develop a sound cyber security strategy is somewhat dependent upon senior management within the organisation having a clear understanding of information security risk management, and in some cases this will not be the case. Again, it goes back to the concept that this is about developing a security culture with frequently technical solutions.

Organisations can also consider their cyber security capabilities in terms of any of the Capability Maturity Models,[33] which are often used for software development but which have many parallels in the cyber security environment.

Cyber security standards and implementation

As you will see in Appendix A, there are literally dozens (if not hundreds) of standards in the information and cyber security domains. Some of these are largely generic and apply to a wide range of security topics, while others are highly specific, being applicable to a single technology or function.

Unfortunately, many of the mandatory requirements of the existing standards are more relevant to larger organisations and therefore difficult for individuals and SMEs to use effectively.

There is also a danger, especially for larger organisations, of believing that gaining certification to ISO/IEC 27001 means that they are fully secure and that all they now have to do is ‘keep turning the

handle'. This could not be further from the reality of the situation, since complacency is often the cause of organisations and individuals missing a new threat or vulnerability and being successfully attacked as a result. In the case of SMEs, however, certification to ISO/IEC 27001 may be less attractive for a number of reasons:

- Although there are many excellent standards (mainly the US National Institute of Standards and Technology (NIST), BSI and ISO/IEC standards) in the cyber security field, few of them are easily adaptable to SMEs.
- Implementation guidelines tend also to be more suited to larger organisations, and therefore SMEs may find it challenging to adapt them to their own situation.
- Many of the international standards carry the implication that organisations will have implemented some higher-level processes and procedures that many smaller organisations may not have been able to undertake.
- SMEs may not feel able to commit to the level of expenditure that might be required to achieve ISO/IEC 27001 accreditation.

Although these may appear insurmountable, in Chapters 8 and 9 of this book we shall cover many of the recommendations that both individuals and SMEs can undertake without the need for extensive knowledge or skills, and without resorting to expensive work in interpreting and implementing the international standards. This is where the UK government's Cyber Essentials scheme comes into its own.

1. See https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy
2. See https://www.theguardian.com/uk-news/2022/jul/04/legislation-aims-to-shield-uk-internet-users-from-state-backed-disinformation
3. Transferring the proceeds of criminal activity through bank accounts in countries that have a more relaxed attitude to crime and are happy to turn a blind eye.
4. I recall my employer in the late 1970s paying around £100,000 for a 128 kilobyte memory cabinet. It took up the same space as a double wardrobe and consumed more than a kilowatt of power.
5. See www.bbc.co.uk/news/19959726
6. See https://eu.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/
7. See https://www.theregister.com/2022/07/06/marriott_hotels_suffer_yet_another/
8. See www.bbc.co.uk/news/technology-35213415
9. See https://www.cybersecurityintelligence.com/blog/amazon-web-services-fights-off-massive-ddos-attack--5046.html
10. Links to each of these are provided in Appendix E.
11. For more information on dark patterns, please visit www.darkpatterns.org
12. See https://www.theguardian.com/uk-news/2022/jul/06/50-chinese-students-leave-uk-in-three-years-after-spy-chiefs-warning
13. See http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet/
14. Supervisory Control and Data Acquisition.
15. See https://www.wired.com/story/how-30-lines-of-code-blew-up-27-ton-generator/
16. See https://www.theguardian.com/us-news/the-nsa-files
17. See https://www.whatsapp.com/security/
18. See https://www.apple.com/customer-letter/
19. See https://www.theguardian.com/technology/2022/aug/16/ask-all-the-time-why-do-i-need-this-how-to-stop-your-vacuum-from-spying-on-you
20. Just because you click ‘Accept’ on the Terms and Conditions it does not mean that you agree with them, but usually that you have no choice but to accept them if you wish to use the application or service.
21. See https://yiu.co.uk/blog/who-can-view-my-internet-history/
22. See www.bbc.co.uk/news/technology-38068078

23. See https://www.statista.com/statistics/285374/online-retail-spending-in-the-united-kingdom-uk/
24. See https://www.theguardian.com/technology/2022/aug/11/meta-injecting-code-into-websites-visited-by-its-users-to-track-them-research-says
25. See https://hothardware.com/news/wikileaks-publishes-cia-guide-for-weeping-angel-samsung-smart-tv-tool
26. See https://www.pcisecuritystandards.org
27. See www.hhs.gov/hipaa/for-professionals/privacy/
28. See www.soxlaw.com/
29. See https://www.ncsc.gov.uk/cyberaware/home
30. See https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
31. See https://gdpr.eu/right-to-be-forgotten/
32. See https://www.gdprsummary.com/schrems-ii/
33. See https://www.itgovernance.co.uk/capability-maturity-model

3 CYBER TARGETS

In this chapter, we shall examine the various potential targets of cyber-attacks. I have tried to separate the targets into the following categories since the motives for these attacks may vary:

- individuals;
- businesses;
- critical national infrastructure;
- buildings;
- academia and research;
- manufacturing and industry.

INDIVIDUAL TARGETS

Whether we like it or not, we are all potentially the target of cyber-attacks. In the case of individuals, attack is most likely to come from cyber criminals who may not target us directly, but they will certainly do so as part of a larger plan – for instance, acquiring credit card

details of thousands of individuals that they can then sell on to other criminals who will target us more directly.

This means that our personal information and, to a certain extent, we ourselves have become a commodity – a product to be bought and sold.

There is little, if anything, we can do about the criminals' larger game plan, but we can take ownership of our individual part of the problem by securing our computers, smartphones, tablets and networks, being careful to whom we give personal information, being aware of and avoiding scams and generally being more cyber-savvy – just as we hold a bag close when walking through cities where pickpockets have a reputation for preying on tourists.

We will deal with these topics in Chapters 8 to 11, when we examine methods of improving our security.

BUSINESS TARGETS

Businesses are a major target for attackers since there are potentially rich rewards to be gained if attacks are successful.

- Where the actual target is not the business itself, the gain could be something the business has, such as a database of customers and their credit card details.
- Where the target is the business itself, potential gains could include its intellectual property – something the business has developed, like a new product or service; something the business is planning, such as the takeover of a rival organisation; or simply details of the organisation's financial

position as the object of a possible takeover, if it's the attacker's intention to cause immediate financial or reputational damage.

Businesses, both large and small, may be much better placed than individuals to understand cyber risks, but may often ignore them, thinking either that they're too small or uninteresting to attract an attacker, or believing that they have nothing that might be of value to one. This is potentially a major mistake, since attackers may not target a specific business but might gain some benefit if an employee unwittingly provides them with a way into the organisation's network.

A successful attack on a small maintenance company might, for example, allow an attacker to gain access to a larger organisation for which it is working, and which is actually the attacker's real target. For example, it is believed that when the Stuxnet attacks took place against the Iranian nuclear research programme, the attack was conducted by delivering the malware to five of the research centre's strategic suppliers, at least one of whom then unknowingly took the malware into the centre, probably on a Universal Serial Bus (USB) memory stick. This illustrates that regardless of an organisation's security arrangements, malware can be introduced by a third party, and it demonstrates the need to ensure that all software entering the organisation is verified.

Another example of a situation in which a business might be attacked is if the attacker perceives that the organisation had committed some offence or injustice and needs to be publicly exposed or rebuked. The media are occasionally complicit in this kind of activity since they can (and frequently do) add fuel to an already burning fire.

Businesses are not always targeted directly for actions of this kind – in recent years, dissatisfied customers and disgruntled employees have adopted the use of social media to spread the word, often resulting in damage to the organisation's brand and reputation, loss of business and more.

While this type of action may not qualify as a direct cyber-attack, it would seem prudent for organisations to consider the possibility as part of their incident response and business continuity strategy.

CRITICAL NATIONAL INFRASTRUCTURE (CNI) TARGETS

Attacks against CNI organisations are extremely common, and may often originate not from cyber criminals but from foreign nation states, terrorist organisations or hacktivists such as Anonymous, since their objectives are usually to disrupt the target nation in as many ways as possible, as described in this book's preface.

The UK's Centre for the Protection of National Infrastructure (CPNI) has defined the following 13 areas of critical infrastructure, and the CNI sectors in other countries, if not identical, will be very similar:

- chemicals;
- civil nuclear;

- communications;
- defence;
- emergency services;
- energy;
- financial services;
- food;
- government;
- health;
- space;
- transport;
- water.

Chemicals

Chemical plants produce many of the items that we use in everyday life, giving us food products such as sugar, agricultural products such as fertilisers, and chemicals used both in the home, such as cleaning agents, and in industrial processes, such as acids and alkalis.

As with other areas, the impact of cyber-attacks on chemical production facilities could be highly harmful, with compounds being incorrectly mixed, resulting in poisoning of products, crops and people; or with dangerous toxic or explosive mixtures being generated, resulting in widespread pollution. Therefore, chemical manufacturing and storage remains a strong potential target.

Civil nuclear

Although we normally think of civil nuclear activities as being in the realm of power generation, there are many requirements for radioactive products used in medicine, where it is utilised in some calibration sources, radioactive drugs and bone mineral analysers;

and in engineering where radioactive isotopes are used in the detection of pollution, carbon dating and the quality control of welding operations.

Although the Chernobyl incident in 1986 was not triggered by cyber means, a cyber-attack against a nuclear power station in India in 2019 was successful. Whether this was an attempt either to degrade electricity generation or to drive the reactor core into instability, resulting in a devastating explosion with radioactive material being dispersed over a wide area, it is not known, although the reports assert that North Korea was responsible. Even though it was claimed that only an administrative area of the power station's network was compromised as opposed to the reactor control systems, it does demonstrate that such an attack is feasible.[1]

Attacks on other nuclear facilities might create a significantly less dramatic impact but could result in hospitals being unable to diagnose or treat illnesses; and in major engineering projects being unable to progress.

Communications

The communications portion of the CNI consists of several different areas. The public fixed (landline) and public mobile networks are the most obvious manifestation, but some private networks are included as well, especially the Airwave network that provides communications for the emergency services and related government organisations and some non-government ones.

Attacks on the fixed and mobile public networks are normally directed at the main network signalling system (typically Signalling System number 7, or SS7 as it is more commonly known). Such

attacks require a reasonably high degree of skill and knowledge to undertake, although spoofing the Calling Line Identifier (CLI) is extremely common and requires a much lower level of skill to achieve.

Although less used in the UK, satellite communications are also a part of the CNI, and these tend to be used for both public and private communications in areas where the public fixed and mobile networks do not provide complete or reliable coverage.

Last, but not least, is the internet, which, although provided nationally and occasionally locally by ISPs, is centrally connected through a number of peering points, which make the interconnections between ISPs at a national level and with ISPs in other countries.

Two particularly fragile components of the internet are occasionally subjected to cyber-attack. The first is the Border Gateway Protocol (BGP), which determines how data packets travel between one part of the internet and another. Once one gateway router is hijacked, it can, for example, advertise the fastest route as being to a malware site. The second is called domain name system (DNS) cache poisoning, in which a cyber-attacker makes changes to the domain name system to redirect traffic to another destination. Both of these types of attack require a significant level of skill.

Defence

The defence sector is made up primarily of the armed forces – nominally army, navy and air force – and also organisations providing research and development or supply services to the military.

Armed forces

Any individual or organisation that conducts a cyber-attack on the armed forces of a major nation can probably expect swift and painful retribution. However, this does not prevent nation states from trying their hand as a means of testing the strength of the opponent's cyber security, and occasionally conducting intrusive attacks.

The majority of these attacks will almost certainly go unreported, since the victim country would not wish that news of a successful cyber-attack become common knowledge. Conversely, if one nation state was able to conduct a successful and undetected cyber-attack on another, they too would be keen to ensure that news of this was not made public so as not to alert the target nation state, so that further cyber-attacks could take place.

Some people define these attacks as acts of cyber warfare, and in part this is true, since one nation state (or terrorist group) has conducted an attack on the defence sector of another; but at the same time, since the origin of the attack may be unclear or even point to another possible attacker, a state of war does not necessarily exist between them.

Military suppliers

Cyber-attacks against military suppliers are very common, and have two fundamental purposes:

- First, they are conducted in order to steal intellectual property such as the designs of new technology used in weaponry and defence systems. An example of this is the attack (attributed to China) on Lockheed Martin, in which designs for the F-35 fighter jet were stolen.[2]

- Second, they may be conducted in order to change the way in which military software operates or to plant malware in weapons or defence systems. It is not difficult to imagine what might result if the engine management system of a fighter jet cut out when the pilot was making an attack run, or the effect of a radar system suddenly failing to display incoming enemy aircraft.

This might sound like fantasy, but you can be certain that many countries will have thought of the idea, and that some countries may have actually succeeded in making it happen.

The arms race that took place in the latter part of the 20th century was a serious affair. East and West spent vast sums of money in trying to develop weapons and defence systems that would allow them to defeat their enemies – often relying on the element of surprise and leaving their opponent with little or no time or capacity to retaliate, and it was eventually concluded that the end result of this could be nothing less than ‘mutually assured destruction’.

This has not prevented or even slowed down the development of both conventional and new weaponry or defence systems, but it has become clear that in the event of another worldwide conflict, conventional ground, sea and air forces would be heavily supplemented by pre-emptive cyber-attacks in an attempt to reduce the enemy’s ability to operate their command-and-control structure, as in the case of Ukraine in 2022.

Nation states have therefore invested heavily in developing cyber weapons and cyber defences, and there is a distinct possibility that another major war could actually be conducted without a single shot being fired.

Emergency services

The next CNI area is that of the emergency services. This covers not only the police, fire and rescue and ambulance services, but also mountain rescue and the Maritime and Coastguard Agency.

People who do not necessarily intend to commit cybercrime, but who intend to undertake some other form of criminal activity, can try to attack the networks and systems of the emergency services. They may realise that by causing some form of distraction they are able to carry out their intrusion, robbery, or whatever, and feel that it is perfectly within their right to do so. Whether undertaking a DDoS attack (see Chapter 2) on the website of any branch of the emergency services would aid them is uncertain.

Alternatively, they may hold some form of grudge against one of the services and feel that a cyber-attack is a perfectly justified response.

The principal target of such an attack is most likely to be the police, but none of these services would be immune to a determined attacker.

The fact that a cyber-attack might potentially cost someone their life might not even occur to an attacker. Fortunately, however, the incidence of this type of attack appears to be very low.

Energy

Next, we move to the energy sector, which is split into three distinct areas, each of which has slightly different arrangements:

- electricity;
- gas;

- oil.

Electricity

The electricity sector consists of three separate components – generation, which may be from a variety of sources; fossil fuels, including coal, oil and gas, and nuclear, all of which are non-renewable sources; and renewable resources such as hydropower, biomass, biofuels, wind, solar and geothermal.

The second component of the electricity sector is the transmission of power from the generation point through the National Grid to the various distribution network operators (DNOs) around the UK, although some industries, such as steelworks, require large quantities of electricity and may be connected directly to the National Grid with whom they have a direct contract rather than with a distribution network operator.

Finally, the distribution network operators then sell the electricity to homes, businesses and industry.

Just about everything we do on a personal, business, commerce and especially critical infrastructure level depends ultimately on the supply of electricity, so cyber-attacks are most likely to target the electricity generation facilities since there are many of them and therefore there is a chance that some may not have as strong a cyber security management process as others. The transmission management centres, however, would come a close second, since considerably more damage might theoretically be achieved with just one attack.

In April 2022, it was reported that Russian hackers had planted malware on computers in the Ukrainian Power Grid.[3] Working with Ukraine, a Slovakian cyber security team were able to foil the attack. However, this does demonstrate the point that critical infrastructure is potentially a major target.

Gas

Supplies of gas come from natural (non-renewable) resources below ground, known as onshore resources, and beneath the oceans, offshore resources, and, increasingly, gas is imported from overseas.

The transmission and distribution work in much the same way as electricity, with a central body delivering the supply to DNOs who then sell the gas to homes, businesses and industry, but the onshore gas storage facilities are likely to be the major targets.

At the time of writing, it is believed that hackers supporting Ukraine have been attacking Russia's gas production and distribution capability, among other facilities such as banks and corporations.[4]

Oil

Oil has similar beginnings to gas – indeed, the acquisition of the raw product uses almost identical techniques, but that is where the similarity stops, since crude oil must be refined and turned into useable products such as heating oil, petrol and diesel.

On leaving the refineries, as with gas, much of it is delivered by underground pipes to storage depots from which distribution is either by road or rail, or again sometimes by underground pipes as in the case of distributing aviation spirit to major airports.

Although it did not result from a cyber-attack, the explosions in December 2005 at the Buncefield oil storage depot at Hemel Hempstead in the UK resulted in considerable disruption to the fuel supply as well as to local residents and businesses.[5]

Offshore oil production platforms and smaller onshore production facilities are likely targets as well as the storage and distribution sites.

It is worth adding at this point a brief note about a technology used in the energy, water, civil nuclear and chemicals sectors of critical infrastructure known as Supervisory Control and Data Acquisition (SCADA), which is widely used both to monitor the state of elements of the generation and production distribution systems, and to control their operation.

The generation and distribution networks themselves tend not to have actual connections to the internet, but the SCADA systems that monitor and operate them frequently do. Hence, attacks against these sectors may well commence with an attack on the SCADA systems. This is discussed in greater detail later in this chapter.

Financial services

The finance sector has to be one of the most serious targets. Cyber thieves who can find ways of extracting funds from banks and financial services companies stand to make a killing. Finance organisations therefore take cyber security extremely seriously, since a successful security breach could cause them to go out of business, regardless of any potential fines levied by the Financial Conduct Authority (FCA).

Before internet-based financial transactions were commonplace, bank robbers targeted the bank buildings themselves. Now, in the 21st century, although the money is still largely under the control of the banks, thefts by cyber-attack can be undertaken at considerably less risk and can be infinitely more profitable for the criminals.

The various sectors in the financial service sector include:

- banks (including credit unions);
- building societies;
- insurance companies;
- stock exchanges.

Increasingly, banks are making use of two-factor authentication such as one-time passkey generators and text messages in order to secure access to customers' bank accounts. The passkey has a short useful life, usually measured in minutes, after which it becomes useless and another passkey must be generated. This greatly lessens the risk to the customer unless the attacker can either manipulate the system and conduct a 'man-in-the-middle' attack, discussed later, or can persuade the customer to part with both the card and PIN or mobile phone.

DoS attacks against financial institutions are also on the increase. According to cyber resilience supplier UpGuard, attacks against financial services organisations increased by 238 per cent in the first half of 2020 with an average of almost US $6 million in 2021.[6] The implication of this is that not only would customers be unable to access their accounts, but in a worst-case scenario, inter-bank transfers could be affected. While this might appear unimportant to many people, recent instances of banks making changes to their

(often legacy) IT systems have resulted in services being badly affected for days at a time; property purchases failing because monies are not transferred in time; salaries and accounts unpaid; and much more.

As an example, in 2014 the Royal Bank of Scotland was fined £56 million by the regulator after a 2012 software issue left millions of customers unable to access their accounts.[7]

Food

Cyber-attacks on organisations in the business of growing, importing, producing, distributing and retailing food are not particularly frequent, but occasionally we read of situations in which an activist group decides to take on a multinational organisation related to food, whether this is to cause denial of service or to steal.

In May 2021, the world's largest meat-packing company, US-based JBS, was hit by a ransomware attack. The result of this was a dramatic increase in meat prices, both at a wholesale and retail level, with resulting shortages. The company eventually settled with the hackers at a cost of US $11 million. JBS's quick reaction, however, resulted in the loss of less

> than one day's production, and a small decrease in its normal level of order fulfilment.[8]

Government

Government departments and agencies have always been a target for attackers. Fortunately, in the UK a government department, a part of GCHQ called the National Cyber Security Centre (known simply as the NCSC),[9] has responsibility for providing guidance to all government departments – national, regional and local – and also to official government websites such as the Driver and Vehicle Licensing Agency (DVLA).

The NCSC brings together and replaces CESG (the former name of the information security arm of GCHQ), the Centre for Cyber Assessment (CCA), Computer Emergency Response Team UK (CERT-UK) and the cyber-related responsibilities of CPNI.

Its purpose, outlined on its website, is to:

> support the most critical organisations in the UK, the wider public sector, industry, SMEs as well as the general public. When incidents do occur, we provide effective incident response to minimise harm to the UK, help with recovery, and learn lessons for the future.

The NCSC's Certified Cyber Security Consultancy (CCSC) acts as the accreditation agency for government Certified Cyber Professionals (CCPs). The scheme is outsourced to three private certification bodies and CCPs offer their services via a CCSC unless they are employed directly in a government department.

Government departments and agencies operate their own cyber security standards and processes, and the NCSC also provides

highly useful advice and guidance to private sector organisations through its website.

Another government organisation that has a significant input into the UK's Cyber Security Strategy is the CPNI,[10] which maintains strong links with all the sectors described in this part of the chapter.

Health

The health sector deals primarily with public-facing services – hospitals, health centres and general practitioner (GP) surgeries – but also ties in closely with the need for medical research, investigating all health matters and researching new medicinal and surgical treatments for patients.

Hospitals, health centres and GP surgeries

Why would anyone want to attack a hospital? Well, it seems that some attackers simply don't care who their targets actually are. In March 2016, the Medstar group, which runs ten hospitals in Washington DC and Maryland, was the subject of a ransomware attack that blocked staff access to many of the group's IT systems.[11] Several other hospitals in the US have also reported this kind of attack, and some pundits have speculated that there is also the possibility of an attacker taking control of life-critical systems, which puts an entirely different perspective on the issue of cyber security.

There is another potentially sinister aspect to this area – that of internet-connected health-related devices. It is not difficult to imagine that the administration of some drugs and medicines could be achieved remotely, and that mechanisms could be connected to the internet to enable this. Delivery of too much or too little medication could be life-threatening, and if we ever reach the stage where heart

pacemakers become part of the Internet of Things (IoT), security will have to be absolute.

> A former colleague who lives in the Netherlands and worked there with the author was recently fitted with a pacemaker following a heart attack. This pacemaker has Bluetooth connectivity (highly secure, as it transpires) built in, so that the surgical team can monitor the device status and make adjustments if necessary. Ironically, my colleague was once the chief medical technician at the hospital where the pacemaker was fitted, and having considerable previous knowledge of the various types of device enjoyed an informative discussion with the surgeon prior to it being fitted.

A successful attack on National Health Service (NHS) systems could allow an attacker to obtain details of our medical history, which could potentially be sold to an interested party – an insurance company or a drug manufacturer for example. We normally consider these types of organisation in the UK to be beyond reproach, but those overseas might not be so honest. Additionally, if an attacker were able to access our medical records, they could alter the content either to improve or worsen our history, the results of investigations and tests, recommendations for treatment and the prognosis.

> In January 2017 Barts Health Trust, the largest NHS trust in England, was hit by a cyber-attack that resulted in file sharing across its four main hospitals being turned off to limit the spread of the impact.[12]

Finally, if a hospital's systems were compromised as part of a larger physical terrorist attack, the result would certainly be panic among the general population, and this could severely reduce the hospital's ability to treat patients, especially those requiring emergency treatment.

Medical research

One of the areas in which there is massive scope for cyber-attacks, especially where the theft of intellectual property is concerned, is that of medical research. The amount of time, effort and money that pharmaceutical organisations invest in the development of new drugs and medicines is enormous, and this goes some way to explaining the cost of new medical treatments as the developers try to make a return on their investment.

If attackers were able to steal the formula for a new cancer drug, for example, they could potentially sell this to less honest manufacturers who would naturally undercut the developer's selling price.

In an even worse scenario, between the testing of a new drug and its final production an attacker could potentially alter the list of ingredients or change the process by which the drug is manufactured. The result could at the very least be contamination, and could bring about serious side-effects or threaten lives.

Space

The UK is not normally the first country that springs to mind when we talk about space, but in fact we are one of the leading countries that design and manufacture satellites for communications and research, and we were an active partner in the European Space Agency.

Similar cyber-attacks to those discussed in the air transport section of this chapter, below, are not beyond the bounds of possibility, and although there are no officially confirmed incidents in which one nation state has attacked the space technology of another, it remains a real possibility, especially if viewed as being part of cyber warfare. A cyber-attack that alters the orbital characteristics of a satellite might, for example, move it into or across the orbit of another country's satellites (or even a space station such as the International Space Station (ISS)), causing catastrophic damage. The 2013 science fiction film *Gravity* illustrated what might happen under similar conditions.[13]

Transport

The transport sector covers commercial air transport, road, rail and merchant shipping for both passengers and cargo.

Air

Increasingly, commercial aircraft are fitted with monitoring systems (especially for jet engines) that allow maintenance teams to see in real time how they are performing, and to understand when to have spare parts delivered to an airport, often before a problem has actually manifested itself. There is no value to an airline in keeping an aircraft on the ground when it could be earning its keep filled with passengers or cargo.

Fortunately, current standards do not permit control of commercial aircraft from the ground (unlike drones), and it is to be hoped that the events of 11 September 2001 (9/11) will dissuade manufacturers from combining control with monitoring, since the prospect of the more frequent use of civil airliners as a weapon of mass destruction is too horrible to contemplate.

> There was also an unverified report in 2015 of a cyber security expert taking control of an aeroplane's flight control systems via the in-flight entertainment (IFE) system while it was airborne.[14] While this is currently just a theoretical possibility, it remains to be seen whether it eventually becomes a practical form of attack.

Another aspect of cyber targets in the transport area of critical infrastructure would be that of the infrastructure that supports air traffic control. At any one time, there are thousands of civil aircraft in the skies, each one of which relies on an air traffic control centre to direct it out of the flight path of other aircraft by ensuring physical separation both horizontally and vertically. If this infrastructure were to be successfully attacked, it could turn aircraft into weapons of mass destruction without the need to target individual aircraft.

However, a major IT systems failure in March 2022 caused British Airways to suspend all flights for a period of several days until the issue had been resolved.[15] This illustrates that an attack on an airline's IT infrastructure can have a major impact on its operational

capability, resulting in travel cancellations and chaos for thousands of passengers, spreading the financial cost much wider than just the airline itself.

Road

The European Commission placed a requirement that by March 2018, manufacturers of all vehicles sold in the EU must be provided with a system known as eCall,[16] which automatically alerts the emergency services in the event that the vehicle is involved in a collision. On the surface, this appears to be a highly noble undertaking, since faster response to an accident could save lives. Many vehicle manufacturers pre-empted the requirement, and in addition to eCall systems installed event data recorders (EDRs) in their vehicles.

The EDR has the ability to store a large number of parameters, including location, speed and direction of travel, throttle position and cornering data. The driver has no knowledge of exactly what data is being collected, or what might be done with it. While this would be helpful to insurance companies and to the police investigating an accident, it follows also that the vehicle manufacturer is likely to be using that data to help in developing better vehicles – again, a positive development.

However, the driver has no control whatsoever over the data, and there is also the potential that the vehicle manufacturer could be selling it to insurance companies. The potential for abuse has yet to be fully debated, since one could reasonably argue that the data was collected without the agreement of the driver.

Far worse, in 2015, security experts were able to demonstrate their ability to take over a Jeep Cherokee under controlled conditions in the USA.[17] They were able to enter through the vehicle's cellular phone connection to access the entertainment system, from which they broke out into the vehicle's Controller Area Network (CAN) and took control of a number of the engine control units (ECUs). If this type of attack becomes commonplace, the implications are frightening.

Motorways and some trunk roads in England, Wales and Scotland have overhead gantries on which display signs are mounted. These can warn of incidents, impose speed restrictions, and indicate the estimated journey time to junctions further along the motorway. They are managed by the Highways Agency in England and Wales, and by Traffic Scotland. If an attacker was able to gain access to the systems that control this signage, traffic could be brought to a halt or diverted down smaller connecting roads, causing complete chaos. Fortunately, there appear to have been no reported incidents of this type.

Rail

Although driverless trains are something of a rarity, they do exist. On the London Transport system, there are driverless trains on the Victoria Underground line and on the Docklands Light Railway. Rather less obvious examples exist at airports such as Gatwick, where driverless trains shuttle passengers between the north and south terminals.

Railways rely totally on electronic signalling to control the movement of trains, and should the infrastructure become internet-connected, one could imagine that considerable chaos, financial loss, damage and potentially loss of life could ensue.

More recently, railway companies in a number of European countries have been installing train monitoring systems that can report information on passing railway stock about weight distribution, wheel loading, wheel defects and noise emission. Identification of the type of rolling stock is carried out by measuring the distance between axles.

> An interesting software bug discovered in 2016 was that if a train running on the Swiss railway network has exactly 256 axles, the monitoring system will reset the truck count to zero, indicating that there is no train on the particular stretch of line.[18] It is rumoured that the company works around this problem by connecting additional trucks to 256-axle trains to ensure that they always show up. If an attacker wishing to cause a major accident were able to penetrate the monitoring system and tamper with the code that counts axles, a great deal of damage could be done.

Water

Cyber-attacks against water companies do not appear to be too widespread, but it has been reported that in 2016 a hacktivist group associated with Syria attacked a water treatment works in the

USA.[19] Although their exact motivation is unknown, it appears to be that the group wanted to alter the balance of chemicals added in the drinking water treatment process, with the aim of contaminating the supply.

Fresh water distribution and wastewater treatment both make use of industrial control systems similar if not identical to those used in other sectors, and therefore exhibit the same vulnerabilities.

Similar attacks could take place against treatment works for wastewater, in which an attacker could again conceivably alter the balance of chemicals used in the treatment process, rendering the resulting output harmful to human and animal life alike, or could release untreated sewage into rivers and water courses.

In 2017, Defra, the Department for Environment, Food and Rural Affairs, produced a cyber security strategy for the UK's water industry, which among other things recommended that the information technology and operational technology systems should each be completely isolated to ensure that no virus infections could spread from one to the other. Likewise, the strategy recommended that the cyber security monitoring systems should be similarly separated but should operate under a single set of policies.[20]

BUILDING TARGETS

One does not always think of the potential for buildings to be targets for cyber-attacks, but they are becoming increasingly internet-connected for the purposes of management, mainly for heating, ventilation and air conditioning (HVAC), where the management of systems is outsourced to suppliers who are better equipped to

control them centrally and only send out an engineer when something cannot be fixed remotely.

Access to a building's HVAC systems would permit an attacker to raise or lower internal temperatures to unacceptable levels, causing staff to have to leave or causing the temperature of critical environments to exceed operational requirements – an entire data centre could be taken out of service in this way.

Also, an attacker might be able to gain access to the building's access control system, allowing doors to be locked or unlocked, preventing staff from entering or leaving, or providing the attacker with the opportunity for physical ingress.

The types of building that might be attacked in this way include:

- factories, such as car manufacturing plants where an attacker might take control of an assembly line;
- warehouses and distribution centres, especially where high value goods are stored;
- transport hubs, such as airport terminals and railway stations;
- operational buildings, such as call centres, telephone exchanges and air traffic control installations;
- office buildings;
- hotels, where an attacker could lock or unlock guests' doors at will;
- sports and recreation buildings, with the potential to access scoring systems as well as HVAC;
- retail properties, including shops, shopping malls, petrol stations and restaurants.

Private houses

There has been much recent interest in home automation, with the ability to connect to a central heating system online from an application on a smartphone; to control blinds, curtains and windows; and also for manufacturers of white goods to receive alerts of potential failure of appliances.

Unfortunately, the manufacturers of home automation systems hardware are not always as skilled as they should be in writing secure code (discussed in greater detail in Chapter 4). As the market for home automation devices continues to grow, attackers are ideally placed to target well-publicised vulnerabilities in these systems.

There have been cases where baby video monitors have had little or no security software included, resulting in unauthorised people being able to watch and communicate with a child remotely.[21]

Ironically, some security systems are also vulnerable. CCTV systems that make use of a digital video recorder to capture images may allow an attacker to gain access to an organisation's data network through backdoors in the recorder, and smart TVs equipped with a camera and microphone can also present a means of an attacker gaining access.

We are being made increasingly aware of the IoT and how it has the power to transform our lives. Many of the interconnected devices already being sold in the area of home automation have been implemented with little or no security, thus presenting an attacker with almost unlimited opportunity to cause mayhem and render our homes vulnerable to burglary.

Smart meters are now being installed by energy companies around the UK. However, it has been discovered that there are a number of fundamental flaws in the design, rendering the meters susceptible to cyber-attack and also vulnerable as an entry point to private domestic networks. It could also be possible for a cyber-attacker to under- or over-report the usage of energy, or to remotely shut off the power to the building.[22]

In a similar vein, if not protected against unauthorised access, home central heating control systems could be vulnerable to attack. Systems such as Hive and Google Nest make use of a private home's Wi-Fi system to allow communication between the thermostat and the control system itself. It is not difficult to imagine the impact if a home's heating was turned down or off, possibly resulting in frozen pipes (or occupants), or turned up, resulting in sky-high fuel bills.

Additionally, the Google Nest Protect system allows carbon monoxide and smoke detectors to be connected into the same smartphone application, which could remove the homeowner's ability to receive alerts in the event of problems.

This also raises potential issues with other smart devices such as doorbell/camera combinations that, on the face of it, are eminently sensible security measures, but again, if hacked, could allow an intruder to be aware when a property was unoccupied with a view to gaining entry, having disabled the camera and alerting function.

Finally, there are the smart home devices, such as the Amazon Alexa and Google Dot, both of which allow the home user to access all kinds of information by voice command; to control home products such as those described above; and to contact others who use the

same sort of device. The amount of data these devices collect is incredible and can include all spoken commands as well as internet search Uniform Resource Locators (URLs). However, it is possible to delete this data.

ACADEMIA AND RESEARCH TARGETS

Many universities have been the victim of cyber-attacks. In March 2021, a major DDoS attack was launched against the University of Northampton, resulting in much-reduced network and telephone connectivity that lasted for almost a whole week.[23] Since then, the NCSC has issued an alert to the UK's education sector regarding ransomware attacks by cyber criminals.[24]

Academic networks present tantalising opportunities for attackers. Many networks (or network segments) are poorly secured, due partly to the spirit of openness that exists in the academic world, and partly through the enthusiastic efforts of students to secure unauthorised network access off campus as well as on.

Additionally, academic networks frequently have links into organisations that conduct commercial research and to government or military organisations, meaning that they can be used as a stepping stone to rich pickings.

It is thought that not all of the attacks originate from outside the universities themselves, but often from within, with students testing their hacking skills. The first example of a

form of malware known as a worm was released in 1988 by Robert Morris, a graduate student at Cornell University in the USA, and caused devastation on the early internet. Morris was eventually identified and prosecuted under the USA Computer Fraud and Misuse Act.

As a result of this attack, the Defense Advanced Research Projects Agency (DARPA) funded the establishment of the Computer Emergency Response Team/Coordination Centre (CERT/CC) at Carnegie Mellon University.

In his book *The Cuckoo's Egg*,[25] Clifford Stoll describes the events that began with a loss of 75 cents in inter-departmental accounts at the Lawrence Berkeley National Laboratory in California and ended up identifying spies working for the Soviet Union who were hacking into American universities and military systems in an attempt to steal military development secrets.

MANUFACTURING AND INDUSTRY TARGETS

Industrial systems, whether involved in planning and design, development or actual manufacturing, have been a target for cyber-attacks for many years. Some attacks are used to conduct industrial espionage, while others are designed to cause disruption to industrial processes.

Manufacturing and industrial control systems

SCADA is one of the most commonly used methods of monitoring and controlling industrial processes. It was developed to permit the monitoring and control of diverse manufacturers' hardware in the form of programmable logic controllers by a single management system using standardised automation protocols.

SCADA systems consist of five discrete levels:

- Level 0, containing the devices to be controlled, such as sensors and control valves;
- Level 1, containing the input/output modules that report the sensor readings and control valves referred to above;
- Level 2, containing the computer systems that integrate the sensor readings, generate alerts and apply control instructions;
- Level 3, containing the production monitoring and targeting systems;
- Level 4, containing the production scheduling systems.

The attacks, such as the Stuxnet attack described in Chapter 2, target Level 1 and Level 2 devices, so that false data is passed up from Level 1 to Level 2, and incorrect instructions are passed back down as a result. Other attacks against SCADA-based industrial control systems have been reported, but Stuxnet is the highest profile case reported thus far.

Attacks on industrial control systems can be used against any area of the CNI, such as water treatment plants, power stations, oil production platforms and the like.

In recent years, the move from largely manual construction and assembly in the manufacturing industries to automated manufacturing has been a major industry in its own right. Although some of the more delicate aspects of production still require manual (and often highly skilled manual) labour, machines are able to carry out repetitive work without tiring and often with much greater accuracy than a human.

The concept of an assembly line being hacked and aspects of the production being altered were unwittingly suggested by a Citroën car advertisement from 2012 in which the robot spray painting systems begin to make unplanned changes to the design on the production line.[26] While this was simply a tongue-in-cheek reference, a cyber-attack on an assembly line could easily result in locking nuts not being sufficiently tight or wiring looms being wrongly connected, either of which could cause significant rework in the factory or might not show up until the vehicles were on the road, with potentially fatal results.

There is also the possibility of a cyber-attacker making changes to the operating software of computer-based products while in production. Many devices nowadays rely on microprocessors to control their basic and more complex functions, from washing machines to cars, and from network routers to fighter aircraft. If there is no highly rigid system of control over software between initial development and deployment, these areas become an easy target for an attacker.

