Mapping the Coverage of Security Controls in Cyber Insurance Proposal Forms

Article *in* Journal of Internet Services and Applications · August 2017

DOI: 10.1186/s13174-017-0059-y

4 authors:

Daniel W Woods
The University of Edinburgh
43 PUBLICATIONS **374** CITATIONS
SEE PROFILE

Ioannis Agrafiotis
University of Oxford
54 PUBLICATIONS **1,005** CITATIONS
SEE PROFILE

Jason R. C. Nurse
University of Kent
205 PUBLICATIONS **4,162** CITATIONS
SEE PROFILE

Sadie Creese
University of Oxford
175 PUBLICATIONS **3,046** CITATIONS
SEE PROFILE

RESEARCH ARTICLE

Mapping the Coverage of Security Controls in Cyber Insurance Proposal Forms

Daniel Woods*, Ioannis Agrafiotis, Jason R.C. Nurse and Sadie Creese

Abstract

Policy discussions often assume that wider adoption of cyber insurance will promote information security best practice. However, this depends on the process that applicants need to go through to apply for cyber insurance. A typical process would require an applicant to fill out a proposal form, which is a self-assessed questionnaire. In this paper, we examine 24 proposal forms, offered by insurers based in the UK and the US, to determine which security controls are present in the forms. Our aim is to establish whether the collection of security controls mentioned in the analysed forms corresponds to the controls defined in ISO/IEC 27002 and the CIS Critical Security Controls; these two control sets are generally held to be best practice. This work contains a novel research direction as we are the first to systematically analyse cyber insurance proposal forms. Our contributions include evidence regarding the assumption that the insurance industry will promote security best practice. To address the problem of adverse selection, we suggest the number of controls that proposal forms should include to be in alignment with the two information security frameworks. Finally, we discuss the incentives that could lead to this disparity between insurance practice and information security best practice, emphasising the importance of information security economics in studying cyber insurance.

Keywords: Business security; security controls; cyber insurance; SANS20 controls; ISO/IEC 27000 series

1 Introduction

Insurers are taking on liability for ever more cyber risk; a 2015 report revealed that cyber insurance gross written premiums now stand at over $2 billion [1]. The same report reveals that demand for cyber insurance is expected to double by 2020. This is unsurprising given that company boards are beginning to better understand the nature of the risks that they face and realise the existence of gaps in traditional insurance coverage, as can been seen in a 2015 Cyber Risk Survey Report commissioned by Marsh [2]. For example, a 2015 study of 350 companies from 11 countries revealed the average cost of a data breach is $3.8 million [3]. While data breaches take the headlines, there are a multitude of other risks ranging from cyber extortion to unintended virus propagation, many of which can be covered by a range of new cyber insurance policies [4].

Despite soaring demand, underwriters are struggling to understand each consumer's cyber risk profile; a 2015 Cyber Liability Insurance Market Trend report showed the number one barrier to selling cyber policies is 'not understanding exposures' [1]. Getting this process wrong can be very costly. Target$^{\text{TM}}$ were reimbursed $90 million by their insurer following their 2013 data breach [5]. Traditional insurance techniques involve creating actuarial tables of loss histories across defined risk profiles. These are inapplicable for two reasons, the first being that insurers do not know the properties and attributes which delimit different risk profiles, while the second is that insurers do not have the loss history data to create the actuarial tables. In fact, relevant loss history may never exist given the dynamic nature of cyber risk. At present, all that insurers can rely on to quantify cyber risk is the information they collect in the assessment process. However, the evidence regarding the presence or not of specific security controls that insurers require in these assessment processes may have further consequences.

It is suggested that security decisions driven by insurers inform policy discussions in the US [6], the UK [7] and the EU [8]. Implicit in these discussions is the assumption that the insurance industry can have a meaningful and positive impact on the management of cyber security. One argument in support of the assumption is that insurers have been successfully dealing in risk for hundreds of years. A more fine-grained view of the insurance industry reveals that

*Correspondence: daniel.woods@cybersecurity.ox.ac.uk
Department of Computer Science, University of Oxford, Oxford, UK
Full list of author information is available at the end of the article

there have been examples of insurers making systemic oversights. For example, the solicitors' professional indemnity market saw prominent insurers 'move away from the bottom of the market' during the 2010 crisis as the Irish insurer Quinn fell into administration [9]. With this in mind, the assumption that cyber insurance will have a positive impact on security posture of organisations requires further investigation.

The aim of this paper is to explore how well the current cyber insurance assessment process aligns with established network security best practice, as provided by the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) 27002 and the Center for Internet Security (CIS) Critical Security Controls Version 6.0. Our approach investigates insurance proposal forms, a self-assessed questionnaire that applicants are expected to complete as an initial part of the cyber insurance application process. The key value of the results of our study is that they allow us to highlight neglected aspects of the assessment process. This can inform policy-makers by providing empirical evidence as to the success of cyber insurance in promoting established risk management standards. Further, it can help cyber insurers refine the assessment process grounded in security best practice.

Our paper is structured as follows: in Section 2 we outline how the insurance industry has developed, the coverage offered presently and the industry's method of assessment. Section 3 reviews related work on cyber insurance from a range of disciplines. Section 4 details our methodology, which focuses on one aspect of the assessment process and analysing self-assessed proposal forms. In Section 5, we compare the security controls that the insurance application process focuses on with the controls in the CIS Critical Security Controls and ISO 27002 frameworks. Section 6 provides a discussion of these results, and centres around lessons to be learned. Section 7 concludes with a discussion of how the assessment process will have to adapt to a changing market; particularly how an increase in demand from smaller businesses could lead to a greater reliance on the self-assessed forms analysed in this paper.

2 Cyber Insurance Industry

The first standalone Internet-based insurance policies were the hacker insurance policies of the late 1990s, in which an insurer partnered with a technology company to offer a policy covering the insured firm's first party loss [10]. As firms outside the technology industry became increasingly dependent on their networks, it became clear that the coverage which traditional policies offered left significant gaps. For example, most business insurance policies used to cover tangible property often exclude liability relating to electronic data loss [11]. In response to this, insurance companies started to offer standalone cyber insurance policies. These policies are broken down into a number of sub-policies, with coverage offered for a specific set of risks. For example, First-Party Coverage covers the 'the cost of replacing or restoring lost data'. Table 2 includes the most common coverage and the risks that it provides liability for, it was chosen on the basis of studies of insurance policies [10, 12, 13]. The range of coverage found in Table 2 will form an *extensional definition* for cyber insurance.

The current market for standalone cyber insurance consists of insurers offering coverage to large companies. In the US, we find that 26% of companies with a revenue of $5 billion or more have cyber insurance, in stark contrast to less than 3% of those who return less than $500k [14]. In the UK, a 2015 report revealed that 2% of large companies use standalone cyber insurance while cyber insurance penetration is 'negligible' for smaller firms [15]. The demand for cyber insurance among smaller may increase. Smaller firms see a 'higher incidence of Cyber Crime' and the three biggest risks that smaller firms face are business interruption, privacy events and fraud [15]. Further, the current cyber insurance coverage offered, as detailed in Table 2, covers these risks.

There is a danger that a firm may apply for cyber insurance in the knowledge that they have little security infrastructure in place. This is the problem of adverse selection — which occurs when a more informed party engages in strategic behaviour at the expense of another party they are in contract with. Insurers address this issue via extensive ex-ante assessment, which involves collecting information on an applicant, in order for an underwriter to classify the applicant into a given risk category and then set the insurance premium [16]. Much of this information is collected in a questionnaire filled out by an applicant, known as a proposal form. Table 3 contains a selection of the information that these forms seek to collect, along with the questions asked. For example, the insurer seeks information relating to the type of data collected by the applicant, via the question 'Do you store, process and/or transmit any Sensitive Data on Your Computer System (Tick all that apply)'. These were selected to give the reader an insight into the questions asked, a full picture can be found by investigating the forms presented in Table 1.

