Does Cyber Insurance promote Cyber Security Best Practice? An Analysis based on Insurance Application Forms

RODNEY, ADRIKO*
Institute of Cyber Security for Society (iCSS), School of Computing, University of Kent, Canterbury, UK, ra596@kent.ac.uk

JASON, R.C. NURSE
Institute of Cyber Security for Society (iCSS), School of Computing, University of Kent, Canterbury, UK, j.r.c.nurse@kent.ac.uk

The significant rise in digital threats and attacks has led to an increase in the use of cyber insurance as a risk treatment method intended to support organisations in the event of a breach. Insurance providers are set up to assume such residual risk, but they often require organisations to implement certain security controls a priori to reduce their exposure. We examine the assertion that cyber insurance promotes cyber security best practice by conducting a critical examination of cyber insurance application forms to determine how well they align with ISO 27001, the NIST Cybersecurity Framework and the UK's Cyber Essentials security standards. We achieve this by mapping questions and requirements expressed in insurance forms to the security controls covered in each of the standards. This allows us to identify security controls and standards that are considered – and likely most valued – by insurers and those that are neglected. We find that while there is some reasonable coverage across forms, there is an underrepresentation of best practice standards and controls generally, and particularly in some control areas (e.g., procedural/governance controls, incident response and recovery).

CCS CONCEPTS • Human and societal aspects of security and privacy • Security services

Additional Keywords and Phrases: Cyber insurance, cybersecurity, information security, ISO 27001, NIST Cybersecurity Framework, UK Cyber Essentials, security standards and controls, insurance proposal forms

1 INTRODUCTION

Cyber insurance has increasingly emerged as a topic of IT and computer security practice and research, yet there are still many unanswered questions regarding its role, especially as it relates to its contribution to organisational security. A key motivator for the first cyber insurance policies was to respond to computer crime and support data breach notifications, with the first standalone internet-based policy issued in the 1990s. Since then, cyber insurance has expanded and now is viewed as a feasible – and even recommended [1] – mechanism to allow businesses to transfer residual cyber risk; this includes the provision of coverage for incident response, data breach counsel, public relations, and wider recovery. This type of insurance has featured in industry and policy discussions in the US [2], UK [3] and EU [4], and has recently become even more salient due to the use of insurance to cover ransom payments where policyholders have succumbed to a ransomware incident. These incidents have drawn close public attention to insurance as discussions take place regarding whether the cyber insurance market, through covering payments, is partially responsible for the increase in ransomware attacks [5, 6, 7, 8]. It should be noted that this topic is still currently heavily debated and various authors and researchers hold differing views. For instance, [6] asserts that the actual capacity for cyber insurance to impact the rise of ransomware and its broader societal consequences, whether positively or negatively, is practically restricted.

Prior to underwriting an insurance policy, insurers will typically assess the cyber security posture of the applying organisation as this also influences the risk to them from entering into the policy agreement. Herath and Herath [9] suggests that calculating cyber risk exposure is quite complex and involves several factors including calculations of attack likelihoods and impact costs based on historical data. The problem with this approach, however, is that vast amounts of historical data are often not readily available and may not be

ACM 2576-5337/2024/7-ART
https://doi.org/10.1145/3676283

available soon due to the rapidly changing landscape of cyber-attacks. As such, insurers often rely on information that is gathered through other touch points, particularly cyber insurance application forms (also known as cyber insurance proposal, or 'prop', forms), in the first instance.

Cyber insurance application forms can vary by insurance carrier and broker, but in general these self-assessment questionnaires typically request information including the size and sector of the organisation requesting an insurance policy, its nature of business, any personal data held, and its security posture (i.e., what security controls they possess or standards they adhere to) [10]. Depending on the business and their responses, insurance providers may follow-up with telephone interviews, on-site visits, automated risk assessment tools and audits (as now particularly popular with InsurTech firms [11]), to ascertain whether an applicant should be offered a policy and if so, to determine an appropriate premium. Appreciating that these follow-up options are resource intensive, the reality is that many insurers will rely primarily on insurance application forms – and the carefully selected set of questions included therein – due to the ease and reduced resource burden. This may especially be the case where applicants are small-to-medium-sized enterprises or businesses (SMEs/SMBs) and the comparatively small premiums do not justify large initial resource investment.

An intriguing research question that arises based on the aforementioned points is *how do the security controls that are viewed as crucial by insurers – i.e., those featuring in application forms – compare to (or align with) security best practice as defined by international and national standards?* This article investigates this question and thus the wider assertion that cyber insurance currently promotes cyber security best practice in organisations. Although we acknowledge that standards might not consistently improve or enhance security and can have specific limitations depending on the context, in this article we operate under the assumption that standards embody best practices as intended. Subsequently, we explore how insurance forms align with these standards. We conduct a thorough examination of the forms used by insurance providers to assess applicant's cyber posture to determine the extent to which the current assessment methods align with three well-regarded security standards and schemes: the ISO/IEC 27001 international security standard, the NIST Cybersecurity Framework (NIST CSF) and the UK's government-backed Cyber Essentials (CE) scheme.

Our work is inspired by, and builds on, prior research by [12] and it presents a novel contribution, in comparison, in several ways. First, [12] did not consider the NIST CSF, yet this standard is of great interest to insurers in the context of risk management [13], particularly in advanced security and insurance markets such as the US and UK. Second, that study excluded Clause 5; Information security policies of the ISO 27001 which arguably forms the core of a cybersecurity program; we seek to accommodate this in our analysis. Third, our research includes a comparison of application forms to the UK's CE scheme with the intention of exploring how a small set of controls deemed to be the most critical (i.e., 'essential') to security by the UK government feature in insurance forms. Finally, we provide an updated analysis which is able to appreciate the significant changes that have occurred in the cyber insurance market and technology landscape since [12], which is based on data from 2008-2016. Although reviewing cyber insurance application forms is a common practice within the insurance industry, our research brings additional value by subjecting this practice to rigorous academic scrutiny against established and widely used cyber security standards. Typically, insurers do not directly compare competitor forms with cyber security standards but rather, tend to evaluate their own forms in relation to those of other insurers. By critically evaluating the alignment of insurers' requirements with cyber security standards, we aim to provide insights into whether insurers' cyber security control requirements reflect best practices in cyber security risk management as seen in the ISO/IEC 27001, NIST CSF or CE. This study extends beyond routine competitive analysis to make a meaningful contribution to the academic literature on cyber security risk management and policy formulation. While there are various other articles generally related to our research (e.g., [14, 15, 16, 17]) as will be discussed below, they focus on other areas and therefore complement our article's contributions to the security and digital threats field. It should be noted that this article adopts the framework version of ISO 27001:2013, active from 2013 to 2022, with revisions in 2014 and 2015. While we acknowledge that this version was eventually updated in October 2022, we have chosen the 2013 version due to its historical significance, offering a nuanced exploration of the evolution of information security standards in insurance proposal forms over an extended period. It also enables a meaningful comparative analysis with existing literature [12] and covers 94% of the forms in our study since 64/68 forms were issued before the update. Additionally, we posit that the practical constraints faced by insurers, and the

temporal relevance of the standard during the studied period further support our decision to use this version. This approach ensures a comprehensive understanding of the dynamics shaping information security practices in the insurance sector. To ensure transparency, we have also included a translation of the ISO 27001:2013 to the updated version in Appendix B.2.

We structure this article as follows. Section 2 provides a review of related work pertaining to cyber insurance. In Section 3, we present an overview of the methodology employed in this study which involves a systematic assessment and analysis of cyber insurance application/proposal forms. Section 4 reports the results of this study including the comparison of controls in the forms with controls in the three frameworks; thus, enabling the assessment of the alignment of insurer's requests with these standards. The findings are discussed in Section 5 and reflect on our research's aim. The work then is concluded in Section 6 and avenues for further research are considered.

2 RELATED WORK

Cyber insurance has become an increasingly popular component in risk management as it allows organisations to transfer residual risk to a third-party, particularly to cushion them from the adverse effects of a breach. Tsohou et al. [18] identify the challenges for organisations that are pushing them to seek cyber insurance including supply-chain attacks, ransomware, business email compromise and funds transfer fraud. This is partly corroborated by [6] who conclude that the growth of ransomware has fuelled the growth of cyber insurance because it has provided more clarity on the costs of cyber risks as compared to prior cyber risks and organisations have become more aware. With all these attacks, the effectiveness of a business' response during and after an incident is crucial to its sustainability and effort to maintain its reputation [19, 20]. As such, support by qualified services (e.g., incident response firms, crisis management teams, insurance) is crucial to avoid poor response.

Deliberations on the impact of insurance on cyber security have taken place for over two decades. These have presented positions for and against the ability of insurance to improve security [14, 21, 22], with little definitive conclusion. One area of particular interest is that of security controls and the extent to which insurers place pressure on policyholders to improve their security practices. Although this can incentive implementation of controls, it is essential to carry out a Cost Benefits Analysis to carefully assess the expenses associated with adopting these measures against the financial advantages gained from the reduction in premiums. It is crucial to ensure that the cost of adopting these measures do not outweigh the financial benefit derived from the reduction in premiums. Franke [23] conducted interviews with security professionals to investigate the Swedish insurance market and found that insurers do impose security controls requirements on customers to reduce their exposure and build the insured's resilience to avoid attacks and claims. A comparable finding was reached in [7] based on an analysis of the UK market, albeit not as conclusive. Mott et al. [6] acknowledge the fact that insurers are imposing higher cyber security standards upon their insureds, thereby compelling them to cultivate commendable cyber security practices. However, the authors argue that this hardening of the market caused by mandated security controls may result in a negative situation of cyber insurance unavailability and inaccessibility, thereby leaving numerous businesses vulnerable without essential insurance coverage [6]. In contrast, [24] concludes that, despite the promise of cyber insurers to enhance their insureds' cybersecurity posture, the promise remains just theoretical. According to their viewpoint, this can be attributed to the concept of 'race to the bottom' which is a situation where there is intense competition in the market, leading insurers to offer lower premiums which may not necessarily contribute to improving the overall cyber hygiene. Whereas some insurers may take a deep dive into the applicant's risk and security controls, many assess the security posture of applicants using self-assessment questionnaires called application, or proposal, forms (e.g., [44], [61], [62], [74]). These forms provide unique insight into the perspective of each insurer and arguably hint towards what security controls they view as most important to reduce cyber risk and a business' exposure to it. A key reality is that each insurer's forms can vary considerably in what risk management controls they request, thereby making it even more appealing to reflect on them as a whole to assess what controls they all view as useful (or unnecessary).

Two noteworthy pieces of research have sought to assess the content of cyber insurance proposal forms to identify questions asked and areas of concentration. Woods et al. [12] was the first study to critically analyse cyber insurance application forms. From an assessment of 24 forms from the US and UK (covering 2008-2016),

they provided evidence regarding the notion that adoption of cyber insurance may promote certain cyber security practices. Their study compared controls requested by application forms to the ISO 27001 and the Centre for Internet Security Critical Security Controls (CIS CSC) information security standards. They concluded that insurers are more focused on controls that mitigate risks for which they bear monetary responsibility such as malware defense, backup, and use of encryption, and less emphasised controls like secure configuration and keeping an inventory of hardware and software. While this work was seminal in elucidating a new insurance industry related to security, there are various avenues for improvement. For instance, they did not include NIST CSF (one of the most pertinent security standards today), a control of ISO27001 was excluded, and it is unfortunately outdated given the various changes in the market – including rise in insurance purchasing, and adoption of new technologies [25] – since 2016. We also expand further upon the number of standards assessed by considering three, instead of two.

The second study, [15], analysed 34 security-focused insurance questionnaires gathered from states in the US and covering a period of 2007-2017. They adopted a more inductive approach to analysis (and for instance, did not assess form alignment with any security control standards) and instead identified four broad sections from the forms' data. These included questions centred on Organisational (e.g., data collection and handling), Technical (e.g., security infrastructure), Policies and Procedures, and Legal and Compliance components. These four categories are very similar to the structure of the new ISO/IEC 27002:2022 [78], albeit the paper being released in 2019. Their findings demonstrated a clear prominence of policies and procedures, followed by data collection and handling, information, and data management, information, and network security policy, and legal and compliance in applications. On the other hand, there were minimal questions targeting personnel hiring practices and access control. Comparing these findings to [12], who also studied the US, there is a similar emphasis on risk prevention mechanisms and on backup procedures, but there appear to be some differences in significance of legal and compliance issues. These may be linked to the regulations present in the US, and prominence of acts and laws such as Health Insurance Portability and Accountability Act (HIP-PA) and Gramm-Leach-Bliley Act (GLBA). This is in line with [26] who concluded that in the context of cyber insurance, insurers do more than just pooling and spreading risk but can act as compliance managers for organisations dealing with cyber security threats. Through the analyses of insurance application forms, these articles provide insight into the security controls that insurers have requested of their clients and the factors that influence their decisions.

The discussion about cyber insurance is increasingly relevant to the security and digital threats fields because insurance providers – whether intentionally or otherwise – are emerging as ways to prevent and respond to attacks on organisations. Their influence is driven by organisations' need to manage residual cyber risk and lower the premiums paid for instance, thereby being more accepting of security requirements placed by insurers.

3 METHODOLOGY

3.1 Research objectives

To address the research question posed in Section 1, we define two objectives. The first is to collect a set of cyber insurance application forms that would be appropriate to our research problem and would be suitable for analysis. The second, and more prominent, objective is to examine the questions posed by cyber insurance providers in the collected application forms and align them to control categories in a series of well-recognised security standards. This will allow us to identify security controls that are most or least advocated, at least in the first instance, by insurers. In addition, this provides some evidence to further strengthen or negate the assertion that adoption of cyber insurance promotes established cyber security best practice standards.