---

1. See https://arstechnica.com/information-technology/2019/10/indian-nuclear-power-company-confirms-north-korean-malware-attack/

2. See https://freebeacon.com/national-security/nsa-details-chinese-cyber-theft-of-f-35-military-secrets/
3. See https://www.reuters.com/world/europe/russian-hackers-tried-sabotage-ukrainian-power-grid-officials-researchers-2022-04-12/
4. See https://foreignpolicy.com/2022/04/11/russia-cyberwarfare-us-ukraine-volunteer-hackers-it-army/
5. See www.hse.gov.uk/comah/buncefield/buncefield-report.pdf
6. See https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services
7. See https://www.fca.org.uk/news/press-releases/royal-bank-scotland-fined-£56m-failing-properly-report-over-third-transactions
8. See https://cybersecurityguide.org/industries/food-and-agriculture/
9. See https://www.ncsc.gov.uk/guidance
10. See https://www.cpni.gov.uk
11. See https://www.healthcareitnews.com/news/medstar-attack-found-be-ransomware-hackers-demand-bitcoin
12. See https://www.theguardian.com/technology/2017/jan/13/london-nhs-hospital-trust-hit-by-email-cyber-attackers
13. See https://www.imdb.com/title/tt1454468/
14. See https://www.telegraph.co.uk/news/worldnews/northamerica/usa/11611058/Cybersecurity-researcher-made-plane-climb-after-hacking-in-flight-entertainment-system.html
15. See https://inews.co.uk/inews-lifestyle/travel/british-airways-systems-down-ba-flights-cancelled-it-failure-heathrow-airport-1548133
16. See https://europa.eu/youreurope/citizens/travel/security-and-emergencies/emergency-assistance-vehicles-ecall/index_en.htm
17. See https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/
18. See https://www.reddit.com/r/softwaregore/comments/4s755a/trains_in_switzerland_must_not_have_exactly_256/
19. See www.theregister.co.uk/2016/03/24/water_utility_hacked/
20. See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/602379/water-sector-cyber-security-strategy-170322.pdf
21. See www.bbc.co.uk/news/technology-34138480
22. See www.bbc.co.uk/news/technology-29643276

23. See https://www.bbc.co.uk/news/uk-england-northamptonshire-56500434

24. See https://www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector

25. Clifford Stoll (1991) *The Cuckoo's Egg*. London: Pan Books.

26. See https://www.youtube.com/watch?v=6vuZWx11RLM

4 CYBER VULNERABILITIES AND IMPACTS

In this chapter, we shall examine the reasons why cyber-attacks succeed – cyber vulnerabilities. These include policy, process and procedure vulnerabilities, technical vulnerabilities, people-related vulnerabilities, and physical and environmental vulnerabilities. We will also consider the damage or consequences that can result from a successful attack – cyber impacts. These include personal impacts and organisational impacts.

CYBER VULNERABILITIES

Any weakness that can be exploited to mount an attack on a network, system or service is termed a vulnerability.

While we may be unable to take preventative action to ward off threats and hazards, vulnerabilities are things that we can often take steps to reduce or even eliminate altogether, such as software bugs.

Some vulnerabilities reflect the nature of the asset, for example the ability of data on magnetic media to be overwritten or deleted. These are sometimes referred to as intrinsic vulnerabilities since they are part of the essential nature or constitution of the subject matter. Others result from some accidental or deliberate action or inaction, for example failure to undertake regular backups. These are extrinsic vulnerabilities, as they are not part of the essential nature or constitution of the subject matter but arising from something outside it.

The vulnerabilities themselves, and indeed the methods (or controls) we may use to treat them, come in many shapes and sizes. Most of them arise from failures to have or to adhere to policies, processes and procedures. Significantly less frequent, but also potentially serious, are the technical vulnerabilities. People-related vulnerabilities are also a major area of concern, as are environmental vulnerabilities.

Policy, process and procedure vulnerabilities

While many organisations have robust policies and procedures in place – either to ensure that the right things happen and in the correct sequence, or to ensure that the wrong things don't happen or happen in the wrong sequence – they are occasionally either overlooked or simply given lip service. This section highlights some of the key policies and procedures that organisations might overlook or fail to undertake.

Failure to have an overall information security policy

The failure of an organisation to put in place an overall information security policy comes right at the top of the list of vulnerabilities. Security policies do not need to be lengthy or complex but should

state clearly and simply what formalities the organisation requires to be in place and make it clear that people must adhere to them.

The lack of, or poorly written, access control policies

A formal access control policy or one that is inappropriate for the needs of the organisation is the next port of call, and the lack of suitable policy, or one that is not properly communicated to staff, can cause severe repercussions. Access to buildings (especially data centres), computer rooms and network facilities, systems, applications and information should only ever be given on the basis of the user's business need and should always be approved by their line manager and countersigned by the manager responsible for the location, system, application or information.

Failure to change user access rights when changing role or leaving the organisation

Another vulnerability connected with this is poor access control procedures for users changing roles or leaving the organisation. Continued access to locations, systems, applications and information is frequently overlooked when an individual changes role. A method of combating this is that of role-based authentication, in which the user gains access by means of both their job function and their identity, rather than by their identity alone.

On leaving the organisation, the user's access rights should be immediately revoked so they can no longer access the organisation's premises, network, systems, applications and information.

Inadequate user password management

One of the most frequent vulnerabilities is poor password management. In the past, this included the failure to enforce regular password changes together with a test of password strength.

However, the US NIST has recently deemed that frequent changes are unhelpful to users and that strength checkers may not be sufficiently robust. Instead, new guidelines have been developed[1] that rate password length and hashing method[2] (a process of one-way encryption of the password) as being more user-friendly by placing the burden on the verifier rather than the user.

The continued use of default system accounts and passwords

An extremely common vulnerability is the continued use of default factory-set accounts and passwords for new and upgraded systems. Many individuals in the hacking world are aware of these and circulate them around the community. The failure to change or hide wireless network identities or service set identifiers (SSIDs) will allow an attacker to pinpoint target networks, and if the default administrator passwords have not been changed or the security level enhanced, these provide a simple and highly attractive entry point into an organisation's network.

The continued use of inbuilt system accounts and passwords

Worse still than the continued use of default settings, there may sometimes be a tendency to allow one system to connect to another by embedding user IDs and passwords within applications. This is a highly dubious practice since a change on one system or another can easily result in application failures.

The lack of security of mobile devices

Many organisations fail to secure mobile devices, whether these are supplied by the organisation or brought in by the users themselves (bring your own device; BYOD). Unless configured to a pre-determined standard, mobile devices generally are relatively

insecure and easily lost, mislaid or stolen, making both the device and the network to which it can connect equally vulnerable.

The lack of network segregation

Network segregation is commonplace in larger organisations, in which different networks are constructed according to the business requirement, and particularly according to their confidentiality, integrity and availability requirements. For example, an organisation with a significant research capability might well place this on a different internal network than that for finance or general administration use.

Failure to restrict access to networks according to use is a very common vulnerability and may allow people to reach resources to which they have no entitlement.

Failure to impose a clear-desk and clear-screen policy

The lack of a clear-desk and clear-screen policy again is a very common vulnerability. Some organisations make it a disciplinary offence for an employee to leave confidential materials in plain view or to fail to log out of or secure their workstation when they are away from their desk.

Restriction of administration rights usage

Unwarranted access to administration accounts is a frequent vulnerability. Only trained and authorised personnel should have administration rights and that should include user computers as well as central systems and networks. Also, administrators should have two accounts, one with the administrator rights for undertaking such work and a second ‘standard’ user account for day-to-day activities such as email, internet access and office work.

The use of untested software

It is good practice for organisations to test new or updated software, including the testing of patches before they go into a production or general-use environment. Untested software may not only cause operational issues if it fails to work as expected, but in cases where it is used in conjunction with other applications it can have a knock-on effect resulting in an embarrassing chain of consequences. See also ‘The lack of a patching and updating regime’.

Failure to restrict the use of system utilities

Although a relatively minor vulnerability, the failure to restrict the use of system utilities such as a terminal console application – normally by setting access privileges within the user’s profile – can result in users carrying out activities that are detrimental to their own device or to other systems, applications or information within the organisation.

Lack of separation of duties

In some situations, it is possible for staff to allow attackers to take advantage of access to information that they might not normally have. This ties back into access control, in which access to information might benefit from being role dependent.

Staff should not be placed in a position, for example, where they can not only raise requisitions for orders but also authorise them for purchase.

Inadequate network monitoring and management including intrusion detection

Inadequate network management, including the monitoring of hacking and intrusion attacks, will mean that successful attacks and intrusions may be overlooked, and little or nothing known about their

occurrence until much later when the network change has been implemented.

The use of unprotected public networks

Many attacks are caused by unprotected public network connections, which allow an intruder to gain easy access to an organisation's network, including the use of shared computers in public environments such as internet cafés and the use of unauthorised and unsecured or poorly secured wireless access points (WAPs).

The uncontrolled use of user-owned wireless access points

Occasionally, users of an organisation's networks will discover ways of subverting the organisation's security procedures and will attempt to connect their devices to parts of the network to which they have no entitlement. One way in which this is achieved is by connecting in a 'rogue' WAP to which they have unrestricted access. One of the main issues with this is that the security settings of such WAPs might not be as strict as those of the organisation itself, and while the users may be able to access the network, so might an attacker if the access point has either poor or no security configured.

Poor protection against malware and failure to keep protection up to date

Malware protection software, especially antivirus software that is not kept up to date, will make an attacker's job much easier. Attackers will take advantage of any means of access available to them, and often are aware of vulnerabilities in applications and operating systems long before a supplier's update is available. Delays in updating these applications leaves an organisation wide open to attack.

The lack of a patching and updating regime

As with the regular updating of malware protection software, the failure to install manufacturers' software patches will leave operating systems and application software open to attack. See also 'The use of untested software'.

Inadequate and untested backup and restoral procedures

Most organisations nowadays carry out regular backups of user data. However, it is far rarer for them to verify that these backups are actually fit for purpose and that information can actually be successfully restored from the backup media. This again presents a serious vulnerability, since backup media that does not fulfil its objective is just as bad as having no backup regime at all.

Improper disposal of 'end of life' storage media

Once storage media have reached their end of life, they should be properly disposed of or wiped before reuse. There are numerous stories in the press regarding people who have bought second-hand computers only to find that the hard drives still contain sensitive or personal information that had not been securely removed prior to the sale. Some organisations will not allow magnetic media of any kind to be resold and insist that disposal is irreversible.

There are examples of computers that have been bought with the original user's data still intact, as well as computers left on trains without password protection.[3]

The lack of robust 'bring your own device' policies

The concept that an organisation's staff can bring their own device to work has become very popular, since it can reduce the IT hardware costs to an organisation. However, the lack of appropriate policies for its use and the lack of enforcement can bring about serious

breaches of security, especially in situations where other members of a user's family have access to the same device.

In 2010, one organisation was badly affected by a virus that was brought in on a user's own personal computer. The machine had been used over a weekend by the user's teenage son, who had unwittingly accessed a website that contained malware. The resulting infection spread throughout a large part of the organisation's network and took its entire IT department several days to clear up. The user (a senior manager) was cautioned, but unfortunately the same event happened the following week, and the user was then banned from bringing in his own machine. What action he took against the offending teenager remains a mystery to this day.

Inadequate change management procedures

Inadequate change control can lead to software and patches being rolled out to the user population, new systems and services and network connections being made and redundant systems being removed without full consideration (and risk assessment) of the consequences. In smaller networks, change control can easily be vested in one or two people on a part-time basis, but as an organisation's network grows, it may be necessary to employ a full-time team with representatives from multiple business units.

The lack of audit trails, non-repudiation of transactions and email messages

In some sectors, it is vital that online transactions and email correspondence are subject to detailed logging and non-repudiation. In many applications, this audit trail is built into the operating software, and in the event of a dispute regarding 'who did what', or

‘who said what’, those organisations that are able to produce evidence in their favour will greatly reduce their risk profile.

The lack of segregation of test and production systems

Those organisations that employ large-scale systems and application testing prior to roll out are open to problems if they fail to separate test and operational facilities, since users may inadvertently connect to a test system resulting in failed transactions. Likewise, users who are supposedly testing a new system might inadvertently cause problems on a live system.

Unacceptable use

It is not only good practice for organisations to include acceptable use statements in contracts of employment, but it should be mandated, whether for hiring permanent staff or taking on external contractors, so that staff members and contractors have no excuse for not knowing that they may not visit inappropriate websites, send or receive inappropriate emails via the organisation’s network, or post inappropriate material on social networks or web blogs.

The uncontrolled copying of business information

Operational management should limit the uncontrolled copying of information by users who have no need to access it – again, this is also largely an access control issue, but the identification of such activity may fall into a different management area. This includes the use of USB memory sticks and shared network drives.

Poor management of remote users

Although working from home was prevalent prior to the Coronavirus outbreak, it suddenly became a major factor in allowing organisations to continue operations, albeit possibly in a much reduced capacity. Even those organisations that had previous

experience of this found themselves in the position of having to drastically increase their remote access capability, while those who had never experienced it suddenly found themselves at the mercy of both hardware and broadband suppliers.

Both kinds of organisation, faced with similar issues, stood the chance of allowing security considerations to be forgotten in the haste to equip their infrastructure.

Not only does working from home require a process to define how users connect to the organisation's infrastructure, but also what physical network changes will be required in order to accommodate a larger number of external users, and a correspondingly reduced number of internal ones. Such a policy would need to be sufficiently flexible to allow for sudden alterations to the configuration as the working from home/working from the office situation changes.

Technical vulnerabilities

Technical vulnerabilities are sometimes less obvious to spot but are frequently highly dangerous. These could also be considered to be failures of policy, process or procedure, but are sufficiently significant to warrant their own section.

Poor coding practice

Poor coding practice is potentially one of the most serious issues around today. The IoT has brought us an increasing number of internet-connected products such as baby monitors, CCTV systems, home entertainment systems and environmental control systems. Many of these have been shown to have little or no security within the application software that runs within the IoT device itself, and also frequently in any application that is used to control it.

Such failings will undoubtedly have drastic consequences, since an attacker can not only attack and take control of the device itself but may well use it as a stepping stone to other devices on the network. Even if a vulnerability is discovered and hopefully fixed, the chances of it being possible to roll out the corrected code to the entire user base are not great, especially if a device has already been compromised.

In January 2017, it was announced at the Consumer Electronics Show (CES) that a number of manufacturers are developing routers with inbuilt security software designed to protect IoT devices that have inadequate security.[4] This might be a possible solution to the problem, since consumers will only have to place their trust in one system to protect all their IoT devices and applications, but it will almost certainly encourage laziness from the manufacturers of IoT devices and applications as they will feel there is no point in trying to make their product secure.

It also implies that a security breach of the user's router would become a single point of failure in the overall network, thereby allowing an attacker to access multiple IoT devices at will.

Indeed, poor coding practice is not limited to the IoT environment – it affects operating systems and applications as well, and combined with backdoors that allow a programmer to test code more easily, these types of vulnerability are among the oldest in the book.

Poor specification of requirements

Poor coding practice often originates from poor specification of requirements for the product or service. It is a long-held view that it is always better to design security into a product from the beginning rather than trying to patch it in later on, and this concept is now a

legal requirement within the GDPR to build data protection into devices that make use of personal data (Article 25), but many organisations still persist in this bad practice, and some have been fined as a result.

Poor quality assurance and testing

Hand in hand with poor coding practice runs poor quality assurance and testing. It is easy to imagine that a programmer developing the software for an IoT device might well also be responsible for its functionality testing, in which case (given the lack of a security requirement in the product's specification) the problem will be exacerbated, since the developer/tester will be oblivious to any likely security issues.

Single points of failure

Any organisation that delivers services over the internet, or indeed internally to its staff, must consider the possibility of single points of failure (SPoFs) as a major vulnerability. These SPoFs include the main computer system, its operating system, software applications, firewall technology, network connectivity, web servers and any front-end load balancing systems. The service design must consider the possibility of failure of any one of these components, leading to an overall failure of service, and the design must be planned so that this does not happen. Many organisations have found to their dismay that certain members of staff can also represent a single point of failure.

At the time of writing, the EU has provisionally agreed the introduction of the Digital Operational Resilience Act (DORA), designed to ensure that the information and communications technology (ICT) systems of financial institutions are sufficiently

resilient to failure, although, following the UK's departure from the EU, the UK will not be obliged to follow the EU reforms. However, financial entities operating in the UK, together with their service providers, should be aware that the finalised Act may have some bearing on the more general ICT risks they will be obliged to assess under current UK law and regulation. Following the Queen's speech in May 2022, the UK government will look to introduce a 'Financial Services and Markets Bill', which would replicate the EU's DORA legislation.

Technical attack vectors: end point devices

Internet Protocol cameras

In recent years, partly as a result of the dramatic reduction in their cost, people have installed IP security cameras to allow them to view visitors to their property. Some are simple cameras, pointed at (for example) an entrance to the property. Others allow a degree of point, tilt and zoom (PTZ) capability. These are generally passive in nature, allowing the user to connect to them and view the current situation; others can generate a notification to the user if someone enters a prescribed area. Other cameras are contained within the doorbell button, and will not only allow notification to the householder, but also an ability to respond in voice to the visitor.

While these cameras provide a degree of security (or at least the feeling of security), they can also be a weakness, since (if compromised) they could be sending video information to an unknown IP address, allowing, for example, an intruder to know when the property is unoccupied.

Fitness treadmills and body-worn fitness trackers

The more advanced fitness treadmills are internet-connected, allowing the user to track the distance they run, monitor their heart rate, and interconnect with other users as part of a virtual team. Fitness trackers not only replicate some of the treadmill's actions, but additionally record the user's whereabouts while exercising. The resulting fitness data can usually be downloaded onto a computer in order to keep track of their progress over time.

Again, if these devices are not sufficiently well secured, they could reveal information about the users that they may not wish to be publicly available.

Thermostats and smoke detectors

These devices are becoming much more widely used. The thermostat can display information about the temperature within one's property, and, knowing the property location, can also display the outside temperature – very useful in winter months, when a sudden drop in outside temperature can be dealt with automatically. These devices can control not only the central heating but also the hot water, giving the user considerable control over their energy consumption. They are also able to detect (through the presence of a mobile phone) whether the house is occupied, and can reduce the temperature or turn off the water heating automatically.

Smart smoke and carbon monoxide detectors can also be installed and, together with the user's smartphone application, permit the user to know when something is wrong.

While highly useful, these devices, too, present a vulnerability if they are poorly secured, or if the manufacturer's network with which they interconnect has security weaknesses.

People-related vulnerabilities

There are numerous people-related vulnerabilities, some of which arise from the lack of training and awareness provided by an organisation, while others arise from people's inability to think and act logically or to follow instructions.

Social engineering

Social engineering may best be defined as an act that influences a person to take an action that may not be in their or their organisation's best interest. This includes persuading them to divulge personal or confidential information or to transfer money to an attacker's bank account.

People are frequently susceptible to social engineering or to coercion when an attacker who may have carried out research on the individual is able to gain their confidence through flattery or by offering some inducement that the individual is likely to accept.

Social engineering is a skill that many cyber-attackers work hard to develop, since assistance from inside an organisation can save them a great deal of time and effort.

One example of social engineering is the use of dark patterns, in which the user is lured into carrying out an action they had not intended. These are discussed in greater detail in Chapter 5.

Lack of awareness

An extremely effective technique for delivering malware is to provide people with free memory sticks infected with malware. Not only can this be achieved by handing them out at conferences and

exhibitions, but also by leaving them on the ground near a target user's house or place of work.

Thinking they're getting something for nothing, people will happily plug these into their computers without contemplating the possible consequences.

Failure to comply with company policies and good practice

This is one of the most common forms of vulnerability. Computer users, especially in a corporate environment, may find that they are constrained by organisational policies, processes and procedures in which they see no point, or which they view as an obstacle to their work. In this case they may try to find ways of defeating or working around them. This may be the result of the policies, processes and procedures not being effectively communicated to them in the first place.

Typical among this type of vulnerability is people writing down key passwords, especially passwords for root access to systems, and sharing passwords with colleagues who either have forgotten their own, or more frequently should not have access in the first place.

Simple passwords

Occasionally, users will choose a simple password (for example, 1234) when using an application or service. Good password management techniques should prevent this, but occasionally users will still find ways of circumventing the system. Other vulnerabilities in this area include passwords that can be easily guessed or cracked, such as one's mother's maiden name or the make and model of one's car.

Poor response to training and awareness

As with users failing to comply with policies, processes and procedures, a poor response to training and awareness may well be the result of ineffective communication on the part of the organisation.

In Chapter 10 we will cover techniques for training and raising awareness. It is important that this is not a one-off event but an ongoing process, so that users are regularly updated on security matters they need to be aware of, and that they continue to be trained in the correct way of doing things. However, some aspects of users' behaviour will continue to require line management action when they fail to comply, and some organisations penalise staff who repeatedly ignore their training.

Physical and environmental vulnerabilities

There are some areas in which physical and environmental vulnerabilities will have an effect, and the impact of these can be dramatic.

Building and equipment room access

It may sound obvious that physical access to key buildings and sensitive areas within them should be carefully controlled, but all too frequently this is not the case, leaving the way clear for an intruder to enter unobserved. Theft is frequently a motive for this kind of entry, sometimes enabled by careful social engineering and sometimes by distraction of security staff, but it may also provide an attacker with the opportunity to introduce malware into a system.

Physical access to individual items of equipment

In addition to equipment room access, poor security can also allow an intruder to gain access to the individual systems where malware

can be introduced. This often happens when a number of systems are located within a single rack space, so that having physical access to one automatically gives an intruder physical access to all the others.

Locking equipment cabinets is an obvious solution, but all too frequently keys are left in the cabinet lock.

Heating, ventilation and air conditioning

Key systems are invariably located in controlled environments such as computer and equipment rooms, but these bring about a potential single point of failure, since all will rely on the environmental controls to maintain a steady temperature and humidity.

Provided that these are maintained within specified limits, the risk is minimal, but once the temperature changes, especially increasing beyond recommended levels, equipment can cease to operate. However, some data centres now run their equipment rooms at slightly higher temperatures than are comfortable for humans, realising that a few degrees' increase in temperature will not cause problems, but will save a considerable amount of money on cooling in the long term.

However, there also exists the danger of server rooms becoming overheated during heatwaves (such as the UK is experiencing at the time of writing), resulting in organisations having to hire in industrial fans and cooling systems.

Power

The loss of or interruption to power is the main vulnerability of all systems, and while the loss for any long period of time can cause severe problems, equipment is rather more vulnerable to being

powered off and on again repeatedly and is much more likely to suffer catastrophic failure.

These days, no self-respecting organisation with a major IT infrastructure would consider anything but an uninterruptible power supply system to run its essential computer room or data centre, and this would normally be backed up by a system of standby generation. Such systems often also provide power to other essential services such as those used by the supporting operations staff.

CYBER IMPACTS

Cyber impacts or consequences are the result of some unwanted event – when a vulnerability has been exploited by a threat. Impacts come in many shapes and forms, but all require some sort of decision to be made. Some impacts can be tolerated because they are not serious, but many cannot be tolerated and require some form of countermeasure, control or treatment in order to remove or minimise them.

Many impacts will be felt on a personal or individual level, while others will have a much wider impact on organisations. We'll take a look at personal impacts first.

Personal impacts

This section covers many of the impacts that will affect individuals in the home or SME environment as well as those working in larger corporate organisations.

Loss of or unauthorised changes to personal information

One of the most worrying impacts on individuals is the loss or exposure of personal information. This could be almost anything about our private or professional lives that we would prefer to keep to ourselves but for whatever reason could become awkward or embarrassing if it became public knowledge, or would simply render us vulnerable to some kind of loss.

> Two data breaches in particular have hit the headlines in recent years – that of the dating site Ashley Madison in 2015,[5] and the Grindr data breach in 2018.[6] It was reported after these data breaches that there were resignations, divorces and even suicides when it was discovered that people had been exploring relationships outside their marriages.

It is amazing how much information you can accumulate about someone without either having heard of them before, or without them being in any way aware of the fact.

There are quite a number of people around the UK who share the same name as me, and who apparently have a very similar email address. I regularly receive emails intended for them. Over a period of time, and quite unintentionally, I have built up a fuzzy picture of some of them. I know most of their full names; often their occupation; roughly, and in a couple of cases, exactly where they live; occasionally, their interests; and some of their shopping habits.

I am sure that if I put my mind to it, I could find out much more, but the more important fact is that they either are completely unaware of

this or possibly unconcerned that much of their personal information has reached a person for whom it was never intended.

> This is due to one simple fact – they, or the person sending them an email, has typed their email address incorrectly. Within the space of 48 hours, I found it necessary to contact a gardening company who needed authorisation to carry out work, a theatre where my namesake had tried to register for an account on their booking system, and a company selling car wheels that my alter ego had ordered. These are just recent examples – in the past, I have incorrectly received cancer patients' highly confidential medical records and demands to pay armed services mess bills.

I always attempt to contact either the individual themselves or the person who has emailed them, but while they could at least apologise for the inconvenience and thank me for pointing out their error, sadly all too frequently there is no response at all. Whatever happened to good manners when we joined the connected world?

Sometimes people give my mobile phone number instead of their own, and I have received numerous text messages from various organisations advising of delivery times and appointments. These too have told me where someone lives and what they have ordered, but I have (so far) resisted the temptation to text back and make changes.

We happily join social networks and post information about ourselves. Facebook (Meta), Instagram, Twitter and LinkedIn are just four examples of social networks where an enormous amount of information can be discovered about us, including our earlier education, university life, job history, interests and hobbies, family life and much, much more.

It's not only individuals who can cause problems for themselves. Take the case of a CEO who was having regular meetings with the CEO of another organisation with a view to a merger. On one occasion he took his family with him and his teenage daughter posted a photograph of the town they visited, together with a comment about her father being in a meeting at a particular company.

Someone following her on the social network put two and two together and made a couple of telephone calls, which resulted in a highly sensitive discussion becoming public knowledge, affecting the companies' share prices, and effectively ruining the entire project.

This is perhaps an extreme example, but it does illustrate the possible consequences of seemingly innocent actions.

Loss of or unauthorised changes to personal credentials

Individual people's credentials are big business. Details of bank and credit card accounts, usernames, email addresses, passwords and the like are bought and sold on the internet for surprisingly little money.

Attackers who can acquire these in bulk can monetise the data in a number of ways – either by using the credentials themselves to

mount attacks on the individuals concerned, or by selling them on in bulk to others who are better equipped to mount the attacks.

The impact on the individual can be far-reaching, depending upon the type of credentials. If the individual is lucky, they may discover the attack early on, and may just lose a small sum of money. If they are unlucky, it can be much more devastating.

Loss of money and other financial instruments

Money is a major motivator for cyber-attackers, so naturally they will try to steal as much as they can if the opportunity presents itself. In some situations, where the individual can show that they have taken due diligence over their credentials and have protected their computer and bank cards as well as they reasonably can, the finance organisation will accept responsibility for covering the losses, but where individuals have been careless or negligent, they have the potential to lose considerable sums of money.

A knock-on effect of this is that one's financial standing or credit worthiness might also be affected, if, for example, the loss empties one's bank account immediately prior to a direct debit being taken for a mortgage payment, and this is subsequently marked against the individual's credit rating.

Damage to personal reputation

Cyber-attacks can easily ruin reputations. If you consider the example of someone whose email account is stolen, or whose account username is used by an attacker, it is quite simple to send out malicious emails that could destroy their reputation overnight. Often, especially if they know the individual well, recipients accept that the account has been abused, but the repercussions of having

malicious communications sent to someone you don't know are potentially far more serious.

Reputations, like trust, are rather like eggs – very easily broken, and almost impossible to piece back together again.

Loss of personal trust

Trust goes hand in hand with reputation. People with a sound reputation tend to be trustworthy and vice versa, and the loss of trust in an individual implies that their word is no longer reliable.

The importance of trust cannot be overstated, whether this is in connection with conventional business or with online transactions. We shall talk more about trust in Chapter 11.

Loss of or unauthorised changes to intellectual property (IP)

The theft of IP is closely related to the theft of money, since although no actual money is stolen, the potential to have earned it through sales will have been denied to the IP owner. A secondary and rather more serious loss of IP is when an attacker steals the original material and claims it as their own, in which case the original IP owner will be at a very serious disadvantage.

An example of this type of loss reported by the Intellectual Property Office in its 2020/2021 IP Crime Report[7] is the abuse of the set-top boxes designed to allow users to collect music, videos, photographs and games in a single application. Illegal third-party add-on software can allow users to download pirated material from film companies and television companies. The report flagged this kind of IP theft as being one of the top three it is investigating.

Identity theft

Some years ago, a colleague was targeted by an organised group who used her email address to send out hate mail to everybody in her list of contacts, stole money from her bank account, ran up credit card bills, and almost destroyed her personal and professional life.

However, she was actually extremely fortunate, as she discovered what had happened at an early stage and took remedial action to limit the damage, but while the perpetrators were identified they were never brought to justice since they were beyond the jurisdiction of the European security services.

She believes that the reason for targeting her was that on several occasions she had been publicly very outspoken about the integrity of a large overseas organisation.

Identity theft is often closely coupled with cyber theft, since an attacker may reveal their identity if they carry out too many actions using the stolen identity, whereas in the case of a quick ‘smash and grab’ the attacker can discard the identity as soon as they have the money.

Personal injury

This aspect of cyber security is rather new. In December 2016, in response to an article he had posted, *Newsweek* journalist Kurt Eichenwald reported having received a tweet containing flashing images that caused him to suffer an epileptic attack. Clearly the sender was aware of Mr Eichenwald’s medical condition, and the matter is under investigation by police in the USA.[8]

Such conduct raises the question as to what the consequences might be, for example, for patients undergoing kidney dialysis at home with equipment that is internet-connected.

Organisational impacts

Many of the impacts that affect individuals will also affect organisations. However, because of the scale of organisations, both in terms of numbers of people and in the amounts of finance involved, the overall impacts will potentially be significantly greater. These could easily include partial or complete failure of an organisation or severe job losses.

Brand and reputation

The organisation's brand will invariably suffer a major impact when a cyber-attack is successful, especially if it became clear that the organisation concerned had not taken appropriate steps either to prevent the attack happening in the first place, or because it had failed to deal with it effectively once it had occurred. On occasions, it is because both of these have resulted in the organisation losing intellectual property, or customer information.

Organisations that suffer this kind of impact may find that customers no longer trust them and decide not to do business with them in the future.

Financial impacts

The impact on an organisation's revenue streams can be devastating. Cyber-attacks frequently result in an organisation being unable to trade online since customers will be unable to place orders. This will not only cause an immediate loss of revenue but can often also result in downstream losses later on, as customers take their business elsewhere.

Following a successful cyber-attack that results in damage to the organisation's brand, the organisation's share price may well suffer a

sharp decline. Under normal circum- stances a reduction in share value is a day-to-day occurrence and would not be a major cause for concern, but in these unusual circumstances it might take an organisation months or years to recover its share price.

Additionally, cyber-attacks can cause an organisation to be unable to order goods from its suppliers, pay them for goods already received, or be unable to pay staff their wages or salaries.

Under certain circumstances, and particularly in highly regulated sectors, organisations can be fined for mismanagement of customer data, especially if their actions contravene data protection legislation. They can also suffer further financial losses with interest being charged for late payments, especially to His Majesty's Revenue and Customs (HMRC) for late payment of corporation tax.

On top of any revenue losses, organisations will find that there are costs involved in putting matters right after a successful cyber-attack, which will probably include the introduction of remedial information security controls.

Also, as discussed earlier in this book, there is the possibility that an organisation will be subjected to a ransomware attack and will have to pay the ransom to decrypt their data. The alternative would be for the organisation to face expending considerable effort in recovering all its affected systems. In some cases, the cost of such a recovery process could well exceed the ransom demanded.

Operational failures

If an organisation's operational systems, such as development systems, production control systems, stock control systems and the like are impacted by a cyber-attack, the impact would be potentially

catastrophic, as the organisation may be completely unable to operate for the duration of the problem.

Most, if not all of these, failures will inevitably link back to financial impacts, since the organisation's ability to provide its customers with products or services will result in loss of revenue, and quite possibly in damage to the organisation's brand and reputation as well.

An example of this is the case of an IT systems failure at TSB in in April 2018, which resulted in 1.9 million customers being unable to access their online accounts, receive incoming payments and make transfers to other accounts for as long as several weeks. The problem arose while the bank was migrating customer accounts to a new IT system. The bank lost an estimated £330 million, and five months later its chief executive stepped down.[9] While this is not a specific cyber security incident, it does illustrate what can happen when system upgrades are not tested prior to roll out.

People impacts

The final impact that organisations might suffer following this kind of event is the loss of staff who have to be laid off due to the financial losses or operational failures, or who choose to leave the organisation because they have lost faith in its ability to adequately plan for and respond to cyber security disruptions.

---

1. See https://pages.nist.gov/800-63-3/sp800-63-3.html
2. The technique of hashing uses a one-way encryption algorithm that makes it impossible to recover the password from the encrypted or 'hashed' original. Imagine dicing a potato into small cubes and then trying to reassemble it.
3. See http://news.bbc.co.uk/1/hi/uk/7449927.stm
4. See www.bbc.co.uk/news/technology-38415067

5. See https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked
6. See https://www.reuters.com/article/us-grindr-dataprotection-norway-idUSKBN29V0NJ
7. See https://www.gov.uk/government/publications/annual-ip-crime-and-enforcement-report-2020-to-2021
8. See www.bbc.co.uk/news/technology-38365859
9. See https://www.theguardian.com/business/2019/oct/28/number-of-it-failures-at-banks-and-other-firms-is-unacceptable-say-mps

5 CYBER THREATS

In this chapter, we shall examine the various types of threat that individuals and organisations face, including types of attacker, types of attack, the motivations for and the benefits of launching an attack, the risks involved in doing so and how attacks typically are conducted.

There are a number of terms associated with cyber threats that are worth exploring before we look into the types of threat in greater detail:

- **Threat source or sponsor** is the person or organisation that wishes to benefit from attacking an information asset. Threat sources often pay or otherwise pressurise threat actors to attack information assets on their behalf.
- **Threat actors or agents** are the individuals or groups of individuals who actually execute a cyber-attack.
- **Threat actions** describe the actual attacks. These are often not a single isolated event, but can consist of many discrete

activities, involving surveillance, initial activities, testing and the final attacks.

- **Threat analysis** describes the process of understanding the level of threat – this is referred to in more detail in Chapter 6.
- **Threat vectors or attack vectors** are the tools, techniques and mechanisms by which an attacker conducts the attack on their target.
- **Threat consequences or impacts** are the results or impacts of a cyber-attack, which we dealt with in Chapter 4.

While some attacks are more likely to take place than others, the level of impacts does not necessarily mirror the type of organisation affected or the likelihood that they will occur. Any individual or organisation can be attacked, and many very probably have been.

Before we can begin to plan to put preventative measures in place or to develop the means to respond to cyber-attacks, we need to understand the kinds of people and organisations that will attempt them, together with their possible motivations for doing so. Once we have a clear understanding of this aspect of cyber security, we will be much better placed to deal with them.

Any attacker or criminal requires three distinct things in order to achieve their goal:

- Motive – there must be a reason for them undertaking a cyber-attack – even if it appears to be a rather futile one. Most cybercrime is motivated by money, but there are elements who attack systems for revenge; to establish their perceived superiority; to make a political statement; or simply to be a nuisance.

- Means – the attacker must possess a minimum level of skill in order to mount a successful attack. Often attackers with little or no skill will fail in their endeavours and will probably be identified and face justice, while those with sufficient motivation will persist, and further develop their skills over time.
- Method – a more experienced attacker will develop a plan for their attack. This may require an interim break-in, followed by extended periods of reconnaissance before the real attack takes place.

Some of these attackers will be individuals, operating entirely on their own; some will be groups of individuals, often organised into a loose community (such as the Anonymous group); while others will be highly organised criminal gangs. At the other end of the spectrum are the nation states, and while some will be using the attack for purely espionage purposes, others will have a far more sinister agenda.

TYPES OF ATTACKER

Attackers fall into a number of categories:

- script kiddies;
- hacktivists;
- lone wolves;
- investigative journalists;
- minor criminals;
- organised criminals;
- terrorists;
- insiders;

- security agencies.

Before we examine their motives, means and methods, it is worth examining attackers' capabilities, as these will vary considerably.

External attackers

We shall begin with those attacker types who conduct cyber-attacks from outside conventional organisations.

Script kiddies

Script kiddies are beginners in the cyber security game. They need not be young but are generally relatively inexperienced in computing and cyber security matters and are on a learning curve. Their attacks will typically involve downloading free malware from internet resources and attacking 'soft' targets where there is less chance of causing damage, leading to their being caught. More experienced hackers tend to look down on script kiddies, despite that fact that this is where many of them may have started.

Hacktivists

Most hacktivists already have a cause to support. Some of these will be political; some religious; some may be concerned with the protection of civil liberties; some will be attacking a major corporation whom they feel has caused them some injustice; some will be trying to save the planet from destruction by humanity.

Whatever their cause, hacktivists will invariably target major websites, often defacing the organisation's landing page, or replacing them with their own versions of what they perceive to be the 'truth'.

Since hacktivists rarely attack individuals, and are not usually motivated by theft, they present relatively little threat to us as individuals, unless, for example, we work in a laboratory that conducts experiments on live animals, or in some other similarly controversial area. To organisations, however, they are a major nuisance, causing public embarrassment and occasionally causing the targeted organisation some financial loss, both of which are usually very much the hacktivists' primary objectives.

Hacktivists normally take advantage of known vulnerabilities in website applications to conduct their attacks. Once identified, these are relatively easily corrected, but in the meantime, if they have enjoyed sufficient exposure, the hacktivists feel that their point will have been made.

A small minority of hacktivists are just out to cause mischief and are usually less concerned about making a particular point; rather they have identified and exploited a vulnerability, and deface a website just to show their prowess.