It is common practice to supplement this form with further assessment such as on-site audit and/or interviews with senior technology (IT) staff [17]. This supplementary assessment focuses on network security design and implementation, alongside organisational culture [16]. The aim of our paper is to assess the questions relating to the applicant's security controls in the self-assessed proposal forms. Our analysis will not consider more general information such as the applicant's financial situation, type of data collected or previous loss history. We believe that the self-assessed forms provide a scalable assessment process that could help meet increased demand from smaller businesses.

3 Related Work

Cyber insurance has been part of academic discussion since Dan Geer first advocated for risk management techniques [18]. Bruce Schneier outlined his vision of cyber insurance detailing how security decisions are driven by an insurer's checklist and the corresponding insurance premium [19]. The benefits of such an approach have become consensus in the literature and it appears increasingly representative of the reality of industry. We draw a distinction between two bodies of academic work; the first tends to focus on the insurance market at large, the second is a multidisciplinary look at individual cyber insurance policies.

The first is a stream of literature of the field of Security Economics, which was founded upon the realisation that misplaced incentives play a part in explaining why many security systems fail [20]. In this vein, various works conclude that insurers offering reduced premiums provides incentives for security investment, which corroborates Schneier's early predictions [17, 21, 22]. There have been many attempts to model different aspects of the insurance market. A unifying framework is provided by Böhme et al. [23], which draws a distinction between two aspects of the market. First of all, the focus on how security investments accrue benefits to all parties in a system, not just the investor— particularly, how these positive externalities can reduce the risk an insurer faces [24–27]. Secondly, there have been various considerations of systemic risk, in which many firms make claims arising from the same event because of the interdependency of networks [28–30].

In addition, information asymmetries are considered in the context of principal-agent problems. Moral hazard, in which an agent engage in riskier behaviour because they know a principal protects them from the consequences, is explored by Shetty et al. [31]. Bandyopadhyay et al. consider the situation where the insured chooses not to report an incident because the amount of indemnity received is smaller than the costs relating to reputation damage [32]. The problem of adverse selection, which we discussed earlier, is examined in the literature. For example, if a firm knows they are relatively exposed to cyber risk they are more likely to seek cyber insurance [33]. It is suggested that this will lead to expensive premiums across the market [34]. Our work directly addresses the problem of adverse selection by analysing the information collected that insurers use to determine the applicant's exposure to cyber risk.

The second body of work focuses on investigating cyber insurance policies. Parts of insurance literature provide an analysis of the insurability of cyber risks using the KARTEN framework [35] and the Berliner insurability framework [36]. This analysis reveals that 'Randomness of loss occurrence' and 'Information asymmetry' are problematic aspects of cyber insurance. As 'Information asymmetry' relates to adverse selection and moral hazard, this supports the results of the first body of literature. In addition, this stream of literature considers gaps in traditional policies [37]. Legal scholarship reflects on the issue of tangible property and data [11] and whether liability covers international cyber torts [38]. Business literature investigates the role of insurance within a risk management strategy [39], how insurers deal with moral hazard [16] and the type of coverage available [4]. There is further work analysing cyber insurance policies to understand coverage offered. Six policies are examined by Baer et al. [12], 14 are analysed by Marotta et al. [13] and Majuca et al. [10] focus on 7 different policies offered by AIG. We used these analyses of coverage to form our definition of cyber insurance.

We believe there is much to be gained from pooling the knowledge of these two bodies of work. The broad explanatory power of the Security Economics work can inform the empirical research undertaken in much of the second body of literature. Equally this second body can provide the empirical data to help refine the theory in the Security Economics literature. Our paper fits into the second body of work because we focus on the business processes of a cyber insurer. More specifically, we aim to analyse the effectiveness of the insurer's assessment, with a view to mitigating the adverse selection problem. We do this through the analysis of 24 different proposal forms. To our knowledge, this is the first time any such proposal forms have been systematically analysed in such a volume.

4 Methodology

In this paper we analyse 24 cyber insurance proposal forms, each corresponding to a different cyber insurance policy offered by a UK or a US insurance firm. These forms were chosen because they were publicly available, which provides an opportunity to investigate the initial part of the assessment process. The subsequent stages which involve processing and analysing the forms, as well as further assessment via on-site audit or telephone interview, require privileged access to much of what insurers consider intellectual property.

The proposal forms were all created between 2008 and 2016, with 20 of our forms being created in the last four years. Some examples of the forms considered include those from AIG [40], Hiscox [41], Great American Insurance Group [42], ACE Insured [43] and CFC Underwriting [44] and the full spectrum can be found in Table 1. These organisations fall into two categories; underwriters and brokers. An underwriter decides whether to offer the client a policy, receives the premium and takes on the responsibility of paying the insured's claims. A broker will represent one or more underwriters by brokering the deal between the insurer and the insured. The analysed forms are offered by a mixture of underwriters and brokers and consisted of 14 underwriters offering 16 policies and 8 brokers offering 8 policies.

The sample of proposal forms was collected by searching publicly indexed web page results. This search looked for variations upon, and not limited to, 'cyber security insurance proposal form'. These forms were collected using new search terms or more results for the same search term. The search ended when either of these stopped revealing new proposal forms. Forms not offered by a UK or US company, or forms that were offered outside the UK and US, were considered out of scope. Our rational being that these two countries are leading the cyber insurance market globaly [14, 15]. Many of the international forms were adaptations of the parent company's forms offered in the US or the UK. The forms were analysed using the ISO/IEC 27002 (ISO) and CIS Critical Security Controls frameworks.

The proposal forms were investigated using a form of content analysis known as deductive thematic analysis [45]. We selected a qualitative content analysis in order to build a conceptual model to describe the process of assessment in the insurance application process. This was chosen over a quantitative approach because we are trying to infer from the questions what information the forms seek to collect; a qualitative analysis can better capture these "meanings and intentions" [45]. While some have described content analysis as a "counting game" [46], others have identified its ability to "identify critical processes" [47]. A deductive approach was chosen because the themes, which are perceived as concepts by which models are structured, are provided by existing knowledge, avoiding issues related to their creation with other approaches [45].

ISO/IEC 27002 is an internationally recognised security management scheme [48]. It contains 19 sections, of which we focus on sections 6 to 18 as these contain actionable security controls. ISO/IEC 27002 was chosen over other standards in the 27000 series as it prescribes detailed controls, which are not applicable to a particular organization. This allows us to consider proposal forms without worrying about the specific organisations that they are intended for. The Center for Internet Security (CIS), led the development of the CIS Critical Security Controls (CSC). This involved a process of engagement with individuals, from a range of sectors and a range of roles, to ensure they are a 'prioritized, highly focused set of actions' [49]. We chose the CIS' CSC 20 Controls because they provide a more detailed perspective, as compared to ISO 27002, but can also be essential at identifying infrastructure vulnerability [50]. The version of CSC 20 that we used was version 6.0.

Both frameworks consist of broad controls with a number of sub-controls containing more detailed guidance. The content of the proposal forms will be referred to as questions in the rest of the paper. Our approach was to count for each sub-control the number of forms requesting information about that sub-control. The process of classifying units of analysis under themes is "one of the most challenging aspects of the study" and '"may be difficult to put into words" [45].

We illustrate this process by means of an example. In the CFC Underwriting's Esurance C&P proposal form [44], question 3.6 is 'Have your systems been subject to a third party security audit?' Considering the ISO framework, this question corresponds to sub-control '*18.2: Information Security Reviews*'. A similar rationale was applied throughout our analysis. This allowed a comparison between the information collected and the established best practice relating to network security.