3.2 Form collection and selection

To collect cyber insurance application forms, and thus address the first research objective, we rely on a series of online searches given the success of this approach in prior work ([12]) and proven ability to return a robust and diverse set of forms. We utilise Google Search considering its market dominance, and examine documents (.PDF, .docx) results from the terms cyber insurance application or proposal form and variations of them. The search is scoped to forms created between 2016 and 2023 to allow for a more up-to-date analysis of the insurance

industry; we also do not consider forms analysed by [12] in 2016 as this could allow us to then compare the works later. Consequently, the following search queries are used: "*cyber insurance application form" filetype:pdf after:2016; cyber insurance "application form" filetype:docx after:2016; "cyber insurance" application form filetype:docx after:2016;* and *cyber insurance "application form" filetype:docx after:2016;* we also executed these queries using 'proposal' instead of 'application' and stopped when the search no longer yielded relevant or new forms. These search results are then evaluated to identify all cyber insurance application forms returned to determine those that fit the criteria for inclusion in this analysis. The search was conducted in December 2022 and again in March 2023. To enable this study to identify the latest trends in the market, proposal forms from insurers in the US, UK and Australia are selected as these countries are regarded as leaders in the market [27]. In addition, [28] projects the UK, US, and Australia to be the countries expected to dominate the cyber insurance industry in Europe, North America, and the Asian-Pacific regions respectively. It is noteworthy to highlight that the current article focuses exclusively on the proposal forms or questionnaires provided by insurers and does not include policies that have been underwritten for the insured parties.

A total of 68 cyber insurance forms resulted from our selection process with ~43% (29/68) of them dated within 2020-2023. A similar percentage (42.6% (29/68)) of the forms are from insurers in the UK whereas ~38% (26/68) and ~19% (13/68) were from the US and Australia respectively. The full list of forms considered in this study is shown in Table 1, but examples include [32], [44], [61], [62], [74] and [86].

Table 1: Cyber insurance forms by insurance provider, year, and country of origin

Form Id	Insurer and Year	Country	Form Id	Insurer and Year	Country
PF1	360 Underwriting Solutions (2020) [29]	Australia	PF35	Tokio Marine HCC (2018) [112]	UK
PF2	Absolute Insurance Brokers (2018) [30]	UK	PF36	Travelers Insurance (2019) [114]	US
PF3	AIG (2017) [31]	UK	PF37	AmTrust North America (2016) [33]	US
PF4	Allianz (2019) [32]	UK	PF38	AXIS Insurance (2020) [44]	US
PF5	Ascent (2016) [37]	UK	PF39	Beazley Insurance (2017) [48]	UK
PF6	AustBrokers (2021) [41]	Australia	PF40	Corvus Insurance (2021) [60]	US
PF7	AustBrokers (2017) [40]	Australia	PF41	G & M (2018) [68]	UK
PF8	Berkley Insurance (2020) [49]	Australia	PF42	HSB (2020) [74]	US
PF9	Brooklyn Underwriting (2020) [53]	Australia	PF43	Tokio Marine HCC (2021) [113]	US
PF10	CFC Underwriting (2020) [55]	UK	PF44	Ando insurance (2021) [34]	UK
PF11	CHUBB (2017) [57]	US	PF45	Travelers Insurance (2020) [115]	UK
PF12	DUAL (2020) [56]	UK	PF46	BGi.uk (2017) [50]	UK
PF13	Emergence (2020) [67]	Australia	PF47	Professional Insurance Agents Ltd (2019) [99]	UK
PF14	Global Re Broking Solutions Ltd (2018) [69]	UK	PF48	Optimum Specialty Risks (2021) [97]	UK
PF15	Great American Insurance Group (2018) [70]	US	PF49	Axis Capital (2021) [43]	US
PF16	Hiscox Insurance (2019) [72]	UK	PF50	Apex Insurance Brokers (2019) [35]	UK
PF17	Liberty Specialty Markets (2017) [81]	Australia	PF51	Hartford Steam Boiler Inspection and Insurance Company (2020) [71]	US
PF18	London Australia Underwriting (2020) [82]	Australia	PF52	The Hanover Insurance Group, Inc. (2017) [109]	US
PF19	Management and Professional Risks (2018) [83]	UK	PF53	United States Liability Insurance Company (2021) [116]	US
PF20	Management and Professional Risks (2019) [84]	UK	PF54	CFC Underwriting Limited (2017) [54]	US
PF21	AtBay (2020) [38]	US	PF55	ATC Insurance Solutions Pty Ltd (2022) [39]	Australia
PF22	Marsh (2020) [86]	Australia	PF56	Nova Casualty Company (2018) [95]	US
PF23	MFL Professional Insurance Brokers (2017) [89]	UK	PF57	Cowbell Cyber Inc (2023) [62]	US
PF24	Miller Insurance (2018) [90]	UK	PF58	Biz Lock (2021) [52]	UK
PF25	NIG (2018) [92]	UK	PF59	Corvus Insurance (2023) [61]	US
PF26	NMU (2017) [94]	UK	PF60	The Hartford (2022) [110]	US
PF27	OBF Insurance (2018) [96]	UK	PF61	Beazley Insurance (2023) [47]	US
PF28	ProRisk (2019) [100]	Australia	PF62	Distinguished Programs (2020) [64]	US
PF29	QBE Insurance (2016) [101]	UK	PF63	Arch Insurance Company (2018) [36]	US
PF30	Routen Chaplin (2017) [104]	UK	PF64	CM&F Group (2019) [58]	US
PF31	Royal & Sun Alliance (RSA) Insurance (2017) [105]	UK	PF65	CRC Insurance (2019) [63]	UK
PF32	Sura Technology Risks (2020) [106]	Australia	PF66	Biz Lock (2020) [51]	US
PF33	TDC Specialty Underwriters (2017) [107]	US	PF67	The Doctors Company (2017) [108]	US
PF34	TK Specialty Risks (2019) [111]	Australia	PF68	Beazley Insurance (2018) [46]	US

For companies such as AustBrokers, Management and Professional Risks, and Travelers Insurance Company Limited where two or more different forms are included, the forms relate to either different cyber insurance products or services offered in distinct markets. For example, AustBrokers' [41] was used to perform assessment for corporate entities whereas [40] was used by the same insurer to assess Small to Medium Enterprises (SMEs) and Travelers Insurance's [114] is used to assess companies in the UK while [113] is used to assess companies in the UK.

3.3 Forms assessment method

The second research objective is achieved by the critical assessment of the collected forms and reflection on the alignment results. Directed Qualitative Content Analysis is used to assess the forms as it enables us to identify and categorise themes to derive meaning and insight from the questions posed in the forms [79]. This data analysis technique is well known for its capacity to "identify critical processes" from a range of texts [66] and was also applied in related works. We map the information requested via the questions in each form against three well-supported, best practice security control sets: the NIST Cybersecurity Framework (CSF) [93], ISO/IEC 27001 [77], and the UK Cyber Essentials [91]. These versions of the frameworks are carefully selected because their availability overlaps significantly with the years of insurance application forms and as such, an objective analysis of the conformance of the forms to the standards can be carried out.

3.3.1 Cyber security standards

The CSF is published by the National Institute of Standards and Technology (NIST) and helps organisations to manage cybersecurity risk by integrating industry standards and best practices to suggest actionable controls that boost cyber resilience and defence [93]. The framework consists of five Functions which have several Categories, and each Category has a set of related Subcategories. It provides guidelines on how both internal and external stakeholders of organisations can manage and reduce their cybersecurity risk. This framework is unique in that unlike many standards and compliance regulations that are aimed at improving security within a specific industry, it is designed to be used for individual organisations across industries. The version of NIST that was used in this study was version 1.1; see [93].

The ISO/IEC 27001 (hereafter ISO 27001) is an internationally recognised standard that presents guidelines to organisations on information security, cybersecurity and privacy protection including implementing information security controls based on internationally recognised best practice and developing organisation-specific information security management guidelines [78]. It is a generic standard that applies to any organisation that wants to implement commonly accepted information security controls [78]. As such, it allows us to examine proposal forms without regard for the type of enterprise that fills the form. This article employs the framework version of ISO 27001:2013, which pre-dates the current ISO 27001:2022 Standard. The aforementioned standard was in effect between 2013 and 2022, with revisions in 2014 and 2015, until it was eventually replaced by the updated version of the ISO 27001 standard in October 2022. We use the ISO 27001:2013 framework, chosen for its historical significance and practicality, to analyse information security standards in insurance proposal forms from 2013 to 2022. This allows for a comparative analysis with existing literature [12], covering 94% of the study's forms issued before the 2022 update. The decision considers practical constraints faced by insurers, ensuring a comprehensive understanding of information security practices in the insurance sector. The framework consists of 14 Security Clauses, each with several Security Control Categories which each have related Controls.

The UK Cyber Essentials (CE) is a basic control set that contains five Technical Control Themes with no explicit sub-controls; Examples of controls include Malware protection, Patch management and Access control [91]. CE is heavily supported by the UK government and even required to bid for certain central government contracts. The reason behind its selection in this study is to explore how a small set of controls deemed critical to security features (or fail to be aligned with the control requests) in insurance forms. In addition, 42.6% of the forms are from UK insurers and as such, it could be advantageous to determine how these forms are aligned with such a government-backed standard. For our analysis, we use the CE version as of December 2021 given that this version's availability overlaps with the years of insurance application forms. Although this Standard was later updated in April 2023, the Technical Control Themes were still maintained by the NCSC (NCSC, 2023).

Tables A.1, A.2 and A.3 in Appendix A provide an overview of the contents of each core part of NIST CSF, ISO 27001, and CE respectively.

3.3.2 Mapping forms to controls.

Content analysis is used to determine the forms that contain *all* Controls, Security Categories, or Security Control Categories from a Technical Control Theme (CE), Function (NIST) or Security Clause (ISO) respectively (we consider these to be fully cover/aligned), those that contain *at least one but not all* (we consider these to be partially cover/ aligned), and those that *do not contain any* Controls, Security Categories, or Security Control Categories (we consider these to be not cover/not aligned). The numbers of forms are then computed as percentages to determine the percentage of forms that cover all, part, or do not contain any of the controls respectively. The analysis involves examining the questions in the proposal forms and aligning them with the relevant control grouping or classification for each of the three standards. For example, the question *"Do you use anti-virus software?"* present in an application form would correspond to clause "A.12.2 Protection from malware" of the ISO 27001 framework, Function 3; Detect of the NIST Framework and Technical Control Theme 4; Malware of the UK Cyber Essentials Framework. Table B.1 in Appendix B shows sample form mapping to ISO 27001 and the NIST CSF. We illustrate this with an example basing on a mapping of the security-related questions asked in an insurance application form [53] against ISO 27001.

It is crucial to emphasize that insurers might prioritize distinct areas or risks, and consequently, their selection of specific control measures can be influenced by their expertise, leading to a lack of comprehensive standards coverage across various forms. Given this reality, achieving uniformity among proposal forms becomes exceedingly challenging due to the diverse landscape of insurance, encompassing variations such as exclusion clauses or the addressing of different facets of cyber loss. However, assessing the controls most frequently encountered or requested offers valuable insights, allowing us to draw conclusions about coverage and alignment without assuming a convergence among these controls.

ISO/IEC 27001:2013 – Summary of Annex A

Security clauses	Security control categories	Controls
A.5 Information security policies	A.5.1 Management direction for information security	A.5.1.1 Policies for information security
		A.5.1.2 Review of the policies for information security
A.6 Organization of information security	A.6.1 Internal organization	A.6.1.1 Information security roles and responsibilities
		A.6.1.2 Segregation of duties
		A.6.1.3 Contact with authorities
		A.6.1.4 Contact with special interest groups
		A.6.1.5 Information security in project management
	A.6.2 Mobile devices and teleworking	A.6.2.1 Mobile device policy
		A.6.2.2 Teleworking
A.7 Human resource security	A.7.1 Prior to employment	A.7.1.1 Screening
		A.7.1.2 Terms and conditions of employment
	A.7.2 During employment	A.7.2.1 Management responsibilities
		A.7.2.2 Information security awareness, education & training
		A.7.2.3 Disciplinary process
	A.7.3 Termination and change of employment	A.7.3.1 Termination or change of employment responsibilities
A.8 Asset management	A.8.1 Responsibility for assets	A.8.1.1 Inventory of assets
		A.8.1.2 Ownership of assets
		A.8.1.3 Acceptable use of assets
		A.8.1.4 Return of assets
	A.8.2 Information classification	A.8.2.1 Classification of information
		A.8.2.2 Labelling of information
		A.8.2.3 Handling of assets
	A.8.3 Media handling	A.8.3.1 Management of removable media
		A.8.3.2 Disposal of media
		A.8.3.3 Physical media transfer

Figure 1: Mapping of sample form [53] to ISO 27001 – The Controls and Security Control Categories that are highlighted are those that have been found in the form.

In our approach, we first examine the questions in the application form [53], then identify the controls present in the form and map them to the relevant Control of the ISO 27001 standard. As depicted in Figure 1, the mapped Controls and Security Control Category are highlighted to depict that they have been addressed.

The overall Security Clause is marked as having been fully covered if all Security Control Categories are highlighted as addressed in the form. Focusing on the specific form in Figure 1, we found that no questions were presented in [53] regarding requirements for an Information Security Policy and a review of the policies. This would mean that none of the controls required for Security Control Category *A.5.1 Management direction for information security* have been covered and as such, the Security Clause *A.5 Information security policies* is deemed to have not been covered in the form. The case is, however, different for Security Clause *A.6 Organization of information security* since the form presents a question that addresses Control *A.6.2.2 Teleworking*. This would mean that the Security Control Category *A.6.2 Mobile devices and teleworking* has been addressed by the form. However, since there are no questions that address any controls under Security Control Category *A.6.1 Internal organization*, we conclude that the overall Security Clause *A.6 Organization of information security* has only been partly covered/addressed since only one of the two Security Control Categories has been considered in the form.

