Cyber Security Predictions

for 2024

A look forward to the coming year

Huntsman®

Defence-Grade Cyber Security

Introduction

Organisations, and security teams, are still having to respond rapidly to changing business, technology and geo-politics environments. The COVID pandemic, the war in Ukraine, the growing unrest in Gaza and Israel, and the wild swinging of political pendulums everywhere are making the world an unsettled place.

The dramatic events of the last few years have certainly made things more opaque and future trends more difficult to anticipate. Cyber security too, is increasingly like an Infinite Game[1], where the closest thing to winning is staying in the game, with the aim of becoming more resilient in a volatile environment.

We are still experiencing the legacy of a 1-in-100yr pandemic. Interest rates are at 22-year highs and inflation, the cost of living, and energy are all uncharacteristically high too. No wonder both consumer and business confidence has taken a hit. A recent government cyber security survey in the UK reported a reduction in the level of cyber-attacks amongst the majority of respondents. It turns out that the reduced levels of detection were because many small companies have chosen to reprioritise their security spending in these tough times.

The technology that has moved the needle this last year is, undoubtedly, generative Artificial Intelligence (AI) and AI more broadly. The ChatGPT service, launched just after last year's predictions paper, offers a natural language interface that enables conversations, the presentation of results and answers to questions. With the appropriate instruction it can even write essays or software code. The world has certainly changed in a very short time – with individuals, companies and governments all watching with a combination of excitement and trepidation to see what the future holds for this type of technology.

Looking to 2024 and beyond, we anticipate the following six areas will have noteworthy impact on the cyber security landscape:

1. **The need to consider AI benefits, risks and compliance frameworks.**
2. **Operational resilience requirements to hit boardrooms.**
3. **Corporate governance rules around cyber security will tighten.**
4. **"Data-driven cyber security" will digitally transform cyber risk management.**
5. **Continued emphasis on resolving the skills issue.**
6. **The "green shoots" of economic recovery continue.**

Click here to review our success with last year's predictions

[1] The Infinite Game, Simon Sinek, Portfolio, 2019

Huntsman®

Predictions for 2024

1 The need to consider AI benefits, risks and compliance frameworks

Artificial Intelligence (AI) is an obvious place to start our predictions for 2024. There are a number of areas where the continued rise of AI will have a big impact and these are the topic of much discussion; but let's look at cyber security.

One concern is the credible reports suggesting that threat actors are looking for new ways to extort organisations; and utilising malicious AI engines that can be trained to overcome traditional defence tactics and build code for various nefarious purposes. It's a troubling development, as leaders already battling to protect their organisations, will soon have the added threat of defending against AI enabled adversaries. There's even talk of emerging marketplaces where pre-generated AI phishing emails and malware can be made to order.

Current phishing tests and simulation training may not be enough to combat this new wave of generative AI malware. We predict it will take both the added fortification of cyber posture as well as further staff education and enhanced technologies for organisations to maintain their resilience.

On a slightly less unnerving note, leveraging traditional white-hat AI requires the input of key points of knowledge in order to generate content out of AI engines like ChatGPT.

The risk to organisations, lies in not knowing what information is being shared with AI engines to generate the output. This is a classic case of operational policies and legal guidelines, already running too far behind the nascent AI sector. The genie is already out of the bottle!

We are now seeing software developers utilising generative AI to develop code as a new path to increased productivity and output. Depending on the trustworthiness of the AI engine, it will require organisations to review cyber security policies and governance practices.

AI is already using synthetic data and training in the pharmaceutical and medical research space. As this becomes more mainstream, we anticipate the growing requirement for organisations to adopt data protection and intellectual property risk and compliance frameworks around AI usage.

Regulators in most jurisdictions are yet to exert formal guidance on lawful behaviour. Although in June 2023, the European Parliament passed the precursor to the Artificial Intelligence Act (the "AI Act"). The European Council is currently in the consultation phase[2]; but the intention is to limit the use of AI in activities that might limit or impact on an individual's rights or safety.

Will this lead to a security team that is better able to deal with the volume and complexity of today's threats? Or will it mean that fewer security resources are necessary, with AI systems to safeguard networks? It's hard to say right now. What is clear, however, is that AI in the hands of adversaries, will undoubtedly enhance their malicious capabilities. So, organisations should review the adequacy of their cyber governance policies and procedures.