A degree of subjectivity is inevitable; a handful of questions corresponded loosely to a sub-control and a judgement was made. For example, both the CSC sub-controls 5.7 and 16.2 mention passwords 'longer than 14 characters', which did not correspond to the question 'Does the company enforce passwords that are at least seven character...?' asked in ACE's Privacy Protection policy [43]. This method favoured controls phrased more generically because a higher degree of specificity means a given question is less likely to correspond to the control. This was done to maintain consistency throughout our analysis.

5 Results

In order to reason about the results of our qualitive analysis of the assessments, we devised two simple metrics. The first numbers the times that every sub-controls was refered to in all 24 assessment forms. This metric allows us to identify the most popular controls as well as those neglected by insurers. The second indicates the percentage of sub-controls referred in the forms for every control. The rationale being that in order for a security control to be effective the majority of the sub-controls are required to be in place. Therfore, a low percentage would indicate that the controls is not properly addressed. Figure 1 and Figure 2 show the total number of sub-controls addressed per control for each of ISO/IEC 27002 and the CIS CSC. This presents an overview of how the forms align with each of the frameworks. This is complemented by a more in-depth look at a select few controls. Due to space economy, we choose the three most and least addressed controls, exploring which specific sub-controls were and were not mentioned. Table 5 and Table 6 detail the average percentage of sub-controls addressed per control, providing an insight into which sub-controls were not addressed.

5.1 ISO 27001

In this section, our analysis follows ISO/IEC 27002:2013. Figure 1 presents the number of sub-controls that were addressed by a given form and we then aggregate this information for all the forms and each control. The number of sub-controls in each section increases the maximum possible score. We note that every ISO control was addressed by at least one form. The three highest scoring controls were *Section 8*, *Section 12* and *Section 18* which relate to asset management, operational security and compliance respectively.

The sub-controls which were mentioned most often were *10.1 Cryptographic controls*, *12.2 Protection from malware*, *18.1 Compliance with legal and contractual requirements* and 1*2.3 Backup* with scores of 18, 23, 22 and 19 respectively. These scores correspond to the number of forms that ask about the sub-control. For example, 23 of the forms asked for information relating to the applicant's protection from malware.

Only two forms did not address a sub-control related to *18.1 Compliance with legal and contractual requirements*, which involves managing obligations to external authorities such as regulation regimes. Table 4 contains a number of these regulatory frameworks, along with the number of forms that it was mentioned in. Regulatory framework is used as an umbrella term to describe government regulation, compliance standards and security approaches. ISO 27001 and UK Cyber Essentials are included as they tended to be mentioned in the same section as formal regulation like HIPAA or GLBA.

Figure 1 demonstrates that the controls with the lowest scores were *Section 13: Communications security, Section 14: System acquisition, development and maintenance* and *Section 16: Information security incident management.* Section 13 contains two sub-controls, the first relates to secure networks and the second secure communication with third parties. The first was occasionally addressed through network segregation, which is mentioned in the sub-control. The second is addressed through non-disclosure agreements.

Section 14 relates to the development and procurement of products, particularly relating to security requirements. None of the forms addressed security requirements, though two US firms mentioned the use of open source code in development, which is relevant to the development process. Finally three forms asked about test procedures. Section 16 relates to incident response, which is mentioned in only eight forms; none of these forms mention insider threat. Since there is only one sub-control, however, this results in a relatively high score in Table 6. Table 6 shows, for each ISO control, the average percentage of sub-controls with at least one question relating to that sub-control in each form per control.

Only four sub-controls had no corresponding questions in any of the analysed forms. In ISO, *12.1* looks at controlling and documenting changes to operating responsibilities and procedures, *12.5* relates to controlling the installation of software, *12.7* looks at minimising the adverse effects of IT audits and *14.1* to specify security control requirements. All of these scored zero. Only one form contained a question relating to *14.2*, which looks at software/systems development processes. Only two forms contained questions corresponding to each of *13.2*, about policies and agreements regarding communications with third parties, and *9.3*, which relates to user's responsibilities including choosing strong passwords.

A low score in Table 6 suggests that many of the sub-controls have not been addressed, which suggests there is relevant information that has not been collected. It is unsurprising that Control 10, which relates to cryptography, scores well because there is only one sub-control and most of the forms mention cryptographic protocols. Similarly, Section 18 scores highly; this is because the first control relates to compliance and the second to external security audits, each of these sub-controls is well-represented in the proposal forms. This analysis reveals *Control 12: Operations Management* has much room for improvement, despite the sub-controls relating to malware control, backups and patching scoring highly. Control 12 contains some sub-controls which were entirely ignored such as *12.5 Control of operational software* and *14.1 Security requirements of information systems.*

5.2 CIS Top 20 Security Controls

In this section we detail our analysis of the forms based on the CIS Top 20 Critical Security Controls

(CSC). Figure 2 uses the same methodology as Figure 1, the difference being that the controls are provided by the CSC. Controls which have scored highly include: *CSC8: Malware Defenses*, *CSC10: Data Recovery Capability*, *CSC 13: Data Protection* and *CSC 14: Controlled Access Based on the Need to Know.* On the other hand, we note that *CSC1: Inventory of Authorized and Unauthorized Devices*, *CSC2: Inventory of Authorized and Unauthorized Software*, *CSC 5: Controlled Use of Administrative Privileges* and *CSC 7: Email and Web Browser Protections* had no corresponding questions in the proposal forms.

More specifically, *CSC8: Malware Defenses* scored highest in this analysis. Table 7 details the sub-controls of *CSC8: Malware Defenses* and the number of forms that ask a question relating to each sub-control. Table 7 reveals that 8.1 was the main factor for this high score, which asks for anti-virus and personal firewalls on all work stations. Control 8.2 was consistently mentioned in the forms; this sub-control relates to installing system updates to machines. However, the other six sub-controls were left completely unaddressed. For example, 8.4 relates to malware and removable media. Only two forms mention removable media outside of the context of encryption, both of which relate to downloading sensitive information, not malware defences. Similarly none of the forms mention searching for executables in network traffic, anti-exploitation features or DNS query logging.

CSC10: Data Recovery Capability consists of four sub-controls and we detail our analysis of this control in Table 8. Note that only one sub-control was not mentioned in the forms, compared to six in *CSC8: Malware Defenses.* Control 12.4 aims to ensure key systems have a back-up, which is not 'continuously addressable through operating system calls'. While some forms do ask if the back-up is housed off-site, this question does not fully comply with the sub-control, since a cloud provider could be housed off-site but still being continuously addressable through operating system calls.

Many controls had very low scores, such as *CSC17*, which relates to staff awareness and training. Only eight forms asked about delivering security training and two forms asked about periodic testing. The first two in terms of priority CSC controls relate to keeping an inventory of authorised software and hardware; yet none of the forms contain any of the followings words: inventory, authorised, unauthorised, blacklist or whitelist. One UK firm asks for 'approximate number of devices on network'; while this necessitates some form of crude inventory, it does not sufficiently address any of the sub-controls in *CSC1: Inventory of Authorized and Unauthorized Devices.* We will discuss whether keeping an inventory is implicit in other controls in Section 6.

Operating systems (OS) and applications were particularly under-addressed despite controls such as *CSC 18: Application Software Security.* Only three forms mentioned 'software' in a capacity beyond security software (such as AV or firewall) or patching. Two of these related to providing software to other firms — one of these related to supplying software using open source software. None of the following recommendations of *CSC2: Inventory of Authorized and Unauthorized Software* were mentioned: monitoring software installed on machines, software version installed or air-gapping high risk applications.

Further, only three forms mentioned operating systems; these related to standard configuration, the type of operating system (OS) in use and whether the OS continued to be supported by the manufacturer. The first falls under *CSC3: Secure Configurations for Hardware and Software* and was the only form to correspond to a sub-control under this control. CSC 5 outlines *The processes and tools used to track, control, prevent, correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.* Yet we found that only one of the form mentions administrative privileges, which was in connection with social media accounts.