Finally, for Security Clause *A.7 Human resource security*, there is a question that addresses at least one Control in each of the Security Control Categories i.e., *A.7.1 Prior to employment*, *A.7.2 During employment*, and *A.7.3 Termination and change of employment.* As such, we conclude that the clause has been fully covered since the form asks questions that cover each of its Security Control Categories. This process is continued until all questions in all the forms in scope are mapped to the standard. For Cyber Essentials, occurrence of one question that relates to a Technical Control Theme is considered to fully address the requirements of the Technical Control Theme as it shows that an insurer had the Technical Control Theme in mind when framing the question. This is perhaps the most challenging part of the study as some questions may correspond to more than one control sub-categories. In such instances, some degree of subjectivity is inevitable, and a decision is made to classify the question into the best category basing on the perceived intention of the insurer for collecting such information (e.g., considering the section heading where the query is placed).

The approach used in this study is inspired by [12] who numbered the times every sub-control was referred to in all assessment forms and the percentage of sub-controls referred in the forms for every control. In attempting to quantitatively present the results of this qualitative analysis, this study develops three similar but related metrics. The first metric depicts the numbers of forms that do not address any controls in the Function, Security Clause, or Technical Control Theme, whereas the second metric numbers the forms that partially address (address one but not all) requirements of controls in the Function, Security Clause, or Technical Control Theme. The final metric numbers the forms that include all requirements in the Function, Security Clause, or Technical Control Theme of the standards. We selected this approach because in addition to examining the controls, we can focus on the forms themselves and determine their alignment rather than focusing purely on the questions by determining the proportion of forms that contain full, part or none of the controls in a category.

To further explain our analysis approach, we use the following example. If a form is being assessed based on *Clause 7 Human resource security* of the ISO 27001 framework (which has 3 Security Control Categories), the form is deemed to be fully aligned if it addresses all 3 Security Control Categories, partially aligned if it addresses 1 or 2 and not aligned if it does not address any of the Security Control Categories. The rationale behind this assessment is that for a security control to be effective, the majority of the sub controls/Security Control Categories that are required need to be implemented. For purposes of comparative analysis, these numbers are then converted into percentages to determine the percentage of forms that cover all, part, or none of the Security Control Categories. We also illustrate this by example; if we assess 7 forms against Clause 7 Human resource security of the ISO 27001 framework and find that 4 of them address all 3 Security Control Categories, then the percentage of fully aligned forms will be calculated as 57% basing on the calculation; (4/7) *100 = 57%. Relatedly, if we find that 2 of them address some but not all 3 Security Control Categories, then the percentage of partially aligned forms will be calculated as 29% basing on the calculation: (2/7) *100 = 29%. This would mean that for the remaining 1 form that does not address any of the security controls categories, the percentage would be 14% based on the calculation (1/7) *100 =14%. These percentages allow us to quantitively measure which control sections or Security Clauses are covered in depth by insurers, those that are partially covered and those that are not extensively covered.

4 RESULTS

4.1 Overview

The analysis of proposal forms indicated that insurers typically ask an average of 26 questions related to the applicant's cyber posture and the associated security controls. Achieving equilibrium between an extensive or limited questionnaire at this stage of assessment is crucial for optimizing the usefulness of form data. There were, as to be expected, outliers with some insurers ([49, 86, 94, and 54], among others) opting for a very limited question set (e.g., with less than five questions), while others ([43, 44, and 31]) pose a substantially higher number of questions ([44] for instance had 168 questions). Forms often began by collecting information such as the industry in which the applicant operates, financial information for the most recent 5 years, type of business and the size of the applicant in terms of assets. Some insurers request a copy of the applicant's most recent audited Financial Statements; this is undoubtedly linked to determining the financial risk to ensure that the applicant can continue operating its business for the foreseeable future. Many insurers such as [41, 47, 53, 61] ask applicants for a breakdown of their revenue by geographical region. This may be necessary especially when assessing concentration risk of applicants due to over dependency on a single client or region. The questions that fell under these categories were not mapped to any control because they are for informational purposes rather than reviewing the applicant's cyber security posture.

Another key area of concentration was around the nature of information that is collected, stored, or processed by the applicant especially Personally Identifiable Information (PII), Debit/Credit card details, medical records, and other sensitive data such as Social Security Numbers (SSN). For example, [37] asks applicants to "Identify the type of PII retained on their network". We also note that some forms such as [29] attempt to further evaluate the security of this data by asking questions such as *"Is all sensitive data encrypted whilst on your network?"*. This suggests that at least some insurers are aware of the implications of exposure of such data and make attempts at this early stage to evaluate their potential exposure via the protection processes put in place by the applicants.

The following sections present an in-depth assessment of the alignment of forms with the three cyber security schemes. To draw conclusions, we concentrate on which control categories were most covered and least covered. However, the full mapping of all forms with each of the frameworks is provided in Tables C.1, C.2 and C.3 in Appendix C. We begin with the UK CE given that it is the simplest to map and explain, and then proceed to ISO and NIST.

4.2 UK Cyber Essentials (CE)

Figure 2 shows the percentage of forms that fully cover each Technical Control Theme of the standard. Due to the basic nature of CE, any mention of a control that falls under any Technical Control Theme of the framework is considered to be fully aligned and fully addressing the aspects of that control Technical Control Theme. For example, any form that covers the need for firewalls is considered to completely address Technical Control Theme 1; Firewalls of the scheme.

From our analysis, we note that each control Technical Control Theme of the CE is relatively well covered by all forms. The best covered controls from this analysis are Technical Control Themes 1, 4 and 5 which correspond to Firewalls, Malware Protection and Security Update Management respectively.

In total, 84%, 79% and 74% of the forms address the controls in CE Technical Control Themes 1, 4 and 5 respectively, while CE Technical Control Themes 2: Secure Configuration and 3: User Access Control are the least covered with 69% and 60% respectively. To reiterate, these scores represent the percentage of forms that cover controls in the relevant Technical Control Theme of the CE. For example, 57 out of the 68 forms mentioned controls that were under Technical Control Theme 1; Firewalls of the CE framework. The controls in this Technical Control Theme relate to protection of the network from unauthorized access using access limitations and router configurations [91].

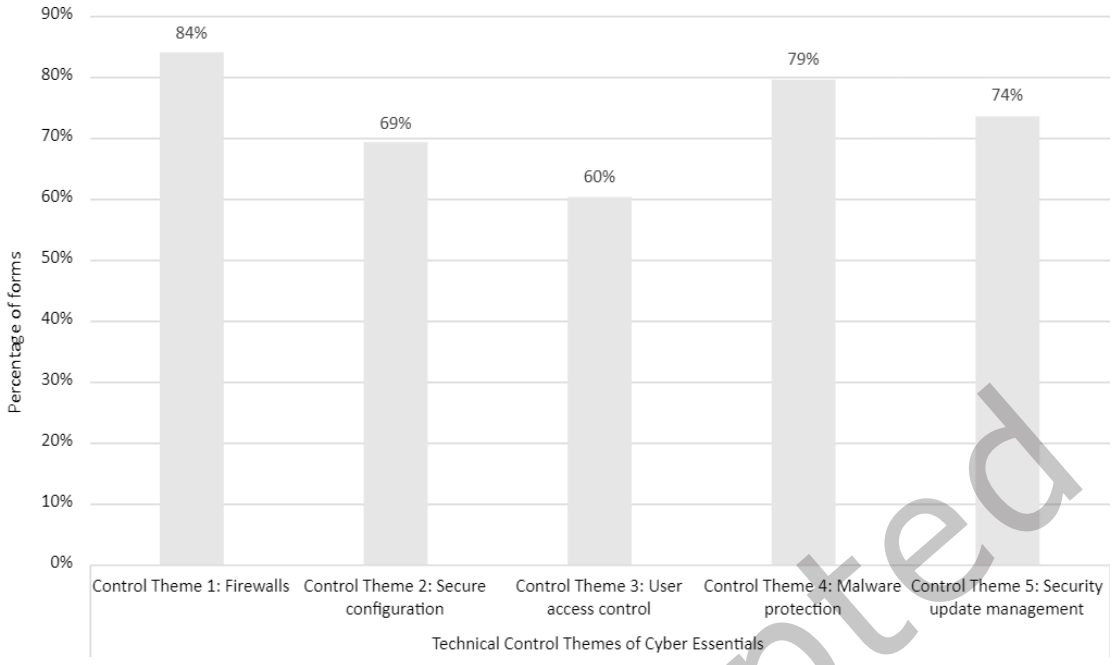

Figure 2: The percentage of forms (n=68) that fully cover each control Technical Control Theme of the UK Cyber Essentials.)

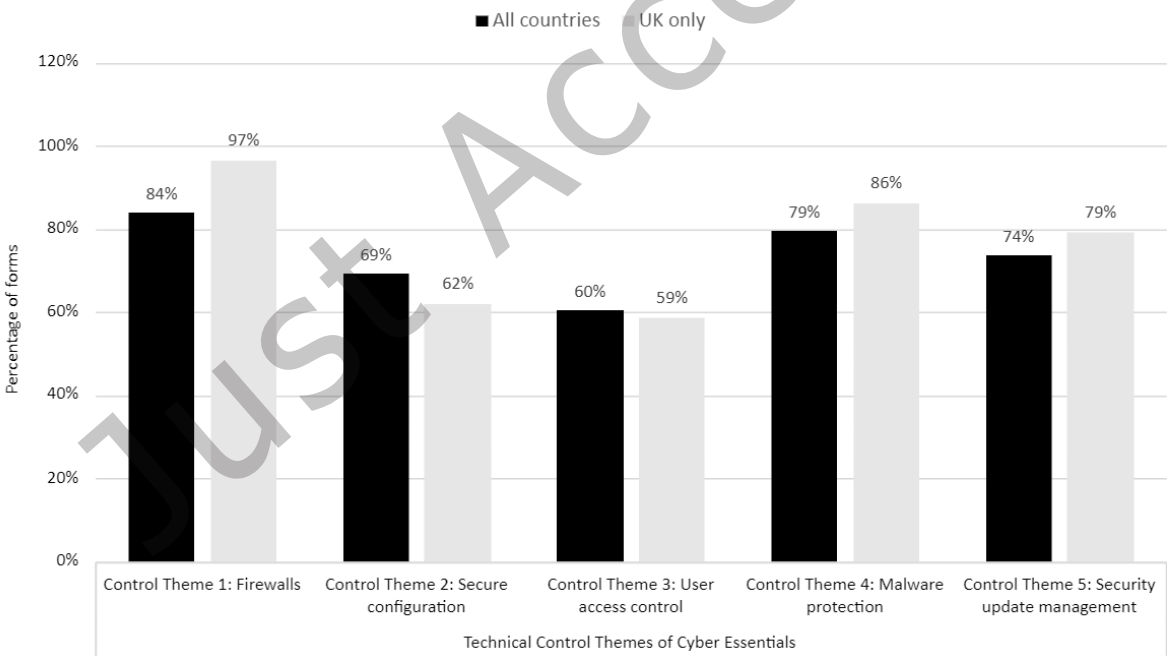

Figure 3: The percentage of forms that fully cover each control Technical Control Theme of the UK Cyber Essentials based on forms from the UK (n=29) and the entire data set (n=68).

Since the CE is a brainchild of the UK government and due to the high percentage of UK forms, we benchmarked forms issued by companies in the UK to see how they align with this standard. Figure 3 provides a comparison of these two by showing the percentage of forms that fully cover each control Technical Control Theme of the UK CE assessing the forms from the UK only (n=29) and the collection of forms from all countries (n=68). We note that the general alignment of forms to mostly Technical Control Themes of the CE increases

or is maintained when only UK forms are considered for the assessment. This is true for all Technical Control Themes of the CE except Technical Control Theme 2; Secure Configuration which drops from 69% to 62% and Technical Control Theme 3; User access control which drops slightly from 60% to 59%. This suggests that more insurers in the UK do not query, and potentially initially overlook, aspects pertaining to secure configuration when compared against the entire dataset. However, recent research suggests that misconfigurations are one of the biggest threats to cloud security [66] and as such, there is a strong argument that default configurations should be at the forefront of an insurance provider's agenda before threat actors exploit them to gain unauthorised access to corporate systems of the insured.

We note that there is a general increase for Technical Control Theme 1: Firewalls, Technical Control Theme 4: Malware Protection, and Technical Control Theme 5: Security Update Management, that increase from 84% to 97%, 69% to 86% and 74% to 79% respectively. Technical Control Theme 1: Firewalls registers the highest percentage increase with 13 percentage points. This analysis suggests that most forms from insurers in the UK are more aligned to the CE as compared to other countries. This is to some extent understandable and undoubtedly influenced by the fact that the framework originated from the UK and as such would be an easier point of reference for UK businesses (insurance providers, brokers, and clients).

4.3 ISO 27001

Next is the analysis of insurance forms based on ISO 27001. Figure 4 summarises the forms on the percentage that cover none, part, or all controls in each of the ISO 27001 Security Clauses.