[2] Lexology Library: Artificial Intelligence Act passed by the European Parliament

2 Operational Resilience requirements to hit boardrooms

Operational resilience will become the new mot du jour. The events of the last few years have shown us just how vulnerable businesses, and the uninterrupted provision of their goods and services, can be – organisations need to increase the rigour of their operational resilience efforts.

Initially in the finance sector, but ultimately, we predict that operational resilience will become a key component of corporate governance across other critical economic sectors.

Already the UK Financial Conduct Authority (FCA) and the Prudential Regulatory Authority (PRA) have published the FCA Operational Resilience Policy Statement PS21/3 for the finance sector. And in Australia, the Government has recently legislated Part 2A of the Security of Critical Infrastructure Act (SOCI Act) requiring critical infrastructure providers of all types (**see here**) to adopt a Risk Management Program to improve their operational risk management efforts.

The FCA Policy Statement PS21/3[3] notes that "cyber resilience is … *complementary* to operational resilience outcomes" and is an important component of a firm's operational resilience and prioritisation program. Monitoring methodologies should already be underway in the UK, and frequent monitoring and reporting is due by March 2025.

The equivalent Australian Prudential Regulatory Authority (APRA) Operational Risk Management Prudential Standard CPS 230 for the finance sector commences in July 2025. Again, risk appetite, definition of tolerance levels and systematic monitoring, analysis and reporting on their operational resilience (and those of their 3rd party providers) is required.

As part of operational resilience, it is important to understand that its nature and scope goes to governance frameworks and informed oversight of operational management. It is part of business as usual for the finance sector; contemplating a full range of operational risks.

"Operational disruptions [no matter the cause] can cause wide-reaching harm to consumers and pose a risk to market integrity, threaten the viability of firms and cause instability in the financial system."[4]

The new EU Digital Operational Resilience Act **(DORA)**[5] requirements look very similar. They are expected to be operational for Q4 2024. DORA clearly establishes senior management accountability for compliance and, like the others, requires the design and implementation of operational resilience governance processes to enable security and operational resilience assessment, risk management, and a better understanding of business tolerances to business service delivery.

Operational resilience requirements will be remarkably similar across governments in the next little while and we predict this requirement will broaden to other sectors quite quickly. Regulators are already reinforcing cyber security as a business issue; and cyber, like other operational risks that can sit outside the immediate control of an organisation, will become specific elements of operational resilience.

[3] https://www.fca.org.uk/publications/policy-statements/ps21-3-building-operational-resilience

[4] ibid

[5] https://www.digital-operational-resilience-act.com/

3 Corporate governance rules around cyber security will tighten

This is a prediction, that having appeared before, seems almost a given except that it is taking so long. The signs of a push towards better governance of organisations and cyber security are everywhere, although the formalisation of some governance rules is jurisdiction dependant.

We predict an uptick in regulatory focus on cyber governance, particularly in Western democracies. An interesting comparison of the status of cyber regulatory adoption can be found here.

At a recent cyber security conference in Sydney, the Chairman of the Australian Securities and Investments Commission (ASIC) warned that "if boards do not give cybersecurity and cyber resilience sufficient priority, [it will] create(s) a foreseeable risk of harm to the company and thereby exposes the directors to potential enforcement action by ASIC based on the directors not acting with reasonable care and diligence"[6].

In the UK the NIS critical infrastructure directive is likely to follow the path of the FCA Policy Statement PS21/3 and the finance sector. Imposing stiffer controls on some sectors and expanding its reach to new types of businesses like managed service providers, marketplaces and payment processors.

In the EU, things are likely to be similar. The introduction of DORA with its specific new oversight and governance requirements around operational resilience for the finance sector (See Prediction 2) will be matched in the NIS2 legislation introduced for the critical infrastructure sector earlier in 2023. The US White House published a National Cyber Security Strategy 2023 which focused on defending critical infrastructure, driving cyber resilience, and encouraged greater collaboration between stakeholders.

So, while regulatory bodies may provide compliance guidance, right now the insistence by insurers on particular controls being in place, and the desire for directors to meet their statutory obligations and protect their reputations (and those of their organisations) continues to drive cyber governance processes. The adoption of Operational Resilience[7] in the UK and EU is likely to change that with regulators, even beyond those in the finance sector, prescribing more specific governance requirements around cyber security and other operational risks.

Organisational leadership can no longer deflect responsibility for the effective management of security risk to other team members. Shortly they will be required to maintain a steady line of sight across all governance-level risks, especially cyber security, with an obligation to identify and protect an organisation's 'crown jewels' and their ongoing operational capabilities. As interpretation tightens around directors and their responsibilities, we expect to see further focus on cyber security – coming from the top down – in organisations everywhere in the coming year.