CSC 7: Email and Web Browser Protections was a new addition to version 6.0 of the CSC; its sub-controls involve disabling unnecessary plugins, add-ons and scripting languages in all web browsers and clients, logging URL requests, maintaining network based URL filters, scanning and blocking email attachments with malicious code, among others. There are eight sub-controls comprising this control and none of the forms analysed contained a question corresponding to any of them.

As with the ISO analysis, Table 5 includes the average percentage of sub-controls addressed per control. The only factor affecting the scores relative to in Figure 2 is the number of subcontrols, which range from 4 to 12. *CSC10: Data Recovery Capability* and *CSC 17: Security Skills Assessment* had very few sub-controls, consequently they score higher. While *CSC 12: Boundary Defense*, *CSC 13: Data Protection* and *CSC 16: Account Monitoring and Control* had many sub-controls, thus a lower score was asigned.

6 Discussion

Policy makers, organisations seeking insurance and insurers have different priorities and will interpret these results accordingly. Organisations can prioritise the controls in place before applying for insurance, policy makers may gain an insight into the extent to which insurance promotes security best practice, and insurers can address areas of cyber security they neglect to collect information about. We will discuss the specific lessons learnt in this section.

6.1 Organisations Seeking Insurance

The results presented in this paper provide organisations in the US and the UK that consider to apply for cyber insurance with a view of the minimum security controls that will be sought. While we do not know how the information collected translates to premium pricing, it is reasonable to assume that the controls mentioned will lead to a reduction. Further, implementing information security management schemes, such as ISO/IEC 27000 and the CSC, can be a challenge. This is particularly true for organisations operating under resource constraints, such as small and medium sized enterprises. Organisations must prioritise which controls to implement first, if at all. We suggest that the insurance industry could be used to help organisations prioritise which controls to implement. Insurers' exposure to multiple organisations with similar functionalities gives them a greater understanding of the risks that they hold. Consequently, insurers have a greater awareness of the financial losses that are occurring as a result of cyber attack and which controls are important to mitigate this loss.

With that in mind, the results suggest that cryptographic controls, malware protection, compliance with legal requirements and maintaining an effective back up, should be prioritised first, since these are the most commonly asked by insurers. This is in contrast to the CIS guidance that states "Controls CSC1 through CSC5 are essential to success and should be considered among the very first things to be done" [49]; these include keeping an inventory of devices and software, ensuring secure configurations on all devices, continuous vulnerability management and controlling administrative privileges.

This is a worrying discrepancy. One cause could be the difference in scope; the CSC are a set of "security actions" [49] and are restricted accordingly, meanwhile an insurer has no such restriction. This difference between organisational controls and security controls can account for some of the disparity. Measures such as the existence of a Chief Information Officer, maintaining a business continuity plan or being certified PCI compliant are not in the scope of the CSC. However, it does not explain why cryptographic controls and malware protection, which are covered in *CSC8: Malware Defenses* and *CSC10: Data Recovery Capability*, are mentioned so often, while the Critical Security Controls with a higher priority are not mentioned at all.

One possible explanation is that insurers consider these controls more effective at mitigating the risk they are liable for. It is important to remember that gaps in coverage mean that insurers have different incentives when assessing the effectiveness of controls. Another consideration is that compliance with legal requirements may address certain controls, so the forms need not. Additionally, insurers may seek more specific technical information in the interview process. Finally, the CSC are updated annually and some forms in our study were created before 2010. However, 20 of the forms were created in the last four years and although the CSC are updated, many of the controls remain constant throughout.

Refelcting on the recent incidents, the presence of the afforementioned controls might have mitigated the impact of the Wannacry attack in the NHS, where more than 40 hospital have been affected [51]. In these attacks, hackers used a well-known exloit to infect systems before encrypting all data and rendering them unavailable until a ransom is paid. As a consequence, many hospitals reverted to using paper and IT systems were discharged [52]. The presence of a back-up system as well as a malware defense system would have mitigated the impact of the attack and might have prevented the incident for happening. However, these controls mainly focus on mitigating the risk insurers are liable for and still allow room for the attack to take place.

6.2 Informing the Insurance Assessment Process

Our results provide two distinct evaluations that can be used to improve the insurance process and address the problem of adverse selection. The first revolves around the results presented in Figure 1 and Figure 2 that present the absolute number of sub-controls mentioned in the forms. The second focuses on the analysis provided in Table 5 and Table 6 which explains what additional information is required to adequately represent the specific control into question. Regarding the first evaluation, it gives an overview of which controls are in the proposal forms and which controls have been overlooked. This analysis suggests systems development and acquisition, communications management and incident management deemed of the highest priority.

However, this presentation of results may not be appropriate for all purposes. Figure 1 suggests that *ISO: Section 12* is well addressed. Yet Table 6 shows that there is a majority of sub-controls which are not accounted for. The first presentation may be appropriate for insurers with a relatively low maturity of assessment, where any additional information would help the underwriting process. Meanwhile, the second presentation of results is useful for high-maturity assessment seeking to collect information relating to all critical controls.

The results show that the information gathered by the forms is more aligned with the ISO/IEC 27002 framework. This is understandable given that the CSC relate to network security and many controls may be too detailed for the assessment process. In spite of this, there is still much we can learn from the CSC because appropriate network security is vital to mitigating many of the risks that cyber insurance covers. For example, the authors of the CSC deem *CSC5: Controlled Use of Administrative Privileges* to be of high priority. As a result, it was moved from being *CSC12* in Version 5.0 to *CSC5* in Version 6.0 of the CSC [49]. Yet none of the forms directly address any of the sub-controls pertaining to *CSC5*. Similarly, *CSC 7: Email and Web Browser Protections* relates to application security. However, none of the forms address the corresponding sub-controls, which is worrying given that applications are increasingly being considered as a "prime [attack] vector into an organisation" [53].

Addressing the lack of questions referring to *CSC1* and *CSC2* could provide valuable benefits for the insurer. An inventory of hardware and software could help the underwriting process by putting a value on the assets at risk. Further, it will help with forensic investigation and support other goals such as revoking access to devices once an employee has departed from the organisation. Here, our discussion touches upon the interdependence of security controls. One consideration is that the interdependence of controls mean that some controls are implicitly addressed. For example, some of the proposal forms ask for security software 'on all desktops, laptops and servers'. It could be argued that this necessitates an inventory of hardware, meaning there is no need to ask about *CSC1*.

Assessing the existence of controls alone provides a 'check-box compliance' view of network security. This has been raised as one criticism of regulation [54]. If the insurance industry is to evolve towards accurate risk assessment it must take a holistic and responsive view of risk management. We suggest that a wider coverage of the CSC sub-controls can provide provide guidance on how to manage the implementation of a control, rather than merely check of its existence. For example, many of the questions merely ask whether the firm is 'conducting regular penetration tests'. More alignment with the specific advice contained within *CSC20: Penetration Tests and Red Team Exercises* could provide a clearer view of the implementation of this control and help insurers better understand an applicant's network security practices. However, it is important to be aware of the tension between the need for more information and the ease of the application process, which is the second largest obstacle to selling cyber insurance according to a 2015 survey [1].

Reflecting on the afforementioned incident that crippled NHS services, it is evident that the controls offered by CIS would have not only mitigated the problem but might have prevented it from occurring in the first place. An inventory of hardware and software is a critical step in any business continuity plan and in the case of NHS systems were shout down because there was no clear indication of the software they were using [55]. Additioanlly, Microsoft had provided a patch for the exploit, however, most hospitals used obsolete operation systems and did not update their sytems due to the "complexity of keeping systems up to date" [55]. Having had inventories and system updates, three of the most important CIS controls, these atatcks may have been avoided. It is clear that there is an overlap but a small discrepancy as well between the controls suggested by best practice frameworks and those requested by the insurance community. Therefore, there should be further discussions between policy makers and the insurers on how to bridge this gap.