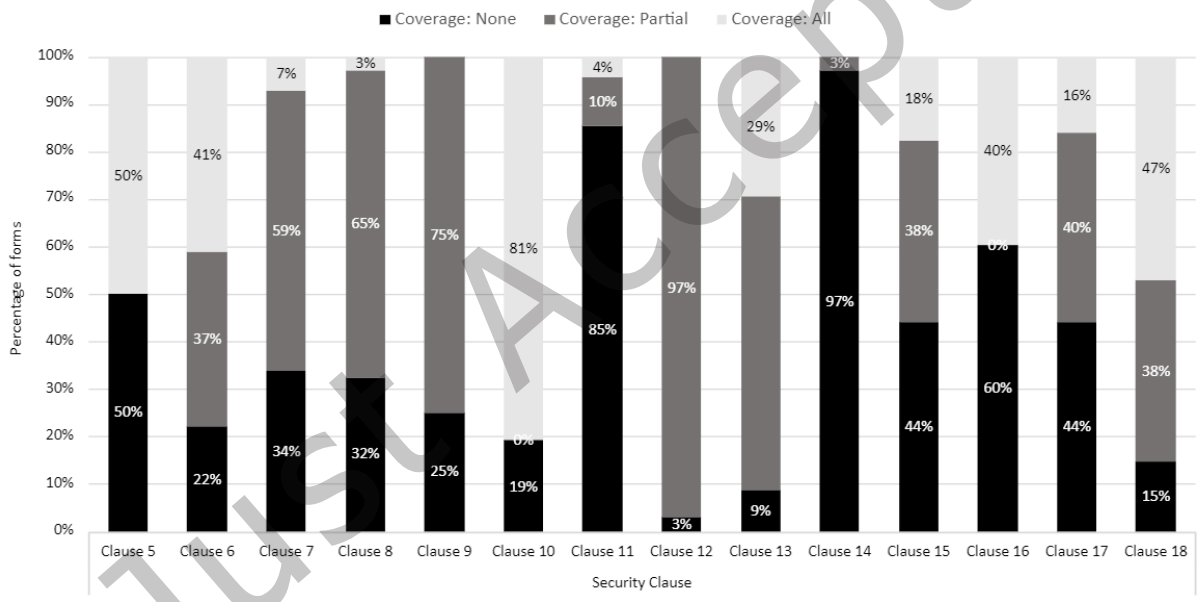

Figure 4: The percentage of forms that cover none, part, or all controls in a security clause for the ISO 27001

We note that there is general alignment with the ISO 27001 standard as each of the Security Clauses in the framework is addressed by at least one form. The clauses that are most comprehensively covered are Clause 10: Cryptography, Clause 5: Information security policies and Clause 18: Compliance with percentages of 81%, 50% and 47% respectively. This means, for example, that 81% (55) of the 68 forms analysed covered all Security Control Categories relating to Security Clause 10. The high scores for Clause 10: Cryptography can be attributed to requirements for encryption of data (at rest, in use or in motion) by several regulations such as the General Data Protection Regulation (GDPR) to reduce the impact of security breaches. Beazley Insurance [47] for instance, asks applicants whether data is stored and encrypted at several levels including laptops, Portable Media, Back-up Tapes or "at rest" within computer systems. Further, [67] asks, *"Do you protect all Personally Identifiable Information and other sensitive data through Encryption?".* These exemplify some of the types of queries posed around Clause 10.

The high scores for Clause 18, which contains Security Control Categories such as Compliance with legal and contractual requirements and Information security reviews, may be attributed to regulations around privacy and protection of privacy rights of data subjects (such as the GDRP and Health Insurance Portability and Accountability Act (HIPAA) that have exposed organisations to fines for noncompliance). As such, adherence to these regulations will support a policyholder's compliance – as well as reducing the potential likelihood of large regulatory fines – which also subsequently reduces the insurer's risk exposure.

The clauses that receive the lowest score in terms of full coverage are Clause 9: Access control, Clause 12: Operations security and Clause 14: System acquisition, development and maintenance which all score 0%; i.e., none of the forms covered all Security Control Categories under Clauses 9, 12 and 14. Security Clause 12 has 7 Security Control Categories, which is the highest of all the clauses followed by Clause 9: Access control with 4 Security Control Categories. As such, it may not have been possible for insurers to fully cover all Security Control Categories in these clauses due to this detail. There is, of course, a balance that needs to be reached between asking too many questions, particularly at this early a stage where insurers are assessing a potential client. The result for Clause 12: Operations security should also not be viewed in isolation as absence of questions to address this Security Clause because from the review of forms that partially cover controls (cover at least one but not all Security Control Categories) in a Security Clause, Clause 12: Operations security scores highest with 97% of forms covering at least one Security Control Category from this Security Clause. In addition, Clause 9: Access control scores 75% in the assessment of forms that partially cover the requirements of this clause.

Table 2: The percentage of forms that partially cover (cover at least one but not all) requirements of the Security Control Categories of ISO 27001.

Security Clause	Percentage
Clause 5: Information security policies	N/A
Clause 6: Organization of information security	37%
Clause 7: Human resource security	59%
Clause 8: Asset management	65%
Clause 9: Access control	75%
Clause 10: Cryptography	N/A
Clause 11: Physical and environmental security	10%
Clause 12: Operations security	97%
Clause 13: Communications security	62%
Clause 14: System acquisition, development, and maintenance	3%
Clause 15: Supplier relationships	38%
Clause 16: Information security incident management	N/A
Clause 17: Information security aspects of business continuity management	40%
Clause 18: Compliance	38%

Clauses 5, 10 and 16 are all N/A because they only contain one Security Control Category and as such, they are either fully covered or not covered at all. This means that they would not have any scores for forms that partially address the required Security Control Categories.

Table 2 shows the percentage of insurance forms that partially cover (cover at least one but not all) requirements of Security Clauses of ISO 27001. We note that Clause 12: Operations security receives the highest percentage of partial coverage at 97% followed by Clause 9: Access control and Clause 8: Asset management which are partially covered by 75% and 65% of the forms respectively. The majority of questions relevant to Clause 12: Operations security are centred around basic cyber hygiene controls such as malware protection, patch management, backup and recovery, and monitoring of network activities. Many forms analysed asked questions about backup and recovery mechanisms such as, *"[Do you] conduct back-up and recovery procedures on all sensitive and financial data on at least a weekly basis."* by [86]. Some forms even went a step further to ask questions about the security of the backups: *"Is the backup of Your Critical Data stored in a secure locked location with access restricted to authorized personnel only?"* by [30] and *"Do you perform backups of data, applications, and system configurations at least weekly. If these are physically stored off-site, are they encrypted."* by [106]. This is ideal and demonstrates that at least some insurers know robust security practice extends beyond only possessing backups to ensuring that backups are regular and are adequately stored.

In addition, there were several questions corresponding to 12.4: Logging and monitoring which covered various controls including monitoring of user access and user activity, collection and protection of log information and installation of Intrusion Detection Systems (IDS). Many forms asked about the existence of a vulnerability management plan or system; [114] and [83] for instance, asked whether there was a process in place to regularly download, test, and install patches and whether this process was automated. A majority of forms required applicants to describe the policy and provide more information especially in regard to the frequency of updates; for example, [114] asked whether critical patches were installed within 30 days of release and [74] asked, *"Do you update and patch critical IT-systems and applications on at least a monthly basis?"*. It is notable, however, that controls 12.5: Control of operational software and 12.7: Information systems audit considerations were barely addressed by any of the forms.

The results show that 62% of the forms mentioned at least one Security Control Category from Clause 15: Supplier relationships through asking how the applicant manages its relationship with third parties and their dependency on these third parties. Many forms also asked the applicants to list the nature of services offered by these service providers such as cloud providers. For example, [44] asks whether all written agreements require the third party to defend or indemnify the applicant against liability because of a security or privacy incident on the third party's network or caused by the third party. With the significant increase in the uptake of outsourced services such as cloud computing and co-location services and the resilience issues they have faced [103], it is not surprising that insurers are initially looking more closely into risks and disruption that could be brought about by third parties.

Figure 5 focuses on the percentages of proposal forms that do not address any of the Control Categories in the various ISO clauses. From the figure, we can see that 50% of the forms did not address Clause 5: Information security policies. This is somewhat surprising as Information Security Governance forms the core of cyber resilience strategies and drives the security program. Neglecting this control may put insurers, and their clients, at risk because regardless of the controls that may be in an environment, these may be less effective if there are no governance procedures and structures to determine how these controls should be applied and how the security program can be continuously improved.

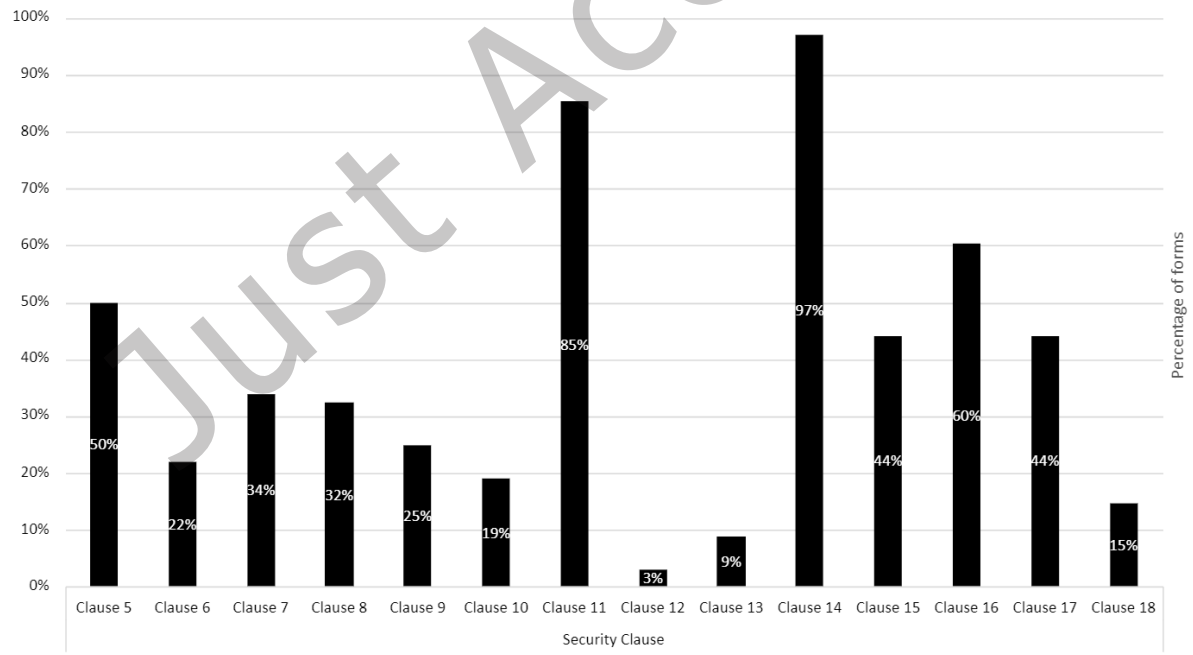

Figure 5: The percentages of forms that do not address any of the defined Security Control Categories in the various clauses of the ISO 27001.

The results indicate that controls related to systems aspects and physical security are the least covered. In particular, 97% of forms do not request any Control Category in Clause 14: System acquisition, development, and maintenance whereas 85% do not address any in Clause 11: Physical and environmental security. The third

worst covered clause (at 60%) is Clause 16: Information security incident management for which, although it has only one Security Control Category, only 40% (27) of forms ask any question that relates to it. Ascent [37] addresses Clause 14: System acquisition, development, and maintenance by querying the applicant on whether they develop software and whether this is reviewed by legal counsel prior to release. This legal focus is intriguing and is likely to relate to understanding and limiting any future liability. In addition, the form seeks to understand the quality control processes of the applicant by asking; *"Do you have quality control procedures in force to test all software and products prior to release?"*. This lack of coverage of Clause 14: System acquisition, development and maintenance could be because the expectation of insurers is that many applicants are not involved in software development; or potentially there are other bespoke forms that we are not privy to. Yet, considering applications and software can process a substantial amount of data, there are several potential data protection implications basing on how they process and store data.

As it pertains to Clause 11 and Clause 16, these are also surprising findings. While many modern-day systems do not require physical access to conduct an attack, physical security is necessary as an added layer of protection. Clause 11 could protect against local attackers (e.g., insider threats) for example. Clause 16's lack of coverage is notable because managing incidents is critical to robust security risk management. Effective management can reduce the harm caused by incidents and aid quicker recovery, thus benefiting the policyholder and insurance provider. One argument for its underrepresentation may be those insurers themselves, as part of or alongside their policies, will often offer incident response services; see [55, 60] for example. This, however, is not always the case and insurers may have strict (financial) limits on their provision of such third-party offerings.

In the overall analysis, valuable insights have emerged regarding the control level of ISO 27001. The primary questions in the forms focus on Security control categories, particularly emphasizing 13.1 Network security management, encompassing elements such as network controls, security of services, and network segments. Additionally, Security categories A.18.1 Compliance with legal and contractual requirements and A.18.1.1 Identification of applicable legislation and contractual requirements feature prominently, suggesting an evaluation of the applicant's commitment to enhancing compliance efforts.

Several questions are also asked in line with A.71 on Information Security continuity and A17.2 Redundancies, which are centred on technologies ensuring coverage and resilience through redundancies and alternative processing facilities. A.6.1 Internal Organization is also notable, with questions focusing on Information Security roles, responsibilities, and Segregation of Duties. Finally, the examination reveals a strong emphasis on A.10.1 Cryptographic controls and the closely linked A.12.2 Protection from malware, underscoring the importance of security measures against malware.

4.4 NIST Cybersecurity Framework (NIST CSF)

Finally, we assess cyber insurance proposal forms when benchmarked against the NIST CSF with an aim of investigating the extent of their alignment.

Figure 6 shows the percentage of forms that request none, part, or all Security Categories in a Security Function for the NIST CSF. As depicted, only Function 3; Detect (identifying the occurrence of malicious activity or events) of the CSF was fully covered by 2 (3%) of the forms analysed. However, none of the forms presented questions that cover all requirements for controls under the remaining 4 Functions of the NIST CSF, i.e., Identify (developing an organizational understanding to manage cybersecurity risk), Protect (developing and implementing controls to ensure delivery of business services), Respond (taking action against the occurrence of a malicious event) and Recover (maintaining resilience and restoring business operations after an incident). One reason for this may be the more granular nature of the controls in the NIST CSF. Unlike the ISO 27001 where some Security Clauses like Clause 5: Information security policies and Clause 10: Cryptographic controls have only one control, all Functions under the NIST CSF have a minimum of three security categories making it difficult for an insurance application form to addresses all controls without being excessively long and as such, potentially unusable.