[6] https://www.smh.com.au/business/companies/watchdog-takes-aim-at-company-directors-over-cybersecurity-20230918-p5e5h9.html

[7] https://www.bis.org/fsi/fsisummaries/op_resilience.pdf

4 “Data-driven cyber security” will digitally transform cyber risk management

We observed in our 2023 predictions, that there remains an absence of digital transformation occurring across cyber security processes themselves. This is somewhat surprising given (i) the industry is suffering from a continuing lack of skilled practitioners; and (ii) the sheer scale, volatility and range of tasks required to protect organisations.

The market for solutions to provide cyber security posture reporting and attack surface management is validated. It's replete with a diverse set of solutions and claimed functionality. The truth is, however, that available offerings are firmly directed at technical buyers rather than risk and governance teams; with little available for executives and boards responsible. Some are top-down and use probabilistic determinations to establish risk while others detect varying attack vectors as they emerge from the bottom-up. Comparing the solutions is difficult and at times confusing; but ultimately it depends on the integrity of the information you choose to inform your cyber risk management practices. We predict that clarity will emerge in 2024 as directors seek to regularly verify their cyber risk and gain accurate and timely situational awareness to better inform their resilience and statutory reporting requirements.

Cyber security is a big data problem with thousands of endpoints and vulnerabilities contributing to a constantly changing array of potential attack vectors. With a seemingly infinite number of attack permutations, it's little wonder the sector is starting to talk about more scalable solutions.

The UK's National Cyber Security Centre's (NCSC) advice[8] lays a solid foundation for the digital transformation of cyber security controls assessment. It advocates a move away from informal, infrequent, and ad hoc methods of security reporting to a more systematic and objective process that gathers data, analyses it, and generates appropriate outputs across all key controls. The process can even be automated to enable an efficient, timely and reliable approach.

Progress towards operational resilience in the UK and Europe and the looming deadline for NIS2 will require streamlined cyber security management methods that can only realistically be met using automated and data-driven processes. Scale and timeliness are quickly becoming major issues for existing “resource intensive” security practices. So too in Australia, where only systematic and data-driven cyber solutions will enable organisations to meet some of their mandatory obligations under the SOCI Act. Without these newer digital techniques that embrace scientific methods, the qualitative assessments and anecdotal judgements so common right now, will remain unable to provide the more rigorous governance sought by more recent cyber laws.

The growing imperative from these global legislative developments is that cyber and operational risk management need to be embedded in an organisation's business strategy – part of regular business-as-usual resilience activities - rather than as stand-alone or annual tasks.

The value of automated, data-driven security information systems for volatile threat environments is now clear; and we think digital cyber management techniques will be recognised as the fit for purpose solution in the next 12 months.

[8] https://www.ncsc.gov.uk/blog-post/data-driven-cyber-transforming-cyber-security-through-an-evidence-based-approach

5 Continued emphasis on resolving the skills issue

The skill shortages in cyber security have been obstructing the security efforts and control effectiveness of many organisations for a number of years.

Until recently, cyber security posture was an anecdotal assessment arrived at by a "security expert", rather than a "granular" but measurable assessment of the potential attack vectors that threaten an organisation. **But to manage resilience, we predict that new technologies and practices (see Prediction 4) will shift the demand for skills considerably.**

Reports indicate that cyber security and AI skills are in high demand in Australia[9] this year, and in the UK 50% of all businesses have a cyber security skills gap[10]. This may prompt a rising sense of dread in any HR team, but, the growing shift to digital innovation and automation should provide a sense of hope for organisations. As we head into 2024, we believe that workforce growth will not be the only means of improving cyber compliance. Digital automation will bring about more "fit for purpose" solutions. As with all good catalysts for revolution, this adverse pressure around staffing skill shortages will bring about smarter work practices that can scale to meet the changing demands for the effective management of cyber security.

Technical innovation and process redesign to better leverage the growing power, speed and analytical capabilities of machines, is undoubtedly the way forward. Cyber security systems and processes that rely on high levels of specialist consulting and interpretation (rather than evidence) are no longer fit for purpose - they just won't scale to the task at hand.

While executives are looking to improve the quality of their risk information to enhance their cyber hygiene and risk governance processes; skill shortages are impacting those ambitions. Poor cyber hygiene levels continue to be observed by regulators everywhere[11] and executives and boards are being told to act. Cyber security runs at machine speed and frankly humans, even skilled ones, are unable to keep up.