6.3 Implications for Policy Makers

In the introduction we discussed the public-private partnership for cyber insurance. One insurance contribution to the partnership is to 'promote established risk management standards', with the UK policy document naming ISO 27000 [48]. Our results provide some evidence verifying the adoption of ISO 27000. For instance, no section of ISO/IEC 27002 is entirely unaddressed. However, the results show that there are controls contained in ISO/IEC 27002 and the CSC which are not covered in the forms. This could be an issue for policy makers and we discuss potential reasons behind it.

One reason for the absence of ISO/IEC 27002 and CSC controls could be that insurers are focused on best practice from other lines of insurance. For example, 15 of the forms mention a business continuity plan, which does not form part of the CIS Security Controls framework. Note that this is an important control for mitigating the losses that would fall under business interruption coverage, which is traditionally offered by insurers.

Another reason could be that insurance contracts tend to only last a year. Consequently, the insurer has a financial incentive to prioritise controls that will have an immediate effect. Such controls include security products, maintaining back-ups and encrypting sensitive data. However, for some controls and procedures the length of time they have been in place becomes an important factor. For example, appointing a Chief Information Security Officer (CISO) will have little immediate affect but will pay off in the long term as changes in the structure of the organisation are being realised at a much later stage. This is also true for secure software engineering practices where the current policy is less important than the policy in place when the system was developed. Insurers are incentivised to focus on controls with an immediate effect.

Another factor to consider is that insurers may focus on the risks they are liable for as they do not cover all of the cyber risks that an organisation might face. Table 2, which details the range of coverage available, does not include reputation damage or intellectual property theft. For example, controls relating to data encryption or a functioning back up system, which mitigate the risk of data breach and data corruption respectively, scored very highly. Meanwhile, controlling administrative privileges was not mentioned, despite it comprising a whole Section of the CSC. One reason could be that it does not directly mitigate a risk the insurers are liable for.

A rational insurer is concerned with the controls which directly mitigate the risks that they are liable for, creating a question of misaligned incentives. In the literature, the insurer is assumed to be the victim of moral hazard. We suggest that where an applicant expects the insurer to manage their cyber risk exposure, the presence of gaps in coverage can lead the insurer to select security controls which expose the insured party to risks not covered by the policy. Such a case is an example of moral hazard in which the insured party is the victim and the insurer is the "guilty" party.

7 Conclusion and Future Work

We analysed 24 self-assessed proposal forms offered by UK and US insurers, using themes from two established information security frameworks. The analysis reveals that self-assessed proposal forms predominantly focus on a small range of controls related to malware defences, managing back-ups and use of encryption. Our results can inform the conscious evolution of the insurance application process. In particular, future proposal forms could include controls such as managing secure configuration, keeping an inventory of hardware and software, control of administrative privileges and application security. It is important to be conscious of the burden on the applicant, who must complete the proposal form.

Given insurer's understanding of risks, we suggest that our results could help inform organisation's security decisions. However, as insurers only ask for security controls which directly mitigate the risks that they bear financial responsibility for, misplaced incentives could lead to poor security decisions. It is important for organisations to bear these considerations in mind when purchasing cyber insurance and making investment decisions once insurance policies are purchased.

These incentives should be considered by policy makers given that they are not necessarily aligned with the public interest. Anderson et al. illustrate how misaligned incentives explain many security failures [20]. Forward thinking policy makers could anticipate misaligned incentives in the cyber insurance domain and try to correct these ahead of time to avoid failures in security. Further, our results support the assumption that cyber insurance will promote established risk management standards, particularly ISO/IEC 27002. This assumption requires further research as we have only looked at one part of the application process.

To our knowledge, this is the first systematic analysis of cyber insurance proposal forms. Consequently, there are many novel directions for the study of proposal forms. Our methodology is rooted in the themes provided by two information security frameworks. Yet cyber insurance covers areas distinct from information security. It would be interesting to see an analysis of the controls in place to mitigate Multi-Media Liability (outlined in Table 2) such as review by a qualified attorney. Especially in light of the different nature of risks such as international cyber torts [38]. Future work could use an inductive approach to capture controls not included in our analysis. Another direction could involve usability studies to investigate the trade offs between information collected and ease of the application process.

Proposal forms are but one piece of the puzzle. In future work we hope to interview key actors in the insurance industry to better understand how the telephone interviews and on-site audits fit into the rest of the insurance process. These interviews could also investigate why the controls that we have identified are lacking in their proposal forms. Further research could shed light upon the motivation of the insurance market for requesting information on certain controls. The relative importance of factors such as the nature of the claims made from insured organisations, the regulatory fines paid, the proposed legislation regarding security practices, the evolution of the threat intelligence community and the advices provided by security industry is still unclear and subject to further research.

List of abbreviations

CIS – Center for Internet Security
CSC – Critical Security Controls
IEC – International Electrotechnical Commission
ISO – International Organization for Standardization
IT – Information Technology
OS – Operating System

Availability of data and materials

We have provided a list of some of the main cyber insurance forms assessed in the body of this article. For instance, AIG, Hiscox, Great American Insurance Group, ACE Insured and CFC Underwriting. Readers can contact the corresponding author if a more complete list is required. We would be very happy to provide this.

Competing interests

The authors declare that they have no competing interests.

Funding

This research was conducted primarily by a doctoral student; project funding considerations do not apply in this context.

Author's contributions

This article is the product of project research at the University of Oxford by Daniel Woods (DW), supervised by Ioannis Agrafiotis (IA), Jason R. C. Nurse (JN) and Sadie Creese (SC). As a result, the core research and experimentation was conducted by DW, with IA, JN and SC providing direction and guidance during the research. All parties assisted in the journal manuscript drafting stage. All authors read and approved the final manuscript.

Acknowledgements

The authors acknowledge that this work was inspired by research conducted with Novae Group plc, on a project aimed at Investigating the Relative Effectiveness of Risk Controls and the Value of Compliance.

Author's information

DW is a doctoral student in the Centre for Doctoral Training in Cyber Security; IA is a Research Fellow in Cyber Security; JN is a Research Fellow in Cyber Security and a JR Fellow at Wolfson College; and SC is Professor of Cyber Security. All authors are based in the Department of Computer Science at the University of Oxford in the UK.