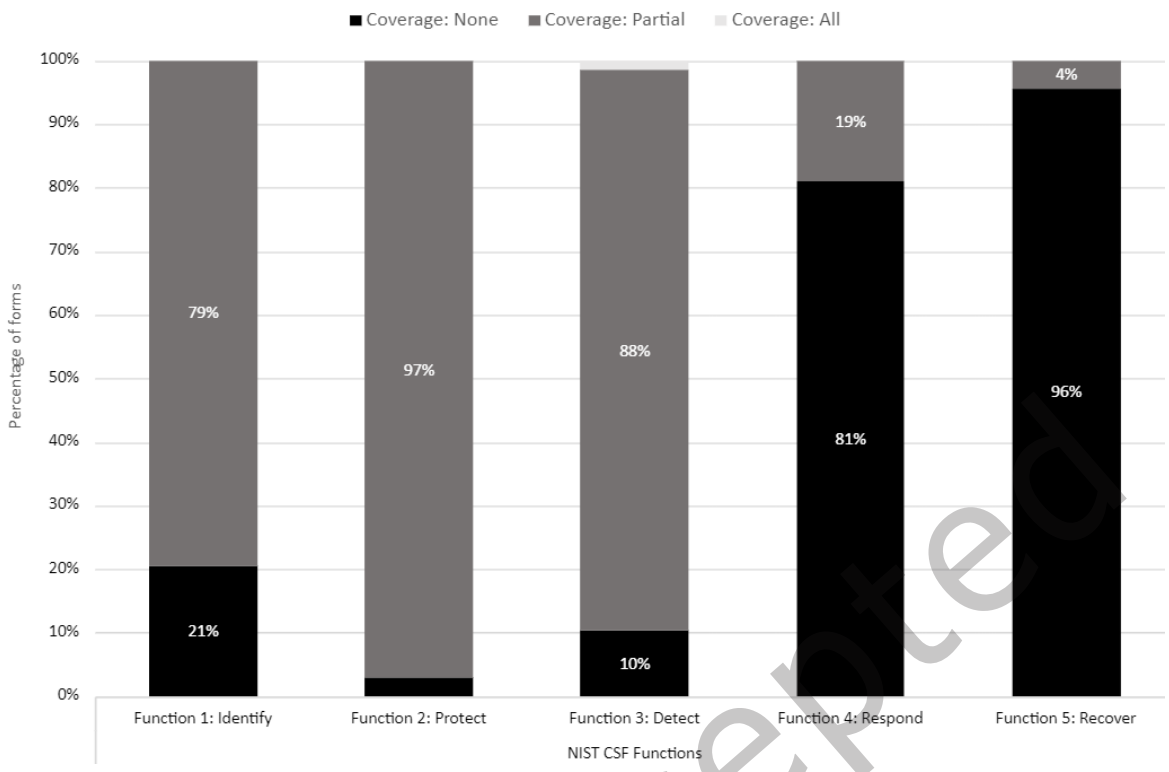

Figure 6: The percentage of forms that do not address any of the defined Security Control Categories in the various clauses of the NIST CSF

From the analysis of forms that partially cover the requirements of each of the Security Functions, i.e., mention at least one Security Category, we noted that 97% of the forms cover questions relating to Function 2: Protect. The majority of Security Categories under this Function such as backup and recovery, audit logging and vulnerability management are similar to Clause 12: Operational procedures and responsibilities of the ISO 27001 framework which also scored highly in the ISO 27001 assessment. Questions such as *"Do you maintain daily offline back-ups of all critical data?"* by [55] would fall under this category. This highlights a concentration of questions around preventative controls in the protection of information assets. We hypothesize that this could be because insurers regard protective controls as central to reducing cyber risk. In addition, backup is a key control in ransomware attacks – one of the most salient attacks over the last five years – and could therefore save both insurers and organisations.

A noteworthy finding from our analysis is that no form appears to address the Security Category Maintenance (PR.MA) from Function 3: Protect. This Security Category is concerned with maintenance and repairs of industrial control and information system components to check that they are performed in a manner that is consistent with policies and procedures. Neglect of this control may prove pivotal because organisations (i.e., those applying for insurance) may give access to third parties for system support and maintenance through remote access and this control requires that such access is approved, logged, and performed in a manner that prevents unauthorised access. This may be dangerous especially with outsourcing of services that requires remote support which, if compromised, could be exploited for malicious intent. In the recent past, we have seen a substantial rise in security breaches linked to third parties such as Solar Winds [85], Kaseya and Log4j that have highlighted third party dependency risk [42].

The second-most covered Function is Function 3: Detect which is covered by 88% of the forms. This Function is primarily concerned with security categories such as anomaly detection, security continuous monitoring and the detection processes necessary to ensure that incidents are detected early enough, and response strategies instituted to combat them. The Detection Processes (DE. DP) category in this Function for example, requires several controls such as: roles and responsibilities for detection should be defined for accountability, detection should comply with all applicable requirements and that detection is tested and continuously improved. Our

analysis identified that none of the forms goes into detail about how detection is implemented but instead focus on checking whether detection has been implemented. Questions such as "Do you utilize Intrusion detection or prevention systems" asked by majority of the forms including [31] and [96] do not seek to evaluate – even at a preliminary level – the setup, implementation, or effectiveness of the detection process.

We also find that Function 1: Identify is partially covered by 79% of the forms and is third in terms of coverage of Security Categories. This is somewhat surprising as this Function is concerned with the processes that involve identification of key risk sources through risk assessment, risk management, asset management and information security governance. One might expect that these would be key areas as they feed directly into protection mechanisms that should be implemented to counter related risks. This Function also covers controls pertaining to ensuring that legal and regulatory requirements including privacy and civil liberties obligations are understood and managed. One interesting pattern is that some forms do not only ask whether a privacy policy exists but also go a step further to check whether the policy is published and has been reviewed by an attorney or privacy specialist. An example is presented by [107] who ask, *"Do you have a written privacy policy?"* and then go further to state "*If yes; has it been reviewed by a HIPAA specialist or attorney?"*. Detail such as this is encouraging to see and demonstrates that some insurers (and thus, forms) are maturing in their assessment of cyber risk, even at the initial stage.

Table 3: The percentage of forms that do not address any requirements in the Security Categories required for each Function.

Function	Percentage
Function 1: Identify	21%
Function 2: Protect	3%
Function 3: Detect	10%
Function 4: Respond	81%
Function 5: Recover	96%

Table 3 presents the percentage of forms that do not cover any requirements of Security Categories required for each Function. The results reveal that 96% of the forms do not cover any requirements for Security Categories in Function 5: Recovery of the NIST CSF. This post-incident control finding is similar to Clause 16: Management of information security incidents and improvements of the ISO 27001 that was not covered by 60% of the forms. This indeed is alarming because enterprises need to possess controls to ensure that they quickly recover from a cyber incident. One reason for this finding could be that insurers posit that a good assessment of controls in Functions 1, 2 and 3 will ensure that incidents do not occur as there has been an effective measurement of risk exposure and the corresponding controls; this, of course, is not guaranteed and would not be good resilience practice. In addition, as some insurers provide response and recovery services – as mentioned earlier – they may not believe that there is a critical need to request or evaluate recovery capabilities of applicants at this stage.

The second Function that is least covered by the forms is Function 4; Respond which is concerned with Response Planning, Communications, Mitigation, and so on. 84% of forms did not address any requirements in Function 4 of the NIST CSF. Poor external and internal communication after an incident can have devastating effects on an organisation's brand and reputation. Over the years, there have been an increasing number of cases of poor incident response and communication even amongst large corporations [20, 80]. As such, a neglect of controls in this area can have effects on the cyber exposure of the applicant. Like Function 5, the absence of such controls may suggest that insurers are more interested in preventative measures and would view their role as directly supporting incident response. While it is impossible to decipher the reasons from this study alone, we would expect that insurers also value response and recovery.

Our analysis at the NIST category and subcategory levels also revealed some noteworthy findings. For instance, Function 1: Identify, Governance (ID. GV) emerged as a frequently occurring category, addressing policies, procedures, and processes crucial for organizational governance and guiding the cybersecurity program. Subcategories like ID. GV-2 (Cybersecurity roles and responsibilities), ID. GV-3 (Legal and regulatory requirements), and ID. GV-4 (Governance and risk management) that focus on cybersecurity risks fall under this category. Notably, Supply Chain Risk Management (ID.SC), vital for third-party relationships, is less

explored in this context. The Protect Function's Awareness and Training (PR.AT), Data Security (PR.DS), and Identity Management, Authentication, and Access Control (PR.AC) which governs logical and physical assets attracts insurers' attention due to the several questions asked, as does the Protective Technology (PR.PT) category, emphasizing technical security solutions like firewalls for system and assets resilience across the business enterprise.

Finally, considering that NIST CSF is a US-oriented standard, we also assessed the alignment to forms used by U.S. insurers (this is similar to our CE and UK analysis). For completeness, we have included Table D.1 in the appendices to show the percentage of coverage of each Function of the NIST CSF based on forms from the US (n=26) and the entire data set (n=68). Notably, when focusing solely on U.S. forms as opposed to the entire dataset, there is an increase in the percentage of forms that do not encompass any of the NIST Functions' requirements. Functions 2 and 3 show a 5% increase each, moving from 3% to 8% and 10% to 15%, respectively, while Functions 4 and 5 exhibit a 4% increase. Additionally, there is a general decrease in forms covering partial requirements of controls within the NIST Functions. Functions 3 and 2 experience the most significant decreases, with 7% and 5%, respectively. Regarding forms covering all requirements of controls in the NIST Functions, there are no significant changes, except for Function 3, where the percentage increases from 1% to 4% when only U.S. forms are considered. In contrast to the Cyber Essentials Scheme, this suggests that U.S. insurers might not actively embrace the NIST framework, indicating a comparatively low adoption in the U.S.

The next section builds on the findings herein and discusses the results considering the goal of our research. We first reflect on the general aim and the question of insurance's promotion of best practice. Next, we reflect on the value of current insurance application forms, but also the challenges that they face. Finally, the findings of this research are compared to the state of the art to understand changes in the sector, while also highlighting our work's novelty.

5 DISCUSSION AND IMPLICATIONS

5.1 Cyber security best practice and cyber insurance

This research primarily sought to investigate the assertion that cyber insurance currently promotes cyber security best practice in organisations, through an analysis of how security controls viewed as crucial by insurers – i.e., those featuring in application forms – compare to (or align with) security best practice as defined by international and national standards. Best practice, in our context, is defined by the ISO/IEC 27001 international security standard, the NIST Cybersecurity Framework (NIST CSF) and the more fundamental UK Cyber Essentials (CE) scheme. The insights from this research are pertinent and topical to the security community given the growing uptake of cyber insurance, and the influence that providers can have on the security posture of businesses.

Broadly, while our analysis reveals that there is some notable level of alignment between forms and control standards, it is far from a natural match to the extent where it may be concluded that insurance clearly promotes all security standards and best practices. In NIST CSF, in particular, it was extraordinary to observe the extremely low coverage of recommended practices from the Response and Recovery security control domains in the forms. There could be several reasons for this, but one may stem from the perspective that forms are particularly useful for assessing SMEs' risk posture. In this case, although SMEs arguably have a high frequency of incidents, the severity is low, and the insurer's liability is capped at the indemnity limit. While recent research indicates a rise in the frequency of cyber incidents over the past two decades, the overall severity of these incidents has not seen significant changes [117]. This trend could therefore prompt insurers to shift their assessment focus. Rather than solely considering incident severity, insurers are increasingly inclined to prioritize assessing applicants based on their protective measures. This shift is evident in the emphasis on preventive controls and risk reduction strategies among insured SMEs, aligning with capped liability limits. Notably, this approach considers the interconnected relationship between incident severity and the effectiveness of Response and Recovery measures, distinguishing it from the frequency of incidents and other control measures. Even in the case where response and recovery services are provided by insurers (or their delegated parties), it is reasonable from a security risk management perspective to expect that there should be some partial representation of these topics in forms.

For ISO 27001, there was arguably a stronger association with forms, though system acquisition, development and maintenance, information security incident management, and physical and environmental security are exceptions. Incident management is the most salient of these given it applies to all organisations; thus, there is a clear justification for it to be requested (i.e., the opposite of our finding). Even the less obvious topic of System acquisition is critical if we reflect on the evolving nature of businesses and technology, and the fact that companies often go through changes including Mergers and Acquisitions, technological changes like remote working and cloud computing which present new sources of risk. Overall, application forms aligned the best to UK CE, likely due to the more fundamental and constrained focus of the scheme. The Technical Control Themes with the lowest representation in this case were Secure Configuration and user access control, but even these were present in a majority (>60%) of forms.

Reflecting across the standards and forms, we found an imbalance between technical control questions (e.g., those presenting best practices around the presence of firewalls, use of encryption, etc.) and procedural/governance control questions (focused on policies and procedures), with the former often favoured. This can be motivated by various factors, such as a preference for tangible, technical security practices/controls, which would not be unforeseen given the move by some insurance providers towards schemes oriented around security products; see [87]. This is also in concert with broader studies that argue that cybersecurity is often narrowly seen as only a technical issue, disregarding its broader aspects like economics, psychology, management, and legal concerns. [118] highlighted that security failures are not solely due to design flaws but are equally influenced by inadequate incentives. This underscores the importance of non-technical factors like incentives, human behaviour, legal frameworks, and organizational structures in shaping cybersecurity. Taking a holistic approach that addresses these multidimensional aspects is vital for building robust cybersecurity strategies and mitigating risks across various domains. There also was an indication that insurers are particularly interested in assessing preventive and protective abilities and security practices of applicants. Questions asked by the application forms are generally skewed towards protective technical controls rather than administrative controls that provide the measure for strategic alignment. In addition, there appears to be a general lack of corrective controls aimed at containing cyber incidents (as seen with CSF and ISO 27001 specifically) though there is notable concentration on the backing up of company data. Some forms including [52] go ahead and ask whether this backup is encrypted and stored in an isolated part of the network which cannot be affected by a breach on the insured's core network.