However, some hacktivist attacks have had a much higher profile, as in the example of the Anonymous attack on the Church of Scientology following its legal action against YouTube for publishing one of its propaganda videos.[1]

Lone wolves

Lone wolves are frequently newcomers to hacking. Although not restricted to the Hollywood vision of a brilliant teenager hunched over a computer in a darkened bedroom, they often begin as 'script kiddies', who learn their basic hacking skills from chatrooms and blogs on the internet, download malware and try their hand at attacking increasingly high-profile websites.

Their motivation is usually to gain kudos from their peers but may also be to cause a certain amount of mischief, and this type of lone wolf sometimes graduates from minor hacking into minor crime or hacktivism.

Another, more benign type of lone wolf is motivated purely by inquisitiveness, and is more reminiscent of the original hacking community, who simply wanted to find out how things worked, and if possible, to improve them. This type of hacker will often graduate to become a security specialist or penetration tester.

Investigative journalists

Investigative journalists are an interesting group. While their intentions may be honourable, they frequently resort to underhand methods to achieve their goals. Some such activity has been hacking into the voice mailboxes of celebrities, politicians and members of the UK royal family – deemed ‘illegal interception’ – and attributed largely to journalists working for the News International group of papers during the mid-2000s.

It is not hard to imagine that a journalist willing to illegally access someone’s voicemail would also be prepared to illegally access someone’s computing device, email messages or internet browsing records, whether they achieved this themselves or by some form of proxy – that is, paying a hacker to undertake the technical aspects.

Minor criminals

I have referred to this group as minor criminals simply because they represent a community who will usually target individuals and smaller businesses, rather than major corporations. Their motivation is generally either financial or information theft.

In the first instance, they will enjoy direct financial gain from someone's bank account or by abuse of their credit card; in the second, they may simply post copies of software, music or films on torrent websites so that others may download them free of charge. Naturally, this causes a financial loss to the copyright owner of the pirated material.

Minor criminals can drift either into major crime, especially if their expertise comes to the attention of the organised criminal fraternity, or can become respectable security specialists. Their choice is sometimes decided by how much money they can make, and whether or not they have been caught.

Organised criminals

We now move up another layer in the hierarchy of cybercrime to that of organised criminals. This group are almost exclusively motivated by financial gain, although instances have been reported in the media where known organised criminal gangs have undertaken cyber-attacks on behalf of terrorist groups or nation states in order to disguise the true identity of the sponsor.

Occasionally, the threat actors (as opposed to the threat sponsors) will be acting in their own interests and will benefit in full from their activities. At other times, they will be acting on behalf of others, who will pay either a fixed fee or a cut of the 'take' for executing the cyber-attack.

Organised criminals will often purchase information such as lists of valid credit card names and numbers for use in mass financial scams or will set the threat actor a specific task to obtain information of value, which can then be sold on to the highest bidder.

Terrorists

Terrorist groups tend to use cyber-attacks for a number of reasons. The first is to make or reinforce a political or religious point – defacement of western websites is quite typical of this variety. The second is the theft of money from organisations in order to further their beliefs and aims. The third, and far more dangerous, is to attack the infrastructure of their political or religious enemies.

Since the first two methods have already been covered, it is worth focusing on the third here.

All nations have some degree of critical infrastructure. As we saw in Chapter 3, the sectors include:

- chemicals;
- civil nuclear;
- communications;
- defence;
- emergency services;
- energy;
- financial services;
- food;
- government;
- health;
- space;
- transport;
- water.

Of these, the communications and energy sectors are prime targets for terrorism, since a successful attack on either of these will cause enormous disruption to an enemy. All other sectors of course will be considered as useful targets, but the impact may not be felt with such immediacy.

There is a crossover here between cyber-attacks by terrorist organisations and those initiated by nation states. The term ‘cyber warfare’ is frequently used to describe cyber- attacks by one nation state on another, and although there remains no absolute proof of Russia’s guilt, it is widely believed that the cyber-attacks on Estonia in 2007 were essentially an act of cyber warfare by Russia.[2]

Internal attackers

Having examined those attacker types that conduct cyber-attacks outside conventional organisations, let’s now look at those who do so from within them.

Insiders

Until now, we have examined the threats from individuals and groups who are physically located outside the organisation. However, one of the greatest threats comes from people already within the organisation itself. Many of the cyber incidents they cause are unintentional – often brought about by a lack of understanding of the risks involved when someone clicks on a malware link in an email. Others are more deliberate acts, in which an insider steals money or goods, or copies and subsequently steals corporate information that is of value to a competitor or a criminal organisation, or aims to cause system, information or network damage.

In terms of dealing with unintentional insider incidents, this can best be addressed by awareness and training, which we shall explore in much greater detail in Chapter 10.

In the case of deliberate insider activity, the active monitoring of user accounts, internet access and the use of intrusion detection software will identify some of this activity, but organisations can never be certain of completely combating insider cyber security attacks.

An insider who has been well trained and placed specifically within the organisation in order to cause loss or damage will probably be fully aware of the organisation's capabilities in identifying potential attackers and will behave in a way that does not arouse suspicion.

Security agency surveillance

Depending upon the country employing them, security agencies should normally be viewed as 'the good guys', unless of course you are one of 'the bad guys'. There is, however, a very active debate as to whether security agencies are operating completely within the law since they have the ability to intercept our communications at many different points.

It is well known, for example, that GCHQ monitors satellite and fibre optic cable transmissions and that the resulting intelligence is shared with the NSA through their 'special' relationship. It is reasonable to assume that the NSA performs the same kinds of interception, and that they also hand over their results in a 'quid pro quo' arrangement.

However, let's for the moment look on the positive side, and remember that the key role of security agencies is to provide support to the police and the military and to protect the UK from cyber threats, terrorism, serious crime and espionage.

MOTIVES: WHAT DRIVES AN ATTACKER

Different types of attacker will have widely differing motives for conducting cyber-attacks. Although there may be other reasons, the following are the most prevalent.

Financial gain

Many, if not most, cyber-attackers are motivated by the prospect of ‘easy’ money, which will permit them to enjoy a more lavish lifestyle, or to fund further activities that go against the common good (such as crime and terrorism).

Attacks motivated by financial gain generally break down into three distinct areas:

- ransom;
- theft;
- fraud.

Ransom

Ransomware attacks are very much on the increase. According to a survey from Forbes, the incidence of ransomware increased by 50 per cent from 2020 to 2021.[3] All the attacker has to do is gain access to a victim’s computer – usually through some form of email scam in which the user either follows a link to a website containing malware or accidentally executes an application disguised within the email.

> As an example, Fusob now accounts for a substantial proportion of the currently active ransomware. Fusob masquerades as a video player of pornographic films, detects whether the PC's language is of eastern European origin, and if not, locks the device. Purporting to originate from an official authority, it then demands a payment of between 100 and 200 US dollars to unlock the device.[4]

Theft

Theft breaks down into two slightly different areas. The first is one in which the target's banking or credit card credentials are stolen – a crime in itself – and the second is one in which these details are used to purchase goods or services, and the rightful owners of the money are parted unwillingly from it. The credentials may also be sold to other criminals as part of a larger undertaking.

Fraud

This is considered to be slightly different from theft, since fraud leads people to part willingly with their money, and usually delivers little or nothing in return. Cyber fraud often offers for sale expensive computer software (for example Adobe Photoshop) at a knockdown price. The software (if actually delivered) may be useless, impossible to register or may contain malware.

Remember the adage – if it sounds too good to be true, it very probably is.

There is also the love scam, in which people receive an email purporting to be from a family member or close friend who has allegedly run out of money, is stuck in another country, requires

urgent medical treatment or is experiencing some similar plight, none of which are actually true. They are asked to help by sending funds, which are paid directly to the scammer.

> Some years ago, I received such an email purporting to be from a colleague with whom I was working at the European Union Agency for Network and Information Security (ENISA). The sender claimed to be in Wales when I knew for a fact that she had just flown home to Portugal. The best thing to do with such emails is to delete them.

Another example of this is CEO fraud in which someone with financial sign-off rights at the CEO's organisation is tricked into authorising funds to be transferred to the attacker who may use either phishing techniques to gain access to the CEO's email account or may email an employee from an email domain name chosen to resemble the target company's true domain name. This is sometimes referred to as business email compromise or BEC fraud.

Revenge or malicious damage

Some cyber-attacks are carried out in response to an action undertaken or perceived to have been undertaken by the victim. The action itself may have been fully justifiable, but the attacker perceives that they have suffered some injury, deprivation or harm from the action and decides that a cyber reprisal is an appropriate response. The results of revenge or malicious damage attacks can be quite devastating and have almost ruined many careers, since the

statements made and accusations levied in the attack may well be believed, whether they are true or false.

Attacks of this type can lead the attacker into difficult waters, especially if libel actions ensue, or if the material they post is deemed defamatory, racist, homophobic or fits into any one of a number of proscribed categories. These attacks tend to be either one individual against another; one individual against an organisation; or a number of individuals against an organisation, as in the case of the Anonymous attacks on PayPal, Visa and Mastercard in 2010 in response to the blocking of payments to WikiLeaks, known as Operation Payback.[5]

Although the cyber-attack was considered to have been a success for the Anonymous collective, it was less so for the attackers themselves, as they were identified, tried and convicted.

Espionage

Espionage has been included in this section because whatever its purpose, in the cyber security context it invariably involves some form of cyber-attack, and regardless of whose side the attackers are on, the ‘other’ side will see them as hostile. One must assume that the security services are extremely well versed in cyber espionage, and that identifying and tracking down criminals and terrorists is an activity that they undertake just as much as discovering the enemy’s intentions and capabilities.

There is also a distinction between corporate or industrial espionage conducted in order to gain a commercial or other advantage over another organisation; legitimate surveillance conducted by the police

and security services; and finally, espionage conducted by one nation state against another.

However, espionage is a difficult area for many people, since it cuts across our desire for privacy, and although we are generally confident that the security services have our best interests at heart, we do worry that our privacy is being invaded whether it actually is or not.

Cyber espionage generally falls into one of two categories – commercial or military/nation state. In the case of the Lockheed Martin attack mentioned both in Chapter 3 and below, both of these appear to have been the case.

Intellectual property theft

The theft of IP covers many areas including, but not limited to, music, filmography, formulae, industrial processes, software, designs and development. Industrial espionage has been around for decades.

> In the 1960s, the then Soviet Union obtained plans for the supersonic Anglo-French Concorde aircraft, and developed their own Tupolev Tu-144, which for many reasons was not an outstanding success.[6] The potential consequences for British Aerospace and Aerospatiale were of an economic nature but did not amount to much of a blow in the long term. However, it was later suggested that the development team knew of the

Soviets' intention to steal the designs and allowed them to acquire blueprints with inbuilt design flaws.

In another example, from 2009, in an operation known as Night Dragon purported to originate from China, attackers stole proprietary information from six American and European oil exploration companies, including Exxon Mobil, Royal Dutch Shell and BP. The attackers' targets were computerised topographical maps that located potential oil and gas reserves and resulted in the loss of financing information for a number of oil and gas field bids and operations.

Investigative journalism

Another area that touches a raw nerve is investigative journalism. After the Leveson Inquiry, the press managed to convince the government that there was no need for additional regulation for investigative journalism, and that self-regulation would suffice.[7] This may be true, and as long as an investigation is genuinely 'in the public interest', there would be little or no objection other than from those who are under scrutiny.

However, the press in the UK is notorious for its loose interpretation of its own code of conduct, and frequently crosses the line, becoming invasive and causing great distress to innocent people. Hacking into a celebrity's voicemail may not be a difficult thing to do,

but this often results in mere gossip rather than exposing genuine wrongdoing.

It is also worth bearing in mind that some newspapers and television channels prefer to depict fake news (at least on the surface) as true investigative journalism in an attempt – sadly, often successful – to influence public or political opinion.

It is for the individual to try to separate truth from fiction, frequently relying upon the reputation of the media company concerned and the level of trust they are able to place in it.

Whistleblowing

Until recently, few people would have associated whistleblowing with cyber security; then along came Edward Snowden and everything changed.[8]

In early 2013, Snowden, who had been working as a National Security Agency contractor, revealed to three carefully selected journalists that the NSA had been running mass-surveillance programmes against its own citizens. This included information stored by some of the USA's largest technology companies, and data intercepted from global telephone networks and the internet to compile information on millions of US subjects. Snowden also identified the UK's GCHQ as having collected, stored and analysed vast amounts of personal information from global email messages,

telephone calls and other resources. Snowden described this as ‘probably the most invasive intercept system in the world’.

Governments on both sides of the Atlantic began hasty (and possibly ill thought-out) changes to legislation to either make some of their activities legal, or conversely to wrap their more nefarious activities in such legal jargon that they appear to be legal, while providing sufficient leeway for ‘interpretation’.

Snowden, now resident in Russia, was not alone in blowing the whistle on some of these operations – Bradley (now Chelsea) Manning also felt sufficiently strongly about some of the US activities and gave more than 700,000 classified or sensitive documents to WikiLeaks,[9] which landed Manning in prison. At the time of writing, Julian Assange of WikiLeaks is now in prison awaiting the outcome of an appeal in the UK, potentially pending extradition to the USA.

Whistleblowers must be completely committed to their cause, in the full knowledge that although what they expose may be morally or legally reprehensible, the state will probably find ways to present them as criminals and they will almost certainly be punished for doing what they and many other people believe is morally appropriate.

MEANS

Now we should understand how a hacker may go about attacking an individual or an organisation. A quick search on the internet for the term ‘hacking tools’ returned more than seven million results, so it should be no surprise that somewhere in there should be a software tool that will achieve almost any objective.

Many of these tools are freely downloadable, while others may demand some form of payment – either as a one-off fee or on a subscription basis. Hackers, and especially those who possess good coding skills, are becoming increasingly commercially aware.

The low cost and high availability of hacking tools is just one side of the coin – the other is that the tools are becoming much simpler to use, so it is easy to see that almost anyone who has more than a little motivation can mount a cyber-attack, often with little concept of the damage they might cause (as in the case of script kiddies) or the depth of trouble they might eventually find themselves in. More experienced attackers will fully understand both the tools and the possible consequences and will plan their activities accordingly.

As an example, this is just a small selection of the commonly used tools for penetration testing and for hacking:

- Kali Linux,[10] as the name suggests, is a specialised Linux distribution that can be downloaded for most computing platforms. It contains over 600 penetration testing tools that, among other things, are capable of cracking Wi-Fi passwords, creating fake networks and testing for vulnerabilities.
- John the Ripper[11] is a password cracking tool that uses a brute force attack method together with dictionaries of commonly used words. As with all such password cracking tools, the complexity of the password (mix of character types and length of password) will determine how long this takes.
- Nmap[12] is a network scanning tool that allows the user to understand what host systems are available on the network, what services (application names and versions) those hosts are

offering, what operating systems (and OS versions) they are running, and what type of packet filters/firewalls are in use.

- Aircrack-NG[13] is a wireless network tool that includes the capability for capturing packets and exporting data to text files for further processing by third-party tools; replay attacks, de-authentication and fake access points; checking Wi-Fi cards and driver capabilities; and cracking Wired Equivalent Privacy (WEP) and Wireless Protected Access Pre-Shared Key (WPA-PSK) (WPA 1, 2 and 3) passwords.
- Wireshark[14] is a network protocol analysis tool for both Unix and Windows networks. It is able to capture live packet data from a network interface; open files containing captured packet data; import packets from text files containing dumps of packet data; display packets with very detailed protocol information; save captured packet data; export packets in a number of capture file formats; and many more features.
- Nessus[15] is a vulnerability scanning tool that can assess systems, networks and applications for weaknesses; detect malware as well as potentially unwanted and unmanaged software; audit system configurations and content against standards; ensure that IT assets are compliant with policy and standards; and identify private information on systems or in documents. Nessus is available in both free and paid-for versions – updates to the free version are generally around six months behind the paid-for version.
- Angry IP Scanner[16] is a network discovery tool that ‘pings’ each IP address on the network to check whether it responds. It can then resolve the hostname, determine the MAC address, and scan its ports. The amount of information gathered about each host can be extended with plugins.

- Metasploit[17] allows an attacker or a penetration tester to search for security vulnerabilities within networks and systems and has an audit capability. Additionally, Metasploit permits testing of intrusion detection systems.
- Pegasus is a highly sophisticated spyware hacking tool designed by Israel's NSO Group, and (in theory at least) sold to governments for use in the fight against organised crime and terrorism. Pegasus is designed to be installed on most iPhone Operating System (iOS) and Android smartphones without the user taking any action, and is virtually undetectable. Pegasus can be installed either by gaining physical access to the device, or through a nearby wireless transmitter, and can relay the content of emails and text messages, photos, contacts, browsing history and location data as well as information provided by apps on a smartphone.

  Although some Android devices appear to have been infected, it is mostly the Apple iPhone that appears to be the major target, and it has been suggested that this happens through the iMessage applications. It is said that Pegasus can self-destruct if it is unable to contact its command-and-control server for 60 days.

  There have been numerous reports of investigative journalists and anti-government activists in oppressive regimes being targeted, some of whom it is claimed have been arrested, tortured or even killed as a result of the spyware's results.

  In April 2022, it was alleged in *The Guardian* newspaper (among others) that a smartphone in the office of the UK's Prime Minister – 10 Downing Street – had been infected with Pegasus, and that the UAE was the country responsible for the attack.[18]

A quick search on the internet will reveal many more hacking tools.

CYBER-ATTACK METHODS

In this section, we shall examine approaches to conducting cyber-attacks and the methods employed by attackers to achieve their objectives.

Tools and approaches

Cyber-attacks can occur as seemingly random events – often these will be untargeted attacks, in which the attacker uses a scattergun approach to try and hit as many targets as possible. This type of attack may require some preliminary investigation work but is more likely to result from the purchase of something like an email address list or a list of credit card users. The resources or tools required to undertake this type of attack will almost certainly be commodity resources that can be found or bought from sources on the internet.

Another type of attack is posed by more organised individuals or groups, and will usually be targeted directly at individuals, groups of individuals or organisations. Some of the resources or tools required to undertake this type of attack will almost certainly be the ‘commodity’ type referred to above, but in those cases where specialist attackers have been hired, the tools will often form a bespoke malware payload, and may be individually crafted or modified for that particular attack.

For a more complex cyber-attack, it would be unusual for the attacker to use just one tool to carry out the attack. It is much more likely that they would use a mixture of tools, each designed to carry

out a portion of the overall plan, and these are often referred to as ‘blended’ attacks.

Stages of an attack

While the stages of an attack will vary, a sophisticated cyber-attack will typically take a highly structured form, such as the model described by Lockheed Martin’s ‘Cyber Kill Chain’.[19] There are seven distinct stages:

1. Reconnaissance. In the first stage, the attacker will reconnoitre the target’s networks and systems, looking for known vulnerabilities that can be exploited as a means of entry. This reconnaissance itself is likely to be highly sophisticated since it must achieve its aims without alerting an intrusion detection system.
2. Weaponisation (preparation). Once the target has been surveyed and the detailed objectives are understood, the attacker will prepare the software tools required to achieve them. This may involve the modification of existing commodity tools, or in extreme cases the development of specialist bespoke tools.

   Attackers may also take the opportunity to elevate their network or system access status, at least until they have deployed and tested the payload.
3. Delivery. The attacker will now upload the tools onto the target system or systems, or to a targeted user, checking that they are hidden both from normal view and from detection by more sophisticated means. Delivery could be as simple as loading it onto a USB memory stick that will be found by or given to a

user, attaching the malware to an email, or placing it on a social media website or in a ‘watering hole’ website.

4. Exploitation. The attacker needs to be certain that the final attack will be successful, so a known vulnerability on the target system will be exploited in order to execute the malware. This might also be the action of a user clicking on a link or opening an email attachment.
5. Installation. Having gained access to the target system or systems, the attacker will now install the malware. Often the malware suite will contain additional code to ensure that it cannot be deliberately removed and may also be time-stamped by the attacker so that it appears to blend in with other legitimate operating systems or application software.
6. Command and control (C2). Having verified that the tools will work as expected, the actual attack can be executed, by possibly choosing the most appropriate moment, for example when many of the security support staff are not at work; or by staging a major diversion that will draw attention away from the real attack.

   The attacker may use a channel over the internet, DNS or email protocols to achieve this.
7. Actions on objectives. Now the attacker can begin the real work, which may be to harvest user credential information, to escalate privileges so that they can gain access to systems currently out of reach, to exfiltrate other data, or simply to modify or delete data or destroy systems, or to install ransomware.

The theory of the Lockheed Martin Cyber Kill Chain is that if the defending organisation understands the type of attack, with the right tools and techniques they can stop it at any of the earlier stages and

prevent the attacker from achieving their final objectives. However, this presupposes that the defending organisation can either be ahead of the attacker or can at least keep pace with the attack.

In some extreme cases, there will be two separate attacks – the first to establish the exact details of the target, and the second to conduct the actual attack. The whole process can take many months, especially if there is a significant amount of bespoke software to be developed and tested. A simpler approach would be used for commodity-type attacks, in which no further software development is required, and following the initial reconnaissance the payload is deployed and the attack executed very quickly, so as to take advantage of the element of surprise, which might be lost if the time interval is too great.

TYPES OF CYBER-ATTACK AND ATTACK VECTORS

There are numerous types of attack used to breach computers – far too many to list them all in this book, so here is a selection of the most common attack types.

Dark patterns

While not actually a cyber-attack as such, dark patterns are an excellent starting point, since they show what can be achieved while remaining just on the right side of the law.

Dark patterns are perfectly legal (but usually unethical) methods used by website designers to tempt the unwary into making a choice or selection they might not normally make. Each method has a link to an example from www.darkpatterns.org/ in the notes. There are

many more such examples of these on their website. Examples of dark patterns include:

- Bait and switch techniques – an example of which was included in a Windows 10 upgrade offer by Microsoft. When the user clicked the red ‘x’ button, expecting to reject the upgrade, the upgrade was actually initialised instead.[20]
- Disguised adverts, in which clicking on what appears to be a legitimate link to a website the user wishes to visit takes them to somewhere different, and this can be a malware site.[21]
- Enforced subscriptions, in which the user finds they have committed themselves to an ongoing subscription rather than a one-off transaction. Often, the only way to get out of this is to call the organisation’s helpline, which can involve a premium rate call.[22]
- Friend spam, in which you register your email, Facebook or Twitter account with a website, which then publishes content or sends out bulk email, Facebook messages or Twitter messages using your account.[23]
- Hidden costs are a common example of dark patterns. The user begins to make a purchase on a website, but as they progress to the payment they find that additional charges, such as transaction fees, taxes and so on have been added. In other cases the original advertised cost does not include delivery charges to make it appear more attractive.[24]
- Misdirection techniques are used to increase revenues from websites. In one case, Ryanair’s website led customers to believe that it required some ‘Passenger details’, which they duly completed. It then added travel insurance to the total cost of the flights, and the only way to remove this was to select the ‘No

travel insurance' option carefully concealed in a drop-down menu described as 'Country of residence', which defaulted to United Kingdom.[25]

- With price comparison prevention techniques, users are either not permitted to copy and paste details from a supplier's website, as a means of discouraging them from finding a better price, or the organisation refuses to allow its products to appear on price comparison websites, claiming that this gives the shopper a better deal.[26]
- Roadblocks, also known as Roach Motels, are frequently used in order to prevent a user going further with a transaction until they have agreed to something. It frequently requires considerable effort to bypass this type of dark pattern.[27]
- Basket extras can be items in a user's website shopping basket that have unexpectedly changed cost. You may be purchasing a subscription and find that the website has changed your choice to a three-year deal, when in fact a one-year subscription is actually better value for money. This type of dark pattern can also include additional items such as insurance in a user's website shopping basket without their knowledge.[28] However, legislation is currently in development in a number of jurisdictions that would outlaw this practice.

Application layer attacks

Application layer attacks take place when firewall ports are left open for an attacker to use as a means of entry. Unfortunately, if an organisation is to be able to conduct business, at least one port (port 443 – Hypertext Transfer Protocol Secure (HTTPS)) must always be open for general internet traffic. Port 80 – Hypertext Transfer

Protocol (HTTP) tends to be less commonly used nowadays. A further port (port 25 – Simple Mail Transfer Protocol (SMTP)) is used for email traffic. Port 445, used by Microsoft file and printer sharing services, is normally blocked by firewalls. It is through these and other ports that a cyber-attacker can target specific applications – for example a web server application – and take advantage of a known vulnerability.

Botnets

Botnets are a means by which cyber criminals can target a large number of potential victims, most of whom are almost certainly unwilling recipients. Botnets consist of a very large number of malware-infected computers, known as ‘zombies’, which deliver the payload, whether this is spam email or a DDoS attack. These computers will have been accessed at some time by the botnet owner, sometimes known as a ‘herder’, who will probably have gained access either by the user clicking on a link in a spam email or by clicking on a link on a web page, either of which will have downloaded some form of malware onto the user’s computer without their knowledge.

This malware will allow the botnet owner to take control of the computer when they require, using one or a group of command-and-control computers. In cases such as this, the computer’s user is unlikely to be aware that their computer has been compromised.

The botnet owner may not actually make use of the botnet themself but may sell the service to people or organisations who wish to send spam email or mount DDoS attacks without having to create their own botnet.

It is important, however, to understand the difference between botnets, which are an aggressive means of conducting a cyber-attack, and distributed computing, where many computers are linked together in an organised endeavour in research.

Occasionally the law enforcement agencies manage to identify the botnet's command-and-control servers and are able to take down the entire botnet, as in the case of the 'GameOver Zeus' botnet, which at its peak included over a million zombie computers and had been designed to be impossible to be disabled.[29]

Brute force attacks

Brute force attacks are those in which a cyber-attacker attempts to discover something – for example, a password – by testing every possible combination of characters until the correct password is revealed.

Brute force attacks can take extended periods of time to succeed but will invariably find the correct result eventually. The development of faster distributed and parallel computing will reduce the time taken, but it is still a time-consuming activity, and it can often be more efficient to try and discover a password by other means such as social engineering.

Buffer overflow attacks

This type of attack is a well-tried and trusted method of breaking an application by providing it with more input than its designer expected or planned for. For example, if an application suggests one uses a username of up to 20 alpha-numeric characters and the user inputs 21, the application might go into an unknown state unless the

programmer had applied a check to discard the input if the total was greater than 20 characters. One method of deploying malware is to hide it within user input of this type.

Once an application has been broken in this way, it is quite conceivable that a cyber-attacker might be able to use the application's functions as if they were a bona-fide user.

Most recently written software usually takes account of buffer overflows, but occasionally a new one turns up and the cyber-attackers have a field day until a fix can be developed and installed.

Backdoors

Occasionally, programmers will build a 'backdoor' into their code. This will allow them to make changes while the code is being tested. Unfortunately, unless these backdoors are removed prior to the software being sold or distributed, anyone who is able to find such a backdoor will have instant access to the entire code, and (in theory at least) will be able to do anything they like, such as extract personal data, block selected users, skim off money – the world is suddenly their oyster.

The US and UK security agencies have long been concerned that Huawei's networking equipment might contain backdoors, and although they have not explicitly said that such things have been discovered, there is now a move to ensuring that their equipment does not form a major part of the countries' telecommunication networks.

While this is a laudable endeavour, it appears to ignore the possibility that 'home-grown' suppliers might also have backdoors in

their operating software.

Injection attacks

Another form of attack is the injection attack, in which the attacker either injects software code into a program, or otherwise inserts forbidden characters that might cause an application to terminate, leaving access clear for the attacker. An example of this in Structured Query Language (SQL) databases is to inject an '&' character in order to execute SQL commands.

Network protocol attacks

As mentioned in the preface to this book, the protocols that underpin the internet are far from secure. These include the following protocols, without which the internet does not work:

- User Datagram Protocol (UDP),[30] defined in Request for Comments (RFC) 768;
- Internet Protocol (IP),[31] originally defined in RFC 791;
- Transmission Control Protocol (TCP),[32] originally defined in RFC 793, now RFC 9293;
- Network Time Protocol (NTP),[33] originally defined in RFC 1305;
- Internet Protocol Version 6 (IPv6),[34] originally defined in RFC 2460, now RFC 8200;
- Border Gateway Protocol (BGP),[35] originally defined in RFC 1654, now RFC 4271.

There is no real need for the reader to understand exactly how these work or inter-relate – as with the earlier analogy of the motor car engine, we can still surf the internet without this knowledge, but

suffice it to say that if attackers can subvert any of these (and some others), they can do considerable harm.

Rogue update attacks

Rogue update attacks are an extremely popular method of conducting a cyber-attack. They often take advantage of unsuspecting or inexperienced users by suggesting – often in an email or as a pop-up on a website – that some element of the user's computer is out of date and requires an urgent update. This may be either an operating system or a commonly used application and will inevitably end with the computer being infected with some form of malware or ransomware.

Email-borne attacks

Email is very commonly used as a vector for conducting cyber-attacks, since many usernames can be easily guessed by simple software that combines known first names with known surnames, placing a full stop between them, and adding '@' and a known email provider's domain name, such as 'john.smith@gmail.com'.

Software can generate such email address lists extremely quickly, and emails using these addresses can be delivered at little or no cost to the cyber-attacker, potentially reaching thousands of email users at a keystroke. The malware, ransomware or other message that these emails contain will invariably result in some successes, and spammers rely on people's susceptibility to great offers.

Following the Monty Python 'Spam' sketch[36] in 1970, this form of email was dubbed 'spam', and the name has stuck. Fortunately, an increasing number of internet service providers are on the case very

promptly and can identify spam and delete it before it can reach its destination. However, this may, in some cases, require the end user to pay for a premium service. Alternatively, they could purchase the anti-spam service from an independent provider such as Message Labs or AVG.

Wireless network attacks

Cyber-attacks that use wireless connectivity can generally be in one of three areas:

- cyber-attacks on a Wi-Fi (802.x) infrastructure;
- cyber-attacks on a Bluetooth infrastructure;
- cyber-attacks on the Global System for Mobile Communications (GSM), third generation (3G), fourth generation (4G) and fifth generation (5G) cellular mobile infrastructure.

Wi-Fi attacks

Wi-Fi attacks are extremely common and can usually be conducted in one of two ways. The more difficult approach is for the attacker to intercept the signal of a wireless access point, to store the intercepted data, and to attempt to recover the access key by ‘brute force’ searching. Those access points that only have WEP or the original WPA encryption will be much easier to break into than those with WPA versions 2 and 3.

The second (and often more straightforward) method is for the cyber-attacker to introduce their own access point with an SSID similar or identical to that of a genuine access point, for example in any public space offering ‘free’ Wi-Fi. When an unsuspecting user tries to connect, and gives their access key, the attacker’s computer will capture the data and the attacker will be able to access the real

network as if they were a genuine user. Further, if the attacker is even more skilled, they will allow the user's computer to make an onward connection to the real network, creating a 'man-in-the-middle' attack. The attacker can now monitor the user's application login details, providing the attacker with access to at least one system within the organisation, from which they may be able to access other systems, or even find they have administrative access.

Bluetooth attacks

Bluetooth attacks tend to be focused on end-user devices that have their Bluetooth wireless connection enabled, and which can be intercepted and accessed from the attacker's device. These generally lead less to full network access, and if the attacker is targeting a particular user, Bluetooth will be an excellent way of achieving their objectives.

Through Bluetooth, an attacker can gain access to the victim's address book, calendar, email and much more besides. An example of the misuse of Bluetooth is in the case of Dublin Airport, which uses a passenger's Bluetooth identity to track them as they pass through the airport.[37]

If you ever want to see how easy it can be to select a target for a Bluetooth attack, simply go to the Bluetooth settings on your smartphone or laptop computer when you're on public transport, especially a commuter train, and you will see literally dozens of Bluetooth devices advertising their presence.

Similarly, if you go to the Wi-Fi settings, you may see the name of a user followed by the words 'Personal Hotspot' if they have previously used their device as a means of connecting another device to the internet.

A successful cyber-attack based upon either Bluetooth or Wi-Fi also requires a further lack of security awareness on the part of the user, such as blank or easy-to-guess passwords, which may frequently turn out to be the case.

GSM/3G/4G/5G attacks

Cyber-attacks against cellular mobile devices such as smartphones and tablet computers will mostly use either Wi-Fi or Bluetooth as a mechanism for attacking the device, since the cellular networks use a significantly more complex key management and encryption mechanism to protect the device and its data. Attacks against the GSM (2G) encryption standards are demonstrable using a false base station (similar to a fake wireless access point, but rather more complicated), but are relatively rare unless the attacker is being sponsored by a nation state government or security organisation, or a university research department.

The attacker must also ensure that the target is in close proximity to the false base station in order to verify that their phone connects to this rather than to a genuine network base station.

Attacks on third, fourth and fifth generation mobile phones are much less easy to undertake since the key management and encryption standards have been greatly enhanced so as to make interception and key recovery virtually impossible – at least for the time being.

Social media attacks

Attacks using social media methods are extremely common. These focus on two distinct areas:

- acquisition of personally identifiable information;

- tempting users to enter ‘watering holes’.[38]

Acquisition of personally identifiable information (PII)

People using social media sites such as Facebook, Twitter, Instagram, TikTok and LinkedIn frequently provide vast quantities of information about themselves, which could be used by a cyber-attacker not only to gain access to the individual’s social media account, but also to enter their bank accounts and other websites.

Equally problematic is when people’s friends, acquaintances and colleagues post information about an individual on social media, often being thoughtless about the possible consequences.

Many organisations now search for the social media accounts of prospective employees, as this allows them to screen possible recruits covertly.

An attacker looking to discover the names of company directors need only search the Companies House website for free.

‘Watering holes’ and other user temptations

Once a cyber-attacker identifies a potential target on a social media site, they have the opportunity to tempt the target into accessing a website containing malware, known as a ‘watering hole’. For example, some time ago, I received frequent requests through LinkedIn, offering me the opportunity to win an iPad. All of these were traced to malware sites, at least one of which would have resulted in additional personal information being provided as well as the planting of a virus on my computer.

Social engineering

Social engineering techniques are invariably a low-tech method for a cyber-attacker to acquire personally identifiable information or to gain unauthorised access to a computer.

Often this can begin with a simple phone call or email to tempt or invite the individual to part with information or money, or to click on a link to a malware website, as with the watering hole example above.

Other examples of methods of social engineering include an engineer tracing a fault or needing to check the gas/electricity meter; for companies, a person posing as someone from the IT department, often via a telephone call, or a ‘contractor’ attempting to talk their way past the reception desk. Much social engineering is performed by people skilled in ‘sweet talking’ the user, pretending to be trying to help (especially elderly or less technically aware users) and offering to make their computers more secure or to operate more quickly. Frequently these types of call result in the user’s computer being infected with malware or ransomware.

My younger son regularly receives scam telephone calls that refer to his recent ‘accident’. He helpfully plays along by inventing details of the accident and the injuries he received in an attempt to keep the caller on the line for as long as possible. He eventually announces that he has won the prank, having wasted much of the caller’s time, which hopefully would prevent someone else from being scammed.

Data aggregation

Data aggregation itself does not actually constitute a cyber-attack. It simply provides a means of bringing together items of data or information concerning an individual or group of individuals in order to gain a more detailed picture of them with a view to some form of exploitation, as discussed in earlier chapters.

However, when combined with the various methods of cyber-attack covered here, aggregating the resulting data becomes an extremely powerful tool in the hands of a more sophisticated attacker.

THE RISKS OF CONDUCTING A CYBER-ATTACK

There is an old saying, ‘Thou shalt not be found out.’ Much used in the past, the threat of being discovered applies just as much to cyber-attacks as it does to conventional misbehaviour. The impact of being identified as the originator of a cyber-attack varies from one type of attacker to another. Some will result in little more than public embarrassment for the miscreant; others could result in an extended holiday at His Majesty’s pleasure; while some could potentially precipitate an international incident.

The likelihood of being identified will also vary, based on the attacker’s technical abilities and their attention to detail. Inexperienced cyber criminals are more likely to make basic mistakes in their methods, whereas a more mature or experienced attacker or a state-sponsored group is almost certain to mount a highly professional, possibly multi-part attack, using methods described in the ‘stages of an attack’ section earlier in this chapter.

Although we will examine the principles of risk management in the next chapter, it is worth stating here that the impact or consequences that might befall a cyber-attacker, taken together with the likelihood

of their being identified, combine to dictate the level of risk that the attacker faces, and that those individuals or organisations that undertake cyber-attacks must ensure they are equipped to handle them in a skilful manner or accept the consequences.

Prior to the advent of online banking, those who wished to rob a bank were obliged to do so in person, and while on the bank's premises placed themselves at some risk of being overcome by security guards, identified and subsequently arrested. Since the advent of the internet and the World Wide Web, these physical risks have been completely removed, and the risks of identification and subsequent arrest are much reduced.

The cyber-attacker will ultimately balance the risks against the possible benefits of success in the cyber equivalent of a cost/benefit analysis, and make an informed choice either to proceed or to leave well alone. Alternatively, of course, they may simply chance their arm.

At one extreme, an inexperienced hacker who defaces the website of a charitable organisation or posts unsavoury material might expect to find themself being 'flamed'[39] by their peers. At the opposite end of the scale, American government agencies whose networks and systems have been penetrated – however innocently – have been known to demand extradition of the alleged offender.

The message is that unless you are at the very top of your cyber game, don't mess with government or military organisations if you are not prepared to accept the consequences.