References

1. Advisen Ltd: Cyber Liability Insurance Market Trends: Survey Available: http://www.partnerre.com/opinions-research/cyber-liability-insurance-market-trends-2015-survey. [Online; accessed 22-June-2017] (2015)
2. Marsh Insights: UK 2015 Cyber Risk Survey Report Available: http://uk.marsh.com/Portals/18/Documents/UK%202015%20Cyber%20Risk%20Survey%20Report-06-2015.pdf. [Online; accessed 22-June-2017] (2015)
3. Ponemon Institute LLC: 2015 Cost of Data Breach Study: Global Analysis. Available: https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF [Online; accessed 22-June-2017] (2015)
4. Siegel, C.A., Sagalow, T.R., Serritella, P.: Cyber-risk management: technical and insurance controls for enterprise-level security. Information Systems Security **11**(4), 33–49 (2002)
5. Manworren, N., Letwat, J., Daily, O.: Why you should care about the target data breach. Business Horizons **59**(3), 257–266 (2016)
6. Department of Homeland Security: Cybersecurity Insurance Industry Readout Reports. Available: https://www.dhs.gov/publication/cybersecurity-insurance-reports. [Online; accessed 22-June-2017] (2014)
7. HM Government & Marsh Ltd: UK Cyber security: The role of insurance in managing and mitigating the risk. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security _Report_Final.pdf. [Online; accessed 22-June-2017] (2015)
8. The Lawyer: Incentives and barriers of the cyber insurance market in Europe. Available: https://www.thelawyer.com/issues/13-september-2010/as-professional-indemnity-crisis-rumbles-on-the-sra-consults/. [Online; accessed 22-June-2017] (2010)
9. ENISA: As professional indemnity crisis rumbles on, the SRA consults. Available: https://www.enisa.europa.eu/publications/incentives-and-barriers-of-the-cyber-insurance-market-in-europe/at_download/fullReport. [Online; accessed 22-June-2017] (2012)
10. Majuca, R.P., Yurcik, W., Kesan, J.P.: The evolution of cyberinsurance. arXiv preprint cs/0601020 (2006)
11. Beh, H.G.: Physicial losses in cyberspace. Conn. Ins. LJ **8**, 55 (2001)
12. Baer, W.S., Parkinson, A.: Cyberinsurance in it security management. IEEE Security & Privacy (3), 50–56 (2007)
13. Marotta, A., Martinelli, F., Nanni, S., Yautsiukhin, A.: A Survey on Cyber-Insurance. Available: http://www.iit.cnr.it/en/node/36039. [Online; accessed 22-June-2017] (2015)
14. Bradford, J.: Advisen Insight Cyber Insurance Market Update. [Online; accessed 22-June-2017] (2015). http://www.advisenltd.com/2015/01/15/advisen-insight-cyber-insurance-market-update
15. UK Cabinet Office: Cyber Security Insurance: New Steps to Make UK World Centre. Available: https://www.gov.uk/government/news/cyber-security-insurance-new-steps-to-make-uk-world-centre. [Online; accessed 22-June-2017] (2015)
16. Kesan, J., Majuca, R., Yurcik, W.: Cyberinsurance as a market-based solution to the problem of cybersecurity: a case study. In: Proceedings of Workshop of Economic Information Security (WEIS) 2005 (2005)
17. Toregas, C., Zahn, N.: Insurance for cyber attacks: The issue of setting premiums in context. George Washington University (2014)
18. Geer, D.: Risk management is still where the money is. Computer **36**(12), 129–131 (2003)
19. Schneier, B.: Insurance and the computer industry. Communications of the ACM **44**(3), 114–114 (2001)
20. Anderson, R., Schneier, B.: Guest editors' introduction: Economics of information security. IEEE Security & Privacy (1), 12–13 (2005)
21. Baer, W.: Rewarding it security in the marketplace. Contemporary security policy **24**(1), 190–208 (2003)
22. Yurcik, W., Doss, D.: Cyberinsurance: A market solution to the internet security market failure. In: Proceedings of Workshop of Economic Information Security (WEIS) 2002 (2002)
23. Böhme, R., Schwartz, G., *et al.*: Modeling cyber-insurance: Towards a unifying framework. In: Proceedings of Workshop of Economic Information Security (WEIS) 2010 (2010)
24. Ogut, H., Menon, N., Raghunathan, S.: Cyber insurance and it security investment: Impact of interdependence risk. In: Proceedings of Workshop of Economic Information Security (WEIS) 2005 (2005)
25. Kunreuther, H., Heal, G.: Interdependent security. Journal of risk and uncertainty **26**(2-3), 231–249 (2003)
26. Bolot, J.-C., Lelarge, M.: A new perspective on internet security using insurance. In: INFOCOM 2008. The 27th Conference on Computer Communications. IEEE (2008). IEEE
27. Zhao, X., Xue, L., Whinston, A.B.: Managing interdependent information security risks: A study of cyberinsurance, managed security service and risk pooling. ICIS 2009 Proceedings, 49 (2009)
28. Böhme, R., Kataria, G.: Models and measures for correlation in cyber-insurance. In: Proceedings of Workshop of Economic Information Security (WEIS) 2006 (2006)
29. Böhme, R.: Cyber-insurance revisited. In: Proceedings of Workshop of Economic Information Security (WEIS) 2005 (2005)
30. Herath, H.S., Herath, T.C.: Cyber-insurance: Copula pricing framework and implication for risk management. In: Proceedings of Workshop of Economic Information Security (WEIS) 2007 (2007)
31. Shetty, N., Schwartz, G., Felegyhazi, M., Walrand, J.: Competitive cyber-insurance and internet security. In: Proceedings of Workshop of Economic Information Security (WEIS) 2010, pp. 229–247 (2010)
32. Bandyopadhyay, T., Mookerjee, V.S., Rao, R.C.: Why it managers don't go for cyber-insurance products. Communications of the ACM **52**(11), 68–73 (2009)
33. Schwartz, G., Shetty, N., Walrand, J.: Cyber-insurance: Missing market driven by user heterogeneity. preparation, www. eecs. berkeley. edu/nikhils/SecTypes. pdf (2010)
34. Bandyopadhyay, T., Mookerjee, V.S., Rao, R.C.: Why it managers don't go for cyber-insurance products. Communications of the ACM **52**(11), 68–73 (2009)
35. Grzebiela, T.: Insurability of electronic commerce risks. In: System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference On, p. 9 (2002). IEEE
36. Biener, C., Eling, M., Wirfs, J.H.: Insurability of cyber risk: An empirical analysis†. The Geneva Papers on Risk and Insurance-Issues and Practice **40**(1), 131–158 (2015)
37. Lee, A.: Why traditional insurance policies are not enough: The nature of potential e-commerce losses & (and) liabilities. Vand. J. Ent. L. & Prac. **3**, 84 (2001)
38. Crane, M.: International liability in cyberspace. Duke Law & Technology Review **1**(1), 23 (2001)