The significant partial coverage of controls in the standards by insurance forms was to some extent encouraging and should not be overlooked given the reality of the forms (i.e., the fact they need to be as short as possible yet as informative as possible). The CSF, in particular, will always be a challenging standard to compare with considering the detailed guidance (and control sets) provided for companies who adopt the framework. Notwithstanding that point, there is significance in comparing with insurance application forms as they provide insight into how the controls valued by insurers (often based on their own understanding of cyber risk and threats, claims made to them after security incidents [10]) relate to standards and best practices from the security industry. Governments interested in cyber insurance, particularly those in the UK, US, and Australia, may reflect on our findings to initially explore which standards and controls are expected by insurers in their jurisdictions. For instance, the UK's NCSC can note that UK insurers do align well with three of the CE core control areas, but there is room for improvement with the other two. This may even help to explain future eventualities where there is poor representation from these latter two controls; the assumption being that requirements by cyber insurers may be impacting which controls organisations in a country choose to implement.

In sum, our findings allude to an underrepresentation of best practice standards and controls in proposal forms generally, thus partially questioning the assertion that insurance supports all best practice. This is a significant conclusion in light of arguments suggesting that insurance can incentivise security standards and best practices in organisations [7]. [7] identifies various methods through which cyber insurance can encourage cyber security behaviour, although it acknowledges several notable limitations. Their argument suggests that cyber insurers could effectively motivate improved cyber security practices by offering premium discounts as rewards for sound risk management practices. However, our findings, albeit limited to proposal forms, present a contrasting viewpoint. The absence of alignment to security standards, crucial for supporting an

incentivization argument, appears to be non-existent in our study, making it challenging for such benefits to be extended.

5.2 The value and challenges with current insurance application forms

While we are unable to comment on the reasons for this underrepresentation based on our work, potential causes could link to the different processes through which insurers determine and prioritize threats and vulnerabilities, the perspective that insurance forms may be much more dynamic than control standards (thus likely to change based on current threats or attacks), or simply, a difference in priorities (we saw this with insurers concentrating more on preventative as opposed to responsive/corrective controls). Additionally, insurers might prioritize diverse areas or risks, and consequently, their selection of specific control measures may be influenced by their specialization, resulting in a lack of comprehensive coverage of standards across the forms. Given this reality, achieving standardization among proposal forms becomes nearly impossible due to the diverse nature of insurance, involving variations such as exclusion clauses or coverage of distinct facets of cyber loss. Despite this, evaluating the most frequently occurring or requested controls provides valuable insights, enabling us to draw conclusions about coverage and alignment without assuming a convergence among these controls.

In addition to understanding whether insurance forms promote security best practice, there are other considerations that arise from our research. One of these relates to the value of application forms and the second to the issues that may emerge with them. With respect to the former point, forms can be a quick way for businesses to gain some appreciation of what (security controls) an insurer is interested in, and in certain scenarios even provide a gentle introduction to cyber security – this is particularly the case for an SME who may not be security aware. We saw that some insurers like [55, 113] have tried to make the forms usable by providing definitions of key security terms and controls to allow applicants to gain a better understanding of the questions. Such an approach increases the usability of the forms, supports businesses who lack security expertise, and ensures that information collected is useful and can be used to better assess the applicant's security posture. Other providers (e.g., [105]) have also added links for applicants to download and read key security standards like Cyber Essentials, thus again demonstrating the close ongoing relationship between insurance and security. These types of information and activities are positive, however not widespread in forms.

To complement the point above, from the information requested in forms, it is clear that some insurers are also willing to offer immediate follow-on assessments to potential clients based on their responses. For instance, [89] asks applicants whether annual or more frequent penetration tests are performed on their network. For those that respond "No", the insurer asks to connect them to a specialist who can undertake an initial remote audit – i.e., gather further technical information. This audit is beneficial to the insurer as it provides more insight into the risk, and to the prospective policyholder as they may receive some open feedback on their risk posture. Some insurers take an additional step by recommending a free anti-malware solution, as evidenced in [39], where they inquire whether the applicant agrees to receive a complimentary Avast product that necessitates installation within 30 days.

Issues have arisen with forms as well, however. For instance, many questions presented in forms only require information about the existence or design of controls rather than their effectiveness. For example, the existence of an Intrusion Detection System or security awareness program does not speak to whether it is functioning well or that it is setup or configured as appropriate. These are critical points given that misconfigurations are a leading cause of breaches [66] and that security training and awareness is easy to get wrong (e.g., [45]). Adding to this point, a majority of the security questions presented are either overly rigid or ambiguous. For example, "*Do you [...] regularly apply updates/patches?"* is not specific on what is deemed as "regularly". Furthermore, some forms frame questions as *"Do you use anti-virus software and apply updates/patches monthly?"* which may – given forms are formally assessed as input to premiums – prompt companies that do this fortnightly to respond "No" to this question. To better assess the exposure of applicants at the proposal form stage therefore, it seems prudent to request information on the effectiveness of controls deemed critical to developing a realistic risk profile and also that forms are redesigned to be more flexible and better explained. As the insurance market hardens further (i.e., there is less coverage of incidents, lower limits, higher costs of

insurance products, and less providers [6], this will present insurers with the opportunity to rework forms to ask additional pertinent security questions.

Finally, as insurers look to gather more information on organisations prior to brokering or underwriting a risk, there is also a new concern that is worth debating. That is, the reality that malevolent actors may attack insurers for reconnaissance and to map the IT landscapes of many businesses. Questions such as those from [105] that require the make and model of the firewall, the version of the anti-virus software and machine distribution by Operating System could be considered invaluable to attackers (and potentially intrusive to policymakers). The fact is that whereas insurers may want to collect as much information as possible to better assess the business' risk, this may inadvertently expose the applicant to severe consequences because insurers themselves have become targets for hackers [98] as evidenced by the recent attacks on CNA Financial, Tokio Marine and AXA [73,102]. This can add to the tension between insurers and their (prospective) clients, especially now as the insurance market has hardened and insurance providers have much more power to make demands of businesses prior to underwriting a policy.

5.3 Reflecting on related work

Woods et al. [12] and Romanosky et al. [15] are the two closely related articles to our research. Woods et al. [12] engages in an analysis of proposal forms with respect to ISO 27001 and the CIS CSC, and [15] adopts a less structured analysis by using open coding to identify types of controls present in forms. These differences – along with our approach which allows for varying measurement of coverage – make it challenging to meaningfully compare any control areas except ISO 27001 across our work and that of [12] in particular. At a high level, however, we can see a reasonably strong concentration on compliance with regulations in all three pieces of work. Technical controls also feature heavily as depicted in the technical question summary in [15] and the analysis of CSC and ISO in [12]. The most notable differences include the lack of controls on personnel hiring practices in [15] as compared to this work and that of [12], and the fact that [15] were able to report on the presence of questions on the company's security incident and loss history and IT security budget/spending. The latter of these points is attractive for future work as it suggests that if some partial open analysis of text is conducted – instead of only relying only on control-set comparisons – there may be some value to be garnered from the assessment.

Focusing our comparison on ISO 27001 given its coverage in our work and [12], the results of our study show some similarities. Clause 10: Cryptography and Clause 18: Compliance for instance, which are the two of the three most covered clauses in our work match with the second and fourth most mentioned sub-controls in [12] i.e., Compliance with legal and contractual requirements (18.1) and Cryptographic controls (10.1). It is not surprising that compliance with regulation continues to score highly especially as fines on breaches continue to increase. A primary difference in the results is the high score for Clause 5: Information security policies which was not covered by [12]. The forms in our study also reveal concentration on privacy with questions around compliance to GDPR and privacy rights. However, there is neglect of governance aspects including policies and procedures which form the foundation and chart the direction of a cyber security program.

We also noted that Clause 14: System acquisition, development and maintenance, Clause 11: Physical and environmental security and Clause 16: Information security incident management score relatively poorly in both studies. For example, [37] had questions that cover Clause 14: System acquisition, development and maintenance which was similar in the previous study which examined the 2014 Ascent form. AXIS Insurance [44] was the only other form to cover this clause in the self-assessment questionnaire. This means that seven years later, these areas are still being overlooked by most insurers. Additionally, although Clause 16: Information security incident management of ISO 27001 has only one Security Control Category, 60% of the forms do not ask any questions that relate to it. This is further supported by the fact that 96% of the forms do not cover any requirements for controls in a similar Function i.e., Function 5: Recovery of the NIST CSF.

There are areas where differences are apparent which may represent changes in the perceptions of insurers over time as the industry has matured. For instance, in [12]'s analysis, Clause 9: Access Control, Clause 13: Communications security and Clause 15: Supplier relationships were very poorly addressed. In our work, we instead find Clause 9 to be partially addressed by ~75% of forms, Clause 13 to only be excluded in ~9% of forms, and Clause 15 to be fully or partially addressed by ~56% of forms. This, broadly speaking, represents some level

of improvement in the coverage of certain controls. Focusing on Clause 15 as an example, this change is noteworthy especially as it seems to accommodate the growing need to manage the security of supplier relationships. Over the last five years, there has been several significant data breaches, including the attacks on Best Buy, Kmart, and Delta via a third-party chatbot [88] and a damaging security breach at GE due to a hacked vendor [75], which could have had an impact on insurers' risk decisions.

In sum, while there have been updates to cyber insurance proposal forms since [12]'s analysis of forms from 2008-2016, there also appear to be a number of similarities in their alignment with ISO 27001 based on our current analysis (with forms from 2016-2023). The lack of significant change is somewhat surprising considering the shifting technology (e.g., move to remote working due to the COVID-19 pandemic) and security (e.g., the ongoing threat of ransomware) landscape, and hardening cyber insurance market over the last four years in particular. One reason for this may be time and that it is too soon to see changes fully represented in forms. Insurers may still be gathering data on potential threats and insurance policy claims to inform decisions on the most suitable updates to make.

5.4 Limitations

The primary limitation of this work is that it only investigates one stage of the insurance risk assessment process and does not consider other mechanisms of collecting information such as follow-up telephone calls, in-person meetings, and on-site inspection. As such, we do not gather the information that prospective insureds capture in these proposal forms but rather, use the forms as a representation of the controls that insurers want at client premises. In addition, some insurers may use other avenues which have not been considered to solicit information from third-party service providers to understand the applicant's aggregate risk. The relatively new InsurTech industry is one example which relies more on technology (e.g., network scans and other technical mechanisms) in cyber insurance to assess cyber risk. The reason we scope ourselves only to proposal forms is threefold. First, they provide a crucial and highly used initial mechanism to assess the security risk posed by an organisation. Second, these forms may be used alone to underwrite small risks (e.g., SMEs) – where the value of the policy is not large enough to justify additional assessments or resources. Third, the openly available nature of the accessed forms allows insight into an industry that would be challenging otherwise, and as has been seen in other work (e.g., [12]), does have research and practitioner significance. We therefore focus on gathering as many forms as possible to inform our analysis, improving on the numbers of forms in [15] (34) and [12] (24). Moreover, while examining only forms that are available online may represent a limited scope for our work, it has proved an efficient approach to provide insight into the industry and several of the top cyber insurers (as listed in [76]).

Another limitation is that some questions may correspond to more than one control subcategory and as such, some degree of subjectivity is inevitable, and a decision is made to classify the question into the best category based on the intention of the insurer. We are transparent about this process and include an explanation of our mapping, tables for our mapping of each of the forms, and links to forms to allow for future studies to reflect on our work. Finally, it is important to also note that although this study has evaluated forms from countries which are considered as industry leaders in cyber insurance, assessment of forms from other markets (e.g., Sweden, France, Singapore, Canada, Israel, India) may produce different results as to the extent insurance promotes security best practice. Our findings are therefore limited to the geographic regions studied.

6 CONCLUSION AND FUTURE WORK

The security of modern-day systems is more complex than it has ever been. As organisations look to build resilient infrastructures, cyber insurance has emerged as a potential mechanism to transfer residual cyber risk. Within the risk underwriting process, insurers are in a unique position to influence an organisation's security practices, that is, if policyholders agree to adopt certain security controls, then insurers may be more likely to accept the risk and even lower the premium. Cyber insurance application/proposal forms are one of the most common techniques through which insurers gain some initial assessment of the risk posed by companies. In this study, we sought to examine such forms produced in the last seven years to assess applicants' cyber posture to ascertain to what extent the current assessment methods align with the ISO/IEC 27001 international security standard, the NIST Cybersecurity Framework (NIST CSF) and the UK's government-backed Cyber Essentials

(CE) scheme. In total, we conducted a thematic analysis of 68 cyber insurance proposal forms provided by companies in the UK, USA and Australia and benchmarked them against the three established security frameworks. To our knowledge, this work presents a novel research direction as it is the first study to systematically analyse and benchmark cyber insurance proposal forms against the NIST CSF and CE, and to provide an updated analysis of forms – given the significant changes in the cyber security industry over the last three years – against ISO 27001.

Our results provide evidence that insurance forms do, to an extent, promote cyber security best practices but there is also a noteworthy degree of underrepresentation in their coverage of key standards such as NIST, ISO 27001 and CE. There are, however, many areas that are overlooked which suggests that if businesses purely follow guidance from forms, they will miss several critical security controls. This further highlights the tension between controls that insurers may value most versus those viewed as best practice in the security industry. Insurers might prioritize measures that lower the occurrence of attacks on their customers, especially small and medium-sized enterprises (SMEs). Alternatively, they might solely emphasize measures preventing the impact of loss caused by the most financially damaging threat actors. Concerning policyholders, as observed in the Cyber Essentials Scheme Process Evaluation [65], the main driving force behind government contractors embracing Cyber Essentials tended to be more reactive than proactive. This was due to companies aiming to secure government contracts rather than proactively enhancing their cybersecurity stance. Our findings will be of interest to policy makers in assessing the extent to which the insurance industry promotes security best practice and alignment to specific standards. Furthermore, international, and national bodies such as ISO, the NIST and the UK's NCSC, may find value in understanding how insurance requirements align with their control sets.

There are various avenues for future work in this domain. Thus far, research has investigated only the US, UK, and Australia, but in our work, we found proposal forms from Canada, Singapore, India, and many other countries. Follow-on studies could widen the literature base by assessing other countries assuming enough forms can be found. This could provide a basis for comparison with our work, and further inform the influence of cyber insurance internationally. Another complementary area for research is to engage directly with cyber insurance providers – for instance, through interviews or surveys – to understand how they determine controls requested in proposal forms and the extent to which they are influenced by security best practices and standards. Simultaneously, a study could be done with businesses that have purchased or are considering purchasing cyber insurance to explore how controls requested by insurers influences their mid-to-long term security investment decisions.