Recent requirements by the US Securities Exchange Commission (SEC) that US listed entities disclose any material cyber incidents in their environment within 4 days, confirms the problem[12] – organisations that rely on arbitrary manual risk assessments, audit sampling and probabilistic risk assessment cannot make these pronouncements quickly and with confidence. Fundamental changes in current risk assessment and analysis methods are required for an organisation to fulfil these time-sensitive analysis and reporting obligations – at scale and frequency.

The predicted adoption of data-driven solutions and automated, evidence-based reporting will change the sector. It will allow less skilled technicians to enter the market - interpreting, responding and managing large parts of the cyber security process. And it will enable existing security professionals to address more pressing needs, attending to outliers - exceptions, and high-level analytical problems that we will always face.

[9] AIIA's Digital State of the Nation 2023 survey

[10] https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2023

[11] https://www.cisa.gov/news-events cybersecurity-advisories/aa23-215a

[12] https://www.sec.gov/news/press release/2023-139

6 The "green shoots" of economic recovery continue

After a turbulent few years for the world economy, 2024 is touted as being the year when things should become calmer and less punishing overall. The International Monetary Fund is predicting modest global growth overall[13], and with this comes a sense of stability after the economic upheavals since early 2020.

That said, as we finalise these predictions, recent events in the Middle East and geo-political turbulence in a number of countries are casting long shadows across significant parts of the global economy.

For those of us in cyber security – both suppliers and security teams trying to defend networks, systems, and data – we predict a growing need to work with flexibility and adaptability. Gartner is anticipating a 14% growth in global security and risk management spending in the coming year[14] - a likely result of digital transformation starting to impact parts of the cyber security sector.

With expectations that the sector delivers velocity, scope and process integration, and keeps up with changes in skilled staff availability, investment in cyber-physical systems is inevitable for security systems and processes to continue to maintain security controls and safeguard operations.

As we were reminded over the pandemic period, the risks faced by business and individuals fall more acutely on those with less ability and resources to protect themselves; and that applies whether it's the cost of living or cyber security investments. The limited availability of cyber insurance for those without adequate security controls will ensure that smaller businesses – those with smaller cyber budgets and less well-resourced IT and security teams - have relatively more to lose, than larger ones. Yet 98%-99% of UK and Australian businesses are small. And in an interconnected economy, supply chain risks, potentially due to security under-investment, should not be under-estimated by any of us.

At a recent cyber insurance innovation forum in London in September 2023, the NCSC revealed, not surprisingly, that State actors were becoming increasingly active in the security space.

But more telling, was the observation that in general most cyber-attacks were opportunistic; when adversaries having observed poor security controls, took immediate advantage of that fact.

The takeaway was clear: for those seeking to maximise their cyber return on investment – ensure your controls are operating as effectively as you can afford. The likelihood of becoming a cyber-attack victim is directly related to those efforts. And as your business expands again ensure that it is accompanied by an appropriate refresh and upscaling in your security processes, tools, and reporting systems.

[13] https://www.imf.org/en/Blogs/Articles/2023/10/10/resilient-global-economy-still-limping-along-with-growing-divergences

[14] https://www.gartner.com/en/newsroom/press-releases/2023-09-28-gartner-forecasts-global-security-and-risk-management-spending-to-grow-14-percent-in-2024