39. Gordon, L.A., Loeb, M.P., Sohail, T.: A framework for using insurance for cyber-risk management. Communications of the ACM **46**(3), 81–85 (2003)
40. AIG: CyberEdge Application Form. Available: https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Financial-lines/Cyber/aig-cyberedge-application-form.pdf. [Online; accessed 22-June-2017] (2016)
41. Hiscox: Privacy and Data Breach Protection. Available: http://www.hiscoxbroker.com/shared-documents/cyber-data-risks/10049_Privacy_and_Data_Breach_Protection_Mainform_Application.pdf. [Online; accessed 22-June-2017] (2012)
42. Great American Insurance Group: Cyber (Net) Application. Available: http://www.greatamericaninsurancegroup.com/insurance/Specialty-Human-Services/Forms/Documents/F36223-Cyber-(NET)-Application.pdf. [Online; accessed 22-June-2017] (2014)
43. ACE Insured: Cyber & Privacy Insurance Application Form. Available: https://www2.chubb.com/US-EN/_Assets/doc/Cyber-Privacy-Insurance-Application.pdf. [Online; accessed 22-June-2017] (2015)
44. CFC Underwriting: Esurance Cyber & Privacy. Available: http://www.colemanambris.com/docs/documents/cyber-privacy-application.pdf. [Online; accessed 22-June-2017] (n.d.)
45. Elo, S., Kyngäs, H.: The qualitative content analysis process. Journal of advanced nursing **62**(1), 107–115 (2008)
46. Downe-Wamboldt, B.: Content analysis: method, applications, and issues. Health care for women international **13**(3), 313–321 (1992)
47. Lederman, R.P.: Content analysis of word texts. MCN: The American Journal of Maternal/Child Nursing **16**(3), 169 (1991)
48. International Organization for Standardization (ISO): ISO/IEC 27002:2013 Available: http://www.iso.org/iso/catalogue_detail?csnumber=54533. [Online; accessed 22-June-2017] (2013)
49. Center for Internet Security: CIS Critical Security Controls - Version 6.0 Available: https://www.sans.org/critical-security-controls. [Online; accessed 22-June-2017] (2015)
50. Farnan, O.J., Nurse, J.R.C.: Exploring a controls-based assessment of infrastructure vulnerability. In: Lambrinoudakis, C., Gabillon, A. (eds.) Risks and Security of Internet and Systems: 10th International Conference, CRiSIS 2015, Revised Selected Papers. Lecture Notes in Computer Science, pp. 144–159. Springer, Cham (2016)
51. Wired: The NHS trusts and hospitals affected by the Wannacry cyberattack. Available: http://www.wired.co.uk/article/nhs-trusts-affected-by-cyber-attack. [Online; accessed 22-June-2017] (2017)
52. Wired: WannaCry is back! Virus hits Australian traffic cameras and shuts down a Honda plant in Japan. Available: http://www.wired.co.uk/article/nhs-cyberattack-ransomware-security. [Online; accessed 22-June-2017] (2017)
53. Ahmad, D.: The contemporary software security landscape. IEEE Security & Privacy **5**(3), 75–77 (2007)
54. Siponen, M., Willison, R.: Information security management standards: Problems and solutions. Information & Management **46**(5), 267–270 (2009)
55. The Guardian: NHS seeks to recover from global cyber-attack as security concerns resurface. Available: https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack. [Online; accessed 22-June-2017] (2017)
56. CFC Underwriting: Esurance Cyber & Privacy. Available: http://www.colemanambris.com/docs/documents/cyber-privacy-application.pdf. [Online; accessed 22-June-2017] (2008)
57. Philadelphia Insurance Companies: Cyber Security Liability Application. Available: https://www.phly.com/Files/Application %20-%20Cyber %20Security %20Liability %20NY31-927.pdf. [Online; accessed 22-June-2017] (2010)
58. Protection®, A.P.: Cyber and Privacy Insurance. Available: https://www.scribd.com/document/249827931/Ace-Dataguard-Advantage-Application. [Online; accessed 25-October-2016] (2015)
59. CFC Underwriting: Esurance CPM Application Form. Available: http://www.stgilesgroup.co.uk/storage/documents/Cyber %20Proposal %20Form.pdf. [Online; accessed 22-June-2017] (2013)
60. Pinsure: Cyber Liability Proposal Form. Available: http://www.pinsure.co.uk/. [Online; accessed 22-June-2017] (2014)
61. ACE Privacy Protection®: Cyber and Privacy Insurance. Available: https://www2.chubb.com/US-EN/_Assets/doc/Cyber-Privacy-Insurance-Application.pdf. [Online; accessed 25-October-2016] (2015)
62. Risk placement Services, Inc: Cyber Liability Premium Indication Form. Available: https://www.rpsins.com/media/1844/cyber _rps _02.pdf. [Online; accessed 22-June-2017] (2014)
63. Sutcliffe & Co Insurance Consultants: Cyber Liability Insurance. Available: http://www.sutcliffeinsurance.co.uk/Portals/0/docs/cyber %20proposal %20form.pdf. [Online; accessed 22-June-2017] (2013)
64. Ascent Underwriting: CyberPro Application. Available: http://www.ascentunderwriting.com/resources/docs/application.pdf. [Online; accessed 25-October-2016] (2014)
65. Lockton Companies
LLP: Professional Indemnity Insurance for Privacy Protection. Available: https://www.locktonsolicitors.co.uk/cmsUploads/quoteForm/files/LLP1209 %20_Privacy _ProtectionProposalform.pdf. [Online; accessed 22-June-2017] (2013)
66. Sybaris: Cyber Suite Insurance Proposal. Available: http://www.ip-insurance.com/uploads/1/4/6/2/14622220/ssr _2016 _cyber _prop.pdf. [Online; accessed 22-June-2017] (2016)
67. Beazley: Beazley Breach Response. Available: http://www.moagent.org/Products/SiteAssets/Pages/ForYourAgency/Cyber /default/CyberSecureFullApp.pdf. [Online; accessed 25-October-2016] (2014)
68. Markel International: Cyber Insurance Proposal Form. Available: http://www.markelinternational.com/Documents/London %20Market/PFR/PI%20- %20Wordings/Intellectual %20Property/Cyber %20Insurance %20Proposal %20Form %20110116.pdf. [Online; accessed 22-June-2017] (2015)
69. The Compass Group, Inc: Omniguard Cyber and Privacy Application. Available: http://www.bassunderwriters.com/Forms/Cyber %20Liability %20Program.pdf. [Online; accessed 22-June-2017] (2013)
70. Business Insurance 24/7: Cyber/Privacy/Multimedia Liability Proposal Form. Available: http://www.cyber-liability-insurance.co.uk/docs/CYBER_PROP_2015.doc. [Online; accessed 25-October-2016] (2015)
71. Naturesave Insurance: Cyber & Data Security Proposal Form. Available: http://www.naturesave.co.uk/download/Business-Insurance-Documents/Business-Proposal-Forms/Cyber %20Insurance %20Proposal %20Form.pdf. [Online; accessed 22-June-2017] (2014)
72. The Hartford: Cyberchoice 2.09. Available: http://www.thehartford.com/sites/thehartford/files/cyber-choice-application.pdf. [Online; accessed 22-June-2017] (2011)
73. CFC Underwriting: Cyber, Privacy and Media Application Form. Available: http://www.swanmorss.com/usr/Pdfs/Cyber_App.pdf. [Online; accessed 25-October-2016] (2014)
74. OneBeacoN Insurance: Professional @vantage for Financial Institutions. Available: http://www.onebeaconfs.com/sites/FinancialServices/documents/policydocuments /specialty/Cyber %20Liability %20Application %20SCB005 %20ASIC %20FINAL.pdf. [Online; accessed 25-October-2016] (2015)
75. TravelersJ: Cyber Risk Coverage Application. Available: http://www.travelerscanada.ca/brokers/application-forms/documents/CyberRisk%20Application.pdf. [Online; accessed 25-October-2016] (2015)

Figures

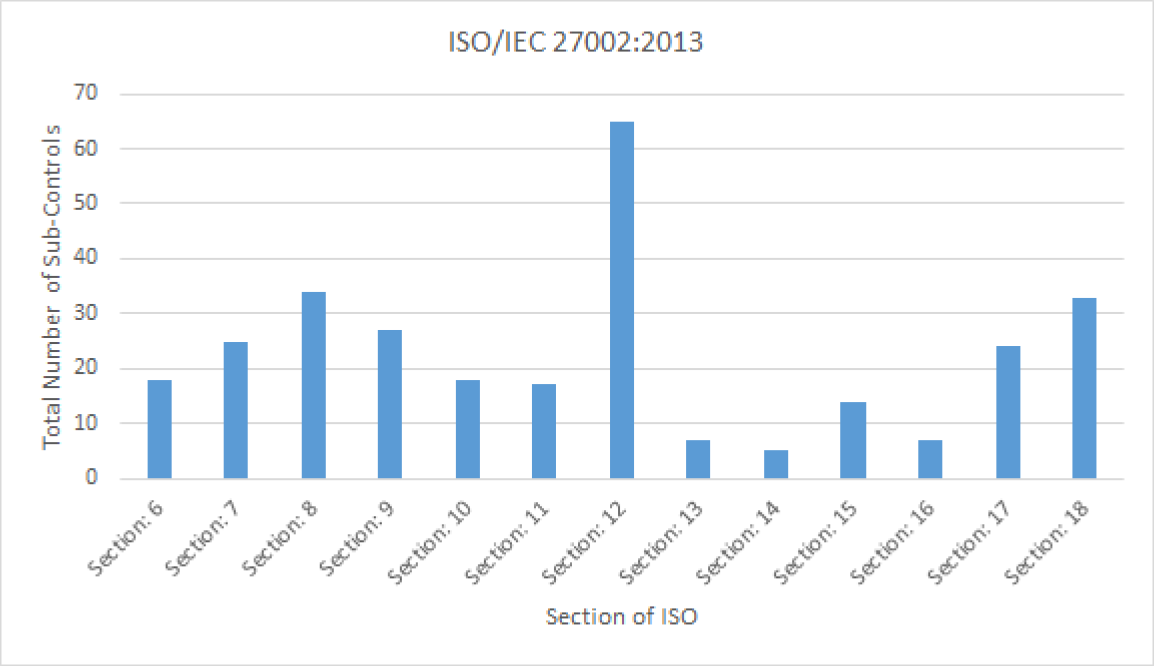

Figure 1 Showing the total number of sub-controls with a question in a form corresponding to that sub-control.