---

1. See https://abcnews.go.com/Technology/GadgetGuide/story?id=4194143

2. See https://cyberlaw.ccdcoe.org/wiki/Cyber_attacks_against_Estonia_(2007)
3. See https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/
4. See https://www.cyber.nj.gov/threat-center/threat-profiles/ios-malware-variants/fusob
5. See https://www.theguardian.com/media/2010/dec/08/operation-payback-mastercard-website-wikileaks
6. See www.aviastar.org/air/russia/tu-144.php
7. Following the News International phone hacking scandal, the Leveson Inquiry recommended an independent body be set up to oversee the press, but this was rejected by the UK government.
8. See https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance
9. See https://www.justiceinitiative.org/litigation/united-states-v-private-first-class-chelsea-manning
10. See https://www.kali.org/
11. See www.openwall.com/john/
12. See https://nmap.org/
13. See www.aircrack-ng.org
14. See https://www.wireshark.org/
15. See www.tenable.com/products/nessus-vulnerability-scanner
16. See http://angryip.org/about/
17. See https://www.metasploit.com
18. See https://www.theguardian.com/politics/2022/apr/19/boris-johnson-must-pay-attention-to-basic-cybersecurity-rules-says-security-adviser
19. See https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
20. See https://www.deceptive.design/types/bait-and-switch
21. See https://www.deceptive.design/types/disguised-ads
22. See https://www.deceptive.design/types/forced-continuity
23. See https://www.deceptive.design/types/friend-spam
24. See https://www.deceptive.design/types/hidden-costs
25. See https://www.deceptive.design/types/misdirection

26. See https://www.deceptive.design/types/price-comparison-prevention
27. See https://www.deceptive.design/types/roach-motel
28. See https://www.deceptive.design/types/sneak-into-basket
29. See https://www.vice.com/en/article/539xy5/how-the-fbi-took-down-the-botnet-designed-to-be-impossible-to-take-down
30. See https://www.ietf.org/rfc/rfc0768.txt
31. See https://www.ietf.org/rfc/rfc0791.txt
32. See https://www.ietf.org/rfc/rfc9293.txt
33. See https://www.ietf.org/rfc/rfc1305.txt
34. See https://www.ietf.org/rfc/rfc8200.txt
35. See https://www.ietf.org/rfc/rfc4271.txt
36. See https://vimeo.com/329001211
37. See https://eu.usatoday.com/story/travel/roadwarriorvoices/2015/11/17/is-your-airport-secretly-spying-on-you-yes-if-you-are-in-dublin/83302142/
38. See https://www.fortinet.com/resources/cyberglossary/watering-hole-attack
39. https://techterms.com/definition/flaming

PART II
CYBER SECURITY SOLUTIONS

6 INFORMATION RISK MANAGEMENT OVERVIEW

In this chapter, we shall review the underlying principle of cyber security – that of information risk management. This chapter is not a detailed review of the subject – you can find this in the second edition of my book *Information Risk Management: A Practitioner's Guide*,[1] also published by BCS.

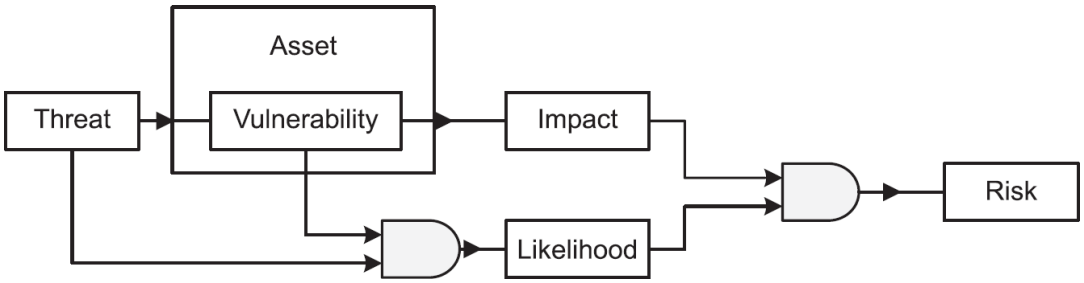
A GENERAL VIEW OF RISK

In Part I of this book, we looked at some of the impacts of cyber-attacks, the threats that can cause them and some of the possible motives behind an attack. Impacts and consequences are just two of the elements of risk management. The others are assets – the things we care about; vulnerabilities – those things that weaken our defences against cyber-attacks; and likelihood or probability – the chance that the threat will be successfully carried out.

We have already covered impacts in Chapter 4 and threats in Chapter 5, both in some detail, so let's consider the others.

Figure 6.1 shows the relationship between the various elements of risk and is described in the following paragraphs.

Figure 6.1 A general view of the risk environment



Looking at the relationship between these elements, we can see that threats act on a vulnerability in an asset, which in turn leads to an impact. Threats also, when there is motivation, combine with the existence of a vulnerability to provide us with the likelihood or probability of the threat being carried out. Following this, impacts and likelihood combine to produce risk.

However, there are two sides to the question of motivation – on one hand, there are attackers who have a strong motive and determination for carrying out the attack, while on the other, there are script kiddies who happen upon an exploit and try it out to see what happens (inquisitiveness). When combined with a vulnerability, either situation can result in the likelihood being high.

Occasionally, people confuse 'threats' with 'risks'. They may say that there is the risk of rain when they actually mean there is the threat of rain. The risk is that if it does rain, we might get wet as a result. As

we shall see later, the difference is subtle, but important when it comes to information risk management.

It is also not unusual for people to confuse probability and likelihood. As we shall see later in this chapter, there is a considerable difference between them, probability being an objective assessment with some form of statistical underpinning, and likelihood being subjective, based on emotions and gut feel.

There are inherent risks in many areas of cyber security, the main one being the possibility that despite all efforts to secure the organisation, an attacker may still find a way of accessing a system and causing damage.

Now let us look at some of the terms used in information risk management.

ASSETS

Assets in the wider sense can be almost anything, but in cyber security terms, assets can include not only the data – information we may be trying to protect – but also the complete technical infrastructure – hardware, software, data and information, HVAC and premises. Last, but by no means least, are the staff who have the technical knowledge and skills to design, implement and manage the appropriate security measures, to maintain them and to respond to incidents.

Although I have drawn the distinction between data and information, for the purposes of this book I have considered both to be assets that have value for their owners and must be equally protected,

although the owner of the original data and the owner of the resulting information may be entirely different entities.

THREATS

Threats are things or events that take advantage of vulnerabilities in order to cause some form of harm to assets. They may be differentiated from hazards that, although they too can cause harm to assets, are generally found more in the physical environment. Examples of hazards are fire, storms, floods, earthquakes and so on. Examples of threats in the cyber security area can be found in Chapter 5.

VULNERABILITIES

Vulnerabilities are things that reduce the level of security within assets and come in two distinct varieties. Intrinsic vulnerabilities are inherent in the very nature of an asset, such as the ease of erasing information from magnetic media (whether accidental or deliberate), whereas extrinsic vulnerabilities are those that are poorly applied, such as software that is out of date due to a lack of patching, or vulnerable due to poor coding practices.

When threats exploit vulnerabilities, this results in an impact to an asset, as shown in Figure 6.1, whether data that is copied or stolen (confidentiality), data that is changed or damaged (integrity) or access to data is prevented (availability).

Vulnerabilities can exist without our knowledge. There may be security issues with an operating system or a bug in an application that a hacker has discovered but is unknown to the software vendor

and the end user – this type of vulnerability is called a zero-day vulnerability.

One of the biggest problems with this kind of vulnerability is that once it becomes known to the hacking community it will usually be ruthlessly exploited until a fix is developed – and more importantly, applied. Once the software vendor announces the fix, knowledge of the vulnerability becomes even wider, and will often result in increased attacks, and an added danger is that individuals and organisations will fail to apply the fix, placing themselves at greater risk.

An interesting twist on the publication of known vulnerabilities is the situation in which attackers reverse engineer the vulnerabilities in order to design and build dedicated attack tools.

Other vulnerabilities are more obvious – such as the lack of antivirus software, which can allow malware to reach the target through email. Disaffected staff can either allow malware through the organisation's defences by reconfiguring them, or by bypassing them completely, introducing malware on a USB stick for example. Computers without passwords, or with default passwords for operating system software and application software or passwords that are shared, present easy pickings for even the least experienced attacker.

As we shall see later in this chapter, and also in Chapters 7 to 11, removing or reducing vulnerabilities will go a considerable way towards improving cyber security.

LIKELIHOOD OR PROBABILITY

The chance that something will happen is called the likelihood. Sometimes the term ‘probability’ is used instead, but it is useful to understand, for our purposes, that there is a considerable difference between the two.

Likelihood is a rather subjective term. If there are dark clouds in the sky, it may rain – but then again it may not. All we can say is that there is the likelihood of rain, and we may think that the chance of rain may be greater or lesser, depending on the amount of cloud. It is not an especially scientific method of predicting the weather but provides us with a general guide as to whether or not we should carry an umbrella.

Probability on the other hand is much more objective in nature. Probability relies on data – usually statistical data – that will underpin our judgement, and is often expressed in percentage terms. Again, it may be incorrect or expressed as having a margin of error, but at the very least, probability has a rather more scientific basis than likelihood. Sometimes you may hear of likelihood being referred to as a qualitative assessment, whereas probability is sometimes referred to as a quantitative assessment.

QUALITATIVE AND QUANTITATIVE ASSESSMENTS

One of the problems we face in information risk management is deciding which of the two types of measure to use – a subjective assessment of likelihood or an objective assessment of probability. In fact, one commonly used technique is to combine the two, referred to as semi-quantitative and semi-qualitative – for example, to use ranges of numerical values to improve the subjective nature of both impact and likelihood, as shown in Tables 6.1 and 6.2.

Table 6.1 Typical impact scales

Level of impact	Operational	Financial	Legal and regulatory	Reputational
Very low	Partial loss of a single service	Loss of less than £25K	Warning from regulatory body	Minor negative publicity
Low	Total loss of a single service	Loss between £25K and £250K	Penalties up to £10K	Local negative publicity
Medium	Partial loss of multiple services	Loss between £250K and £1M	Penalties between £10K and £50K	National negative publicity
High	Total loss of multiple services	Loss between £1M and £25M	Penalties between £50K and £500K	EU-wide negative publicity
Very high	Total loss of all services	Loss exceeds £25M	Penalties exceed £500K	Worldwide negative publicity

Although we have provided boundaries for the levels, there will be a degree of uncertainty about the upper and lower limits of each, but in general the ranges should be sufficient to provide a fairly meaningful assessment. Clearly these ranges will differ from one scenario to another but set a common frame of reference when there are a substantial number of assessments to be carried out.

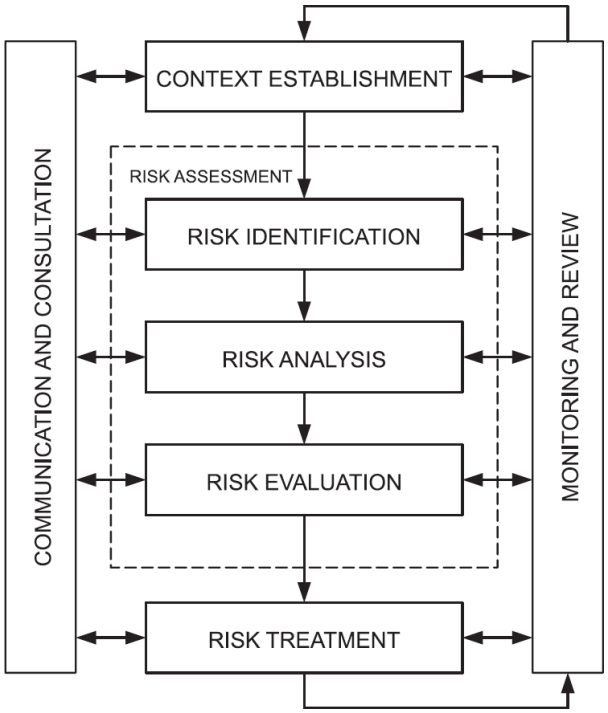
Table 6.2 Typical likelihood scales

Level of likelihood	Hacking, malware and social engineering	Environmental	Errors, failures, misuse and physical
Very unlikely	The event is likely to occur once a week	The event is likely to occur once a decade	The event is likely to occur once a month
Unlikely	The event is likely to occur once a day	The event is likely to occur once a year	The event is likely to occur once a week
Possible	The event is likely to occur several times a day	The event is likely to occur once a month	The event is likely to occur once a day
Likely	The event is likely to occur several times an hour	The event is likely to occur weekly	The event is likely to occur several times a day
Very likely	The event is likely to occur at any time	The event is likely to occur at any time	The event is likely to occur at any time

THE RISK MANAGEMENT PROCESS

The generic process for managing risk is illustrated in Figure 6.2. Since we are only taking a brief look at risk management, we will focus on context establishment, risk assessment and risk treatment and omit the communication and consultation, and monitoring and review stages. A more detailed explanation of all of these stages is given in *Information Risk Management: A Practitioner's Guide*.[2]

Figure 6.2 The overall risk management process



Context establishment

If we look at just the basic components of risk as described above, we can certainly make some form of assessment, but unless this is placed within the context in which the organisation operates, any judgement will have been taken in isolation.

The first stage of the risk management process then is to understand the context in which the organisation operates – financial, commercial and political – so that the later steps take these into account when making decisions about how to treat the risks.

Risk assessment

This second stage of the risk management process is broken down into three distinct areas: risk identification, risk analysis and risk evaluation.

Risk identification

Risk management begins by identifying the assets, deciding what value they have to the organisation, and therefore what the impact might be if they were damaged or lost. All assets require a single clearly identified owner who will have overall responsibility for the asset, even if the asset is shared between a number of departments in an organisation.

Some organisations mistakenly allocate ownership of information assets to the IT department, but this (unless it is an IT-specific asset) is a mistake, since the IT department can easily become the unwitting owner of many assets over which they have little or no influence, despite the assets being held on the IT department's systems. Only the true owner of the asset will be able to estimate its value to the organisation.

Once we have established the assets, their ownership and their value to the organisation, we can move on to understand what might threaten these assets and what (if any) vulnerabilities the assets have, which provides us with a basis for deciding on both the impact or consequence and likelihood or probability.

There is an ongoing debate about which aspects of risk identification come in which order. Some people feel that it is easier to identify the impacts if they understand the threats first; others feel that threat assessment can come later. Whichever approach you favour, it is important that you assess:

- the threats the assets face;
- the potential impact or consequence of the loss or degradation of those assets;
- the vulnerabilities that might contribute to this;

- the likelihood or probability that the threats will exploit the vulnerabilities resulting in an impact.

When assessing the threats, we can make use of a number of models – one of these is referred to by the initial letters D.R.E.A.D. and asks five questions:

- Damage – how bad would an attack be?
- Reproducibility – how easy is it to reproduce the attack?
- Exploitability – how much work is required to launch the attack?
- Affected users – how many people will be impacted?
- Discoverability – how easy it is to discover the threat?

Although rather subjective, the answer to each question is allocated a value (say between 1 for ‘low’ and 3 for ‘high’), and the sum of the five elements delivers the relative threat level.

Impact and likelihood are the two key outputs of this part of the process, and as mentioned earlier there are two methods of deciding the level of them:

- qualitative impact and likelihood assessment;
- quantitative impact and likelihood assessment.

In the case of the qualitative assessment, the outputs are measured in general subjective terms, such as low, medium and high, whereas in quantitative assessment, objective numerical data is used – for example, financial values for impact and percentages for likelihood.

Each method has its own merits – qualitative assessment can be carried out quite quickly (often based on ‘gut feel’) and does not require detailed research or investigation, whereas quantitative

assessment can be time-consuming but will usually deliver more meaningful results.

It is for the organisation to decide whether such a high degree of accuracy adds value to the assessment exercise – if the resulting risk is very high, the problem will require urgent attention, regardless of whether the risk comes out at 90 per cent or 95 per cent.

As already mentioned, there is, however, a halfway house in which qualitative and quantitative assessments are combined in a 'semi-quantitative' assessment. In these, boundaries are set for the values – for example for impact assessments, 'low' might indicate a financial value between zero and one million pounds; 'medium' might indicate a financial value between one million and ten million pounds; and 'high' might indicate a financial value above ten million pounds.

Similarly, for likelihood assessments, 'low' might indicate a likelihood between zero and 35 per cent; 'medium' might indicate a likelihood between 35 per cent and 70 per cent; and 'high' might indicate a likelihood above 70 per cent.

This provides a more meaningful assessment of risk, especially when presenting a business case to the board for approval.

Risk analysis

Once we have conducted the initial risk identification, we then take the impact and likelihood and combine them in the form of a risk matrix as shown in Figure 6.3, which will allow us to compare the risk levels.

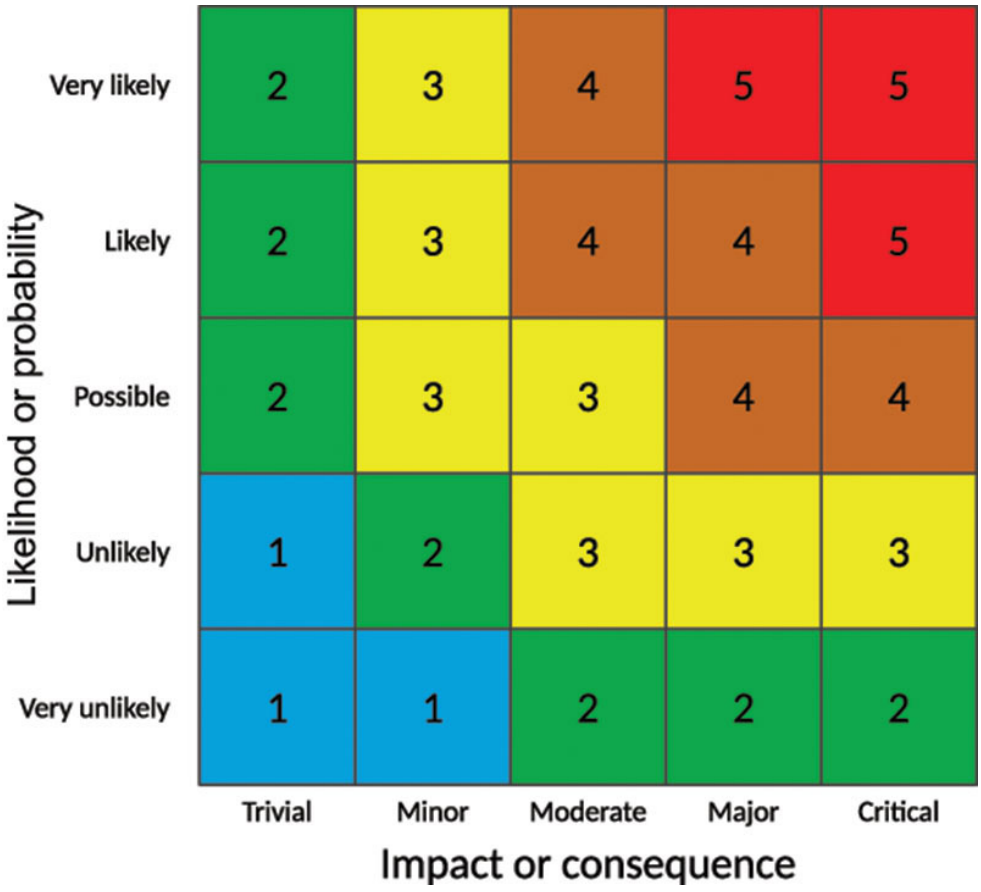
The risk matrix is simply a pictorial representation of the relative levels of all the risks we have identified, and which will help us to understand the order in which we wish to treat them, based on some form of priority or urgency.

Risk matrices most commonly consist of three, four or five ranges of values. Three is often considered to be too few to be meaningful, while five allows the possibility of too many results being in the middle. Four is sometimes thought to be a better choice, since the assessor must choose some value either side of the middle ground, avoiding the problem of a large number of risks being rated ‘medium’.

In conjunction with others, the risk assessor will allocate a risk category to each part of the matrix, in order to assist prioritisation. Alternatively, values can be assigned to each cell in the matrix, which enables grouping of risks. A typical example of a risk matrix is shown in Figure 6.3, where the values of each axis are multiplied together to provide a measurement of the risk.

Risks measuring 1 to 5 might be graded as trivial; 6 to 10 might be minor; 11 to 15 might be moderate; 16 to 20 might be major; and 21 to 25 might be critical.

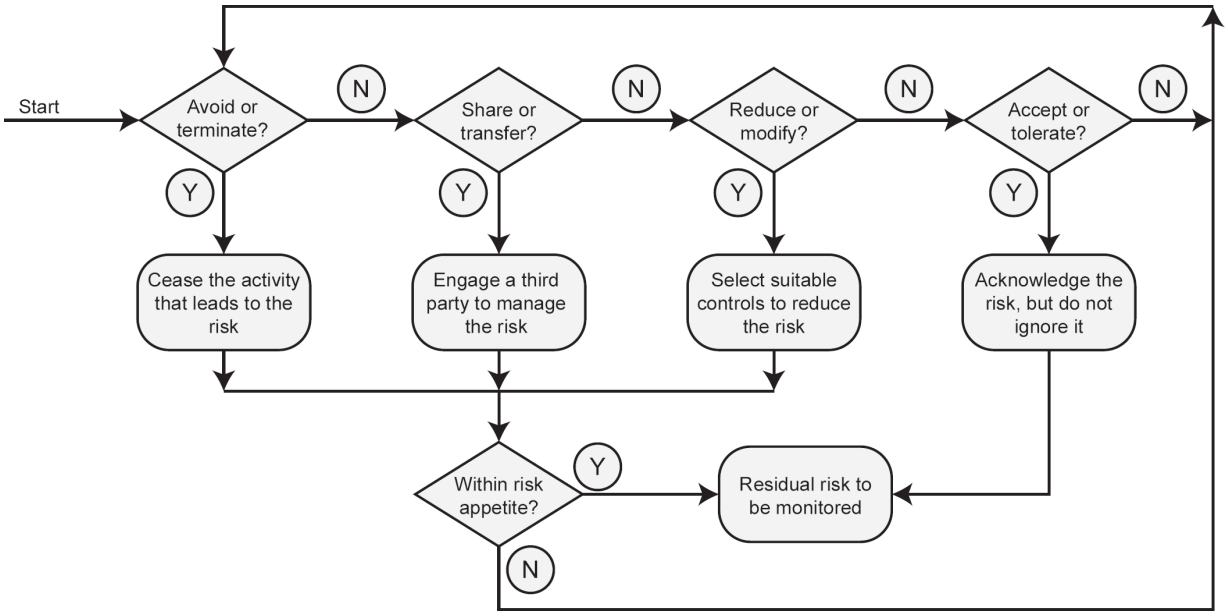
Figure 6.3 A typical risk matrix



Risk evaluation

Finally, we can decide how we are going to deal with the various risks, usually recording the results in a risk register. There are four ways in which we can deal with or treat them, as shown in Figure 6.4.

Figure 6.4 Strategic risk management options



Risk avoidance or termination In this method of risk treatment, we either stop doing whatever it is that has caused or might cause the risk, or if it is a planned activity we simply avoid doing it. While this will usually result in the risk being completely eliminated, it may cause the organisation other problems, for example if an organisation was planning to build a data centre and the risk assessment indicated a high likelihood of flooding in the proposed location, the decision would almost certainly be to avoid the risk by abandoning that location and building elsewhere. However, this might prove problematic, since alternative sites might be difficult to identify, be excessively costly or have other limiting factors. This would result in the organisation reviewing all these risks against one another.

Risk sharing or transfer If we find that we cannot avoid the risk, an organisation may decide to share it with a third party. This is usually in the form of insurance, but it is important to remember that even though the organisation may let someone else share or take the risk, they still own the responsibility for it.

However, some insurance companies will refuse to insure certain types of risk, particularly when the full possible impact is unknown, and in such cases the organisation must find an alternative method of dealing with it.

Risk reduction or modification Some people refer to this as risk treatment, although it is actually just one form of risk treatment. In this option, we do something that will reduce either the impact of the risk or its likelihood, which in turn may require that we reduce either the threat or the vulnerability where this is possible.

It is often the case that threats cannot be reduced – one cannot, for example, remove the threat of a criminal attempting to hack into an organisation's website, but it may in such cases be possible to reduce the likelihood by applying strict firewall rules or other countermeasures.

Risk acceptance or tolerance The final option is to accept or tolerate the risk, especially if it has a very low impact or likelihood. This is not to be confused with ignoring risk – never a sensible option – but is undertaken knowingly and objectively and is reviewed at intervals or when a component of the risk changes, such as the asset value, the threat level or the vulnerability.

Risk acceptance is based largely on the organisation's attitude to risk, known as its risk appetite. Some organisations have a very low risk appetite – for example pharmaceutical companies, who understand that the impact of failure to keep details of their products secure can mean enormous financial loss if they are stolen, or that patients could die if the manufacturing process is tampered with.

On the other hand, organisations like petrochemical companies will have a much higher risk appetite, investing vast sums of money in test drilling for oil reserves, knowing that some attempts will produce no useful results.

Residual risk While some forms of risk treatment will completely remove the risk, others will inevitably leave behind an amount of residual risk. This residual risk is either not possible to treat, or, more frequently, too expensive when compared to the cost of the likely impact. Residual risk must be accepted by the organisation and will require monitoring and regular reviews to ensure that it does not grow and become a treatable risk.

Risk treatment

Once we have decided the most appropriate method of treating risks, we move to the final stage of the risk management process – risk treatment and the use of controls or countermeasures to carry out our decisions.

Risk treatment is also sometimes referred to as risk mitigation, which is generally taken to mean a reduction in the exposure to risk (the impact or consequence) and/or the likelihood or probability of its occurrence.

There are four distinct types of controls:

- detective controls, which allow us to know or be made aware when something has happened or is actually happening;
- directive controls, which invoke some form of procedure that must be followed;
- preventative controls, which stop something from happening;

- corrective controls, which fix a problem after it has happened.

Directive and preventative controls are proactive in nature, since they are carried out before an attack has occurred in order to reduce its impact or the likelihood of it occurring.

Detective and corrective controls are reactive in nature since they take effect once an attack is already happening or has actually happened.

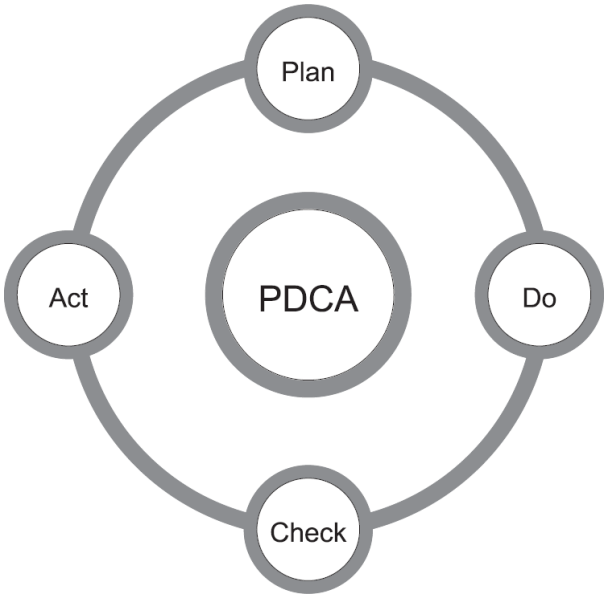
The four types of control are implemented in one of three ways:

- Procedural controls, which dictate what actions must be taken in a particular situation. An example of a procedural control would be one in which users are required to change their system access passwords at regular intervals. Procedural controls might include the vetting of staff by the HR department.
- Physical controls, which prevent some form of physical activity from taking place, such as fitting locks on computer room doors to prevent unauthorised entry.
- Technical controls, which change the way in which some form of hardware or software operates, such as configuring firewall rules in a network.

Sometimes, the risk treatment options – avoid/terminate, share/transfer, reduce/modify and accept/tolerate – are referred to as *strategic* risk treatment controls; the four types of control – detective, directive, preventative and corrective – can be referred to as *tactical* risk treatment options; and finally, the three methods of implementing the controls – procedural, physical and technical – are sometimes referred to as *operational* controls.

Although it is not strictly speaking an information risk topic, for many years, and for a variety of purposes, organisations have linked the risk management process with a system known as the Plan–Do–Check–Act (PDCA) cycle, otherwise known as the Deming cycle,[3] illustrated in Figure 6.5.

Figure 6.5 The Plan–Do–Check–Act cycle



The PDCA cycle has been widely adopted as a basic reference framework in the cyber security, information security, information risk management and business continuity management disciplines as well as in many others.

The four stages are described as follows:

Plan

In this stage, we establish the objectives and the processes necessary to deliver the required results. In the cyber security context, this equates to understanding the organisation and its context.

Do

The next stage of the process implements the plan, initially as a means of testing that the plan has been successful. In the cyber security context, this equates to implementation of the information risk management framework.

Check

In this stage, we examine the results we have achieved by either measurement or observation. In the cyber security context, this equates to testing, monitoring and review of the framework.

Act

In the final stage, we put the validated plans into action when an incident occurs and bring lessons learned from incidents into revisions of the plan. In the cyber security context, this equates to continual improvement of the framework.

Although the descriptions above relate to the wider area of information risk management, in cyber security terms any of these methods can be used to treat risk, since cyber threats can be made equally easily against poor procedures, a lack of good physical security and poor technical security.

We will examine the kinds of controls best suited to cyber security in Chapters 7 to 11.

---

1. David Sutton (2021) *Information Risk Management: A Practitioner's Guide*. Second edition. Swindon: BCS.
2. David Sutton (2021) *Information Risk Management: A Practitioner's Guide*. Second edition. Swindon: BCS.
3. See http://whatis.techtarget.com/definition/PDCA-plan-do-check-act

7 BUSINESS CONTINUITY AND DISASTER RECOVERY

In this chapter, we will briefly examine the concepts of business continuity (BC), which looks at the business as a whole, and disaster recovery (DR), which looks at just the IT infrastructure and which usually forms a component part of an organisation’s business continuity programme.

Although business continuity covers a much broader area than just cyber security, it is important to understand the underlying principles since it is a means of preparing for possible cyber security incidents. Likewise, disaster recovery is not all about cyber security but can play a major part in recovering from cyber security incidents.

Both business continuity and disaster recovery have a proactive and a reactive element to their contribution to cyber security; the proactive side attempts to reduce the likelihood that a threat or hazard may cause a disruption, and the reactive side is intended to take care of the recovery if one does occur.

Generally speaking, the longer a disruption lasts, the greater the impact on the organisation, so it helps to clarify the type of disruption, its duration and impact, and how an organisation manages the situation. Table 7.1 provides an example of this, and the failure types are covered in more detail below.

Table 7.1 Incident durations and recovery methods

Timescale	Seconds	Minutes	Hours	Days	Weeks	Months
Failure type	Glitch	Event	Incident	Crisis	Disaster	Catastrophe
Recovery by	Equipment	Equipment	Operations	Management	Board	Government
Recovery mode	Automatic	Automatic	Process	Improvisation	Ad hoc	Rebuild
Action	Proactive	Proactive	Proactive	Reactive	Reactive	Reactive

FAILURES

Glitches

These are extremely short occurrences, usually lasting just a few seconds at the most, and are generally caused by brief interruptions in power or loss of radio or network signal. Activities usually return to normal following most glitches as equipment self-corrects automatically.

Events

Events normally last no more than a few minutes. As with glitches, the equipment they affect is frequently automatically self-correcting, but may on occasion require a degree of manual intervention.

Incidents

Incidents are usually viewed as lasting no more than a few hours. Unlike glitches and events, they require operational resolution, normally involving manual intervention that follows some form of process.

The methods of dealing with glitches, events and incidents are mostly proactive in nature in that processes and procedures are developed in advance and are followed when the incident occurs.

Crises

Crises can often last for several days. Although organisations may have plans, processes and procedures to deal with them, and although operational staff will carry out any remedial actions, some degree of improvisation may be required. Crises almost invariably require a higher layer of management to take control of the situation, make decisions and communicate with stakeholders and the media.

Disasters

Disasters frequently last for weeks. As with crises, operational staff will carry out immediate remedial actions, although at this stage a degree of ad hoc action may be necessary. Although a higher management layer will control activities, the senior management layer will usually take overall charge of the situation.

Catastrophes

Catastrophes are the most serious level, often lasting for months, or in some cases for years. Their scale tends to affect many communities, and so although individual organisations may be

operating their own recovery plans, it is likely that local, regional or even national government will oversee the situation and that either a partial or complete rebuilding of the infrastructure may be required.

Despite any proactive planning or activities to lessen their impact or likelihood, crises, disasters and catastrophes all require significant reactive activity, and each will demand an increasing amount of incident management capability.

It is important for organisations to understand that the more time spent in proactive work, the less time will generally be required in reactive work following a cyber-attack.

Business continuity and disaster recovery share the same fundamental Plan–Do–Check–Act cycle as discussed in Chapter 6. During the ‘Plan’ stage, we carry out the risk assessment (risk identification, risk analysis and risk evaluation); in the ‘Do’ stage, we implement the risk treatment options and assemble the plans; in the ‘Check’ stage, we verify that the plans are fit for purpose by testing and exercising; and finally in the ‘Act’ stage, we put the plans into practice when a disruptive incident occurs.

BUSINESS CONTINUITY

Putting business continuity into practice is strongly linked to the process of risk management described in Chapter 6, in which we identify all the organisation’s assets, owners and impacts; assess the likelihood of risks happening; and combine the two to provide a perceived level of risk. From this, we are able to propose strategic, tactical and operational controls, one of the main components of which will be the business continuity plan (BCP) itself.

The plan should include the actions that will cause it to be triggered; who (or which departments) will be responsible for what actions; how they will be contacted; what actions they will take; how, where and when they will communicate with senior management and other stakeholders; and finally, how they will determine when business has resumed a pre-determined level of normality.

The plan itself may not always contain detailed instructions, as these may change at intervals, but they should be referred to in the plan.

Although cyber security covers only a part of the overall business continuity process, there are certain aspects, especially with regard to the ongoing availability of information and resources, that are very much an integral part of cyber security.

The most obvious of these is that of disaster recovery of ICT systems, in which the systems that are likely to be impacted require some form of process in order to permit short-term or even immediate recovery.

Business continuity is often referred to as a journey rather than a destination. It looks at the organisation as a whole as opposed to just the IT aspects. However, that said, the generic business continuity process applies extremely well to cyber security and can be used to help an organisation to place itself in a very strong position.

The Business Continuity Institute (BCI) describes business continuity as: ‘The capability of the organisation to continue delivery of its products or services at acceptable redefined levels following a disruptive incident.’ It provides excellent guidance on the entire process, and its latest *Good Practice Guidelines* (2018 version)[1] can

be purchased for around £30 for a downloaded copy, free of charge to BCI members.

Over several years, the BCI has developed a business continuity management life cycle, with six distinct areas known as Professional Practices (PPs). It is basically a variation on the theme of risk management.

Firstly, there are two Management Professional Practices:

PP1 *Business continuity policy and programme management*, in which the overall organisation's business strategy is used to develop the programme of work, each component of which is then managed as a project.

PP2 *Embedding business continuity into the organisation's culture*, which includes training, education and awareness, and is covered in Chapter 10 of this book.

Then there are four Technical Professional Practices:

PP3 *Analysis* is all about understanding the organisation, its priorities and objectives, its assets, potential impacts, its threats or hazards and the vulnerabilities it faces. From this a risk assessment can be undertaken, and the key metrics such as the recovery time objective (RTO),[2] maximum acceptable outage (MAO)[3] and maximum tolerable data loss (MTDL)[4] can be derived.

PP4 *Determining the business continuity management strategy* (also referred to as Design) and designing the approach to deliver this can now take place, based on the metrics arrived at in the analysis stage, and decisions can be made regarding what proactive measures should be put in place; how response to an incident will be organised; and how the organisation will recover to normal operational levels or to a new, revised level of normality.

PP5 *Implementing the business continuity response* will require the efforts of people in various parts of the organisation to put in place the proactive and reactive measures agreed in the previous stage.

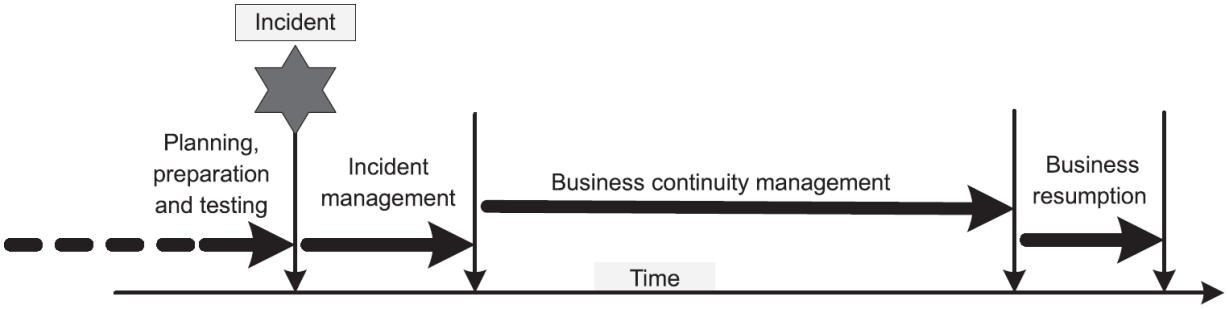
PP6 *Validation*, which includes exercising, maintaining and reviewing, is a separate activity to embedding the business continuity culture into the organisation, since it deals with the inclusion of people who may already have been involved in the previous stages, and who need no introduction to the subject; rather they need to be

able to exercise the various response and recovery plans, validate them and fine-tune them where necessary.

The general timeline for business continuity is illustrated in Figure 7.1. If the organisation is well organised, all six stages of the life cycle should have been completed before an incident occurs.