Insurers might incentivize applicants to implement specific security measures and offer reduced premiums as a result. However, solely relying on the forms might not provide a comprehensive understanding of this practice. Future research could incorporate pricing data to build a more conclusive argument regarding the correlation between adopted security controls and the potential impact on premiums. Finally, during our search for proposal forms, we found that there are an increasing number of cyber insurance policy documents available online (e.g., [59]). As such, further research could be conducted to analyse the content of these forms to ascertain the extent to which security controls are explicitly required, and how the security requirements in proposal forms are replicated (if at all) in the policy documents themselves. These works would be extremely informative at elucidating the interplay between cyber security and cyber insurance.

REFERENCES

[1] H. R. Skeoch. 2022. Expanding the Gordon-Loeb model to cyber-insurance. 112, (July 2022), 102533.

[2] CISA. 2014. Cybersecurity Insurance Industry Readout Reports. Retrieved June 5, 2022. from https://www.cisa.gov/publication/cybersecurity-insurance-reports

[3] HM Government & Marsh Ltd. 2015. UK Cybersecurity: The role of insurance in managing and mitigating the risk. Retrieved June 5, 2022 from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf

[4] ENISA. 2012. Incentives and barriers of the cyber insurance market in Europe. Retrieved June 5, 2022 from https://www.enisa.europa.eu/publications/incentives-and-barriers-of-the-cyber-insurance-market-in-europe/at_download/fullReport

[5] A. Cartwright, E. Cartwright, J. MacColl, et al. 2023. How cyber insurance influences the ransomware payment decision: theory and evidence. 48, (July 2023), 300–331. DOI: https://doi.org/10.1057/s41288-023-00288-8

[6] Gareth Mott, Sarah Turner, Jason R.C. Nurse, Jamie MacColl, James Sullivan, Anna Cartwright, and Edward Cartwright. 2023. Between a rock and a hard(ening) place: Cyber insurance in the ransomware era. 128, (July 2023), 103162. DOI: https://doi.org/10.1016/j.cose.2023.103162

[7] J. MacColl, J.R.C. Nurse, and J. Sullivan. 2021. Cyber Insurance and the Cyber Security Challenge. (July 2021). Retrieved from https://rusi.org/explore-our-research/publications/occasional-papers/cyber-insurance-and-cyber-security-challenge

[8] Threatpost. 2021. Cyber-Insurance Fuels Ransomware Payment Surge. Retrieved June 14, 2022 from https://threatpost.com/cyber-insurance-ransomware-payments/166580/

[9] H. Herath and T. Herath. 2011. Copula-based actuarial model for pricing cyber-insurance policies. 2, 1 (July 2011), 7–20.

[10] J.R.C. Nurse, L. Axon, A. Erola, I. Agrafiotis, M. Goldsmith, and S. Creese. The data that drives cyber insurance: A study into the underwriting and claims processes. In International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), IEEE.

[11] McKinsey 2021. Global perspectives on insurtechs. Retrieved June 5, 2022 from https://www.mckinsey.com/industries/financial-services/our-insights/global-perspectives-on-insurtechs

[12] D. Woods, I. Agrafiotis, J.R.C. Nurse, and S. Creese. 2017. Mapping the coverage of security controls in cyber insurance proposal forms. 8, 1 (July 2017)

[13] Advisen. 2020. The NIST Cybersecurity Framework and its role in Cyber Risk Management and Cyber Insurance. Retrieved June 5, 2022 from https://www.advisenltd.com/the-nist-cybersecurity-framework-and-its-role-in-cyber-risk-management-and-cyber-insurance/

[14] R. Pal, L. Golubchik, K. Psounis, and P. Hui. 2014. Will cyber-insurance improve network security? A market analysis. In IEEE INFOCOM 2014-IEEE Conference on Computer Communications, IEEE.

[15] S. Romanosky, L. Ablon, A. Kuehn, and T. Jones. 2019. Content analysis of cyber insurance policies: How do carriers price cyber risk? 5, 1 (July 2019).

[16] G. Uuganbayar, A. Yautsiukhin, F. Martinelli, and F. Massacci. 2021. Optimisation of cyber insurance coverage with selection of cost-effective security controls. 101, (July 2021), 102121.

[17] N. Shetty, G. Schwartz, J. Walrand, A. Acquisti, S.W. Smith, and AR. Sadeghi. 2010. Can Competitive Insurers Improve Network Security?. In Trust and Trustworthy Computing. Trust 2010. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-642-13869-0_2

[18] A. Tsohou, V. Diamantopoulou, and S. Gritzalis. 2023. Cyber insurance: state of the art, trends and future directions. 22, (July 2023), 737–748. DOI: https://doi.org/10.1007/s10207-023-00660-8

[19] I. Confente, G. G. Siciliano, B. Gaudenzi, and M. Eickhoff. 2019. Effects of data breaches from user-generated content: A corporate reputation analysis. 37, 4 (July 2019), 492–504.

[20] R. Knight and J.R.C. Nurse. 2020. A framework for effective corporate communication after cyber security incidents. 99, (July 2020), 102036.

[21] Marc Lelarge and Jean Bolot. 2008. Network externalities and the deployment of security features and protocols in the internet. In *Sigmetrics Performance Evaluation Review - SIGMETRICS*. DOI: https://doi.org/10.1145/1384529.1375463

[22] J.M. Lemnitzer. 2021. Why cybersecurity insurance should be regulated and compulsory. (July 2021), 1–19.

[23] U. Franke. 2017. The cyber insurance market in Sweden. 68, (July 2017), 130–144.

[24] Shauhin A. Talesh and Bryan Cunningham. 2021. The Technologization of Insurance: An Empirical Analysis of Big Data and Artificial Intelligence's Impact on Cybersecurity and Privacy. (July 2021), 967. DOI: https://doi.org/10.26054/0d-9y6k-1t55

[25] Association of British Insurers (ABI). 2022. Cyber insurance – growing the market to meet the global threat. Retrieved June 12, 2022 from https://www.abi.org.uk/news/blog-articles/2022/02/cyber-insurance-growing-the-market-to-meet-the-global-threat/

[26] S.A. Talesh. 2018. Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses. 43, (July 2018), 417–440. DOI: https://doi.org/10.1111/lsi.12303

[27] Rutherford, S. 2018. Who Has Cyber Risk Insurance Around the World? Retrieved June 14, 2022 from https://www.fico.com/blogs/who-has-cyber-risk-insurance-around-world

[28] MarketWatch. 2021. Cyber Insurance Market Size In 2021 with Top Countries Data, Leading Manufacturers Including Munich Re Group, Lockton and Key Insights to 2025 | Updated 108 Pages Report. Retrieved June 5, 2022 from https://www.marketwatch.com/press-release/cyber-insurance-market-size-in-2021-with-top-countries-data-leading-manufacturers-including-munich-re-group-lockton-and-key-insights-to-2025-updated-108-pages-report-2021-08-13

[29] 360 Underwriting Solutions. 2020. Cyber Insurance Proposal Form. Retrieved January 5, 2022 from https://www.360uw.com.au/wp-content/uploads/2020/05/360CYPFV420-Cyber-Proposal-Form.pdf

[30] Absolute Insurance Brokers. 2018. Cyber Risk Insurance - Proposal Form Retrieved January 5, 2022 from https://absoluteinsurancebrokers.co.uk/images/documents/Cyber_Proposal_Form_05032018.pdf

[31] AIG. 2017. Cyberedge Proposal Form. Retrieved January 5, 2022 from https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Financial-lines/Cyber/cyberedge-proposal-form-word.docx

[32] Allianz. 2019. Cyber Select Proposal Form. Retrieved January 5, 2022 from https://www.allianzebroker.co.uk/content/allianzebroker/en_gb/application/content/documents/commercial-products/speciality/cyber-insurance/cyber-select-proposal-form/_jcr_content/documentProperties/currentDocument.res/cyber-select-proposal-form_ACOM8380.pdf

[33] AmTrust North America. 2016. Cyber Liability & Data Breach Response Coverage Application. Retrieved January 5, 2022 from https://amtrustfinancial.com/getmedia/420f9c3a-c3f5-439c-aba6-13cefa78bee5/AFSI_Cyber-Liability-Application-10-18-16-FINAL.pdf

[34] Ando insurance. 2021. ando-cyber-event-protection-proposal. Retrieved March 15, 2023 from https://www.ando.co.nz/forms/ando-cyber-event-protection-proposal.pdf

[35] Apex Insurance Brokers. 2019. OSR_Proposal_Form1. Retrieved March 15, 2023 from http://apexinsurancebrokers.co.uk/wp-content/uploads/2020/01/OSR_Proposal_Form1.pdf

[36] Arch Insurance Company 2018. Arch-Cyber-Application. Retrieved March 15, 2023 from https://brokerresins.com/wp-content/uploads/2018/09/Arch-Cyber-Application.pdf

[37] Ascent. 2016. Ascent CyberPro Full Proposal. Retrieved January 5, 2022 from https://www.ascentunderwriting.com/docs/cyber/Ascent%20CyberPro%20Full%20Proposal.pdf

[38] AtBay. 2020. Technology & Cyber Insurance Application. Retrieved January 5, 2022 from https://www.at-bay.com/wp-content/uploads/2021/02/AB-TEO-APP-02-At-Bay-Technology-Cyber-Insurance-Full-Application.pdf

[39] ATC Insurance Solutions Pty Ltd. 2022. Cyber-SME-Proposal-Form-Declaration-EXTF176-v2. Retrieved March 15, 2023 from https://www.atcis.com.au/assets/downloads/Cyber-SME-Proposal-Form-Declaration-EXTF176-v2.pdf

[40] Aust Brokers. 2017. Cyber Insurance Proposal Form (SME). Retrieved January 5, 2022 from https://irp-cdn.multiscreensite.com/5e59d05e/files/uploaded/Cyber%20Proposal.pdf

[41] Aust Brokers. 2021. Cyber Insurance Proposal Form (Corporate). Retrieved January 5, 2022 from https://abcyberpro.com.au/documents/ACP-Cyber-Proposal(Corporate)2021.pdf

[42] Hilary Tuttle, 2022. Risk Management Magazine - 2022 Cyber Landscape. Retrieved July 21, 2023 from https://www.rmmagazine.com/articles/article/2022/02/01/2022-cyber-landscape

[43] Axis Capital. 2021. axis-1012098-0122. Retrieved March 15, 2023 from https://www.axiscapital.com/docs/default-source/default-document-library/axis-1012098-0122.pdf?sfvrsn=5de2cfe_0

[44] AXIS Insurance. 2020. AXIS Cyber Application AXIS 1012098 1020. Retrieved January 5, 2022 from https://www.axiscapital.com/insurance/cyber-technology-e-o/cyber#resource=8de4937e-1dc4-4cbc-8ad6-617fde1fb753

[45] BBC. 2021. West Midlands Railway sent staff fake bonus email in cyber-security test. Retrieved April 5, 2022 from https://www.bbc.co.uk/news/uk-england-birmingham-57065311

[46] Beazley Insurance. 2018. beazley-tmb-infosec-application. Retrieved March 15, 2023 from https://www.beazley.com/sites/default/files/2022-09/beazley-tmb-infosec-application.pdf

[47] Beazley Insurance. 2023. f00657_112017_ed._-_bbr_2017_-_full_application. Retrieved March 15, 2023 from https://www.beazley.com/sites/default/files/2023-02/f00657_112017_ed._-_bbr_2017_-_full_application.pdf

[48] Beazley Insurance. 2017. BEAZLEY BREACH RESPONSE APPLICATION. Retrieved January 5, 2022 from https://www.beazley.com/documents/TMB/Applications/beazley-bbr-fullform-application.pdf

[49] Berkley Insurance Company. 2020. Information Technology Liability Proposal Form. Retrieved January 5, 2022 from https://berkleyinaus.com.au/wp-content/uploads/2020/09/Proposal-Form-Information-Technology-Liability-2020.pdf

[50] BGi.uk. 2017. BGi-CrM-Proposal-Form. Retrieved March 15, 2023 from https://bgi.uk.com/wp-content/uploads/PDF/BGi-CrM-Proposal-Form.pdf

[51] Biz Lock. 2020. Cyber_App_V8.1.7. Retrieved March 15, 2023 from https://bizlock.net/downloads/Cyber_App_V8.1.7.pdf

[52] Biz Lock. 2021. BIZLock-TMHCC-Application-Short. Retrieved March 15, 2023 from https://www.moverschoiceinfo.com/wp-content/uploads/BIZLock-TMHCC-Application-Short.pdf

[53] Brooklyn Underwriting. 2020. Cyber Insurance Application Form. Retrieved January 5, 2022 from https://www.brooklynunderwriting.com.au/LiteratureRetrieve.aspx?ID=218444

[54] CFC Underwriting Limited. 2017. CFC-Cyber-App-9-2017-1-page. Retrieved March 15, 2023 from http://www.titleliability.com/wp-content/uploads/2017/12/CFC-Cyber-App-9-2017-1-page.pdf

[55] CFC Underwriting Limited. 2020. Cyber Private enterprise Application form. Retrieved January 5, 2022 from https://www.cfcunderwriting.com/media/3280/cyber-combined-application_private-enterprise_uk_w-cover.pdf

[56] DUAL. 2020. Cyber proposal form Security & privacy protection. Retrieved January 5, 2022 from https://www.dualgroup.com/sites/g/files/mwfley616/files/inline-files/DUAL%20Cyber%20proposal%20form%200820.pdf

[57] Chubb. 2017. Chubb Cyber Enterprise Risk Management Policy: New Business Application. Retrieved January 15, 2022 from https://www.chubb.com/content/dam/chubb-sites/chubb-com/microsites/titleagents/global/documents/pdf/cyber-privacy-insurance-new-business-application-short-form.pdf

[58] CM&F Group. 2019. CMF-Cyber-Liability-Insurance. Retrieved March 15, 2023 from https://www.cmfgroup.com/wp-content/uploads/2019/10/CMF-Cyber-Liability-Insurance.pdf

[59] Corvus Insurance. 2021. Corvus Policy for Smart Cyber Insurance™. Retrieved January 15, 2022 from https://info.corvusinsurance.com/hubfs/Corvus%20Smart%20Cyber%20Policy%20Form.pdf

[60] Corvus Insurance. 2022. Risk + Response Services. Retrieved April 15, 2022 from https://info.corvusinsurance.com/hubfs/Services/Risk%20and%20Response%20Services%20-%20Corvus.pdf

[61] Corvus Insurance. 2023. Corvus Smart Cyber Application. Retrieved March 15, 2023 from https://info.corvusinsurance.com/hubfs/Corvus%20Smart%20Cyber%20Application.pdf

[62] Cowbell Cyber Inc. 2023. Cowbell-Cyber-Prime-250_Renewal-Application. Retrieved March 15, 2023 from https://cowbell.insure/wp-content/uploads/2022/05/Cowbell-Cyber-Prime-250_Renewal-Application.Nov21.pdf

[63] CRC Insurance. 2019. Cyber Short form-Indications. Retrieved March 15, 2023 from https://www.crcgroup.com/Portals/0/Images/SectionDocuments/Cyber%20Short%20form-Indications.pdf

[64] Distinguished Programs. 2020. CyberNewBusinessApp2020-1. Retrieved March 15, 2023 from https://distinguished.com/wp-content/uploads/2020/12/CyberNewBusinessApp2020-1.pdf

[65] GOV.UK. 2023. Cyber Essentials scheme process evaluation. Retrieved 07 September, 2023 from https://www.gov.uk/government/publications/cyber-essentials-scheme-process-evaluation/cyber-essentials-scheme-process-evaluation.