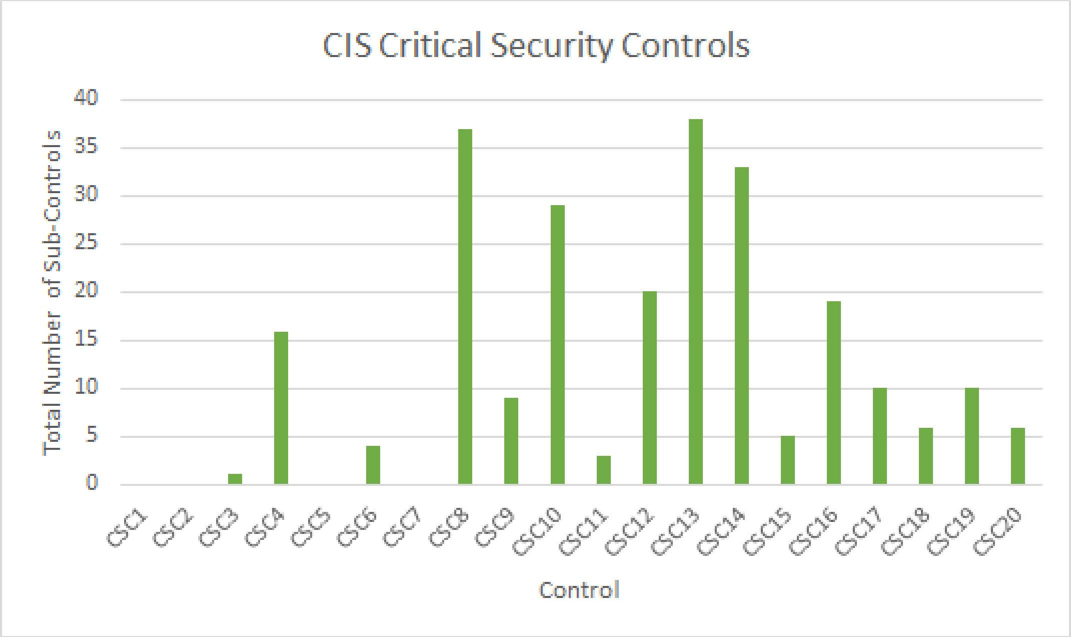

Figure 2 Showing the total number of sub-controls mentioned in the forms per control.

Tables

ACE Insured [43]	CFC Underwriting [56]	Philadelphia Insurance Companies [57]
ACE Privacy Protection [58]	CFC Underwriting [59]	PInsure [60]
ACE Privacy Protection [61]	Great American Insurance Group [42]	Risk placement Services [62]
AIG [40]	Hiscox [41]	Sutcliffe & Co Insurance Consultants [63]
Ascent Underwriting [64]	Lockton Companies [65]	Sybaris [66]
Beazley [67]	Markel International [68]	The Compass Group [69]
Business Insurance 24/7 [70]	Naturesave Insurance [71]	The Hartford [72]
CFC Underwriting [73]	OneBeacon Insurance [74]	TravelersJ [75]

Table 1 Forms included in our study and the insurer offering them.

Coverage	**What It Covers**
First-Party Coverage	Coverage for the cost of replacing or restoring lost data. Excludes intellectual property.
Data Privacy and Network Security Liability	Coverage for liability claims of a third party like a data breach or unintentional transmission of a computer
Business Interruption	Covers revenues lost as a result of network down time.
Cyber-Extortion	Cover for investigation costs, sometimes the extortion demand.
Public Relations	Fees for Public Relations firm to manage reputation in the event of a breach.
Multi-Media Liability	Costs relating to the content of a firm's website like copyright infringement.
Professional Services	Liability relating to a service offer such as web hosting or internet service.

Table 2 Showing the range of coverage available.

Information Collected	**Question in the Form**
Revenue	Gross Annual Revenue Last Year £
Type of Data Collected	Do you store, process and/or transmit any Sensitive Data on Your Computer System (Tick all that apply): Credit card info □ Customer info □ Money/Securities info □ Healthcare info □ Trade secrets □ IP Assets □
Volume of data collected	Approximately how many private individuals do you hold sensitive data on:
Loss History	In the past 5 years has the company ever experienced any of the following events or incidents?: Sustained an unscheduled network outage that lasted over 24 hours Yes □ No □ Portable media that was lost or stolen and was not encrypted Yes □ No □
Out Sourcing/Suppliers	Current Network and Technology Providers (if applicable): Internet Communication Services *Please Provide Information on.* Credit Card Processor(s) *Please Provide Information on.* Website Hosting *Please Provide Information on.* Anti-virus Software *Please Provide Information on.* Managed Security Services *Please Provide Information on.*

Table 3 The type of information collected and questions asked in the ex-ante assessment.

Regulatory Approach	**Questions**
Payment Card Industry Data Security Standard (PCI DSS)	17
Health Insurance Portability and Accountability Act (HIPAA)	11
Gramm Leach Bliley Act (GLBA)	8
ISO 27001	7
UK Data Protection Act	5
UK Cyber Essentials	1

Table 4 Compliance, Regulation and Standards

Control	%
CSC 1: Inventory Authorized Devices and Unautorized Devices	0
CSC 2: Inventory Authorized Devices and Unautorized Software	0
CSC 3 : Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	0.58
CSC 4: Continuous Vulnerability Assessment and Remediation	8.33
CSC 5: Controlled Use of Administrative Privileges	0
CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs	2.79
CSC 7: Email and Web Browser Protections	0
CSC 8: Malware Defenses	26.38
CSC 9: Limitation and Control of Network Ports, Protocols, and Services	5.54
CSC 10: Data Recovery Capability	29.17
CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	1.79
CSC 12: Boundary Defense	9.17
CSC 13: Data Protection	4.11
CSC 14: Controlled Access Based on the Need to Know	17.13
CSC 15: Wireless Access Control	2.33
CSC 16: Account Monitoring and Control	5.04
CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps	10
CSC 18: Application Software Security Incident Response and Management	4.58
CSC 19: Incident Response and Management	6.54
CSC 20: Penetration Tests and Red Team Exercises	3.67

Table 5 Percentage of Sub-Controls Addressed per CSC Control

ISO Control	Percentage
Section 6: Organization of information security	37.50%
Section 7: Human resource security	34.70%
Section 8: Asset management	42.70%
Section 9: Access control	28.10%
Section 10: Cryptography	75%
Section 11: Physical and environmental security	35.40%
Section 12: Operations management	38.70%
Section 13 Communications security	14.60%
Section 14: System acquisition, development and maintenance	6.90%
Section 15: Supplier relationships	29.20%
Section 16: Info security incident management	16.70%
Section 17: Business continuity management	50%
Section 18: Compliance	68.80%

Table 6 Percentage of Sub-Controls Addressed per Control

CSC 8: Malware Defenses	Questions
8.1 Automated tools to continuously monitor workstations	23
8.2 Employ software to automatically push regular AV updates	13
8.3 Limit use of removable devices outside approved business need	0
8.4 Enable anti-exploitation features	0
8.5 Identify executables in network traffic	0
8.6 Enables DNS query logging	0

Table 7 Sub-controls for the Malware Defenses control

CSC10: Data Recovery	Questions
10.1 Each system is automatically backed every week	14
10.2 Perform test data restoration process regularly	5
10.3 Backups protected via physical security or encryption where stored	9
10.4 Key systems have a backup not continuously addressable via operating system calls	0

Table 8 Sub-controls for the Data Recovery control.