The first actions will be to respond to the incident itself, bringing together the incident management team, gaining an understanding of the situation and agreeing which aspects of the plan are to be implemented. At this time, it will also be important to consider preparing some form of statement that can be given to the media, customers and suppliers so that their expectations are managed.

Figure 7.1 Business continuity timeline



Next, the processes and procedures that have been developed (which may include disaster recovery mechanisms) will be brought into action, and depending upon the nature of the situation as seen in Table 7.1, may be in progress for some time. If this is the case, follow-up media statements will be required.

Finally, once the situation has been resolved, business can be returned to normal, or if the impacts have been considerable, to a new level of normality.

The international standard ISO 22301:2019 – *Societal security – Business continuity management systems – Requirements* covers all aspects of business continuity.

DISASTER RECOVERY

One of the main features of a business continuity plan is in providing the availability determined by the analysis stage of the business continuity process. Disaster recovery is perhaps a misnomer, since it implies that systems, applications and services have failed catastrophically and need to be brought back online. While this might be the case for some services, it is not necessarily true for all, since an element of proactive work can (and usually should) be carried out, and it may be the case that just one component in the service has failed but that this causes a chain reaction and requires a disaster recovery process to be invoked.

As with any business continuity work, there are both proactive and reactive sides to disaster recovery, and since there are no ‘one size fits all’ solutions, we’ll discuss some of the options in general terms.

Standby systems

Conventionally, there are three basic types of standby system – cold, warm and hot – although there are variants within these. Most well-designed standby operations will ensure that there is an effective physical separation between the ‘active’ and ‘standby’ systems since the loss of a data centre or computer room containing both systems would clearly result in no recovery capability.

Traditionally, organisations work on the basis that a minimum separation of 30 km is sufficient to guarantee that a major incident

affecting one data centre will not affect the other.

Systems, as we refer to them here, can mean any system that is involved in providing the organisation's service and can include web servers at the front end of the operation as well as back-end servers and support systems, and essential parts of the interconnecting networks.

Cold standby systems frequently make use of hardware platforms that are shared by a number of organisations. They may have power applied, and may also have an OS loaded, but they are unlikely to have much, if any, user application software installed, since each organisation's requirements will be subtly different. There will also be no data loaded.

This is the least effective method of restoration, since it may take a significant amount of time and effort to load the operating system (if not already done), to load and configure the user applications and to restore the data from backup media. It will, however, invariably be the lowest cost solution for those organisations who are able to tolerate a longer RTO.

Another disadvantage of cold standby systems is that if they are shared with other organisations there may be a conflict of resources if more than one organisation declares an incident at, or around, the same time. An example of this was the situation on 11 September 2001, when the attacks on the World Trade Center in New York took place. Most organisations had disaster recovery plans, but a number of them relied on the same providers, which completely overwhelmed their capabilities.

Warm standby systems will generally be pre-loaded with operating systems, some or all user applications, and possibly also data up to a certain backup point. This means that the main task is to bring the data fully up to date and this will therefore much reduce the restoration time required.

Warm standby systems are invariably costlier to provide than cold standby, and it is common practice for organisations to use one warm standby system to provide restoration capability for a number of similar systems where this provides an economy of scale. Additionally, those organisations who regularly update their application software may make use of their warm standby systems as training, development and testing platforms before a new or updated application is taken into live service.

Hot standby systems come in several flavours, but increasingly, and especially where no outage time can be tolerated at all, hot standby or high availability systems are becoming the norm. A basic hot standby system will be as similar as possible in design to a warm standby system, except that the data will be fully up to date, requiring a real-time connection between the active and standby systems.

Two slightly different methods of synchronising the systems are in common use – the first (and faster) method is known as asynchronous working, in which the active system simply transmits data to the standby but continues processing without waiting for confirmation that the data has been written to disk. The second, slightly slower (but more reliable) method is known as synchronous working, in which the active system transmits data to the standby

and waits for confirmation that the data has been written to disk before it continues processing.

In the first method, there is always the possibility that some data will not be received by the standby system, and in cases where nothing less than 100 per cent reliability is required (for example in financial transactions) this will not be sufficiently robust.

In the second method, there will always be a slight time lag between transactions since this method will provide 100 per cent reliability at the expense of speed. It will also be costlier to implement, since very fast transmission circuits will be required – usually point-to-point optical fibre.

Networks and communications

While the emphasis tends to be on the recovery of key systems, organisations should not overlook the networks and communications technology that support them. Wherever possible, key elements of the communications network should be duplicated so that the failure of one does not cause a total loss of connectivity. Many organisations now use two different transmission providers to ensure that if one has a major network failure, the other should still be able to provide service. This will of course depend on whether one is acting as a carrier for the other, in which case a failure of the main provider’s network could result in the other losing service as well.

Larger organisations make use of load balancing systems to ensure that in peak demands on their websites they are able to spread the load across a number of servers, and many also duplicate their firewall infrastructure as added insurance.

Separacy is also a wise consideration – the scenario in which a road repair takes out an organisation's communications is all too familiar, and by providing diverse communications cables on routes separated by 30 m or more and using entry points on opposite sides of a building, the likelihood of failure is much reduced.

Naturally, all this costs money, but when compared with the potential losses that would be incurred in the event of a total infrastructure failure, it is a vital form of insurance – and one that can reduce the cost of revenue loss insurance premiums.

In the mid-1990s, the author had arranged to have two fibre optic cables laid between two key buildings about 2 km apart – one cable for normal use, and the second (with a different provider, and diversely routed) to provide resilience, and the chief financial officer (CFO) complained bitterly at the expense. Two days after the installation of both cables had been completed, major roadworks caused a break in the first cable. The routers at either end of the link switched seamlessly to the backup cable with no disruption to service, and the CFO agreed that the cost of the additional cable had been justified.

Power

Power is at the heart of everything. Without it, the systems and networks cannot run, and business would grind very quickly to a halt.

Those organisations that suffer regular power outages will probably already have invested in a standby generator or at least an uninterruptible power supply (UPS) system that will continue to deliver sufficient power for a defined period of time.

More frequently nowadays, the two are combined, so that a UPS system will continue to deliver power and remove any power spikes from the supply, after which the standby generator will cut in and deliver power as long as the fuel supply lasts.

The international standard ISO/IEC 27031:2011 – *Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity* covers many aspects of disaster recovery.

Fire prevention and smoke detection

While this may not immediately appear to be a cyber security issue, access to a fire prevention system could affect an organisation's ability to deliver service. No computer room or data centre would be complete without having smoke detection systems and fire prevention facilities. Systems such as Very Early Smoke Detection Apparatus (VESDA) can identify the release of smoke (and therefore the possibility of fire) before it takes hold and causes real problems.

The system works by sucking air from the area through pipes and sampling the quality of air passing through a laser detection chamber. If the quality falls below acceptable levels, a response can be triggered, and this is often as a result of detection by more than one detector. The gas, normally nowadays an inert gas called Inergen, is discharged to the affected area, and works by reducing the oxygen content to less than 12.5 per cent, at which point combustion cannot occur.

An interesting example of a problem with Inergen was highlighted in September 2016, when ING Bank tested the system in their data centre in Bucharest. The gas discharge produced sound levels in

excess of 130 decibels, which caused excessive vibrations and head crashes in disk drives. The entire data centre was out of action for an extended period of time, preventing access to ING's customers.

---

1. See www.thebci.org/index.php/resources/the-good-practice-guidelines
2. The RTO is the duration of time within which business processes must be restored after a disruptive incident in order to avoid unacceptable consequences to the business.
3. The MAO is the time a system can be unavailable before its loss will compromise the organisation's business objectives.
4. The MTDL is the maximum loss of data or information (whether electronic and otherwise) that an organisation can tolerate.

8 BASIC CYBER SECURITY STEPS

In this chapter, we examine steps that can be taken both by individuals and corporate users to improve their cyber security. We provide details of the general steps that can be taken by any user – technical or non-technical – and then cover those steps that are of a rather more technical nature. Finally, the chapter includes a section on mobile working.

As discussed earlier, the response to cyber issues comes in two distinct areas. The first area is that of proactive response, in which we try to either lessen the likelihood of the event happening, or if we cannot do this we try to lessen its impact.

The other area is reactive response, which will include the disaster recovery capabilities described in the previous chapter, as well as the hands-on work of changing system configurations to apply corrective controls once a cyber security incident has been detected. Either method should reduce the risk, but we may have to accept that there may be some residual loss or damage.

When we leave our house, we take care to lock the doors and windows. This might not prevent a burglar from gaining entry, but it does make the job more difficult. Unless the burglar is specifically targeting us, there is a definite chance that they will go elsewhere and try to enter someone else's property.

It is very much the same with cyber security. If a determined attacker is sufficiently well motivated, skilled and equipped, they will almost certainly eventually succeed in gaining access to our data. However, financial constraints might make it difficult or impossible to repel the attacker, so the emphasis should not therefore be to make 100 per cent sure they are unable to achieve this, since this is an unrealistic expectation. Rather we should try to make the attacker's job so difficult that they give up and go elsewhere.

We shall deal with personal cyber security steps first, since these, for the most part, will apply both to individuals and to people within organisations, and we shall examine the additional steps that larger organisations can take to implement good security in Chapter 9.

GENERAL SECURITY ADVICE

The steps outlined below apply equally to individual home users, SME users and users within larger organisations.

From a cyber security point of view, with every piece of 'smart' equipment you add to your home, the more you increase your risk exposure, and (in theory at least) the safest home from a cyber perspective is actually the dumbest – one without any 'smart' technology at all.

Implementing controls

In Chapter 6, we looked briefly at the process of risk management. This provided us with some high-level options:

- risk avoidance or termination, in which we stop doing whatever it is that gives rise to the risk;
- risk sharing or transfer, in which we share the risk with a third party, often an insurance company;
- risk modification or reduction, in which we find some way of reducing either the likelihood or the impact of the attack;
- risk acceptance or tolerance, in which we accept that some things cannot be readily fixed and that we must accept the consequences.

Most of the actions we can take in the world of cyber security tend to be in the third of these – that of risk modification or reduction, and it is this area that we shall focus on most.

At the next level, there are four general directions we can take. Three of these are proactive in nature:

- detective, in which we put something in place to detect that an attack is in progress, such as IDSs or antivirus software (which will also react to malware it has detected);
- preventative, in which we put additional facilities in place in an attempt to stop an attack from being successful, such as firewalls;
- directive, in which we set out policies, processes and procedures that people must follow in order to reduce the risk, such as password policies.

The fourth direction is reactive in nature:

- corrective, in which we try to fix something that has happened as the result of an attack, such as removing infected files and blocking unnecessary ports.

Finally, we reach the point at which we can examine the actual actions, known as controls or countermeasures, that we can take. There are three options, which we shall examine in greater depth:

- physical controls, such as access control systems, which prevent intruders gaining access to equipment or its environment in order to launch a cyber-attack or otherwise cause damage;
- technical controls, such as firewalls, which directly address the security of systems and software that hold our information;
- procedural controls, which tell people both what not to do and also what they must do before, during or following an attack, and, as mentioned earlier, may include vetting of staff by the HR department.

A number of documents providing sound cyber security advice are available, and would be especially valuable to SMEs:

- The NCSC publishes several cyber security-related advice documents, including the UK government's '10 Steps to Cyber Security',[1] 'Common Cyber Attacks: Reducing the Impact' and '10 Steps: Board Level Responsibility'.
- For those looking for more specific detail, there are more than 200 additional documents published, dealing with all aspects of cyber security.[2]

It is worth making a brief examination of the SANS Institute Sliding Scale of Cyber Security,[3] which provides general guidance starting from a proactive position and potentially moving to a highly reactive one.

At the proactive level, the scheme begins with security designed and planned into the organisation's information architecture, based on the business objectives. This is often the most difficult to achieve since the security aspects of many systems' hardware and software are outside our control. This represents both preventative and directive action.

It continues proactively, with passive defence, in which additional technology is added to the underlying infrastructure to provide protection against cyber-attacks without the need for human intervention. This represents both preventative and detective action.

From this point, we move into the reactive sphere, beginning with active defence, in which security teams respond to events that cannot be completely controlled by passive defence means. This may include gaining a full understanding of the target, the method of attack, and even, if possible, the identity of the attacker. This represents corrective action.

An example of this might be the case in which an organisation finds itself under a massive DDoS attack. One of the defence mechanisms taken in conjunction with the ISP is to move the company's internet presence to a different connection and IP address, and the ISP then points the DDoS attack into a 'sink' or black hole.

Next, we move into the area of intelligence, in which we use the attacker's identity to discover more detail about them, their

motivations, means and methods, which may enable us to prevent further similar attacks. This part of the process will require tools to capture information about the attacker, and also a means of analysing this information to produce viable intelligence.

However, this may be outside the scope of most organisations, and this sort of investigation could well be undertaken by an outside company offering specialist InfoSec skills assisting the attacked company to restore their service. There are a number of models that enable this work: one such is the Diamond Model of Intrusion Analysis;[4] however, it is rather detailed and falls outside the scope of this book, so a link is provided in the notes for you to explore if you wish to do so.

Finally, we arrive at the point where we may choose to react – fighting back. This course of action is not recommended, since it could be fraught with danger, and could constitute a cyber-attack in its own right. Individuals and businesses should be discouraged from any form of retaliation – it's much more sensible to respond by alerting the appropriate authorities where possible and leaving offensive retaliation to security services and, where applicable, military agencies.

Physical security

It would appear at first sight that since we're dealing with cyber security, physical security actions might not feature strongly. While there is an element of truth in this, we should not overlook the fact that if an attacker can gain physical access to a key computer system, they can probably achieve anything they wish just by connecting a USB stick with key-logger software or other malware.

Restricting physical access to business-critical systems should always be the first step in any proactive activities. Not only does this mean keeping the bad guys out of the computer room, but also everyday users, unless they have a very specific requirement to be there. Access to controlled areas should be the exception rather than the rule, and all permissions for access should be subject to a formal procedure and should be reviewed at regular intervals.

It is good practice to ensure that that any visitor to a computer or network equipment room should be accompanied by a trusted member of staff, preferably one of the organisation's system administrators. It should also be noted that cleaners are not exempt from this policy.

Some simple steps that will make a difference include:

- Locking electronic devices (smartphones, tablet computers and laptops) somewhere secure when you have to leave them.
- Never leaving devices unattended in a public place, and keeping them hidden from view when travelling, especially in crowded places like railway stations and airports.
- If you're concerned about your computer's camera being accessed by someone, a very simple solution is to place a sticky note over the top of it.
- If you use a lockable steel security cable to secure a device, make sure that it is fastened to something that cannot easily be removed, and make sure you keep the key with you when you leave.

Individual user steps while surfing the web

You should resist the temptation to install or download unknown or unsolicited applications or programs unless you are confident that they are secure and free from malware. In a corporate environment, no privileged user should use an administrative account for downloading unauthorised software. Their day-to-day user account should not have the level of privilege required to do so.

When visiting a new website, you should avoid clicking on links to other pages unless you are sure they are valid. Some websites shorten the URL, so the final address is hidden. Let the mouse pointer hover over the link before you click to show the link's full address.

Cookies are essential to many internet activities such as online shopping, but many are irritating, and some are harmful by invading our privacy. You should periodically edit the cookie list and clean out any that are not needed.

The Onion Router (TOR) is a browser system that protects users by routing internet traffic through a network of relays run by volunteers all across the globe. It prevents one's internet activities from being observed and prevents the sites we visit from identifying our physical location. TOR should not be used in a corporate environment, since it is well known for subverting end-user security controls, such as anti-malware products.

Online forms frequently ask for information they really don't require. If you think the question is unnecessary or intrusive, give an answer such as 'not relevant'. If you don't think they really need your telephone number for example, type in something like 01234 000000.

You should always delete browser history on public computers. This prevents the next user discovering personal information that may have been inadvertently left behind. It's also a good idea to periodically delete it on home computers as well, since it can eat up valuable disk space.

You should also delete temporary internet files on home computers occasionally, and every time after using a public computer, for example in a library. This is invariably achieved by accessing the security tab in the browser's preferences, since different browsers will store them in different locations. They take up considerable space on the hard disk, and rarely serve any useful purpose. As with browser history, they can also be used to track one's web surfing experiences, although the search engine (e.g. Google) will definitely be doing so.

Internet passwords should be treated in exactly the same way as ordinary system passwords. See the section on user passwords later in this chapter.

Social engineering

One method by which attackers will attempt to break into a network or system is to use their social engineering skills to talk their way around the organisation's security defences.

- Never provide cold callers with your credentials.
- If you receive spam text messages on your mobile phone, report these to your network provider. Use the number 7726, which spells SPAM on the keyboard of non-smartphones.
- Unless you are confident of the originator of a text message that includes 'Text STOP to unsubscribe' or similar, never do so,

since this may be simply a ruse to discover if there is a real person behind the number as opposed to a system of some kind.

- Resist the temptation to reply ‘Go away’ or words to that effect.
- Do NOT call back on telephone numbers that you cannot authenticate – they could lead to a scammer, or simply rack up a substantial telephone bill.

Email

Once an attacker has acquired (or guessed) your email address, they may send offers of apparently attractive goods or services to tempt you into clicking on a link, which is almost certainly going to cause you problems. At best, it will connect you to a website that offers fake goods; at worst, it will download malware onto your device that will be used to extract further information such as banking details, passwords and so on.

If an email looks suspicious, delete it without opening it. To do this, in most email applications you can usually right-click on the message and consign it to the waste bin with no risk at all.

Never respond to emails that invite you to enter your credentials such as bank account number and PIN or password. Banks and credit card companies will never ask you to do this, and even if the email appears to be from your own bank, it may well be a scam. It is a sensible idea to check any such emails against one that is known to be legitimate. However, spammers are becoming increasingly professional, and it is often difficult to discern spam from the real thing. If in doubt, allow the mouse to hover over the URL, and check that this has not been obfuscated.

Phishing attacks often originate from respectable-looking emails purporting to originate from a reputable financial institution requesting that the user verifies their online identity. These are invariably scams and will take the unsuspecting user to a fake website that is to all intents and purposes an identical copy of the real one. It is essential not to respond to these, and it can be helpful to notify the real institution whose genuine website is being abused.

Spam email is a blight. Fortunately, many email providers now have highly tuned filters that detect and delete spam without the user even being aware of it. If spam email does make it through their filter, it may (with luck) wind up in a junk email folder in your mail application, making it simple to identify and delete. Do so. Do not be tempted to reply, since this will merely let the originator know that they have found a working email address, and you may end up receiving even more.

Consider using encrypted email to send sensitive information over the internet. We deal with this in greater detail in the section about encryption later on. For organisations with their own email servers there is the option of turning on ‘opportunistic encryption’ described in RFC 7435: ‘Opportunistic Security: Some Protection Most of the Time’.[5]

Backup and restore

It is incredibly easy to accidentally delete something important, but it is just as easy to make sure you don’t.

It is not recommended that you back up your files to the same hard disk drive that the operating system is installed on, so buy a reliable

backup disk drive and make use of the inbuilt software in Microsoft Windows and Apple Mac operating systems.

As an alternative to a hard disk drive you may consider backing up data to a memory stick or backup hard drive, but always encrypt the data on your backup device.

Always store the media used for backups in a secure location to prevent unauthorised access to your data. A fireproof safe is an ideal storage solution, but keep it separate from your computer.

Pirated software

The best advice for pirated material, including films, music and software is just don’t download it. You don’t know that the material is malware-free, and in any case, much of it is actually illegal since it usually represents the theft of intellectual property.

For a business, legal liability where pirated or illicit material is found on one of its computers lies with the business owner, and not with the user of the computer.

If you discover pirated material, the copyright owner may be interested in hearing about it, and in the case of software, the Federation Against Software Theft (FAST) may take an active interest.[6]

Personal information

Keeping your personal information secure is one of the main objectives of cyber security.

If the information is extremely sensitive, consider whether you should be keeping it on a device in the first place. If the answer is ‘yes’, then consider encrypting it.

Be extremely careful what information you share, and with whom you share it. Consider where the information might be stored, and where it might end up if the person or organisation to whom you are giving it is not as careful about security as you are.

File sharing

Many people and organisations now make use of cloud-based services to share information with friends, family and colleagues. All this is absolutely fine, provided that you have legitimate reasons for sharing information and it does not infringe someone else’s copyright. However, there is increasing use of file sharing mechanisms to distribute material illegally.

Corporate staff who access personal cloud-based file sharing services from the workplace pose an additional threat of the possible exfiltration of corporate data/information.

Films, audio recordings, books and other material is hosted or ‘seeded’ by individual sharers. The user acquiring the information obtains a ‘torrent’ file from a file sharing service and runs this within file sharing download software. The software links to the individual seed computers and downloads small portions of the file, linking them all together.

Only share information with family, friends and colleagues if it is not someone else’s copyright or if you have their express permission to do so.

If you use a file sharing service (such as Dropbox, Amazon Cloud or Microsoft OneDrive), consider encrypting the information, especially if it is in any way sensitive.

Social networks

The use of social networks has increased dramatically in recent years. Facebook (Meta), Twitter, Flickr, LinkedIn and Instagram are just a few examples of the most widely used social networking sites. While the idea behind these is to share information between friends, family and colleagues, there are significant dangers in making use of them.

First, you may not know who is reading them if you have not correctly set your access preferences (which may be difficult to identify). Many organisations now examine the social networking site pages of job applicants before deciding whether to invite them for interview.

Second, you do not necessarily know what other people may be posting about you – that embarrassing photograph taken on a recent night out may have been purely in jest but could reveal some aspect of your character that you would prefer to keep to yourself. It might turn out to be a topic of discussion at your next job interview or annual performance review.

Third, you do not necessarily know the impact of something you have posted about someone else.

Key points:

- Be careful what you post on any social media networking site. It might come back to bite you later on.

- Be very careful about who you accept as a ‘friend’, and who you follow.
- Always ensure your information sharing preferences are set to the most appropriate level.

‘Free’ USB sticks

Anyone attending a conference these days will probably receive a free USB memory stick containing the presentations and usually some form of advertising or marketing material provided by organisers and sponsors. Most of this is harmless, but there exists the possibility that the memory stick may also contain malware, and it is sound practice to run this through a virus scanner on a stand-alone computer before attempting to make further use of it.

It is well worth remembering the phrase ‘There is no such thing as a free lunch’.

A scam sometimes used by the hacking community is to load malware onto a USB memory stick – often a high capacity one – and leave it where their target will be likely to find it. Once plugged into the target’s computer, the malware will install itself without the user’s knowledge, and (if the attacker has done their job well) will then delete itself from the memory stick leaving no trace. The malware can then commence its task.

Key points:

- Always test a ‘free’ USB memory stick on a stand-alone computer before plugging it into any other.
- Never use a memory stick you find lying around – it may well be a trap.

Banking applications

Banks are increasingly trying to persuade us to use their online banking applications, both from fixed computers and from mobile phones and tablets. The reason is simple – it saves them money.

Fortunately, the applications they provide and their web interfaces have been thoroughly tested and appear very robust. Back in 2014 it was a very different story, with vulnerabilities found especially in the mobile applications. However, the last few years' improvements do not mean we should not be vigilant.

- Remember to keep your banking details secure.
- Log out of the banking application when you have finished your transactions.
- If using a public computer, clear the cookies, browser history and temporary internet files.
- Be aware of people 'shoulder surfing' who may be able to see what you are typing on the screen.

TECHNICAL SECURITY ADVICE

There are many activities covered by technical security, so I have tried to break these down into a few distinct areas.

Device locking

Physical locks are fine, provided that no one can access your device without the need to remove it.

- The device should be equipped with a password, and a password-protected screensaver should cut in at a suitable

interval once the device is unattended.

- Further protection can be provided by setting the device to delete its data after a number of incorrect password attempts, but this must take into consideration the need for all the data to be backed up.

Encryption

One relatively simple step to prevent unauthorised access to information on a computer or USB memory stick is to use encryption. There are two distinct methods of achieving this:

- File encryption – in cases where one or two files are of a confidential nature, it is easy to encrypt the individual files, and provide the encryption key securely to those who should have access.
- Drive encryption – in cases where there are multiple files that require protection, or where access to the computer's operating system or applications could constitute a significant threat, the entire drive can be encrypted. When the user switches on the machine, a boot-level password is required to be entered before the computer will even commence loading the operating system. However, drive encryption may only be active when the computer is fully powered down.

Operating systems and applications

Every computer has a specific operating system, whether it be Linux, Windows or MacOS, or indeed a proprietary operating system used by more specialised computer hardware. New or replacement operating systems should only ever be purchased or acquired

through a reputable supplier – normally Microsoft and Apple for their operating systems, and a variety of trusted suppliers for Linux.

Once installed, it is essential to ensure that these operating systems are kept up to date, and the suppliers will usually provide a free online updating system to allow this to happen – provided of course that the facility has been enabled.

The same is true for key applications – for example, computers that run Microsoft Office applications can receive updates at the same time as the Windows operating system updates, and Microsoft Office applications that run on MacOS can check automatically for updates.

Regular updates not only contain fixes for problems, but also from time to time introduce new features. In these cases, larger organisations should always test an updated operating system or application in a sterile environment before introducing it to the user community to ensure that it does not cause any conflict with existing corporate services.

Antivirus software should be installed – especially on Windows PCs, which are the most prone to virus attacks, but also on Apple Mac computers, which although considerably less susceptible are still at risk from malware. Some security specialists claim that antivirus software will only catch around 5 per cent of viruses, but it is always wise to have it installed, since failure to do so could still result in a successful attack. It is also essential to install regular antivirus updates – most antivirus software will do this automatically – and to perform regular scans of the computer in case a virus was already present on the machine before the antivirus software was brought completely up to date.

Key points:

- Ensure that operating systems and key applications are kept fully up to date.
- Enable automatic updates if at all possible.
- Keep antivirus threat databases updated. Even though this doesn’t guarantee 100 per cent protection, a good antivirus system will catch the main viruses.

User Account Control (UAC)

In recent years, Microsoft Windows introduced the concept of User Account Control or UAC. This facility prevents users with non-administrative privileges from installing software.

- If several people share the use of a single computer, make sure that all their user accounts are non-administrative, and retain just one master administrative account that is only ever used when required.
- Even if you are the only user of a computer, it is essential to allocate a non- administrative account and to use this instead of the master administrative account, since unauthorised access to this account will enable the user to take complete control of the computer.
- Similar constraints apply to Apple Mac computers, in which non-administrative users are automatically unable to install software. Additionally, the system can be set to prevent an administrative user from installing software that does not originate from the Mac App Store or from an accredited developer.

Firewalls

If the computer has a built-in firewall capability (for example in later versions of Windows), this should always be enabled, as it is usually quite reliable. There is no need to buy third-party firewall software or enable the firewall that comes with many antivirus products, since doing so can cause compatibility issues. The firewall can be configured (using an administrative user account) to prevent or allow access by certain applications, providing an additional layer of security.

For those people still using Windows 10, it offers built-in firewall software called Defender, although it requires enabling,[7] as does the Apple Mac firewall,[8] which, in the security settings, also allows the administrator to enable full disk encryption.

Antivirus software

Although it is claimed that most antivirus software only traps a small proportion of malware, this small proportion may be sufficient to cause damage or allow malware to infect the user's computer.

Install a reputable antivirus package, such as Norton, AVG or McAfee. Many of these are free. An antivirus option is built into Windows 10 and 11 Defender firewall software.

- Most antivirus packages offer features in addition to antivirus such as protection when surfing the internet, for example URL checking and storing user passwords.
- Enable automatic updating, which will ensure that the latest virus profiles are available.
- Enable the software to conduct regular scans of the computer, so ensuring that any malware that was present before a new virus was identified can be removed.

Java

Although it is an occasionally useful application, Java is known to suffer from a number of vulnerabilities, and unless it is essential that it is used on the computer it is best turned off, so cutting off another means of attack. It can always be turned back on temporarily or reinstalled if required.

Application software updates

Reputable software companies will always provide updates, not only when they have developed new features, but also when they have identified and fixed vulnerabilities in the software.

- If a known application, such as Microsoft Office or Adobe Acrobat, flags up that an update is available, it is always best to allow the update to take place, since popular applications such as these make easy targets.
- Better still, if the operating system permits automatic updates to take place, this is worth enabling, as it means that your applications are up to date without the need for you to decide.

Miscellaneous user activities

User-related activities are often the cause of many of the cyber security issues we face, including misuse – and occasionally abuse – of networks, systems and services. A certain amount of personal discipline is essential, and we shall cover training and awareness in greater detail in Chapter 10.

Keeping users on the straight and narrow is also a management responsibility, and this involves the monitoring of user behaviour and

occasionally some form of remedial (possibly disciplinary) action in order to resolve matters.

There are a number of general guidelines that both individual and company users can and should follow.

User passwords

Passwords are like toothbrushes – they should be changed regularly and never shared. Most people (myself included) struggle to keep track of passwords. Whenever you access a new service on the internet, shop for goods or register for information, you are obliged to select a username and password. There is a great deal of common sense in this – it helps the supplier to identify individual users; it (in theory at least) keeps your transactions separate from those of others; and it provides you as a user with a degree of confidence that the website you are using is relatively secure.

Unfortunately, this means that we have multiple usernames and passwords, and we have difficulty remembering them all, so we write them down somewhere, which is never a good idea since the piece of paper is likely either to be found by someone who should not know your passwords or to be lost forever in the recycling bin.

The great temptation is to use the same username and password for as many logins as possible, but this is the first step on a slippery slope, since if an attacker finds one instance of it, they will have the opportunity to use it elsewhere.

An attacker will often be able to guess your username, since many websites invite you to use your email address for this, so if you do find yourself in the unfortunate position of having multiple

passwords, there are a number of ways in which you can make your life simpler while retaining a measure of security.

As mentioned previously, the NCSC guidelines regarding passwords are worth considering.[9] Their recommendation is to use three random words, since these may be easier for people to remember, and will meet many password length requirements. However, the following should also be considered:

- Avoid all passwords that include all or part of your name, the names of family members (especially your mother's maiden name) and pets. These are usually extremely easy to guess or discover.
- Do not write passwords down where other people can find them. If you find complex passwords difficult to memorise, or if you have a large number of them, use a password management tool such as KeePass[10] for Microsoft Windows or mSecure[11] for MacOS. That way, you will only have to remember the one password to access that. There are many such tools available.

Screen locking

When moving away from your computer in a location where others could obtain access to it, it is always advisable to engage the screensaver, suitably protected by a password. On corporate user computers, this should be set to happen automatically after a pre-determined period of time.

- Configure a screensaver with password protection to cut in after no more than five minutes of inactivity.
- If possible, configure a shortcut to enable the screensaver – a single keystroke or mouse movement are both ideal.

- Never leave a computer unattended in a public place unless the password- protected screensaver has been enabled and the computer is physically secured.

Least privilege

When configuring new users of a system, always follow the rule of least privilege, meaning that they only have the level of access they actually require, as opposed to being made a system administrator. All too often when people buy a new computer, they set their own account as the system administrator. Instead, they should set up the computer using administrative privileges, and then create their own user account without them. Such accounts should only be used for normal day-to-day activities.

If that account's username and password are obtained by someone else, they can only then access a limited set of functions on the system itself, and not be able to make system changes.

As mentioned earlier in the book, organisations with systems administrators must ensure that they have two accounts, one with administrative privileges and one for day-to-day email and office work. It should be a security policy rule that no one should ever undertake day-to-day activities with an account that has elevated or administrative privileges.

Key points:

- Never configure a guest user on a computer to have administrative privileges.
- Always ensure that guest user accounts have password protection turned on.

- Always set up the main user of a computer with a non-administrative account.
- Use the administration account user for essential systems changes only.

Surfing the internet

There is so much information available on the internet that it's difficult to do anything these days without downloading photographs or documents. When visiting websites, and downloading from them, users should take care to ensure that they are reaching a legitimate website. There are proactive preventative steps the user or organisation can take by putting controls into place to reduce the likelihood of a successful attack, and also simple steps that users themselves can take to avoid risks when surfing the web. The latter were covered earlier in the chapter so we will focus on the proactive preventative steps here:

- Internet browsers are able to block pop-up windows that can contain malware or scripts linking to websites that contain malware. Microsoft Edge, Mozilla Firefox, Apple Safari and Google Chrome all have this capability using freely available add-in software, such as AdBlock.
- The 'protected' mode on browsers allows a high degree of anonymous web surfing. It isn't guaranteed to be 100 per cent effective but using it should hide your computer's identity from most prying eyes.
- Parental control can be set in both Microsoft Windows and Apple Mac operating systems to safeguard underage web surfers. In Windows, they are located within the Control Panel or system

settings application and in Mac they can be found under Preferences.

- Adware and spyware are aggravating intrusions that we experience when we surf the internet. Much of this can be disabled within the internet browser, by disabling pop-up windows for example. However, this will only solve part of the problem, so the use of ‘add-ins or extensions’ such as Adblock Plus[12] can block some adware and spyware, and there are commercial adware blockers available to download. Be cautious though – some of these ‘free’ applications can actually install adware and spyware instead of removing it.

Encryption of stored and shared information

Encryption is a method of maintaining confidentiality and integrity by scrambling information, usually referred to as ‘plain text’, so that it cannot be read or changed by unauthorised persons.

In order to encrypt information, a ‘key’ – invariably a very large number – is used in conjunction with software known as an encryption algorithm to change the plain text to ‘cipher text’. The cipher text can only be decrypted by using the correct key in conjunction with the same algorithm.

There are two different types of encryption used to ensure confidentiality:

- Symmetric encryption, in which the sender and recipient of information share an identical key. Symmetric encryption keys are more at risk of being discovered, since more than one person has access to them. For this reason, they must be

changed at intervals, for example daily, or even changed after every time they have been used.

- Asymmetric encryption, also known as public key encryption, in which both sender and recipient each have two keys, one of which is made public, and the other of which is kept private. The recipient's public key is used by the sender to encrypt the information, and the recipient's private key is used by them to decrypt the information.

Both symmetric and asymmetric encryption methods are normally used for the encryption of information being transmitted to others, which can be achieved by using an application such as Pretty Good Privacy (PGP),[13] which not only encrypts the information you wish to send but also allows digital signing of messages, providing an increased level of trust for the recipient. PGP can also be used to encrypt hard disk drives, but this application is less commonly used.

To ensure integrity, a one-way encryption method is adopted, in which a key is used in conjunction with a hashing algorithm that scrambles the plain text in such a way that it cannot be reversed.

Uses of this type of encryption include:

- Hard disk drive encryption in which either the entire hard disk drive or selected files are encrypted. Microsoft Windows (but not all versions) uses an application called BitLocker, while Apple MacOS contains an application called FileVault built into the operating system to achieve this. There are also a number of third-party and open-source drive encryption products such as PGPDisk and SecureDoc.

- The storage of passwords, where the user enters their password, which is then hashed, and the resulting hash value is compared with a previously stored value. Storage of information in the cloud also demands that the information should be encrypted, since this is invariably stored in locations over which users have no control.

Encryption as a technical policy was discussed earlier in the chapter.

MOBILE WORKING

It is always tempting to use ‘free’ Wi-Fi whenever we have the opportunity, but this brings its own set of threats, such as an attacker who intercepts the data being transmitted between the device and the access point, and if sufficient data can be captured, attempts to recover the encryption key in use (if indeed there is one) and uses the recovered key to gain access to the user’s information or the service to which the user has connected.

In the introduction to this book we heard about the company that provided free Wi-Fi in London’s Docklands, but potentially at a terrible cost. This example is extreme, but when we sign up for a free Wi-Fi service, we really have no idea what is happening to our data, since once it has passed through the wireless access point it is normally completely unencrypted.

Out and about

The recommendations for using free Wi-Fi, especially in unknown locations, include:

- Not using the service for anything that involves a financial transaction where your bank or credit card details are passed.
- Not using any service that does not have an encryption key. Most bars and restaurants who provide free Wi-Fi for example will always make use of an encryption key, since this prevents ‘drive-by’ users who are not spending money there.
- Avoiding those free Wi-Fi services that use an insecure key such as WEP or WPA. WPA2 (the next generation) is much more secure and resistant to key recovery. Ensure you select WPA2-Personal (or WPA2-PSK), or WPA3 if your system allows it, with Advanced Encryption Standard (AES) encryption as a minimum.
- For corporate network users, if a Wi-Fi hot spot must be used, then this should always be done by using a virtual private network (VPN) back to the corporate network. Additionally, corporate machines should always be configured to prevent a feature known as split tunnelling, so that when a VPN is in use all traffic is passed over that VPN.

Wi-Fi in the home and the workplace

Most home broadband services nowadays provide the user with a router that contains a wireless access point as well as Ethernet ports, and this is in many ways a much more convenient method of connecting, since we can move around the house without the need to cable up in every room.

There are some basic rules that should be observed when setting up wireless networks in the home and the office:

- Begin by changing the SSID name of the router. Preferably avoid calling it something that would identify your property.

- After setting up the router or wireless access points, change the administration username (if possible), and definitely change the administrator password. See the earlier discussion on user passwords for recommendations.
- Always enable WPA2-Personal, or WPA3 if your system allows it, with AES encryption as a minimum.
- Use a long and complex key, which prevents outsiders from making free use of your wireless network, since you never know what they'll be doing. The router supplier will probably print the default key on the side of the router, and you'll need to use this in order to set it up, but it's essential to change it afterwards.
- If the router supports remote administration, turn this off. If you ever need to use it, you can turn it on locally until you have done what you need to do.
- Again, if your router supports Universal Plug 'n' Play, turn it off, as it is a totally insecure protocol.
- Unless you need to use Wi-Fi Protected Setup (WPS) in order to connect to a wireless printer, you should consider turning this off, since it provides an additional vulnerability.