Summary

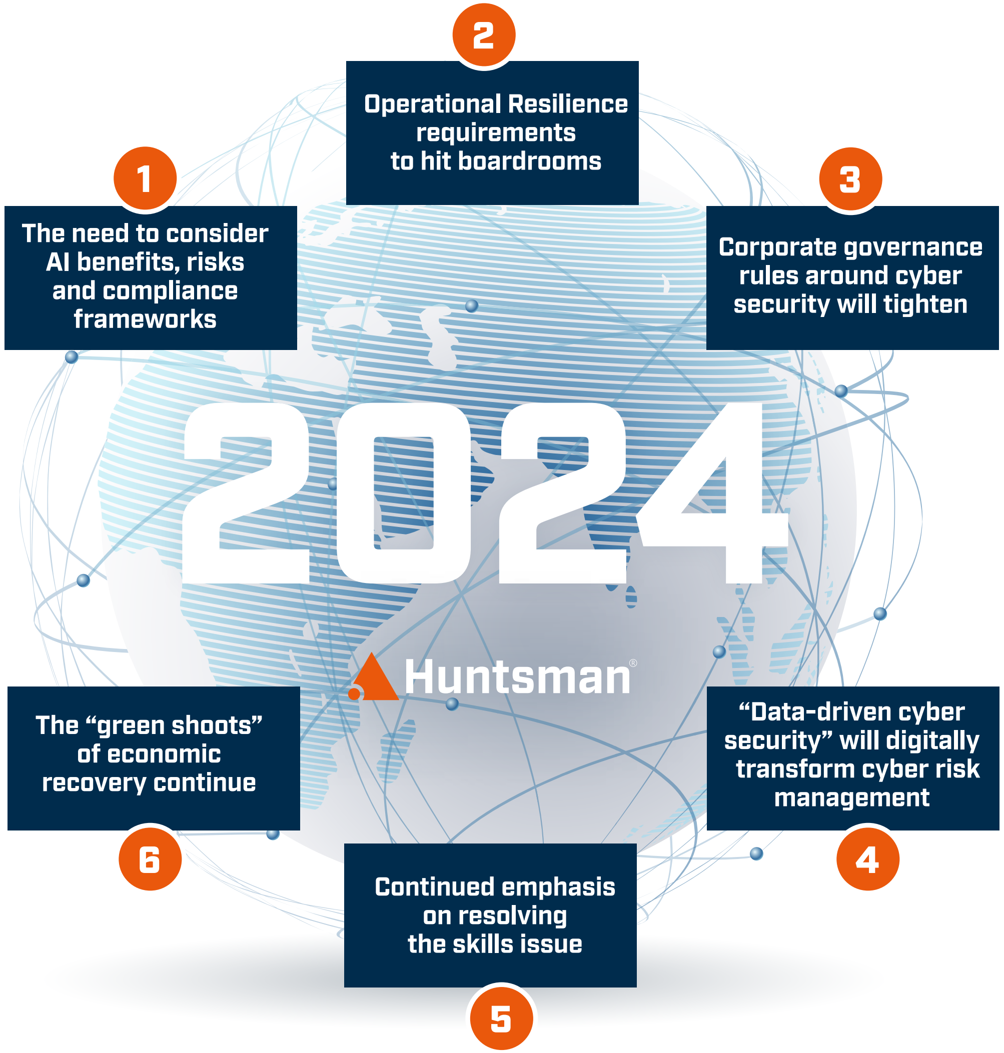
As every year, the technological predictions, the changing threat landscape and the economic and political environment all combine to affect the way security teams work and what their priorities are.

In the last 12 months, the continuing war in Ukraine, the rise of AI and the economic conditions around the globe have caused huge disruption, and that isn't going away any time soon. The effects of the events of the last few years will echo for the next few.

What we've covered here are the six areas and changes that we feel will be most pivotal for cyber security leaders and teams, and the organisations they work for, over the next 12 months.

Huntsman Security

Cyber Security Predictions for 2024



1. The need to consider AI benefits, risks and compliance frameworks
2. Operational Resilience requirements to hit boardrooms
3. Corporate governance rules around cyber security will tighten
4. "Data-driven cyber security" will digitally transform cyber risk management
5. Continued emphasis on resolving the skills issue
6. The "green shoots" of economic recovery continue

Appendix Last Year's Predictions

As we look back at our 2023 predictions, we note that some occurred as we'd expected, some not so much while others didn't really happen at all. In several cases, however, we would ask for your indulgence because while they didn't happen as predicted we think they're still valid for the coming year.

? Cyber security posture management and attack surface management rise to greater prominence

This segment of the cyber security technology market will continue to develop, although the full utility of cyber posture management is yet to be realised. Responsibilities for the management of cyber security are not clearly understood – but this is likely to change in this coming year as the responsibilities of senior executives and directors are better defined. Regulatory pressure, and a growing need to understand security and other operational risks will move the market in the next 12 months (**See Prediction 2**).

✓ Cost of living and economic factors are a major problem for governments and citizens everywhere

This has certainly been the case in the UK, parts of Europe and elsewhere. The reliance on gas and fuel from Russia and even grain from Ukraine for some, has impacted pricing structures, global supply chains and food security for many. Inflation has been a significant challenge, and while Central banks are bringing it under control, the question of whether it was supply or demand side driven is only of academic interest for most.

✓ Pressures on small and medium-sized businesses (SMBs) will lead to a squeeze on investment, including in security

Cost pressures have impacted budgets everywhere. We spoke earlier of a UK Government survey which observed that the majority of smaller businesses had reduced their cyber security investments until cost pressures subsided. One can only conclude that cyber resilience for many organisations has fallen and some will remain at risk for a little time yet.