Bluetooth

The history of Bluetooth vulnerabilities is legendary. There is little that an individual can do to make their Bluetooth devices more secure. In some cases, there are no user settings apart from 'on' or 'off'. Here are a few suggestions that should reduce the likelihood of Bluetooth problems:

- Ensure that the Bluetooth device (for example, a smartphone) is password protected.

- Refuse all connection requests from devices you don’t recognise.
- If you lose a Bluetooth device (for example a headset), remove it from the list of paired devices so that it can no longer be used to connect to yours.
- Switch Bluetooth-enabled devices off when you’re not actually using them.

Location services

This feature applies to mobile devices that make use of GPS to track their location, for example when using a mapping application to plot a route between two points. Many smartphone and tablet applications turn on location services automatically when you install them, meaning that they can track your movements. This may be essential as in the example given above, but there is no justification why a smartphone game should require it at all.

- Think carefully about each application on your smartphone or tablet and make an informed choice about whether location services will enhance your experience, or whether you are simply giving away information to someone about where you are.
- Turn off location services in the general settings menu on all applications that you think should not be making use of them. If the application does require it, it will ask for them to be turned on, and it is your decision as to whether or not you do so. Frequently, you will have the option of turning location services on only when using the application.

1. See https://www.ncsc.gov.uk/guidance/10-steps-cyber-security
2. See https://www.ncsc.gov.uk/index/guidance
3. See https://www.sans.org/webcasts/sliding-scale-cyber-security-100517/
4. See https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf
5. See https://tools.ietf.org/html/rfc7435
6. See www.fast.org
7. See https://docs.microsoft.com/en-us/mem/intune/user-help/turn-on-defender-windows
8. See https://support.apple.com/en-gb/guide/mac-help/mh34041/mac
9. See https://www.ncsc.gov.uk/news/ncsc-lifts-lid-on-three-random-words-password-logic
10. See http://keepass.info/
11. See https://www.msecure.com/
12. See https://adblockplus.org/
13. See http://openpgp.org

9 ORGANISATIONAL SECURITY STEPS

In this chapter, we cover the security policies that organisations should take in order not only to protect their users from being attacked, but ultimately to protect the organisation itself. The chapter covers directive policies, which are aimed at informing users what they may or may not do; administrative policies, which detail how the organisation should prepare for and, if necessary, respond to cyber security incidents; communal policies including business continuity and disaster recovery; and finally, technical policies, which go into greater detail about technical issues.

While all of the personal, physical and technical controls described in Chapter 8 will be sufficient for individuals and small businesses, larger organisations will need to undertake more significant activities in order to maintain good security. However, before we examine these areas, there are two key points that organisations should consider in far greater detail:

- Understand your data – it is absolutely vital that organisations understand the nature of the information over which they have control. This will not only be their own data but may also be other people's or organisations' information for which they are deemed to be data processors in the sense of the data protection legislation, or which they are simply storing, as in the case of a cloud provider.
- Protect the data, not just the perimeter – many organisations concentrate on preventing unauthorised access from outside the network without realising that an equally dangerous threat comes from insiders. While it is essential to protect the organisation's network perimeter, it is vital to ensure that access to information from within is equally well protected, principally by the use of strictly enforced access permissions.

SECURITY POLICIES OVERVIEW

Organisations should produce and maintain an overall security policy, which will set the scene for other policies that may be required. In general, security policies need not be lengthy documents, since they do not require a great level of detail – this can be incorporated in lower-level documents such as processes, procedures and work instructions.

For ease of use and clarity, a security policy should generally contain no more than eight sections:

1. an overview, stating what aspect of the organisation's operations the policy is intended to address;
2. the actual purpose of the policy;

3. the scope of the policy – both what is within scope and what is not;
4. the policy statements themselves – usually the largest part of the policy document;
5. requirements for compliance – including, if appropriate, the penalties for failing to observe the policy, whether these are required by the organisation, the sector regulator, national legislation, national or international standards, or if they are simply good practice;
6. any related standards, policies and procedures;
7. definitions of terms used within the policy;
8. revision history, including who is responsible for the security policy itself.

The overall security policy would normally contain policy statements along the lines of:

- The organisation's information must be protected in line with all relevant legislation, sector regulations, business policies and international standards, in particular those relating to data protection, human rights and freedom of information.
- Each of the organisation's information assets will have a nominated information owner who will accept responsibility for defining the appropriate uses of that asset and ensuring that appropriate security measures are in place to protect it.
- The organisation's information will only be made available to those who have a legitimate business need.
- All the organisation's information will be classified according to an appropriate level of privacy and sensitivity.

- The integrity of the organisation’s information assets must be maintained at all times.
- Individuals who have been granted access to information have the responsibility to handle it in an appropriate manner and according to its classification.
- The organisation’s information must be protected against unauthorised access.
- Compliance with the organisation’s information security policies will be enforced.

Organisational security steps fall broadly into four areas:

- directive policies that state ‘you must’ or ‘you must not’;
- administrative policies, that is those that are underpinned by an administrative function, such as access control;
- communal policies in which large parts of the organisation must work together;
- technical policies that require specific hardware, software or both.

The following policies and operational controls are likely to be implemented both by SMEs and within medium to large organisations.

DIRECTIVE POLICIES

Directive policies are concerned with individual behaviours and tell individuals what they should do or should not do. As with all policies there should be some mention not only of the consequences of failing to adhere to them, but also of the penalties for failing to do so.

Acceptable use

Acceptable use policies are those to which all users of the organisation's network and services, whether temporary staff, contractors or permanent members of staff, should adhere.

Acceptable use will normally include such areas as personal access to the internet (browsing, shopping, etc.) and email. It may also cover use of organisational facilities when posting on blogs and social media.

Data and information retention

The organisation's data and information retention policy will link closely with its information classification policy and where appropriate must consider the requirements of data protection, human rights and freedom of information legislation, since this will impact on the amount of time for which personal information may be stored, for example, as required by Principle 5 of the Data Protection Act 2018.[1]

Information classification

An organisation is likely to possess many different types of information, including publicly available information; information that should be restricted to staff generally; and information that should be available only to very specific members of staff.

The information classification policy should define these levels, avoiding generic terms such as 'confidential' or 'restricted', since these can have different meanings, not only between the public and private sectors, but also between similar organisations.

For each type of information, the policy will dictate how and where the information is stored (and in some cases where it may not be stored); its retention period; how it is labelled; the extent to which it may be shared; how and where it must be backed up; how it is transported; and finally, how it is destroyed when no longer required.

Peer-to-peer (P2P) networking

One of the simplest methods for distributing malware is by concealing it inside files being shared on P2P networks. Unless it is a business imperative, organisations should enforce a policy forbidding the use of P2P networking, including P2P on company computers used at home and on individuals' personal computers used on the organisation's network.

ADMINISTRATIVE POLICIES

Administrative policies deal more with the steps that individuals or groups of individuals take in order to protect the wider organisation. These policies will determine the capabilities of all users within the organisation as opposed to the dos and don'ts of individual users.

Access control

This determines how applications and information are accessed, and can be achieved in a number of ways, including role based, time of day or date, level of privilege, and whether access is read only or read and write.

An access control policy can quite reasonably include the requirement for different methods of authentication, such as single

sign-on, digital certificates, biometrics and token-based authentication.

Change control

Uncontrolled changes are a frequent cause of problems in systems and services. The change control policy will describe the process for making changes to the systems and their supporting network, including the operating system and applications. This may involve detailed analysis of the proposals prior to any attempt at implementation and may also include functionality and load testing prior to roll out.

Hand in hand with the change control function is that of change management, which includes informing users of impending changes and having a back-out process that would be invoked should the change fail for any reason.

Termination of access

When employees leave the organisation, it is vital that their access permissions are terminated. If an employee transfers to a new department or to a new role within the existing department, then existing permissions should still be terminated (as opposed to being modified), and then reinstated at levels appropriate to the new role.

Viruses and malware

Viruses and other malware can infect systems without warning and must be dealt with in a formalised manner rather than an ad hoc approach that may do more harm than good. The policy will define who will address the problem and the procedure they will follow to identify, isolate if possible, and remove or quarantine the virus.

Passwords

Password management is a key aspect of information security policy, and one that is frequently overlooked.

Users are notoriously bad at password management. They will (when they can get away with it) use passwords they find easy to remember, such as their mother's maiden name, their birthday, or the name of their pet, all of which are relatively simple for an attacker to guess or discover. Users should be warned of the dangers of this practice and advised how to create strong passwords.

In the past, the general advice has always been to recommend a minimum password length; to use a complex combination of letters, numbers and other symbols; and to force the user to change their password at intervals.

The USA's National Institute of Standards and Technology has recently changed its view on passwords and has published a draft of a new standard – SP 800-63-3,[2] which deals with digital identity. The draft currently makes three recommendations of things that organisations should do, and four that they should avoid.

Things that organisations should do:

- Since users are only human, instead of placing the burden on the user, place the burden on the verifier. It is much easier to write one piece of software than it is to force hundreds or thousands of users to conform to a set of rules, and this is also less stressful on the users.
- Size matters – check for password length and require users to input a minimum number of characters.

- Check the passwords the users enter against a dictionary list of known poor or bad passwords and require the users to try again if the test proves positive.

Things that organisations should avoid:

- Complex rules for composition, such as a combination of upper- and lower-case letters, numbers and other keyboard symbols. These are almost impossible for users to remember (especially if they are required to have different passwords for each application) and may only result in users writing them down.
- Password hints can help the users remember their passwords, but they can also provide clues to an attacker. Since the originator of a targeted attack may well have undertaken considerable research into their target, such clues could easily betray the user's credentials.
- Credentials chosen from lists are similarly of dubious value. Such choices as mother's maiden name, town of birth, name of first school and so on are just as likely to be known to a serious attacker as the hints described above.
- Expiration of passwords after a finite period of time does little to improve password security, and only serves to complicate matters for the user. Users should have the option to change their password if they feel that it may have been compromised but forcing them to do it without good cause only adds to their burden.

As mentioned in Chapter 8, there is excellent advice from NCSC regarding passwords, which recommends the use of three random words.

The policy should also include a statement regarding the changing of default passwords, especially those that allow root access to systems and network devices such as firewalls and routers.

Occasionally, passwords are embedded within applications, especially in cases where one application must connect and exchange data with another without human intervention. The use of embedded passwords should be avoided wherever possible, since they may be widely known and therefore represent a potential avenue of attack, but if they must be used, they should be changed from the manufacturer's default.

No password is immune from a 'brute force' search in which an attacker's computer tries every combination of characters until it eventually finds the right one. Using long passwords will make this much more complicated, and the attacker may simply give up and move on to another, possibly easier, target.

Users also have a habit of using the same password on multiple systems. Attackers know this, and if they discover one of a user's passwords, it will normally allow them to access other systems as well. Users should have a different password for each system to which they require access.

If users must have multiple passwords and have difficulty in remembering them all, a password management tool may well be an appropriate solution as discussed in Chapter 8; alternatively, single sign-on is a method that can be used to alleviate multiple password issues.

Users should also be discouraged from reusing passwords, and where available, some access control systems, such as Microsoft's

Active Directory, can be configured to forbid reuse within a certain period of time.

Removable media

While many types of removable media are now redundant (e.g. floppy disks and DVDs), some removable media, including USB memory sticks and external disk drives, can be not only a source of malware if they have been infected on another system outside the organisation, but also a means of users removing information from the organisation without authority.

Although not obviously seen as such, there are many USB devices that can easily act as removable media and become a source of malware, including smartphones, tablet computers and even e-cigarettes.

System hardware can be easily configured to prevent the use of removable media unless the user has a very specific, authorised need.

Shared network resources

Shared network drives are an extremely useful resource, allowing staff to move large volume files around the organisation. However, they suffer from one serious failure and that is that there is usually no audit trail of who copied files onto the hard drive and who subsequently copied them off.

Additionally, some forms of malware such as worms can infect multiple shared drives within a network.

If files are to be shared between users within the organisation, or with users outside the organisation, then a collaborative system such as Microsoft SharePoint should be considered, since this allows the organisation to select who can make use of the system to share files, and retain an audit trail of who has done what and when.

Segregation of duties

It is all too easy for organisations to allocate people who understand IT to wide-ranging roles, and in some situations this is a mistake, since it can provide administration-level users with the capability to create and allocate high-level user accounts for people who do not or should not have them.

This can lead, for example, to a member of staff being able both to order goods and to authorise their purchase, which can lead to fraudulent activities. The correct method of addressing this is to ensure that a particular type of user account cannot carry out both functions – in other words, to completely segregate the duties and access permissions of two account types.

Backups and restoral

Organisations should always operate a policy that demands that information is backed up; including the backup intervals (which may differ for different information elements); the backup method (for example, full or incremental); the media upon which backups are stored; whether backup media is kept on the organisation's premises (but not in the same location as that of the data being backed up) or at a third-party location; the maximum time allowed for recovering the data, including transport from third-party sites; and how often backup media is tested for reliable restoral.

Most large organisations will have a backup policy, but as with all policies, this should be regularly reviewed to ensure that the correct systems are being backed up to some form of removable (encrypted) media, which is then stored off-site in a secure location. However, that is only half the story, since many organisations have discovered to their cost that after a period of time some backup tapes or disks cannot be read, and so it is essential to perform a test restoral of data at intervals as a sanity check.

As an alternative to conventional backups, some organisations rely on the use of cloud services to maintain a long-term store of data, and while this might be cost-effective solution, it does require careful planning and management, since it is often very easy to delete files stored in the cloud, which rather defeats the object of the exercise.

Another increasingly popular alternative is where the move to virtualisation has occurred and storage area networks (SANs) are becoming widely used, configured with a second SAN for backup. The SAN can be updated daily or by regular snapshots during the day. However, additional backups to other media would normally be recommended.

Antivirus software

Some organisations have begun to move away from antivirus software, having been put off by stories in the media about its lack of effectiveness, especially when new malware appears but has not yet been addressed by the antivirus software author. These are called ‘zero-day’ vulnerabilities, since once they become known, the author has no time at all in which to provide a fix.

However, even if antivirus software does not identify and trap every vulnerability, it will prevent existing known vulnerabilities from causing problems by neutralising or quarantining the offending virus, so it is still very much worthwhile maintaining an antivirus capability and ensuring that it is kept fully up to date.

Larger organisations are now moving away from dedicated antivirus software loaded on individual computers and are opting instead for Managed Detection and Response (MDR), in which a suitably qualified organisation takes over the responsibility for detecting and dealing with viruses across the organisation's entire network.

Software updates

Many of the key applications upon which organisations rely – for example, Microsoft Windows, Microsoft Edge and Microsoft Office, Adobe Acrobat Reader, Mozilla Firefox or Google Chrome – are all targets in which attackers find vulnerabilities. The authors of this software will invariably produce updates to fix known vulnerabilities at regular intervals, and it is essential that organisations keep these operating systems and applications fully up to date with the latest patches. Failure to do this can result in an attacker taking advantage of the gap between the vulnerability becoming known and the organisation applying the patch to fix it.

Where possible and practicable, automatic updating should be applied since this does not require further manual input from support staff and reduces the 'patch gap' to a minimum.

Additionally, any software update that will result in a major change to the operating system or applications should have a back-out plan so

that the organisation can revert quickly and easily to the original version if problems are subsequently identified.

Remote access/working from home/guest/third-party access

With the advent of the Coronavirus pandemic in 2020, many organisations discovered the urgent need to introduce teleworking or remote access in order to allow staff to connect with the organisation's information, systems and services while working from home, since the government's rules at the time made it either difficult or impractical for staff to travel to their normal place of work.

This brought about the need either to install a completely new remote access infrastructure for those organisations that had never previously worked in this way, or to increase the remote access capability for those organisations that previously had made use of it.

Whether or not an organisation makes use of VPNs for network access, it will be necessary to define how staff and third-party contractors are able to access the network and its systems. This policy will also link closely with other policies such as access control, security awareness and passwords.

Wireless/mobile devices

This type of policy will set out the organisation's requirements for implementing wireless access points around its premises; how the wireless infrastructure devices must be configured and secured, including the encryption method; whether the SSID is broadcast; and which bands and channels are to be used.

When considering devices that make use of Bluetooth for communications, it should only be enabled when it is actually

required and then turned off. Once initially configured for use, the organisation should ensure that the device's visibility is set to 'Hidden' so that it cannot be scanned by other Bluetooth devices. If device pairing is mandated, all devices must be configured to 'Unauthorised', which then requires authorisation for each connection request. Applications to connect that are unsigned or sent from unknown sources should be rejected.

For mobile devices supplied by the organisation, there will also need to be a section of the policy that regulates when and where these may be used over wireless networks that are not owned or provided by the organisation, for example public wireless or third-party networks.

This policy may well also include a definition of what information may be stored on the device; what applications may be loaded onto it; whether it may be used to gain access to the wider internet; and whether the user's personal information stored on the device is or becomes the intellectual property of the organisation.

Increasingly, many larger organisations, especially those that encourage BYOD and remote working practices, are moving to Mobile Data Management (MDM) and Mobile Application Management (MAM) services, in which a degree of control is exerted over the user's device so that it conforms to the organisation's security policies.

Bring your own device (BYOD)

This policy will overlap to a certain extent with the mobile device policy described above, but in this case, the device – such as a laptop computer, tablet computer or smartphone – will be the

personal property of the staff member as opposed to being owned by the organisation.

The policy may include statements regarding use by friends or members of the user's family and may also require separate login procedures for access to the organisation's network and, where necessary, hard disk drive encryption.

Peripherals

By default, many operating systems install auxiliary services that are not critical to the operation of the system, and which provide avenues of attack. When configuring users' computers, system administrators can disable and remove unnecessary services and peripherals such as USB ports and SD card slots, which, once they are removed, cannot be enabled, except by the system administrator, or used. This policy may form part of a more general procurement policy on the organisation's IT infrastructure.

Isolation of compromised systems

Organisations that have detected that a system has been compromised would be well advised to isolate it quickly from the network in order to prevent possible malware from spreading to other systems on the network. Once removed, it would be sensible to perform a forensic analysis on the system, using a specialist organisation if the relevant skills are not available internally, and finally to restore the systems to normal operation using trusted media.

Browser add-ins and extensions

Attacks on internet browsers, add-ins and extensions are becoming increasingly prevalent, and it is critical that attackers should not be able to use vulnerabilities in software such as Microsoft Edge, Adobe's Acrobat Reader or Adobe Flash to gain access to systems. Organisations should make use of the vendor's automatic update or software distribution facilities to install patches as soon as they become available.

AutoRun

AutoRun is a facility provided on Microsoft Windows that permits a command file on media such as a USB memory stick, CD or DVD to execute when it is inserted into the computer. This is an extremely simple way for an attacker to gain access to a system, since the user may be totally unaware that the media is infected and may not notice the program is running.

Turning off AutoRun will probably be a minor inconvenience both to users and to system administrators but is an excellent way of overcoming some attacks on AutoRun.

It is interesting to note that Apple's MacOS operating system does not support this kind of facility.

Adobe Acrobat Reader

Adobe's Portable Document Format (PDF) has become the de facto standard format for sharing information. Almost any file, presentation or document can be exported or converted into PDF format, and will look identical on any type of computer, smartphone or tablet that has Acrobat Reader software loaded. However, an increasing number of

cyber-attacks are being conducted by inserting malware into PDF documents, which are then transferred to the reader's device.

Organisations can protect their machines from such attacks hidden inside PDF files by downloading and actioning the advice from the NSA[3] in order to harden Acrobat Reader.

Outsourcing

Organisations may find it economically advantageous to outsource certain aspects of their operations. This is increasingly so in the case of the organisation's ICT infrastructure, and outsource service providers may offer to provide not only data storage, but also the operating system hardware and software and the application software required for the organisation's operations.

In some cases, this will be provided at a dedicated third-party site, as is frequently used in DR arrangements; or it may be provided in a more virtual environment such as cloud services. In either case, it will be vital that the organisation has a clear policy regarding the selection of suppliers for this type of service, which will form the basis of a service level agreement (SLA) and should also include an exit policy should the organisation decide to move away from a supplier, especially with regard to ownership of indexing of the organisation's information, and the subsequent destruction of any of the organisation's information remaining in the cloud.

The organisation to which the information or infrastructure is outsourced must understand that those members of its staff who are authorised to access this will be bound by the same rules, directives and laws as the outsourcing organisation itself. This also must be made clear in the SLA.

COMMUNAL POLICIES

Communal policies are those that may have an impact not only on individuals within the organisation, but also on the wider context of the business and the environment in which it exists.

Contingency planning

Contingency planning determines how data or access to systems is made available to users during the prescribed hours of operation. The policy will cover what measures are to be put in place to ensure that access is available in the event of failure of either the systems themselves or the means of accessing them such as a web server and the associated supporting network.

A contingency planning policy will often link directly to a business continuity or to a disaster recovery policy.

Incident response

The organisation’s incident response policy will detail how disruptive incidents are reported, investigated and resolved. In the event that certain predefined failure thresholds are exceeded, additional measures such as business continuity and disaster recovery plans may need to be invoked.

A disruptive incident may also require communication regarding the incident to be made available to staff, customers, third-party suppliers, the public at large and, if the organisation is part of a highly regulated sector (such as energy, finance or transport), the incident may also require notification to the sector regulator.

As with business continuity and disaster recovery plans, incident response plans should be reviewed at regular intervals or when any major aspect of the organisation's business changes, and also tested at regular intervals.

User awareness and training

Since many of the cyber security issues we experience are caused by users, making them aware of the risks they face – including the major threats, vulnerabilities and potential impacts – is a highly important step to achieving better cyber security.

Awareness is the first step and introduces users gradually to the things they need to know and understand, so that security becomes second nature to them, and they cease to foster bad security habits and move towards a position where they are fully committed to good security practice. This is then supplemented with training for those people who are more actively involved in day-to-day security operations, and who require specialist training courses in order to properly fulfil their role.

User awareness and training are covered in greater detail in Chapter 10.

TECHNICAL POLICIES

While the sections below refer to technical tools or controls, the implication is that for each there should be an equivalent policy which sets out the requirement. They may be necessary in order to allow other policies previously described to operate successfully, or they may stand on their own.

Spam email filtering

Spam email is the bane of most people's lives. It can range from the simply annoying to the positively alarming. Nowadays, most email service providers check email passing through their systems and filter out those that have been previously flagged as spam.

However, this may not remove all spam email, as new spam messages will always arise, and some filters may either never add them to their blacklist, or it may take time for the spam to be reported. Organisations can make use of their own spam filters such as SpamAssassin,[4] which will remove unwanted email from entering users' inboxes and junk mail folders.

Alternatively, organisations may outsource email scanning to a specialist organisation such as Message Labs. It is also vitally important to instruct users as part of the organisation's awareness programme how to identify spam and junk mail even if it originates from a supposedly known and normally trusted source.

Audit trails

These allow an organisation to follow a sequence of events in cases where security incidents have occurred and, where necessary, to be able to show that a user has or has not carried out a particular action. Such evidence might be required in cases where legal proceedings take place, in which case the audit trail must also be forensically robust.

Firewalls

Firewall policies will determine the way in which firewalls are deployed and configured to form an integral part of the network,

especially with regard to the rules that must be applied and subsequently maintained.

Firewalls should be used to block all incoming connections, from the internet to services that the organisation does not wish to be available. By default, all incoming connections should be denied, and only allowed for those services that the organisation explicitly wishes to offer to the outside world.

Good practice also calls for the IP address of the incoming session to be a valid public IP address and not an IP address associated with the business itself. For example, if the business has a block of 32 public IP addresses these must be filtered out.

In addition to firewalls, it may be advantageous to partition the organisation’s network into separate areas by splitting them according to their function, such as research and development, operations and finance, making it more difficult for an attacker to reach a particular service (see the later item on VPNs). Each area will become an independent security domain with firewall-controlled access between them.

It is also common practice for organisations to create another barrier between the external and internal networks by introducing a demilitarised zone, or DMZ.

Good practice also requires that any outgoing connection from the organisation to the internet originates from a specific proxy server or service located on a DMZ and not from within the main network.

Firewalls come in various shapes and sizes. Many require specialised hardware on which to operate, and well-trained staff to

configure and maintain them. The decision on which type of firewall to use and how it should be configured is best left to specialist advice, since it must not only provide protection for the business against unwanted intrusion, but also meet the business needs as regards what can and cannot be transmitted through it.

Other firewalls come built into desktop operating systems – these are much simpler and require little, if any, configuration. On user computers these should always be enabled, and the user's access should prevent them from changing this: a non-administrative account should be provided to them.

Encryption

The information encryption policy will go hand in hand with the information classification policy, in that it will define, for certain levels of information classification (for example, secret or top secret), how sensitive information will be encrypted and how the encryption keys will be managed and exchanged.

For example, information classified at a certain level could be exchanged between two people using a straightforward encryption mechanism such as PGP, with each owning their own encryption keys, while other information might require the use of a full-blown public key management system, with encryption keys centrally managed and distributed.

The policy should additionally make the distinction between information in transit (for example, within emails) and information at rest – that is, stored on hard drives or other media, especially if stored in the cloud.

For information at rest, encrypting the hard drive of a mobile user's computer is relatively straightforward, and means that the device cannot be used without the user's password to decrypt the data, making the information useless to anyone who steals it.

On Apple Mac computers, turning on the free built-in FileVault software[5] will encrypt the entire hard drive, while for Windows users there are two options. The first, for Professional or Enterprise versions of Windows, is to enable the inbuilt BitLocker software.[6] The second, for other versions of Windows, is to download and install the free VeraCrypt encryption software.[7]

Business data stored in the cloud should always be encrypted, since it is always uncertain in which country or countries the cloud storage is actually located, and those countries' jurisdictions may not place a high level of protection on data, even to the extent of intercepting and analysing it themselves.

Sensitive information that is being moved to another location – whether by some form of media like a memory stick or by email – should always be encrypted, so that, again, anyone who is able to intercept the transmission or steal the media will be unable to access the information.

The key length used by enterprise organisations in symmetric AES is typically 256 bits in length, whereas the keys used in asymmetric or public key cryptography are typically 2048 bits in length and are used in the initial setup of an encrypted session that determines the actual fixed encryption key that will be used by the symmetric algorithm during the session. These keys are not typically used for the main encryption work because they require too much computation resource.

Secure Socket Shell (SSH) and Transport Layer Security (TLS) keys

SSH is a network protocol that provides administrators with a secure method of access to remote systems. It provides a means of strong authentication and encrypted communication between two systems over an insecure network, especially the internet. It is widely used by network administrators for the remote management of systems and applications, enabling them to log on to another system, execute commands and move files between systems.

The TLS protocol provides both confidentiality and integrity between two communicating applications exchanging information such as that between a user's web browser and an internet banking or e-commerce application. TLS is also used in VPN connections, instant messaging services and Voice over Internet Protocol (VoIP) applications.

Both SSH and TLS make use of encryption keys (as described above) to secure the transfers; they are typically 256 bits in length.

Abuse of SSH and TLS keys is not uncommon. In order to reduce the likelihood of insiders taking advantage of these when they leave the organisation, which renders critical network infrastructure open to malicious access, it is recommended that organisations rotate SSH and TLS keys at intervals.

Digital certificates

Digital certificates are widely used to provide authentication of websites, particularly when conducting financial transactions. Digital certificates can be purchased from accredited certification authorities

(CAs) both for personal use and by organisations. However, it is important to remember to renew the certificate (normally annually), since failure to do so renders the certificate useless, and users whose web browser detects this will receive a notification that the certificate has expired. This may result in their deciding not to or being unable to continue with the online transaction.

Email attachments

As an integral part of their awareness training, employees should be instructed that they should not open email attachments unless they are expecting them. Additionally, users should be forbidden to execute software that has been downloaded from the internet unless it has been scanned for viruses and tested for security vulnerabilities. Users who visit a compromised website can unintentionally introduce malware.

Organisations should configure email servers to block or remove emails that contain those file attachments that are commonly used to spread malware, such as .vbs, .bat, .exe, .pif, .zip and .scr files.

Network security

Network security policies are very wide-ranging, considering how the organisation’s networks can be secured against intrusion using a combination of firewalls, intrusion detection software, antivirus software, operating system and application patching, and password protection.

These should include fixed and wireless local area networks (LANs and WLANs), VPNs, wide area networks (WANs) and SANs.

Virtual private networks (VPNs)

The use of virtual private networks is commonplace, especially in larger organisations, and a policy will be required that sets out how and where these are deployed; who may make use of them (for example, for remote access by staff, guests and third-party contractors); and how they are configured and secured.

The use of VPNs should be part of the organisation's strategy that includes network segregation and firewall deployment.

Physical access

This will define how access to the physical areas of the organisation is controlled and may include perimeter fencing and gates with movement detection and/or CCTV systems, electronically controlled gates, and physical security guards.

Within the organisation's sites, physical access control will normally be governed by electronic door access systems, whether by PIN, wireless proximity card or a combination of both. The supporting system will dictate the levels and locations of access available to individual members of staff, visitors and contractors.

Internally, infrared movement detection and CCTV systems are also frequently used, especially in highly sensitive areas.

Intrusion detection systems (IDSs)

As with many security tools, intrusion detection systems are just one weapon in the security manager's armoury. As the name suggests, their purpose is to try to identify when unauthorised intrusion to a network or computer system is being attempted, and they are available in a variety of forms:

- Host intrusion detection systems (HIDS) are installed on individual computer systems and monitor that system's configuration only. If a HIDS perceives an abnormal change in a system configuration, it will send an alert message to a console for a security operator to examine.
- Network intrusion detection systems (NIDSs) are installed on internal networks and subnetworks in order to detect abnormal network traffic such as attacks on firewalls. They will also report to a console if they detect an attack, but additionally can take some form of action, such as to change firewall rules.
- Under certain circumstances it may be necessary to undertake such work using forensic techniques and to retain hard drives and data for possible use in legal proceedings.

---

1. See https://www.legislation.gov.uk/ukpga/2018/12/contents
2. See https://pages.nist.gov/800-63-3/
3. See https://www.scribd.com/document/280616716/Recommendations-for-Configuring-Adobe-Acrobat-Reader-XI-in-a-Windows-Environment
4. See https://spamassassin.apache.org/
5. See https://support.apple.com/en-gb/HT204837
6. See https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview
7. See https://sourceforge.net/projects/veracrypt/

10 AWARENESS AND TRAINING

In this chapter, we cover steps that an organisation can take to ensure that users are better prepared to make use of cyberspace, and to understand not only the issues they may encounter in doing so, but also their responsibilities to the organisation itself.

For the most part, one of the greatest security liabilities in any organisation is the user. They may not act deliberately, but often they will unintentionally perform acts of cyber vandalism that will cause untold problems for the IT and security support staff. Their actions (or inactions) may be that they behave inappropriately and release information or allow information to be released, but this may often be due to the fact that they have not been properly trained by the organisation to react appropriately to information security events.

Some – but not all – of this can be corrected by educating and training the users in good security practice, making them aware of the risks that they will face when using both their own and the organisation’s systems.

The ‘not all’ referred to above covers two different aspects of human behaviour – first, when the user simply forgets or ignores their training, and second, when they are carrying out some act in a very deliberate manner, either to cause loss of the organisation’s information (selling it to a competitor for example) or to cause damage or loss as an act of revenge.

However, making users aware of the threats, vulnerabilities and impacts that they may face is an essential precursor to training.

There is little that the organisation can do to ensure that users never make a mistake, although as a means of reducing the likelihood, one organisation in which the author worked levied a small financial fine on staff who left their computer unattended or left sensitive documents on their desk.

Preventing or reducing the likelihood of information theft or damage to systems and information can be achieved to a certain extent by implementing very strict access control mechanisms and introducing monitoring software that looks for anomalies in user behaviour and flags up an early warning if something out of character is detected. Banks and credit card companies adopt a similar approach as a means of early detection of fraud and will often contact a customer immediately if they appear to be making purchases that do not match previous spending patterns.

Although it may appear obvious, it is worth stating that awareness and training are two different but inter-related concepts. Awareness provides users with the information they need in order to avoid making mistakes, while training equips them with the skills they require to deal effectively with challenging situations when they arise.

This chapter focuses mainly on changing people's behaviour, so that instances of people-related cyber-attacks can be reduced.

AWARENESS

Awareness of cyber security issues permits both individuals and an organisation's users to act as a first – or indeed a last – line of defence in combating cyber-attacks. It is never a one-off activity and should be considered to be an integral part of personal development, while remaining a rather less formal activity than training.

An awareness programme allows people to understand the threats they face whenever they use a computer; the techniques used by social engineers to achieve their goals; the vulnerabilities faced by them or by their organisation; and finally the potential impacts of their actions or inactions.

This doesn't imply that it is necessary to turn everybody into cyber security experts, but that a basic level of understanding is required, similar to that in driving a car – we need to know how to operate the vehicle, the rules of the road and the dangers we face, but we do not need to understand how the engine management system works. At a fundamental level, you should always lock your computer screen when leaving it unattended, remove any printed material that is in any way sensitive, and lock your desk.

As with any process, there are a number of discrete steps in an awareness programme:

- Plan and design the programme:
  - select the most appropriate topics for awareness, such as email etiquette, correct handling of information assets or

password security;
    - make a business case to justify any expenditure;
    - develop a means of communicating with the users.
- Deliver and manage the programme:
    - develop the materials and content;
    - implement the awareness campaign.
- Evaluate and modify the programme as necessary:
    - evaluate the campaign’s effectiveness;
    - improve and update the material with new information.

Like many other aspects of working life, awareness is a journey, not a destination, since new people will join the organisation and need to be included in the programme, and new threats and vulnerabilities will arise.

The campaign should also focus on continuous reinforcement though such things as poster campaigns and pop-ups when people access the internet or log on.

The general trend of user engagement in the programme should be along the lines of:

- initial contact with the user community – letting them know that something will be happening in which they will need to become involved and providing a general idea of what the programme will be all about, so that their expectations can be managed;
- further understanding of the programme, so that they appreciate what the implications will be for them;
- timely engagement, so that they begin to understand that there is a new way of working;

- acceptance by users, in which the user community begin to work in the new way;
- full commitment to new ways of working, so that they do not revert to their old ways;
- evangelism, in which they encourage others to follow their example.

Ways of overcoming obstacles to awareness programmes

It is easy to assume that once an awareness programme is underway all will go to plan, and organisations will only need to react and respond to problems when they arise. However, if forewarned about some of the possible issues, organisations should have a contingency plan in place so that faster reaction is possible.

Some of the issues that organisations may face include:

- **Initial lack of understanding.** When the awareness programme is initiated, it is vital that the communication that goes out to the relevant audience explains not just what the organisation expects to achieve, but also why it is undertaking the work. This will greatly aid acceptance of the programme.
- **The introduction of new technology which complicates a programme that is already underway.** Such changes in the IT infrastructure in an organisation can either enhance the ability to deliver the message or can complicate it; but as long as people from that part of the organisation are involved in the awareness programme, the team should be aware of the possibility before it arises and be able to include it in their programme or work around the problem.

- **One size never fits all.** Every organisation is different, and there are no standard methods of operating an awareness programme, and even within one organisation the different types of audience may have different requirements. Also, there will be a considerable difference in both the size and the scope of an awareness programme between one for a large organisation and one for an SME.
- **Trying to deliver too much information.** Many users in an organisation will be non-technical, and so the focus of the programme must consider that the more technical aspects of cyber security could overwhelm them. It is essential to keep the focus on what the audience needs to know and not try to extend the delivery of information to be too technical. Less is more.
- **Ongoing management of the programme can become a challenge.** If this becomes the case then the probability exists that the programme will flounder due to lack of support from those areas of the organisation that are involved in its delivery, and therefore senior management commitment must be assured.
- **Follow-up failure.** This can and will cause problems for the programme, since it is vital that the team understand how well the message has been received, understood and acted upon by the target audience. Regular monitoring and reviews are essential to delivering a quality programme.
- **Inappropriate targeting of the subject matter.** This can have a negative effect on the programme, since groups within the organisation may be receiving some awareness information that has little or no impact on their role, while others are not receiving information that would be essential to their daily activities.

- **Ingrained behaviours.** These are a constant challenge in this kind of programme. Some people will always challenge the programme, saying, ‘We’ve always done it this way and it has always worked, so why should we change?’ Any organisation running an awareness programme must expect this kind of response and must develop sound arguments against it.
- **Some people will take the view that security is the responsibility of the IT department.** It is essential that they are disabused of this notion at an early stage and throughout the ongoing campaign. Cyber security is everybody’s problem and is not restricted to one department.

Programme planning and design

The process commences with the establishment of a small team who will develop and run the programme. Some of them will naturally have a degree of expertise in information security, while others may represent those parts of the organisation that might suffer serious impacts in the event of a cyber-attack. It may also be beneficial to involve the internal audit function, who may be able to offer constructive advice, since a programme such as this may well be audited at a later stage, and from personal experience I can attest that it’s always good to have audit on your side.

The team’s initial task will be to define the exact goals and objectives of the programme, and this will include whether the target audience is to be the whole organisation or just a small part as a pilot project. This latter option may be a much more beneficial approach, since it should be able to achieve its objectives on a small and therefore less costly scale before the programme is widened to include everyone.

In the initial part of the programme, the target audience might also be limited to one particular type of user, such as:

- **employees working full-time in the organisation's premises.** These are frequently the kind of users who will benefit the most from receiving cyber security awareness training;
- **home-based users,** who will have similar but slightly more complex needs. Due to the different requirements for connecting into the organisation's network, these users may require a slightly higher level of understanding of the issues at stake;
- **third-party users,** such as contractors, outsourced staff and suppliers who require connections into the organisation's networks in order to undertake their work;
- **system administrators and IT support staff,** who will already have at least a general appreciation of the issues;
- **management-level users,** who may be responsible for in-house employees or home-based users, and who need to understand how cyber security issues will affect their departments;
- **senior executive users,** who will be responsible for making many of the business decisions that could well be targets for a cyber-attack.

Alternatively, the organisation may decide to target a cross section of users from different groups so that the overall organisational benefits can be seen, rather than solely those for a particular community.

Some topics will have greater relevance to particular target groups, such as the issues of social engineering, which may possibly be more relevant to staff who have regular contact with customers and suppliers than to those who do not. This does not imply that those

who do not have as much external contact should not be included in that aspect of awareness, but that they might gain less from it.

Next in the development of the programme, the team must clearly identify the topics that will be covered. It is pointless trying to cover all aspects of cyber awareness, since this will simply overwhelm the audience; instead, the programme should focus initially on a very tightly defined subset such as usernames and passwords, spam email or social engineering. The campaign can be widened at a later stage once the results of the earlier work have been examined and the techniques used have been refined where appropriate.

The methods of communicating the message to the user community will vary considerably, and may well consist of some or all of the following:

- posters, which can be placed where staff can easily engage with the message, such as meeting rooms and other shared areas. Some posters might have a humorous focus in order to lighten the message, while others could be somewhat darker;
- newsletters, which can be delivered by desk-drop in office buildings, or by email for offices and home workers alike;
- giveaway items such as coasters, coffee mugs, key fobs and mouse mats, which continue to reinforce the general message for as long as they are used;
- screensavers, which might display a variety of messages, and which could be changed either at regular intervals or when a new message must be given out;
- intranet websites that provide helpful advice, examples of good and bad cyber security behaviour and links to additional informative material and training;

- fact sheets and leaflets, which may be particularly relevant to a group within the organisation, to the whole organisation or to its business sector;
- presentations at team meetings, in which a guest speaker talks for a few minutes on a hot topic and takes questions about the whole awareness programme, keeping the presentation ‘short and sweet’;
- computer-based training (CBT), which delivers a more detailed level of knowledge, and may be a mandatory requirement for the certain users’ work. This might include data protection legislation, for example.

Once this part of the work is complete, the team may well have to approach the senior management team or board of directors to obtain funding approval, since it is unrealistic to expect that the work can be undertaken at no cost.

As with all business cases, the approach should focus on the likely impacts that will occur if the work does not proceed, as well as the benefits that will accrue when it does. This is another reason for keeping the initial part of the campaign to a reduced volume of information, since the costs will be lower, and the board should find it easier to give approval. Success at this early stage will then make it much easier to obtain board approval for further expenditure when the campaign moves on to cover more aspects of cyber security awareness.

The costs can be more easily identified if they are broken down into manageable areas, for example:

- **the hourly costs of staff** who are engaged in delivering the awareness campaign as well as those who will be on the receiving end;
- **development costs,** including development and maintenance of any intranet websites or the production of materials such as posters and newsletters;
- **promotional costs,** such as giveaway items including branded pens, coffee mugs, key fobs, mouse mats and the like;
- **training costs,** where external trainers are brought in to deliver all or part of the awareness campaign.

Some of these will be one-off costs, while others will be recurring, and the board will expect that these will be clearly identified.

It should also be possible to attempt to quantify the potential impacts, since the directors of organisations will need to be certain that the programme will deliver value for money and will wish to understand the consequences of not undertaking the exercise.

Potential impacts can include not only the direct financial losses anticipated if a particular incident occurs, such as the loss of sales revenue and the expenditure that would be incurred in responding to and recovering from the incident, but also the indirect losses such as share value, brand and the organisation's reputation, although these can be rather more subjective in nature, but still require consideration.

Delivery and management of the programme

Although we have called this an awareness campaign, it actually goes further than this, because awareness is only the first stage in

which the target audience is made aware of what they should know and when they are likely to need the information. This may be delivered in a variety of ways, for example by printed material, email, electronic newsletters and intranet portals for those organisations having more sophisticated resources.

The campaign then moves up a level so that the target audience gains an understanding of why they need to be involved and how best they can participate. This may include raising awareness topics at team meetings and delivering specific presentations on the subject matter.

Evaluation and modification of the programme

Finally, the campaign is ready to see results from the earlier work and to evaluate its effectiveness, and as the campaign develops and widens its scope, the organisation will expect to see the benefits in reduced instances of successful cyber-attacks and fewer negative impacts on the organisation’s information and systems.

The team must ensure that the entire exercise has been carefully documented, and that they can demonstrate the resulting benefits at the end of the pilot project so that more of the organisation and additional areas of cyber security awareness can be addressed.

Once presented back to the board, success should breed success, and the team should be better placed to move on to raising awareness for the wider organisation or in more topic areas. The board presentation should focus on both the financial and non-financial benefits, and the value to the business itself and also to its external stakeholders, including suppliers and customers and the sector regulator if applicable. It should be completely honest about

both the overall costs and the potential impacts of not progressing with a full rollout.

Once the board have given their commitment for this, the pilot user group should be given acknowledgement for their involvement, as this will not only reinforce the importance of the programme but will encourage others to become actively involved.

TRAINING

As mentioned earlier in this chapter, awareness and training are two entirely different, but interconnected, concepts. While awareness places cyber security issues firmly in the minds of the user community in an organisation, training will deliver very specific and often highly targeted information to those individuals or groups who have a specific requirement for it.

Training, and especially highly technical training, can be costly, but as with awareness it has a direct payback in terms of reducing the number of incidents and the potential financial impact on the organisation.

Cyber security training falls into two distinct categories:

- Generic training, in which the underlying concepts of cyber security are explained, and which give a sound appreciation of the issues. This may be required by those managers who are responsible for specialist security design and operational staff.
- Specialised cyber security training, in which very specific skills are taught to a limited audience such as those security staff who manage the organisation’s security infrastructure.

Appendix D lists a number of sources of cyber security training and suggests appropriate topics.

A few final points to consider

In the case of product or technology-specific training, it should be considered that technology changes at an alarming rate, and the need for updated courses will undoubtedly become necessary as time progresses. The requirement for ongoing budget allocations for this should be factored into the cost estimates when preparing business cases.

One method of reducing training costs is by identifying those staff who already possess training skills, and who can pass on their knowledge to others. This ‘train the trainer’ approach can work well when budgets are limited, although it may not be the best solution if the people who are intending to deliver the training are inexperienced in how to train others.

The business cases for both generic and specialised cyber security training will need to be developed and presented on a case-by-case basis and should be presented in a similar manner to those for the awareness programme. However, instead of being focused solely on benefits to the organisation as a whole by targeting all users within the organisation, these business cases should also focus on benefits to the organisation by addressing the specific training needs of individual specialists and the general areas in which they will benefit the organisation.

11 INFORMATION SHARING

In this chapter, we will take a look at one of the methods of reducing our cyber security risks – sharing information about threats and vulnerabilities.

It's worth bearing in mind that knowledge of vulnerabilities may lead an attacker to be able to mount a successful attack, but it's only by careful sharing of information that security can be improved. This dichotomy can lead to tensions in the cyber security world, and the occasional holding back of information regarding some vulnerabilities.

The organisations described throughout this chapter all have excellent websites, so rather than repeating their content, a brief description of their activities has been provided with links to the appropriate web pages.

The most important aspects of information sharing are:

- **The whole concept of information sharing is based on trust.**[1] This can exist at a personal level, with one individual

trusting another, or can be between groups of people within organisations who share a common interest in the subject.

- **Information to be shared requires some form of information classification system or mechanism.** Many information sharing initiatives now make use of the Traffic Light Protocol (TLP)[2] for classifying how information that is to be shared must be handled.
- **The information must be accurate.** It is pointless sharing information that has not been verified since it can consume time and resources unnecessarily.
- **Advice to others must be timely.** There is no value in keeping information back from those who would make good use of it, since an attacker may also become aware of it and take advantage of the time lag to initiate a successful attack.
- **Sharing must be done with care.** The circle of interested parties with whom the information is shared must be trusted to handle it in an agreed manner, and not to allow it to fall into the wrong hands. There should be mechanisms built into the process to prevent onward distribution to people or organisations outside the sharing group.
- **It should be possible to anonymise the source of the information.** On occasions, revealing the identity of the organisation that raised the issue could prove detrimental, and a means of passing on the information without attribution is essential.
- **It should be possible to share information with other commercial or critical infrastructure sectors.** Frequently in cyber security, there are issues that will affect many, if not all, commercial or critical infrastructure sectors, and a means of

passing information between them in a controlled manner is essential.

TRUST

Trust between members of an information sharing community is an absolute pre-requisite. But what do we mean by ‘trust’? The Oxford dictionary definition is that trust is ‘the firm belief in the reliability, truth or ability of someone or something’. In the context of cyber security, the implication of this is that we must trust not only the information we receive, but that in order to do so we must first and foremost trust the source of the information, whether this be an individual or an organisation, and also the person(s) or organisation(s) with whom we subsequently share it.

Where information is shared on a face-to-face basis, it is often conducted under the Chatham House Rule,[3] named after the Royal Institute of International Affairs at Chatham House in London, which states:

> When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

A note adds:

> The world-famous Chatham House Rule may be invoked at meetings to encourage discretionary openness and the sharing of information.

As far as the classification of information to be shared is concerned, trust works on two levels. First, the originator must ensure that the information has been correctly classified and must be confident that the recipients will handle the information in line with that

classification. Second, recipients must have sufficient trust in the integrity of the originator so that they can have the same level of confidence in the accuracy and reliability of the information.

One final aspect of trust is the ability to have an independent party, trusted by all members of an information sharing community, who can act as a moderator, and can also perform the role of go-between in certain situations, as we shall see later. This individual is sometimes known as the Trust Master.

INFORMATION CLASSIFICATION

If it is in any way sensitive, information to be shared should be classified according to its level of sensitivity, and whatever method is used, it must be possible for it to be understood by both public and private sectors without the need to cross-reference their information classification schemes.

In the UK government, there is the Government Security Classifications.[4]

In the EU, there is a very similar scheme.[5]

A similar (but somewhat older) scheme also exists in the USA.[6]

As mentioned previously, the Traffic Light Protocol is used by many information sharing initiatives and classifies information as one of four colours:

- RED – Personal, for named recipients only – in the context of a face-to-face meeting, for example, distribution of RED information is limited to those present at the meeting, and in most circumstances will be passed verbally or in person.

- AMBER – Limited distribution – recipients may share AMBER information with others within their organisation, but only on a ‘need-to-know’ basis. The originator may be expected to specify the intended limits of that sharing.
- GREEN – Community-wide – information in this category can be circulated widely within a particular community or organisation. However, the information may not be published or posted on the internet, nor released outside the community.
- WHITE – Unlimited – subject to standard copyright rules, WHITE information may be distributed freely and without restriction.

This method of information classification is widely used in information sharing communities around the world since it is very simple to understand and implement, and additionally can be readily understood in other sectors or countries.

Most of the time, the originator of the information to be shared will determine its classification colour, but on occasion Trust Masters may decide to raise it if they feel that it is set too low.

PROTECTION OF SHARED INFORMATION

When information is being shared, the originator may consider it necessary to restrict its onward distribution, or to ensure that the information can be revoked or deleted in situations where it is no longer valid, or upgraded or downgraded when its level of sensitivity has changed.

This can be achieved by the use of a technique sometimes known as ‘information rights management’, which works by encrypting the information – for example, a text document – and allowing it to be

opened by the recipients provided they can properly authenticate themselves to the central sharing resource.

Further, the document can be provided with additional protection choices so that it, or parts of it, can never be copied – which prevents it being pasted into an unprotected document – or printed, preventing its onward distribution in physical or scanned form.

If the document is able to be forwarded to another recipient, it will be necessary for them in turn to have access rights on the central sharing resource, and if the originator decides to remove the original document, any remaining copies will not be able to be opened since the original document's metadata that enables decryption will also be deleted.

As with information classification, originators must ensure that the information has been appropriately protected, and again, recipients must have sufficient trust in the integrity of the originator so that they can have the same level of confidence in the accuracy and reliability of the information.

It makes good business sense in organisations that have a requirement for very strict confidentiality to run all incoming or outgoing emails through a scanning system that is able to detect and isolate any message containing particular words or phrases, or which can direct encrypted messages to a central verification point prior to their release.

ANONYMISATION OF SHARED INFORMATION

Situations will inevitably arise when a participating organisation does not wish to be identified as having been the victim of an attack

(possibly even more so for a successful attack) or another cyber security situation in which they have become embroiled. The reasons for this are generally connected with commercial interests, and organisations may be reluctant for a competitor who is part of the same information sharing community to know who the incident affected, since this might place that organisation at a competitive disadvantage or have a negative effect on their share price or public reputation. At the same time, however, they might still wish details of the exploit to be made available to the wider community.

In face-to-face situations, such an organisation might well approach the Trust Master and request that they raise the matter without identifying the originator. The Trust Master will take great pains to ensure that this request for anonymity is respected, ensuring that even having omitted the originator's identity the information passed on contains no clues or additional metadata that might reveal, infer, suggest or identify the originator in any way.

In the context of a centralised information sharing system, the Trust Master's role must be performed by the system itself in conjunction with the originator of the information being shared. There are two general courses of action:

- The originator can select an 'anonymise' option on the system's preferences when setting up the specific information to be shared. This will remove any reference as to who originally submitted the information. However, should the information include other documents, for example word-processed documents, spreadsheets or presentations, the originator will be responsible for completely anonymising these.

- The originator can select an ‘anonymise via the Trust Master’ option instead. In this situation, the originator openly sends the information to the Trust Master, who then submits it to the community as if it had come from the Trust Master alone.

Here, the application of trust works slightly differently. Originators must again ensure that nothing in the information being shared can reveal their identity, nor could their identity be inferred from the content detail. They must also have trust in both the information sharing system and the Trust Master that their identity will not be revealed. No additional trust is required here by the recipient.

Organisations, or groups of communities, who wish to provide their own centralised systems for information sharing may later wish to interconnect these so that they can widen the scope of their operations, since some cyber security situational submissions will inevitably be of significant interest to other sectors and sharing information with them would be highly beneficial, if not essential, and this can often avoid possible duplication of effort.

> In order to supplement the ISO/IEC 27001 standard, the ISO produced an additional standard, ISO/IEC 27010:2015, that covers the secure exchange of information between centralised systems.[7]

Contact – and therefore trust – may already have been established between these different groups, communities or sectors, in which case information might be freely shared between them, following the same rules as those for sharing within a sector.

Alternatively, if no previous contact has been established and therefore no degree of trust exists, the Trust Masters in those sectors wishing to share information can act as intermediaries and initiate a limited degree of information sharing – possibly one-way only in the first instance – and subsequently encourage bilateral information sharing as an increasing level of trust develops.

Finally, once trust is fully established between the sectors, the Trust Masters may set preferences in the information sharing system that allow individual sector users to share information – either on a one-to-one basis with a peer in another sector, or more widely to a whole sector.

Originators of information should have the same degree of trust in users within a different sector as they do for users within their own sector. The information should be classified, protected and anonymised in exactly the same way.

From the recipient's point of view, the only thing that matters is that they have trust in the originators of the information and therefore in the information itself.

ROUTES TO INFORMATION SHARING

There are four major routes to sharing information regarding cyber security issues, each of which has its own unique characteristics:

- warning, advice and reporting points;[8]
- the Cyber Security Information Sharing Partnership;
- computer emergency response teams and computer security incident response teams;

- security information exchanges and information sharing and analysis centres.

Additionally, an excellent Good Practice Guide to Network Security Information Exchanges has been written by the European Union Agency for Network and Information Security (ENISA).[9]

Warning, advice and reporting points (WARPs)

WARPs are a UK initiative that began in 2002 under the auspices of the National Infrastructure Security Coordination Centre (NISCC), which is now known as CPNI. WARPs allow their members to receive and share up-to-date cyber threat information and best practice. WARPs are now provided by CERT-UK's CiSP.

Members of current WARPs tend to be regional government, emergency services or military organisations.

Cyber Security Information Sharing Partnership (CiSP)

The CiSP[10] is an initiative set up jointly between UK industry and government in order to share cyber security threat and vulnerability information. The objective is to increase situational awareness of cyber threats with a consequent reduction of impact on UK businesses.

CiSP membership can only be given to UK registered companies responsible for the administration of an electronic communications network in the UK, or organisations that are sponsored by either a government department, an existing CiSP member or a trade body or association.

CiSP members are able to exchange cyber threat information in real time, in a secure environment, operating within a framework that protects confidentiality. Information shared includes alerts and advisories, weekly and monthly summaries, and trend analysis reporting.

Computer emergency response teams (CERTs) and computer security incident response teams (CSIRTs)

CERTs have been in existence for some years now – originally begun by the US Carnegie Mellon University, the practice of collecting, analysing and distributing security advisories has been a major influence on all sectors worldwide. CERTs and CSIRTs carry out the same function, and the mnemonics are used interchangeably.

Many countries now operate a CERT/CSIRT, and even some larger multinational organisations whose enterprises cross traditional national and continental boundaries may do likewise.

In the UK, CERT-UK[11] has four main responsibilities that flow from the UK's National Cyber Strategy:

- national cyber security incident management;
- support to critical national infrastructure companies to handle cyber security incidents;
- promoting cyber security situational awareness across industry, academia and the public sector;
- providing the single international point of contact for coordination and collaboration between national CERTs.

Subscription to a CERT or CSIRT is possible for almost any individual or organisation wishing to receive updates. However, sometimes the volume and frequency of these can be overwhelming.

As an example, CERT-UK provides three main workstreams:

- Alerts – In the exceptional event of a critical national cyber security incident, CERT-UK will issue an alert and appropriate guidance.
- Advisories – CERT-UK issues advisories that address cyber security issues being detected across government, industry or academia, or that offer best-practice updates.
- Best-practice guides – Through CiSP, CERT-UK provides regular advice and guidance on a range of cyber issues, with the aims of sharing information and encouraging best practice among its partners.

Security information exchanges (SIEs) and information sharing and analysis centres (ISACs)

Whereas CERTs and CSIRTs concentrate both on information collection and response to incidents, SIEs and ISACs provide solely a means of exchanging information about threats, vulnerabilities and incidents. SIEs tend to provide raw data about incidents, whereas ISACs tend to provide a deeper analysis and suggestions for response.

SIEs and ISACs generally comprise both public and private sector organisations that form part of a critical national infrastructure, together with their lead government department and any other organisation with a legitimate interest in the security aspects of that particular sector, such as the sector regulator.

In the UK, a number of SIEs are managed by CPNI.[12]

In the UK, CPNI considers that there are 13 areas of national infrastructure, which were discussed in greater detail in Chapter 3 of this book. Other countries adopt a similar approach, and in the USA, for example, their ISACs broadly cover the same areas. Their website notes that there are some cross-sector themes such as technology wherein there may be infrastructure that supports the delivery of essential services across a number of sectors.

---

1. For a detailed view on this topic, please see David Sutton (2015) 'Trusted information sharing for cyber security situational awareness'. *Elektrotechnik und Informationstechnik*, 132 (2) 113–116. DOI 10.1007/s00502-015-0288-3.
2. The Traffic Light Protocol was originally developed by the UK CPNI.
3. See https://www.chathamhouse.org/about-us/chatham-house-rule
4. See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf
5. See https://www.consilium.europa.eu/en/general-secretariat/corporate-policies/classified-information/
6. See https://www.dami.army.pentagon.mil/site/sso/docs/InfoSec/DoD5200_1ph.pdf
7. See ISO/IEC 27010:2015 – *Information technology – Security techniques – Information security management for inter-sector and inter-organisational communications.*
8. See https://www.ncsc.gov.uk/information/what-warp
9. See https://www.enisa.europa.eu/publications/good-practice-guide
10. See https://www.ncsc.gov.uk/section/keep-up-to-date/cisp
11. See https://www.certuk.org.uk/
12. See https://www.cpni.gov.uk/

PART III
APPENDICES

APPENDIX A
STANDARDS

Standards and specifications are directives telling you what should be done, while guidelines and recommendations are informative and tell you how you should go about it.

There are also good practice guides and documents, which, rather than being issued by a standards body, may originate from an organisation that has a legitimate claim to be the main source of knowledge on matters pertaining to it. An example of this is the Information Security Forum's Standard of Good Practice, which we shall examine briefly later in this appendix.[1]

Regardless of their name or definition, standards, specifications, guidelines and recommendations are costly to produce and tend to be developed and distributed by large international organisations, which usually make a charge for them, or by government departments, which may subsidise them to a greater or lesser degree.

Some standards bodies produce their output for local consumption only, whereas the larger ones tend to produce output intended for more widespread use. An example of the former category is Standards Australia, whose output is generally just used within that country and sometimes in New Zealand. An example of the second category is BSI,[2] which has been at the forefront of standards development since 1901, and much of its output is utilised worldwide, often being turned into truly international standards through ISO.

There are a number of countries that produce their own standards of all kinds, but the principal ones for cyber security are the EU, the USA and the UK. However, many of these standards go on to become international standards, so we will deal primarily with those.

The standards body responsible for publishing them is ISO,[3] based in Geneva. Development of new standards can take many years and involves representatives from all over the world who meet both in person and through collaborative file sharing to define and agree the detail.

The best-known series of information security standards is the ISO/IEC 27000 series (IEC[4] is also based in Geneva) and many of the ISO standards are produced in consultation with them.

There are also some excellent British Standards (BSs) and guideline documents as well as many American Federal Information Processing Standards (FIPSs). Finally, and still of interest, are the Internet Engineering Task Force (IETF) Requests for Comment (RFCs) and the International Telecommunication Union (ITU) standards.

At the time of writing, there are more than 40 published ISO standards in the information security area, with several more in the development pipeline. If you would like to see the details of any of them, the best place to look is either the ISO website or the BSI website, as the index of ISO standards is shown there. If you wish to purchase them, you will probably find that the BSI online route is less costly, especially if you become a member of BSI, in which case many of the standards are available at a discounted price.

The security standard considered to be the primary one is ISO/IEC 27001:2022, and it is to this standard that organisations can be accredited.

One thing to beware of is that the ISO standards portfolio is growing rapidly, and by the time you read this book many more will have been produced. However, we have made best efforts to ensure that the list is up to date at the time of writing. Where appropriate, a brief description of the standard has been included.

CYBER SECURITY STANDARDS

There are more standards in this area than you could shake a stick at, so below are some of the most relevant ones.

BS 10012:2017+A1:2018 – *Specification for a personal information management system*

The title of this standard is slightly confusing – it would appear to refer to management of information for individual people, whereas it actually refers to organisational management of people's personal information.

Its main theme is to highlight the organisation's responsibilities with regard to data protection and it is a useful introduction to the European Union General Data Protection Regulation 679/2016 (GDPR). The structure has also been updated to follow the ISO management system structure.

PAS 555:2013 – *Cyber security risk – Governance and management – Specification*

For organisations wishing to achieve a reasonable standard of cyber security without the need for full ISO/IEC 27001 certification, PAS 555 is an excellent beginning. It does, however, only provide high-level statements as opposed to the level of detail that one would find in the full ISO standard. This might appeal to many SMEs.

ISO/IEC 27000 SERIES STANDARDS

ISO/IEC 27000:2020 – *Information technology – Security techniques – Information security management systems – Overview and vocabulary*

Apart from providing definitions of commonly used terms, this standard describes how an information security management system (ISMS) should work and goes on to mention some of the standards listed below.

ISO/IEC 27001:2022 – *Information security, cybersecurity and privacy protection – Information security management systems - Requirements*

Although it covers areas beyond pure cyber security, this is the main standard, and it is against this that organisations can be accredited.

Sections 4 to 10 describe the mandatory elements of the standard, and the abbreviated list of controls in its Annex A are described in much greater detail in ISO/IEC 27002:2022.

ISO/IEC 27002:2022 – *Information security, cybersecurity and privacy protection — Information security controls*

This standard provides detailed descriptions of the controls listed in Annex A of ISO/IEC 27001:2022. The number of controls in the 2022 version of ISO/IEC 27002 has decreased from 114 to just 93. These are organised into four control themes – Organisational, People, Physical and Technological controls. While a number of controls have been merged to avoid duplication and some have been removed altogether, there are 11 new controls:

- Threat intelligence;
- Information security for the use of cloud services;
- ICT readiness for business continuity;
- Physical security monitoring;
- Configuration management;
- Information deletion;
- Data masking;
- Data leakage prevention;
- Monitoring activities;
- Web filtering;
- Secure coding.

ISO/IEC 27003:2017 – *Information technology – Security techniques – Information security management systems implementation guidance*

This standard provides guidance on planning and information security management systems aligned to ISO/IEC 27001.

ISO/IEC 27004:2016 – *Information technology – Security techniques – Information security management measurements*

This standard covers the types of metrics and measurements that can be applied to an ISO/IEC 27001 programme.

ISO/IEC 27005:2022 – *Information security, cybersecurity and privacy protection – Guidance on managing information security risks*

This is the main standard used when conducting an information risk management programme and can form a major input to an ISO/IEC 27001 programme. A somewhat older standard, ISO 31000:2018, *Risk management – Principles and guidelines*, provides principles and generic guidelines on risk management.

ISO/IEC 27006:2020 – *Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems*

Although this standard is less relevant to individual organisations looking to attain ISO/IEC 27001 certification, it does illustrate the guidance for those bodies that provide the certification.

ISO/IEC 27007:2022 – *Information technology – Security techniques – Guidelines for information security management systems auditing*

As with the previous example, this standard is somewhat less relevant to organisations wishing to develop an ISMS programme but has been included for completeness.

ISO/IEC 27008:2019 – *Information technology – Security techniques – Guidelines for auditors on information security controls*

This standard provides a slightly different aspect of the ISMS audit function – this time dealing with guidance on specific controls.

ISO/IEC 27010:2015 – *Information security management systems – Information security management for inter-sector and inter-organizational communications*

This standard was developed with the express intention of exchanging information securely between organisations, especially when concerned with sharing information on security issues, as discussed in Chapter 11.

ISO/IEC 27011:2016 – *Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*

The standard is for telecommunications organisations and will enable them to meet baseline ISMS requirements of confidentiality, integrity, availability and any other relevant security properties of telecommunications services.

ISO/IEC 27013:2021 – *Information technology – Security techniques – Guidance on the implementation of ISO/IEC 27001 and ISO/IEC 20000-1*

This standard provides guidance on what organisations need to do in order to build a management system that integrates ISO/IEC 27001 and also ISO/IEC 20000, which is concerned with service management.

ISO/IEC 27014:2020 – *Information technology – Security techniques – Governance of information security*

This standard allows organisations to make decisions about information security issues in support of the strategic organisational objectives.

ISO/IEC 27015:2012 – *BS ISO/IEC TR 27015:2012 ED1 – Information security management systems – Information security management guidelines for financial services*

This standard is important for any organisation planning to offer financial services covered by an ISMS. It may also be useful to consumers of such services.

ISO/IEC 27016:2014 – *Information technology – Security techniques – Information security management – Organizational economics*

This standard will be useful when making information security investment decisions, as well as for those who have to prepare the business cases for information security investment.

ISO/IEC 27017:2021 – *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services*

This standard will be useful to organisations wishing to become providers or users of cloud services, both by identifying their responsibilities to ensure certification of related security controls, and as a checklist to ensure that potential providers of the cloud service have the necessary security policies, practices and controls in place.

ISO/IEC 27018:2020 – *Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

This standard is applicable to all types and sizes of organisations, including public and private companies, government entities and not-for-profit organisations, which provide information processing services as PII processors via cloud computing under contract to other organisations.

ISO/IEC 27019:2020 – *Information technology – Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry*

This standard is important for any organisation in the energy utility sector planning to operate an ISMS. It may also be useful to related organisations such as utility plant suppliers, systems integrators and auditors.

ISO/IEC 27023:2015 – *Information technology – Security techniques – Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002*

This standard simply does what it says in the title. The earlier (2005) versions of ISO/IEC 27001 and 27002 differed in many ways from the 2013 versions, and this standard provides clarification.

ISO/IEC 27031:2011 – *Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity*

This standard provides guidelines for preparation of information and communications technology systems in meeting business continuity requirements. It relates to ISO 22301, which falls largely outside the scope of this book, since that standard covers all aspects of business continuity.

ISO/IEC 27032:2012 – *Information technology – Security techniques – Guidelines for cybersecurity*

This standard will be of much greater value to those organisations who are investing in protection against cyber security problems. It provides a detailed framework for identifying cyber security issues, and a high-level set of controls for dealing with them.

ISO/IEC 27033-1:2015 – *Information technology – Security techniques – Network security – Overview and concepts*

The first of six standards relating to network security, this standard deals with the main issues that organisations are likely to face.

ISO/IEC 27033-2:2012 – *Information technology – Security techniques – Guidelines for the design and implementation of network security*

This standard takes matters to the next level and defines the network security requirements that are likely to be needed and provides a checklist.

ISO/IEC 27033-3:2010 – *Information technology – Security techniques – Network security – Reference networking scenarios – Threats, design techniques and control issues*

This standard deals with security network design principles and examines the threats and possible controls associated with them.

ISO/IEC 27033-4:2014 – *Information technology – Security techniques – Network security – Securing communications between networks using security gateways*

This standard provides guidance on securing communications between networks using security gateways and firewalls and introduces the concept of intrusion detection systems.

ISO/IEC 27033-5:2013 – *Information technology – Security techniques – Network security – Securing communications across networks using Virtual Private Networks (VPNs)*

ISO/IEC 27033-6:2016 – *Information technology – Security techniques – Network security – Securing wireless IP network access*

This final part of this standard deals with securing network interconnections and how to connect remote users by providing VPNs.

This group of seven standards sets the scene for the secure development of applications, and in particular deals with the application security management process:

ISO/IEC 27034-1:2011 – *Information technology – Security techniques – Application security – Overview and concepts*

ISO/IEC 27034-2:2015 – *Information technology – Security techniques – Application security – Organization normative framework*

ISO/IEC 27034-3:2018 – *Information technology – Application security – Application security management process*

ISO/IEC 27034-5:2017 – *Information technology – Security techniques – Application security – Protocols and application security controls data structure*

ISO/IEC 27034-6:2016 – *Information technology – Security techniques – Application security – Case studies*

ISO/IEC 27034-7:2018 – *Information technology – Application security – Assurance prediction framework*

This group of three standards deals with the management of cyber security incidents:

ISO/IEC 27035-1:2016 – *Information technology – Security techniques – Information security incident management*

ISO/IEC 27035-2:2016 – *Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response*

ISO/IEC 27035-3:2020 – *Information technology – Information security incident management – Guidelines for ICT incident response operations*

This series of four standards examines the security requirements for the relationship between organisations and their suppliers:

ISO/IEC 27036-1:2021 – *Information technology – Security techniques – Information security for supplier relationships – Overview and concepts*

ISO/IEC 27036-2:2022 – *Information technology – Security techniques – Information security for supplier relationships – Requirements*

This standard goes into greater detail regarding the technical security requirements that must be agreed and managed between an organisation and its suppliers.

ISO/IEC 27036-3:2013 – *Information technology – Security techniques – Information security for supplier relationships – Guidelines for information and communication technology supply chain security*

Frequently, supply chains are multi-layered and global, and this standard provides guidance on managing the complex risk environment.

ISO/IEC 27036-4:2016 – *Information technology – Security techniques – Information security for supplier relationships – Guidelines for security of cloud services*

This standard provides cloud service customers and cloud service providers with guidance on:

(a) gaining visibility into the information security risks associated with the use of cloud services and managing those risks effectively; and

(b) responding to risks specific to the acquisition or provision of cloud services that can have an information security impact on organisations using these services.

ISO/IEC 27037:2016 – *Information technology – Security techniques – Guidelines for identification, collection, acquisition and*

preservation of digital evidence

When cyber incidents occur, it may be necessary to preserve evidence of the fact, and this standard provides guidelines for the forensic preservation of evidence.

ISO/IEC 27038:2016 – *Information technology – Security techniques – Specification for digital redaction*

When organisations are required to anonymise information within a document or to redact it completely, this standard provides guidelines on the process and techniques, and may be useful in information sharing situations.

ISO/IEC 27039:2015 – *Information technology – Security techniques – Selection, deployment and operations of intrusion detection and prevention systems (IDPS)*

Intrusion detection and prevention systems can provide an analysis of host and network traffic and/or audit trails for attack signatures or specific patterns that usually indicate malicious or suspicious intent. This standard provides guidelines for effective IDPS selection, deployment and operation, as well as fundamental knowledge about IDPS.

ISO/IEC 27040:2016 – *Information technology – Security techniques – Storage security*

This standard applies to all data owners, IT managers and security officers from small enterprises to global organisations, as well as manufacturers of general and specialised data storage products, and is particularly relevant to data destruction services.

ISO/IEC 27041:2016 – *Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative method*

This standard contains an assurance model with details of how to validate the methods used for investigations and shows how internal and external resources can be used to carry out assurance.

ISO/IEC 27042:2016 – *Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence*

This standard provides a detailed framework for investigation, giving guidance on how to structure and prioritise investigative stages in order to produce analysis and reports that can be used to improve security in the future.

ISO/IEC 27043:2016 – *Information technology – Security techniques – Incident investigation principles and processes*

This standard is intended to aid in digital investigations, with the aim that a suitably skilled investigator should obtain the same result as another similarly skilled investigator working under similar conditions.

OTHER RELEVANT ISO STANDARDS

ISO/IEC 17788:2014 – *Information technology – Cloud computing – Overview and vocabulary*

ISO/IEC 17789:2014 – *Information technology – Cloud computing – Reference architecture*

These two standards should appeal to all kinds of cloud customers – from small enterprises to global organisations – and all kinds of

cloud providers and partner organisations such as software developers and auditors.

ISO/IEC 24762:2008 – *Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services*

This standard takes us into the area of disaster recovery and is aimed at aiding the operation of an ISMS by providing guidance on the provision of information and communications technology disaster recovery services as part of business continuity management.

ISO/IEC 29100:2020 – *Information technology – Security techniques – Privacy framework*

This standard provides a high-level framework for the protection of personally identifiable information within IT systems.

ISO/IEC 29101:2021 – *Information technology – Security techniques – Privacy architecture framework*

The guidance in this standard is applicable to entities involved in specifying, procuring, architecting, designing, testing, maintaining, administering and operating IT systems that process PII. It focuses primarily on IT systems that are designed to interact with PII principals.

ISO/IEC 29147:2020 – *Information technology – Security techniques – Vulnerability disclosure*

This standard provides guidelines for vendors to be included in their business processes when receiving information about potential vulnerabilities and distributing vulnerability resolution information.

ISO/IEC 29190:2015 – *Information technology – Security techniques – Privacy capability assessment model*

This standard provides guidance for organisations in producing an overall ‘score’ against a simple capability assessment model; a set of metrics indicating assessment against key performance indicators; and the detailed outputs from privacy process management audits and management practices.

ISO/IEC 30111:2020 – *Information technology – Security techniques – Vulnerability handling processes*

This standard describes processes for vendors to handle reports of potential vulnerabilities in products and online services.

BUSINESS CONTINUITY STANDARDS

Since cyber security forms an integral part of business continuity, the following standards have been included for completeness.

The first real attempt at producing a business continuity standard in the UK was the introduction of the BSI’s PAS 56 in 2003. Intended as an interim standard it was eventually replaced by BS 25999 Part 1 – *Business continuity management – Code of practice* in 2006 and BS 25999 Part 2 – *Business continuity management – Specification* in 2007. Both of these have now been superseded by the international standard ISO 22301.

As with many BSI and ISO standards areas, there are a number of standards and good practice guides for business continuity. The following is a list of the most relevant, and includes standards

relating to incident and crisis management, both of which may be required as part of a business continuity programme.

ISO 22301:2014 – *Societal security – Business continuity management systems – Requirements*

This is now the definitive business continuity standard, replacing BS 25999 Parts 1 and 2 in 2014.

ISO 22313:2014 – *Societal security – Business continuity management systems – Guidance*

This standard is the guidance document that supports the requirements of ISO 22301. It describes good practice guidelines and recommendations that organisations may adopt to ensure their business continuity management (BCM) programme aligns with internationally recognised best practices.

ISO 22318:2021 – *Societal security – Business continuity management systems – Guidelines for supply chain continuity*

As the title suggests, this standard examines strategies and methods for managing supply chain disruptions.

ISO 22322:2015 – *Societal security – Emergency management – Guidelines for public warning*

This standard describes the processes for monitoring threats and hazards that might cause harm to the public at large, and how to communicate these.

PD 25111:2010 – *Business continuity management – Guidance on human aspects of business continuity*

This standard provides guidelines for the planning of strategies for human resource management both during and following a business-disruptive incident, considering not only staff, but also their families.

PD 25666:2010 – *Business continuity management – Guidance on exercising and testing for continuity and contingency programmes*

Exercising and testing is a key aspect of business continuity programmes, and PD 25666 delivers practical advice on how best to accomplish this, the aims and objectives of exercises, how to present a business case and developing staff competence through training.

BS 11200:2014 – *Crisis management – Guidance and good practice*

Crisis management requires a forward-looking, systematic approach that creates structures, trains people to work within them and is evaluated and developed in a continuous, purposeful and rigorous way.

BS BIP 2142:2012 – *The route map to business continuity management. Meeting the requirements of ISO 22301*

John Sharp, the author of this document, has taken ISO 22301 as a starting point, examined every aspect of its requirements, and explained in BIP 2142 how best these can be achieved. However, he has taken this document much further by adding sections that are not specifically covered by ISO 22301, and also by providing useful templates for the BC practitioner.