✗ Cyber insurance will still drive security control improvements, reporting and security oversight

The impact on cyber security from cyber insurance has been more muted than we foresaw. The introduction of "mandatory controls" and cyber security questionnaires as part of your cyber insurance proposal has successfully enabled insurers to limit much of their own risk around the adequacy of security controls. So perhaps cyber insurers will continue to drive security investment and oversight but, perversely, only for those who have realised their level of residual cyber risk and the need to improve their efforts to better manage it.

? Corporate governance rules around cyber security will converge across jurisdictions

The evolution of cyber governance continues to vary across jurisdictions. There is evidence of the tightening of oversight obligations for organisations and their directors everywhere – although progress is less consistent than anticipated. We would argue that while a common vision for cyber governance is emerging across Western democracies the trajectory of those efforts is variable. Cyber risk governance has had significant focus in Australia[15] and even the US[16] for example, but the UK is currently less prescriptive in much of its efforts, despite a growing recognition of cyber risks at all levels in the UK[17].

✓ More joint advisories, and convergence in cyber security advice and guidance

There have certainly been a number of significant joint advisories issued by national agencies in 2023. While all Western intelligence and cyber security agencies aren't quite speaking with one voice, there is continued and visible coordination and cooperation. Recent examples include publications on state-sponsored attacks on CNI and commonly exploited vulnerabilities.

✓ APIs will increasingly be the way in which companies and systems interact; security will have to keep up

The increased use of API-based interactions is evident. This is the continuation of a trend for systems, applications, and businesses to allow systems to interact directly, rather than forcing users to manually interact with multiple platforms. As organisations continue to transform their business to improve performance and efficiencies, the inter-connectivity between APIs and their associated security implications will become part of cyber resilience.

✓ Growing recognition of the importance of cyber security in Critical Infrastructure (CI)

The importance of CI and the risks from attacks on it have never been more apparent. There have been a number of reminders internationally about the vulnerability of CI assets everywhere. The US CISA strategic plan is only one[18]. Legislative changes in Australia, earlier in the year, to increase the positive cyber security obligations for the CI sector under SOCI Act, Part 2A[19] too confirms the growing priority of CI for governments everywhere.

✓ Cyber security coming of age with a shift from eminence to data-driven decision making

This was a prediction that was spot on; although "optimistic bias" continues to be problematic when it comes to security self-assessment. The shift from qualitative to evidence-based risk assessment is, however, gaining momentum. In Australia the December 2022 release of the ACSC IT risk assessment process guide[20] and the UK NCSC, April 2023 publication of "Data-driven cyber: transforming cyber security through an evidence-based approach"[21] confirm the shift from eminence to evidence-based assessment and reporting.

[15] https://www.aicd.com.au/risk-management/framework/cyber-security/king-and-wood-mallesons-international-comparison-of-cybersecurity-obligations.html

[16] https://www.itnews.com.au/news/us-sec-adopts-new-hack-disclosure-rule-598490

[17] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

[18] https://www.cisa.gov/sites/default/files/2023-08/FY2024-2026_Cybersecurity_Strategic_Plan.pdf

[19] https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/cisc-factsheet-risk-management-program.pdf

[20] https://www.cyber.gov.au/sites/default/files/2023-08/PROTECT%20-%20Essential%20Eight%20Assessment%20Process%20Guide%20%28August%202023%29.pdf

[21] https://www.ncsc.gov.uk/blog-post/data-driven-cyber-transforming-cyber-security-through-an-evidence-based-approach

About Huntsman Security

Since 1999, Huntsman Security has been on the cutting-edge of cyber security software development, serving some of the most sensitive and secure intelligence, defence and criminal justice environments in the world.

Huntsman®

HUNTSMAN | TIER-3 PTY LTD

ASIA PACIFIC
t: +61 2 9419 3200
e: info@huntsmansecurity.com

Level 2,
11 Help Street
Chatswood NSW 2067

EMEA
t: +44 845 222 2010
e: ukinfo@huntsmansecurity.com

7-10 Adam Street,
Strand
London WC2N 6AA

NORTH ASIA
t: +81 3 5953 8430
e: info@huntsmansecurity.com

GINZA EAST SQUARE 4F
3-12-7 Kyobashi Chuoku, Tokyo
Japan 104-003

huntsmansecurity.com linkedin.com/company/tier-3-pty-ltd twitter.com/Tier3huntsman