BS BIP 2143:2012 – *Business continuity exercises and tests. Delivering successful exercise programmes with ISO 22301*

This document covers business continuity exercises and tests, expanding on the requirements of PD 25666 and explaining how best these can be achieved.

BS BIP 2151:2012 – *Auditing business continuity management plans. Assess and improve your performance against ISO 22301*

This document is probably better suited to larger enterprises, where internal audit is widely used, and a strict compliance regime is in operation.

BS BIP 2185:2012 – *Business continuity communications. Successful incident communication planning with ISO 22301*

The business continuity plan itself is only part of the story. Communication with all stakeholders during a business-disruptive incident is essential both in making the plan work and in preserving the organisation's credibility with the media.

BS BIP 2214:2011 – *A practical approach to business impact analysis. Understanding the organisation through business continuity management*

BIP 2214 is one of the most useful documents in the whole of the BSI collection and will guide the reader step by step through the entire business impact analysis (BIA) process.

BS BIP 2217:2011 – *Business continuity management for small and medium sized enterprises. How to survive a major disaster or failure*

This document takes the BCM approach from the perspective of the SME as opposed to that of the larger corporate organisation, at which many other standards and guides are directed.

PAS 77:2006 – *IT Service Continuity Management – Code of Practice.*

By investigating, developing and implementing preventative and recovery options beforehand, an organisation can minimise and manage interruptions to services that threaten the continuity of the business.

British standards can be obtained in PDF or hard copy formats from the BSI online shop: www.bsigroup.com/Shop or by contacting BSI Customer Services for hard copies only: tel: +44 (0) 20 8996 9001, email: cservices@bsigroup.com

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) STANDARDS

There are many NIST standards and FIPSs relating to information security, but these are probably of greatest interest:

NIST SP 800-53A – *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*

NIST SP 800-83 – *Guide to Malware Incident Prevention and Handling*

NIST SP 800-100 – *Information Security Handbook: A Guide for Managers*

NIST SP 800-153 – *Guidelines for Securing Wireless Local Area Networks (WLANs)*

These can all be downloaded free of charge from http://csrc.nist.gov/publications/

NIST Cyber Security Framework (2014) *Framework for Improving Critical Infrastructure Cybersecurity.*[5]

---

1. See https://www.securityforum.org/blog/standard-of-good-practice-for-information-security-2020-now-available-to-members/
2. See www.bsigroup.com/en-GB/standards/
3. See https://www.iso.org/standards.html
4. See https://iec.ch/about-us
5. NIST regularly publishes updates to the original framework, and these can be viewed at https://www.nist.gov/cyberframework

APPENDIX B
GOOD PRACTICE GUIDELINES

There are many examples of good practice guidelines on the internet, making it an impossible task to list them all. However, the following are of particular note, and will direct the reader to those guidelines of interest that will provide the level of detail required.

GENERAL CYBER SECURITY ADVICE

CPNI has a wealth of information covering all sectors of the CNI at https://www.cpni.gov.uk/advice/cyber/Good-practice-catalogue/

Good practice information on industrial control systems can be found at
https://www.cisa.gov/uscert/sites/default/files/recommended_practices/
NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

The UK's Health and Social Care Information Centre (HSCIC) posts good practice information for cyber security at

http://systems.hscic.gov.uk/infogov/security/infrasec/gpg

NCSC promotes cyber security good practice information for both public and private sectors, and guidance documents can be found at https://www.ncsc.gov.uk/guidance

For both public and private sectors, warning advice and reporting points (WARPs) can be found at https://socitm.net/about/warps/

As part of the National Cyber Strategy, the UK's CERT has four areas of responsibility:

1. national cyber security incident management;
2. supporting critical national infrastructure companies to handle cyber security incidents;
3. promoting cyber security situational awareness across industry, academia and the public sector;
4. providing the single international point of contact for coordination and collaboration between national CERTs.

Further information can be obtained from www.ukcert.org.uk

Organisations that are members of the Information Security Forum (ISF) have access to its Standard of Good Practice, the most recent version being from 2013. See https://www.securityforum.org/blog/standard-of-good-practice-for-information-security-2020-now-available-to-members/

UK GOVERNMENT CYBER SECURITY ADVICE

The following is a selection of useful advice and guidance documents from the UK government for both small and larger

businesses:

Help small businesses stay safe online:
https://www.cyberstreetwise.com

What small businesses need to know about cyber security:
https://www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know

The UK Cyber Aware scheme:
https://www.ncsc.gov.uk/cyberaware/home

The UK Cyber Essentials Plus schemes:
https://www.ncsc.gov.uk/cyberessentials/overview

Cyber security guidance for business:
https://www.gov.uk/government/collections/cyber-security-guidance-for-business

10 Steps to Cyber Security: https://www.ncsc.gov.uk/collection/10-steps

IoT Security Assured

The IoT Security Assured scheme provides an opportunity for manufacturers to improve the security of their internet-connected devices and to show they are compliant with best-practice security.

Within the IoT Security Assured scheme, there are three levels of security that a device can be certified to, as follows:

- The Basic is aligned with proposed UK legislation and covers the top three requirements of the European Telecommunications Standards Institute (ETSI) standard.

- The Silver level is aligned with the ETSI mandatory requirements and Data Protection provisions.
- The Gold level is aligned with the ETSI mandatory requirements as well as all the additional ETSI recommended requirements and Data Protection provisions.

https://iasme.co.uk/internet-of-things/about-iot-security-assured-self-assessment/

National Cyber Strategy

Pillar 1: Strengthening the UK cyber ecosystem, investing in our people and skills and deepening the partnership between government, academia and industry

Pillar 2: Building a resilient and prosperous digital UK, reducing cyber risks so businesses can maximise the economic benefits of digital technology and citizens are more secure online and confident that their data is protected

Pillar 3: Taking the lead in the technologies vital to cyber power, building our industrial capability and developing frameworks to secure future technologies

Pillar 4: Advancing UK global leadership and influence for a more secure, prosperous and open international order, working with government and industry partners and sharing the expertise that underpins UK cyber power

Pillar 5: Detecting, disrupting and deterring our adversaries to enhance UK security in and through cyberspace, making more integrated, creative and routine use of the UK's full spectrum of levers

https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

NCSC advice – actions to take

The most important thing for organisations of all sizes is to make sure that the fundamentals of cyber security are in place to protect their devices, networks and systems. The actions they recommend are about ensuring that basic cyber hygiene controls are in place and functioning correctly. This is important under all circumstances but critical during periods of heightened cyber threat.

An organisation is unlikely to be able to make widespread system changes quickly in response to a change in threat, but organisations should make every effort to implement these actions as a priority.

See https://www.ncsc.gov.uk/guidance/actions-to-take-when-the-cyber-threat-is-heightened

APPENDIX C
CYBER SECURITY LAW

There are a number of pieces of UK legislation that are specifically concerned with cyber security, and also regulations and directives from the EU that have been or may be placed within the UK's legislative framework.

UK LAW

Computer Misuse Act 1990

This was introduced in response to a High Court decision to overturn the conviction of Robert Schifreen and Stephen Gold, who in 1985 gained unauthorised access to British Telecom's (BT's) Prestel electronic mail system and eventually accessed the mailbox of HRH the Duke of Edinburgh.

The Act is generally considered as the primary means of prosecuting cyber-attackers in the UK, provided that there is a warning notice on

the computer system concerned requiring a user to confirm they are authorised to access the computer.

Download at www.legislation.gov.uk/ukpga/1990/18/contents

Copyright, Designs and Patents Act 1988

The 1988 Act amends previous legislation and establishes the period of time over which copyright of work exists – mostly for 70 years following the death of the author or creator if known, or 70 years after the creation or publication of the work, but 50 years for computer-generated works.

In order for something to be protected by copyright it must fall within one of the following categories of work:

- literature;
- drama;
- music;
- art;
- film;
- sound recording;
- broadcasts;
- typographical arrangement of published works.

Download at www.legislation.gov.uk/ukpga/1988/48/contents

Data Protection Act 2018

Derived from the EU Data Protection Directive, this is the primary legislation under which all information privacy issues are managed. In April 2016, the EU agreed a major overhaul to the legislation, the

GDPR, and this came into force in 2018. As it is a regulation, and not a directive, it does not require changes to UK law.

Download at https://www.legislation.gov.uk/ukpga/2018/12/data.pdf

Digital Economy Act 2017

In particular, this Act addresses media policy issues related to digital media, including copyright infringement and internet domain names.

Download at https://www.legislation.gov.uk/ukpga/2017/30/contents

Intellectual Property Act 2014

This Act introduced a number of measures and made changes to the law in order to make design law simpler, clearer and more robust. It also introduced changes to patent law, which simplified complex areas and made it less costly and easier to use and defend patents.

Download at www.legislation.gov.uk/ukpga/2014/18/contents/enacted

Investigatory Powers Act 2016

This Act is frequently referred to as the ‘Snooper’s Charter’, since it extends the powers of the security services and police much further than any previous legislation.

It contains a number of key points:

- It allows the security services and law enforcement agencies to undertake targeted interception of communications, the bulk collection of communications data and the bulk interception of communications.

- It creates the Investigatory Powers Commission (IPC) to oversee the use of all investigatory powers, alongside the oversight provided by the Intelligence and Security Committee of Parliament and the Investigatory Powers Tribunal.
- It requires communication service providers (CSPs) to retain for one year UK internet users' internet connection records. This includes which websites were visited but not the individual pages or the full browsing history.
- It allows police, intelligence officers and government department managers to view the internet connection records without a warrant.
- It permits the police and security services to carry out 'targeted equipment interference'. This means hacking into computers or devices (such as smartphones, tablet computers, etc.) to access their data.
- It places a legal obligation on CSPs to provide assistance with supplying targeted interception of data and communications, and with equipment interference in relation to investigations.
- It requires CSPs in the UK to remove encryption applied within their network.
- It creates new criminal offences for the unlawful access of internet data, and also for a CSP who reveals that data has been requested.

Download at https://www.legislation.gov.uk/ukpga/2016/25/contents

Malicious Communications Act 1988

This Act makes it an offence to 'send or deliver letters or other articles for the purpose of causing distress or anxiety'. Its application

in the cyber security environment is that it also applies to electronic communications and has been used successfully to prosecute internet trolls and people posting malicious or offensive remarks on social media.

Download at www.legislation.gov.uk/ukpga/1988/27/contents

Regulation of Investigatory Powers Act 2000

Regulation of Investigatory Powers Act (RIPA) sets out (in theory at least) how public bodies (including the police and security services) may monitor the communications of individuals with the purpose of investigating acts of crime or terrorism.

Download at www.legislation.gov.uk/ukpga/2000/23/contents

NIS Regulations 2018

Download at https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018

EU DIRECTIVES AND REGULATIONS

Network and Information Security (NIS) Directive

This was proposed as part of the European Union's cyber security strategy, created to enhance data security throughout member states. The Directive is intended to foster co-operation between EU nations while legislating expected security requirements for all essential services. It was formalised in July 2016 and had to be implemented by all member states by April 2018.

There are broadly four key areas to the Directive:

1. Member states are required to adopt a national strategy that sets out concrete policy and regulatory measures to maintain a level of network and information security. This includes designating a national competent authority for information security and setting up a CERT that is responsible for handling incidents and risks.
2. The competent authorities in EU member states and the European Commission will form a co-operation network to coordinate against risks and incidents affecting network and information systems. The network will exchange information between authorities, provide early warnings on information security issues and agree on a coordinated response in accordance with an EU NIS co-operation plan.
3. EU member states must ensure that public bodies and certain market operators take appropriate technical and organisational measures to manage the security risks of networks and information systems – these must guarantee a level of security appropriate to the risks and should prevent and minimise the impact of security incidents affecting the core services they provide.
4. Public bodies and selected private sector companies must also notify the competent authority of incidents that have a significant impact on the continuity of these services. The competent authority may decide to inform the public about the incident. The significance of the incident should consider the number of users affected, the duration of the incident and the geographical spread of the area affected by the incident. Hence, these requirements apply not only to private sector companies set out in the list below but also to public bodies.

The Directive would currently apply to the following private sector industries:

- key internet companies (such as large cloud providers, social networks, e-commerce platforms, search engines);
- banking sector and stock exchange;
- energy (such as electricity and gas);
- transport (operators of air, rail and maritime transport and logistics);
- health (such as electronic medical devices and online/electronic personal health and financial information);
- public administrations (such as e-government and e-participation services).

ISPs are already required to provide incident notification under the current EU Telecom Framework Directive.

Download the Directive at https://www.enisa.europa.eu/topics/nis-directive

EU General Data Protection Regulation (GDPR)

The EU GDPR effectively extends the current data protection legislation. It applies both to data controllers and data processors, and, additionally, data controllers will be required to ensure that data processors comply with contractual terms and conditions. Data controllers and data processors must also be able to demonstrate compliance with the GDPR.

It adds to the definitions of personal data, which now include artefacts that can be linked to a person's identity, such as IP

addresses, and to sensitive personal data, such as genetic or biometric information.

It also extends the rights of the individual:

- the right to be informed about what data is held about them and why;
- the right of individuals' access to their data;
- the right of rectification of incorrect data;
- the right of erasure of data that is out of date;
- the right to restrict the processing of data;
- the right to move their data from one organisation to another;
- the right to object to the processing of their data;
- rights related to the automated processing and profiling of their data.

The GDPR also tightens up the requirements for notifications of data breaches and deals with the transfer of data outside the EU.

APPENDIX D
TRAINING AND QUALIFICATIONS

Download further information at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

GENERIC CYBER SECURITY TRAINING AND QUALIFICATIONS

This can cover a number of areas, such as:

- Certified Information Systems Security Professional (CISSP); see https://www.isc2.org/cissp/default.aspx
- information security governance;
- Payment Card Industry Data Security Standard (PCI DSS); see https://www.pcisecuritystandards.org/pci_security/
- information risk management;

- ISO/IEC 27001; see www.iso.org/iso/iso27001
- Sarbanes–Oxley (for organisations listed on the New York Stock Exchange); see www.soxlaw.com/
- Basel III (banking sector); see www.bis.org/bcbs/basel3.htm
- Control Objectives for Information and Related Technologies (COBIT 5); see https://www.isaca.org/resources/cobit
- Certificate of Cloud Security Knowledge (CCSK); see https://cloudsecurityalliance.org/education/ccsk/#info-video1
- governance, risk and compliance;
- information security audit;
- business continuity;
- National Cyber Security Centre (NCSC) NCSC Certified Cyber Professional (CCP) Scheme; see https://www.ncsc.gov.uk/articles/about-certified-professional-scheme
- Systems Security Certified Practitioner (SSCP); see https://www.isc2.org/sscp/default.aspx
- Certified Cloud Security Professional (CCSP); see https://www.isc2.org/ccsp/default.aspx
- information assurance (IA).

BCS offers a number of training courses and accreditations. At foundation level:

- Certificate in Information Security Management Principles (CISMP); see http://certifications.bcs.org/category/15735
- Foundation Certificate in Data Protection; see http://certifications.bcs.org/category/18107

At practitioner level:

- Practitioner Certificate in Information Risk Management (PCIRM); see https://www.bcs.org/qualifications-and-certifications/certifications-for-professionals/information-security-and-ccp-assured-service-certifications/bcs-practitioner-certificate-in-information-risk-management/
- Practitioner Certificate in Data Protection; see http://certifications.bcs.org/category/15742
- Practitioner Certificate in Freedom of Information; see http://certifications.bcs.org/category/15745
- Practitioner Certificate in Information Assurance Architecture; see http://certifications.bcs.org/category/17270

Additionally, there are a number of universities that offer computer and information security management courses at both bachelor's and master's levels, including:

- Edinburgh Napier University: MSc in Advanced Security and Digital Forensics;
- Lancaster University: MSc in Cyber Security;
- University of Oxford: MSc in Software and Systems Security;
- Royal Holloway: MSc in Information Security;
- University of York: MSc in Cyber Security;
- Cranfield University: Cyber Defence and Information Assurance MSc/PgCert/ PgDip;
- University of Birmingham: MSc in Cyber Security;
- University of Southampton: MSc Cyber Security;

- University of Surrey: MSc in Information Security;
- University of Warwick: MSc in Cyber Security and Management.

See also the NCSC list of universities recognised for excellence in cyber security education.

SPECIFIC CYBER SECURITY TRAINING AND QUALIFICATIONS

Rather more specialised cyber security training can take place at several levels, depending upon the nature of the individuals' roles, and is likely to be in any of the following disciplines:

- firewall configuration and management;
- systems hardening;
- secure software development;
- VPN technologies;
- access control, including authentication devices;
- intrusion detection systems (IDSs);
- ethical hacking and penetration testing;
- database security;
- wireless security;
- security incident investigation;
- digital forensics;
- Public Key Infrastructure (PKI) and Transport Layer Security (TLS).

APPENDIX E
LINKS TO OTHER USEFUL ORGANISATIONS

The Copyright Licensing Agency
www.cla.co.uk

The UK Copyright Service
https://www.copyrightservice.co.uk

The Performing Rights Society
www.prsformusic.com/Pages/default.aspx

The British Association of Picture Libraries and Agencies
www.bapla.org.uk/en/page/show_home_page.html

The Intellectual Property Office
https://www.gov.uk/government/organisations/intellectual-property-office

The Motion Picture Licensing Corporation

www.themplc.co.uk

The Design and Artists Copyright Society
https://www.dacs.org.uk

The Federation Against Software Theft
www.fast.org

The UK Cyber Security Council
https://www.ukcybersecuritycouncil.org.uk/

National Cyber Strategy 2022
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf

APPENDIX F
FURTHER READING

There are many books on cyber security-related topics. Here is a sample of those that you might find of interest:

Alexander, D., Finch, A., Sutton, D. and Taylor, A. (2013) *Information Security Management Principles*, Second edition. Edited by A. Taylor. Swindon: BCS. ISBN 978-1-78017-175-3

Bartlett, J. (2015) *The Dark Net*. London: Windmill Books. ISBN 978-0-09959-202-0

Day, P. (2014) *Cyber Attack: The Truth About Digital Crime, Cyber Warfare and Government Snooping.* London: Carlton Books. ISBN 978-1-78097-533-7

The European Network and Information Security Agency. (2010) *The New User's Guide: How to Raise Information Security Awareness.* Luxembourg: ENISA. ISBN 978-92-9204-049-9

Goodman, M. (2016) *Future Crimes: Inside the Digital Underground and the Battle For Our Connected World.* London: Corgi. ISBN 978-0-55217-080-2

Green, J.S. (2015) *Cyber Security: An Introduction for Non-Technical Managers.* London: Routledge. ISBN 978-1-47246-673-0

Hafner, K. and Lyon, M. (1998) *Where Wizards Stay Up Late: The Origins of the Internet.* New York: Simon & Schuster. ISBN 978-0-68483-267-8

Lohr, S. (2015) *Data-ism: Inside the Big Data Revolution*. London: Oneworld. ISBN 978-1-78074-518-3

Rowlingson, R. (2011) *The Essential Guide to Home Computer Security*. Swindon: BCS. ISBN 978-1-90612-469-4

Schneier, B. (2015) *Data and Goliath: The Hidden Battles to Collect your Data and Control your World.* New York: W. W. Norton. ISBN 978-0-39335-217-7

Singer, P.W. and Friedman, A. (2014) *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford: Oxford University Press. ISBN 978-0-19991-811-9

Stoll, C. (1991) *The Cuckoo's Egg. Tracking a Spy Through the Maze of Computer Espionage*. London: Bodley Head. ISBN 978-1-41650-778-9

Sutton, D. (2015) 'Trusted information sharing for cyber security situational awareness'. *Elektrotechnik und Informationstechnik.* 132 (2). 113–116. DOI 10.1007/s00502-015-0288-3. ISSN 0932-383X.

Sutton, D. (2018) *Business Continuity in a Cyber World: Surviving Cyberattacks*. Hampton, New Jersey: Business Expert Press. ISBN 978-1-94744-146-0.

Sutton, D. (2021) *Information Risk Management: A Practitioner's Guide.* Second edition. Swindon: BCS. ISBN 978-1-78017-572-0

APPENDIX G
ABBREVIATIONS AND GLOSSARY

ABBREVIATIONS

3G	third generation public cellular mobile system
4G	fourth generation public cellular mobile system
5G	fifth generation public cellular mobile system
AES	Advanced Encryption Standard
AI	artificial intelligence
ATM	automatic teller machine
BC	business continuity
BCI	Business Continuity Institute
BCM	business continuation management
BCP	business continuity plan
BCS	BCS, The Chartered Institute for IT
BEC	business email compromise
BGP	Border Gateway Protocol

BIA	business impact analysis
BS	British Standard
BSI	British Standards Institution
BT	British Telecom
BYOD	bring your own device
C2	command and control
CA	certification authority
CAN	Controller Area Network
CBT	computer-based training
CCA	Centre for Cyber Assessment
CCP	Certified Cyber Professional
CCSC	Certified Cyber Security Consultancy
CCSK	Certificate of Cloud Security Knowledge
CCSP	Certified Cloud Security Professional
CCTV	closed-circuit television
CEO	chief executive officer
CERN	European Organization for Nuclear Research
CERT	computer emergency response team
CERT/CC	Computer Emergency Response Team/Coordination Centre
CERT-UK	Computer Emergency Response Team UK
CES	Consumer Electronics Show
CFO	chief financial officer
CI	critical infrastructure
CII	critical information infrastructure
CISMP	Certificate in Information Security Management Principles
CiSP	Cyber Security Information Sharing Partnership
CISSP	Certified Information Systems Security Professional

CLI	Calling Line Identifier
CNI	critical national infrastructure
COBIT	Control Objectives for Information and Related Technologies
COPPA	Children’s Online Privacy Protection Act
CPNI	Centre for the Protection of National Infrastructure
CSIRT	computer security incident response team
CSP	communication service provider
DARPA	Defense Advanced Research Projects Agency
DDoS	distributed denial of service
Defra	Department for Environment, Food and Rural Affairs
DMZ	demilitarised zone
DNO	distribution network operator
DNS	domain name system
DoD	Department of Defense
DORA	Digital Operational Resilience Act
DoS	denial of service
DPA	Data Protection Act
DR	disaster recovery
DVLA	Driver and Vehicle Licensing Agency
ECU	engine control unit
EDR	event data recorder
ENISA	European Union Agency for Network and Information Security
ETSI	European Telecommunications Standards Institute
EU	European Union
FAST	Federation Against Software Theft
FCA	Financial Conduct Authority

FIPS	Federal Information Processing Standard
GCHQ	Government Communications Headquarters
GDPR	General Data Protection Regulation
GP	general practitioner
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HIDS	host intrusion detection system
HIPAA	Health Insurance Portability and Accountability Act
HMRC	His Majesty’s Revenue and Customs
HR	human resources
HSCIC	Health and Social Care Information Centre
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVAC	heating, ventilation and air conditioning
IA	information assurance
ICT	information and communications technology
IDPS	intrusion detection and prevention systems
IDS	intrusion detection system
IEC	International Electrotechnical Commission
IED	improvised explosive device
IETF	Internet Engineering Task Force
IFE	in-flight entertainment
iOS	iPhone Operating System
IoT	Internet of Things
IP	intellectual property *or* Internet Protocol
IPC	Investigatory Powers Commission
IPv6	Internet Protocol Version 6
ISAC	information sharing and analysis centre

ISF	Information Security Forum
ISMS	information security management system
ISO	International Organization for Standardization
ISP	internet service provider
ISS	International Space Station
ITU	International Telecommunication Union
LAN	local area network
MAC	media access control
MAM	Mobile Application Management
MAO	maximum acceptable outage
MDR	Managed Detection and Response
MDM	Mobile Data Management
MTDL	maximum tolerable data loss
NCSC	National Cyber Security Centre
NHS	National Health Service
NIDS	network intrusion detection system
NIS	Network and Information Security
NISCC	National Infrastructure Security Coordination Centre
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol
OS	operating system
P2P	peer-to-peer
PAS	publicly available specification
PCI DSS	Payment Card Industry Data Security Standard
PCIRM	Practitioner Certificate in Information Risk Management
PDCA	Plan–Do–Check–Act

PDF	Portable Document Format
PGP	Pretty Good Privacy
PII	personally identifiable information
PIN	personal identification number
PKI	Public Key Infrastructure
PPs	Professional Practices
PTZ	point, tilt and zoom
RFC	Request for Comment
RIPA	Regulation of Investigatory Powers Act
RTO	recovery time objective
SAN	storage area network
SCADA	Supervisory Control and Data Acquisition
SIE	security information exchange
SLA	service level agreement
SLR	single-lens reflex
SME	small-to-medium enterprise
SMTP	Simple Mail Transfer Protocol
SPoF	single point of failure
SQL	Structured Query Language
SSCP	Systems Security Certified Practitioner
SSH	Secure Socket Shell
SSID	service set identifier
TCP	Transmission Control Protocol
TLP	Traffic Light Protocol
TLS	Transport Layer Security
TOR	The Onion Router
UAC	User Account Control
UDP	User Datagram Protocol

UPS	uninterruptible power supply
URL	Uniform Resource Locator
USB	Universal Serial Bus
VESDA	Very Early Smoke Detection Apparatus
VoIP	Voice over Internet Protocol
VPN	virtual private network
WAN	wide area network
WAP	wireless access point
WARP	warning, advice and reporting point
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	wireless local area network
WPA	Wireless Protected Access
WPA-PSK	Wireless Protected Access Pre-Shared Key
WPS	Wi-Fi Protected Setup

GLOSSARY

Some of the following definitions are taken from ISO/IEC 27000:2020 [1], ISO 22301:2019 [2], ISO Guide 73:2009 [3], BS ISO/IEC TR 18044:2004 [4] and ISO/IEC 27032:2012 [5]. A few are not defined in any standards, so I have suggested my own definition.

Access control: The means to ensure that access to assets is authorised and restricted to business and security requirements. [1]

Asset: Any item that has value to the organisation. [1] Assets may be tangible, normally having some physical form such as network equipment, systems and so on, or intangible, having no physical form, such as trademarks or reputation.

Attack: An attempt to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of an asset. [1]

Audit: The systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled. [1]

Authentication: The provision of assurance that a claimed characteristic of an entity is correct. [1]

Availability: The property of being accessible and useable upon demand by an authorised entity. [1]

Business continuity (BC): The capability of the organisation to continue delivery of products and services at acceptable predefined levels following a disruptive incident. [2]

Business impact analysis (BIA): The process of analysing activities and the effect that a business disruption might have upon them. [2]

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes. [1]

Consequence: An outcome of an event affecting objectives. [3] Consequences are also referred to as impacts.

Control: A measure that is modifying risk. [3] Controls come in a number of forms – at the strategic level, they can be to modify or reduce the risk; to avoid or terminate it; or to transfer or share it. At the tactical level, control choices are preventative, to stop something from happening; corrective, to fix something that has happened; detective, to discover when something has happened; and directive, to put processes and procedures into place. Finally, operational controls can be physical, such as locks and barriers; procedural,

such as change control mechanisms; and technical, such as antivirus software.

Cyber-attack: Aggressive cyber action taken against people, organisations, networks, systems and services, and which is intended to cause loss or damage.

Cyber bullying: Cyber bullying or cyber harassment is simply the act of harassing or bullying a person or group of people using cyber-based methods such as social media, text messaging and the like.

Cybercrime: Criminal activity where services or applications in the cyberspace are used for or are the target of a crime, or where the cyberspace is the source, tool, target or place of a crime. [5]

Cyber espionage: Covert surveillance activity conducted over cyberspace.

Cyber hacktivism: Includes individuals or groups who may be stalking someone in an act of revenge for a perceived grievance, looking to expose some wrongdoing, or a business trying to place their competitors on the wrong foot.

Cyber security: Preservation of confidentiality, integrity and availability of information in the cyberspace. [5]

Cyberspace: Complex environment resulting from the interaction of people, software and services on the internet by means of technology devices and networks connected to it, which does not exist in any physical form.

Cyber terrorism: Includes cyber-attacks by terrorists against nation states, business and commerce. It may also include a terrorist group trying to turn people against their own government, or a nation state

trying to unbalance another government. One way or another, it's all a form of terrorism designed to induce fear or to stir up hatred.

Cyber theft: Theft or a fraudulent activity conducted over cyberspace.

Cyber warfare: An attack on another nation state's information or infrastructure conducted over cyberspace.

Data: A collection of values assigned to base measures, derived measures and/or indicators. [1]

Disaster recovery (DR): A coordinated activity to enable the recovery of IT systems and networks due to a disruption.

Event: The occurrence or change of a particular set of circumstances. [3]

Exploit or exploitation: A particular form of attack that takes advantage of one or more vulnerabilities, and in which a tried-and-tested method of causing an impact is followed with some rigour. Exploits are similar in nature to processes, but whereas processes are generally benign, exploits are almost always harmful.

Hazards: A source of potential harm. [3] They are frequently viewed as being natural, as opposed to human-made, events, including such things as severe weather and pandemics.

Impact: An outcome of an event affecting objectives. [3] This is also referred to as a consequence.

Information: An organised and formatted collection of data.

Information assurance: The process of ensuring that data is not lost when critical events or incidents occur. It is generally associated

with computer, cyber or IT security rather than the somewhat wider meaning of ‘information security’.

Information security: The preservation of confidentiality, integrity and availability of information. [1]

Information security incident: An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. [4]

Integrity: Property of protecting the accuracy and completeness of assets. [1]

Level of risk: The magnitude of a risk expressed in terms of the combination of consequences and their likelihood. [1]

Likelihood: The chance of something happening. [3] The terms ‘likelihood’ and ‘probability’ are often used interchangeably, but ‘likelihood’ is a rather general term denoting a degree of uncertainty, whereas the term ‘probability’ has a more statistical underpinning. The term ‘possibility’ is generally not used, since many things are possible, but the term gives no indication whether or not the event is actually likely to take place.

Malware payload: Malicious code that can cause harm to the victim. Malware payloads can be distributed by methods such as worms and emails. Malware authors typically encrypt the payload to hide the malicious code from malware detection systems.

Monitoring: Determining the status of a system, a process or an activity. [2]

Non-repudiation: The ability to prove the occurrence of a claimed event or action and its originating entities, in order to resolve disputes about the occurrence or non-occurrence of the event or action and involvement of entities in the event. [1]

Objective: A result to be achieved. [1]

Organisation: A person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives. [1]

Policy: The intentions of an organisation as formally expressed by its top management. [1]

Probability: The measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty. [3]

Process: A set of interacting activities, which transforms inputs into outputs. [1]

Resilience: The adaptive capacity of an organisation in a complex and changing environment. [3] Although this definition refers to organisations rather than to information assets, the definition holds true in that where an information asset is properly protected, it is able to resist certain threats. However, to make an information asset fully resilient may be a very complex task and require several different methods of protection.

Review: An activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives. [1]

Risk: The effect of uncertainty on objectives. [3] Risk is the product of consequence or impact and likelihood or probability, and is not the

same as a threat or hazard. In the context of information risk management, risk is usually taken to have negative connotations. In the wider context of risk, however, it can also be seen in a positive light and referred to as ‘opportunity’.

Risk acceptance: The informed decision to take a particular risk. [3] Risk acceptance (or risk tolerance) is the final choice in risk treatment once all other possible avenues have been explored. This is not the same as ignoring risks – something that should never be done.

Risk analysis: The process to comprehend the nature of risk and to determine the level of risk. [3] This is the part of risk assessment where we combine the impact and the likelihood (or probability) of a risk to calculate the level of risk in order to plot it onto a risk matrix, which allows us to compare risks for their severity and to decide which are in most urgent need of treatment.

Risk appetite: The amount and type of risk that an organisation is willing to pursue or retain. [3]

Risk assessment: The overall process of risk identification, risk analysis and risk evaluation. [3] This includes identification of the information assets and their owners; impact assessment; threat and vulnerability identification; likelihood assessment; risk analysis; production of the risk matrix; and finally risk evaluation.

Risk avoidance: An informed decision to not be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk. [3] Risk avoidance (or risk termination) is one of the four strategic options for risk treatment. Avoiding the risk should normally remove the risk completely but may leave the organisation with other challenges.

Risk evaluation: The process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. [3]

Risk identification: The process of finding, recognising and describing risks. [3]

Risk management: The coordinated activities to direct and control an organisation with regard to risk. [3]

Risk matrix: A graphical representation of impact versus likelihood used to assist in the prioritisation of risks.

Risk modification: Risk modification (or risk reduction) is the process of treating risk by the use of controls to reduce either the consequence/impact or the likelihood/probability. Sometimes the term ‘risk treatment’ is used in this context, but risk treatment is really a generic term for all four kinds of strategic control. Strangely, ISO Guide 73 does not attempt to define risk modification or reduction, although it does refer to it under the definition of ‘control’.

Risk reduction: See ‘Risk modification’.

Risk retention: The acceptance of the potential benefit of gain, or burden of loss, from a particular risk. [3] Once risks have undergone the risk treatment process, there may be some outstanding risk that cannot be further reduced, transferred or eliminated. This is referred to as ‘residual risk’, and risk retention is the ongoing process of accepting and managing this.

Risk review: The activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives. [3]

Risk sharing: A form of risk treatment involving the agreed distribution of risk with other parties. [3]

Risk termination: An informed decision to not be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk. [3]

Risk tolerance: An organisation or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives. [3]

Risk transfer: Risk transfer (or risk sharing) is a form of risk treatment involving the agreed distribution of risk with other parties. [3] One of the strategic risk treatment options is to transfer the risk to or to share it with a third party. Transferring or sharing the risk, however, does not change ownership of the risk; it remains with the organisation itself, regardless of who else shares the risk.

Risk treatment: The process to modify risk. [3] While this may be technically correct, risk modification is just one form of risk treatment, and alternatively may involve risk transference or sharing, or risk avoidance or termination.

Stakeholder: A person or organisation that can affect, be affected by, or perceive themselves to be affected by, a decision or activity. [3]

Threat: The potential cause of an unwanted incident, which may result in harm to a system or organisation. [1] Whereas hazards are generally viewed as natural events, threats are usually human-made, whether accidental or deliberate, and may include such things as sabotage and cyber-attacks.

Threat actions: The actual attacks. These are often not a single isolated event, but can consist of many discrete activities, involving

surveillance, initial activities, testing and the final attacks.

Threat actor or threat agent: An individual or group of individuals who actually execute a cyber-attack.

Threat analysis: The process of understanding the level of threat – this is referred to in more detail in Chapter 6.

Threat consequences or impacts: The results or impacts of a cyber-attack, which we deal with in Chapter 4.

Threat source: A person or organisation that wishes to benefit from attacking an information asset. Threat sources often pay or otherwise pressurise threat actors to attack information assets on their behalf.

Threat vectors or attack vectors: Tools, techniques and mechanisms by which an attacker conducts the attack on their target.

Vulnerability: The intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence. [1] Vulnerabilities or weaknesses in or surrounding an asset leave it open to attack from a threat or hazard. Vulnerabilities come in two types – intrinsic vulnerabilities, which are something inherent in the very nature of an information asset, such as the ease of erasing information from magnetic media (whether accidental or deliberate), and extrinsic vulnerabilities, which are those that are poorly applied, such as software that is out of date due to a lack of patching.

Sources of standards information:

[1] ISO/IEC 27000:2020 – *Information technology – Security techniques – Information security management systems –*

Overview and vocabulary.

[2] ISO 22301:2019 – *Societal security – Business continuity management systems – Requirements.*

[3] ISO Guide 73:2009 – *Risk management – Vocabulary.*

[4] BS ISO/IEC TR 18044:2004 – *Information technology – Security techniques – Information security incident management.*

[5] ISO/IEC 27032:2012 – *Information technology – Security techniques – Guidelines for cybersecurity.*

INDEX

Page numbers in italics refer to figures or tables.

CYBER SECURITY

The complete guide to cyber threats and protection
Second edition

David Sutton

Cyber security has never been more essential than it is today; it's not a case of if an attack will happen, but when. This brand new edition covers the various types of cyber threats and explains what you can do to mitigate these risks and keep your data secure. *Cyber Security* explains the fundamentals of information security, how to shape good organisational security practice, and how to recover effectively should the worst happen.

This second edition has been updated to reflect the latest threats and vulnerabilities, including updates to standards, good practice guides and legislation. Written in an accessible manner, *Cyber Security* provides practical guidance and actionable steps to better prepare your workplace and your home alike.

- **A valuable guide for current professionals at all levels as well as for those wishing to embark on a cyber security profession**
- **Offers practical guidance and actionable steps for individuals and businesses to protect themselves**
- **Highly accessible with terminology that is clearly explained and supported with current, real-world examples**

ABOUT THE AUTHORS

David Sutton's career in IT spans nearly 55 years and includes voice and data networking, information security and critical information infrastructure protection. He is a Chartered Fellow of BCS, a Member of the Chartered Institute for Information Security (CIISec) and a Freeman of the Worshipful Company of Information Technologists (WCIT).

You might also be interested in:

A very comprehensive primer on cyber security covering issues, solutions and suggestions for further action.

Susan Perriam MBA MSc CMgr MBCS CISSP, Cyber Security Consultant

This latest revision is packed with recent examples, scenarios, tools, and techniques that make it a fascinating read for both industry veterans and recent joiners alike. Highly recommended.

Martin King FBCS CITP CISSP, Chief Technology Officer

This blended use of theory and practical applications sets this book apart, complements industry-leading certifications and makes it a must-read for anyone working within cyber.

Gary Cocklin CITP CISSP, Senior Cyber Security Practitioner, UK Royal Air Force (RAF)

Information Technology

bcs
The Chartered Institute for IT

Paperback available