[66] Truta, F. 2020. Misconfiguration Remains the #1 Cause of Data Breaches in the Cloud. Retrieved May 5, 2022 from https://securityboulevard.com/2020/04/misconfiguration-remains-the-1-cause-of-data-breaches-in-the-cloud/

[67] Emergence. 2020. Cyber Event Protection Proposal Form. Retrieved January 5, 2022 from https://www.emergenceinsurance.com.au/wp-content/uploads/2020/04/Emergence-Proposal-CEP-004.pdf

[68] G & M. 2018. G & M International Cyber Insurance. Retrieved January 5, 2022 from https://www.genmedinternational.com/media/1210/g-m-international-cyber-insurance_-002-002.pdf

[69] Global Re Broking Solutions Ltd. 2018. Cyber Liability Proposal Form. Retrieved January 5, 2022 from https://static1.squarespace.com/static/5885fc321b10e356f5436a0f/t/5ac7943c1ae6cf252760b7a4/1523029054630/GRBS+Cyber+Proposal+Form-+Jan+2018.pdf

[70] Great American Insurance. 2018. Executive Liability, Management Liability Solution Renewal Pro-posal. Retrieved January 5, 2022 from https://www.greatamericaninsurancegroup.com/docs/default-source/executive-liability/management-liability-solution-renewal-proposal-form-d56201.pdf?sfvrsn=cda149b1_6

[71] Hartford Steam Boiler Inspection and Insurance Company. 2020. HSB-Total-Cyber-Insurance-Application-2019. Retrieved March 15, 2023 from https://advisorsmith.com/wp-content/uploads/2021/11/HSB-Total-Cyber-Insurance-Application-2019.pdf

[72] Hiscox Insurance. 2019. CyberClear Proposal Form. Retrieved January 5, 2022 from https://www.hiscox.co.uk/sites/uk/files/documents/2017-04/13403-cyber-and-data-uk-prop.doc

[73] Hope, A. 2021. Cyber Insurance Firm Suffers Sophisticated Ransomware Cyber Attack; Data Obtained May Help Hackers Better Target Firm's Customer. Retrieved June 5, 2022 from https://www.cpomagazine.com/cyber-security/cyber-insurance-firm-suffers-sophisticated-ransomware-cyber-attack-data-obtained-may-help-hackers-better-target-firms-customers/

[74] HSB. 2020. HSB Total Cyber: Cyber Risk Insurance Application. Retrieved January 5, 2022 from https://www.munichre.com/content/dam/munichre/contentlounge/website-pieces/documents/HSB-Total-Cyber-Insurance-Application-2019.pdf/_jcr_content/renditions/original.media_file.download_attachment.file/HSB-Total-Cyber-Insurance-Application-2019.pdf

[75] CPO Magazine. 2020. Third Party Data Breach of GE Vendor Exposes Highly Sensitive Employee Information. Retrieved June 18, 2022 from https://www.cpomagazine.com/cyber-security/third-party-data-breach-of-ge-vendor-exposes-highly-sensitive-employee-information/

[76] Insurance Journal. 2022. Rapid Cyber Premium Growth by Fairfax, Tokio Marine Increased Share of Market. Retrieved June 5, 2022 from https://www.insurancejournal.com/news/national/2022/05/09/666871.htm

[77] ISO/IEC. 2013. ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls. Retrieved from https://www.iso.org/isoiec-27001-information-security.html

[78] ISO/IEC. 2022. ISO/IEC 27001 Information security management systems. Retrieved from https://www.iso.org/standard/27001

[79] N.K. Kibiswa. 2019. Directed Qualitative Content Analysis (DQlCA): A Tool for Conflict Analysis. 24, 8 (July 2019), 2059–2079.

[80] KrebsOnSecurity. 2017. Equifax Breach Response Turns Dumpster Fire. Retrieved June 15, 2022 from https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/

[81] Liberty Specialty Markets. 2017. Cyber Insurance Proposal Form. Retrieved January 5, 2022 from https://assets.libertyspecialtymarketsap.com/proposal-forms/pfr/cyber-proposal-form-au/

[82] London Australia Underwriting. 2020. Combined liability and cyber insurance for information technology, media and telecommunications companies. Retrieved January 5, 2022 from http://www.lauw.com.au/wordpress/wp-content/uploads/2020-01-ComTech_Proposal_Form-2.pdf

[83] Management and Professional Risks 2018. Management and Professional Risks. Crime & Cyber Crime Insurance MPR-Crime-Cyber-Crime-Proposal-Form. Retrieved January 5, 2022 from https://www.mprunderwriting.com/wp-content/uploads/MPR-Crime-Cyber-Crime-Proposal-Form.docx

[84] Management and Professional Risks 2019. Cyber Incident Response and Insurance MPR-CIRI-Proposal-2019 Retrieved January 5, 2022 from https://www.mprunderwriting.com/wp-content/uploads/MPR-CIRI-Proposal-2019.pdf

[85] Mandiant. 2020. Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor. Retrieved June 5, 2022 from https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

[86] Marsh LLC. 2020. Cyber Liability Insurance Application Form. Retrieved January 5, 2022 from https://www.marsh.com/content/dam/marsh/Documents/PDF/en_au/cyber-liability-insurance-application-form.pdf

[87] Marsh LLC. 2023. Using data to prioritize cybersecurity investments®. Retrieved July 5, 2023 from https://www.marsh.com/us/services/cyber-risk/insights/using-cybersecurity-analytics-to-prioritize-cybersecurity-investments.html

[88] Forbes. 2018. Hacked Chat Service Exposes Data From Best Buy, Sears, Kmart And Delta. Retrieved May 25, 2022 from https://www.forbes.com/sites/leemathews/2018/04/09/hacked-chat-service-exposes-data-from-best-buy-sears-kmart-and-delta/

[89] MFL Professional Insurance Brokers. 2017. Cyber Combined Application Form. Retrieved October 5, 2021 from https://www.m-f-l.co.uk/document/cyber-combined-application-from/20-%20Wordings/Intellectual%20Property/Cyber%20Insurance%20Proposal%20Form%206.8.19.pdf

[90] Miller Insurance. 2018. Proposal Form. Retrieved January 5, 2022 from https://www.miller-insurance.com/-/media/Images_and_downloads/Specialisms/Downloads/2021-Solicitors-Proposal-Form.pdf

[91] NCSC. 2023. About Cyber Essentials. Retrieved June 28, 2023 from https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf

[92] NIG. 2018. Cyber Cover Proposal Form. Retrieved January 5, 2022 from https://nig.com/media/3339/nig101009b-05-18-cyber-proposal.pdf

[93] NIST. 2018. Cybersecurity Framework Version 1.1. Retrieved January 5, 2022 from https://www.nist.gov/cyberframework/framework

[94] NMU. 2017. Computer Cyber Insurance Proposal Form. Retrieved January 5, 2022 from https://www.nmu.co.uk/wp-content/uploads/2019/07/NMU_Cyber_Insurance_Proposal_form.pdf

[95] Nova Casualty Company. 2018. cyber-application. Retrieved March 15, 2023 from https://www.safehold.com/siteassets/documents/cyber-application.pdf?v=48f047

[96] OBF Insurance. 2018. Cyber Proposal Form Retrieved January 5, 2022 from https://www.obf.ie/wp-content/uploads/2018/10/12-Cyber-Proposal-form.pdf

[97] Optimum Specialty Risks. 2021. OSR-MidMarket-v1.4. Retrieved March 15, 2023 from https://www.optimumsr.co.uk/wp-content/uploads/2021/04/OSR-MidMarket-v1.4.pdf

[98] Wallace, M. 2021. Why are insurance companies being targeted by hackers? Retrieved April 5, 2022 from https://www.insurancebusinessmag.com/uk/news/cyber/why-are-insurance-companies-being-targeted-by-hackers-260130.aspx

[99] Professional Insurance Agents Ltd. 2019. pia_cyber. Retrieved March 15, 2023 from https://www.professionalinsuranceagents.co.uk/forms/pdf/pia_cyber.pdf

[100] ProRisk. 2019. Cyber & Privacy Liability Proposal Form. Retrieved January 5, 2022 from https://www.prorisk.com.au/siteassets/documents/proposal-forms/prorisk-cyber--privacy-liability-proposal-form-writable-v04.21.pdf

[101] QBE Insurance. 2016. 2016 Full Cyber Proposal Form. Retrieved January 5, 2022 from https://qbeeurope.com/documents/index/2789 https://www.nmu.co.uk/wp-content/uploads/2019/07/NMU_Cyber_Insurance_Proposal_form.pdf

[102] Rapid7. 2022. The Big Target on Cyber Insurers' Backs. Retrieved April 5, 2022 from https://www.rapid7.com/blog/post/2022/02/08/the-big-target-on-cyber-insurers-backs/

[103] Reuters. 2021. Millions of websites offline after fire at French cloud services firm. Retrieved January 5, 2022 from https://www.reuters.com/article/us-france-ovh-fire-idUSKBN2B20NU

[104] Routen Chaplin. 2017. Cyber Insurance Enquiry Form. Retrieved January 1, 2022 from https://routenchaplin.co.uk/images/documents/files/Routen-Chaplin-Cyber-Insurance-Enquiry-Form.pdf

[105] RSA (Royal & Sun Alliance) Insurance. 2017. Commercial Crime Protection & Cyber Risk Insurance. Retrieved January 5, 2022 from https://heraindemnity.co.uk/uploads/RSA_Cyber_Risk_Proposal_form.pdf

[106] Sura Technology Risks. 2020. Cyber Insurance Proposal Form. Retrieved January 5, 2022 from https://www.sura.com.au/assets/Uploads/Cyber-Insurance-Proposal-Form3.pdf

[107] TDC Specialty Underwriters. 2017. Cyber Insurance Application. Retrieved January 5, 2022 from https://www.hpsi-ins.com/wp-content/uploads/2018/07/TDC-Speciality-Cyber-Insurance-App.pdf

[108] The Doctors Company. 2017. cyber_app. Retrieved March 15, 2023 from https://www.tdia.com/files/cyber_app.pdf

[109] The Hanover Insurance Group, Inc. 2017 Private Company Advantage Retrieved March 15, 2023 from https://sites.hanover.com/linec/docs/904-7001.pdf

[110] The Hartford. 2022. cyber-choice-application. Retrieved March 15, 2023 from https://s0.hfdstatic.com/sites/the_hartford/files/cyber-choice-application.pdf

[111] TK Specialty Risks. 2019. Proposal Form Cyber Liability Insurance. Retrieved January 5, 2022 from https://www.amcinsurance.com.au/wp-content/uploads/2019/08/Cyber-Proposal-Form.pdf

[112] Tokio Marine HCC. 2018. Cyber Security Insurance Proposal Form. Retrieved January 5, 2022 from https://www.tmhcc.com/-/media/RoW/Documents/PI/Cyber/Cyber-Proposal-Form.pdf

[113] Tokio Marine HCC. 2021. NetGuard® Plus Cyber Liability Insurance Application. Retrieved January 5, 2022 from https://www.crcgroup.com/Portals/34/Flyers/NetGuard%20Plus%20Application%20March%202021_NGPNBA-12021.pdf?ver=2021-04-29-081903-530

[114] Travelers Insurance. 2019. CyberRisk Application. Retrieved January 5, 2022 from https://www.travelers.com/iw-documents/apps-forms/cyberrisk/cyb-14102.pdf

[115] Travelers Insurance. 2020. Tech PI Cyber UK NB Proposal Form. Retrieved March 15, 2023 from https://www.travelers.co.uk/iw-documents/uk/documents/Tech%20PI%20Cyber%20UK%20NB%20Proposal%20Form%20TRV3009.pdf

[116] United States Liability Insurance Company. 2021. Dapp_Professional_cyberliability. Retrieved March 15, 2023 from https://customers.usli.com/sites/dapps/Dapp_Professional_cyberliability.pdf

[117] Eling, Martin, and Ibragimov, Rustam and Ning, Dingchen. 2023. Time Dynamics of Cyber Risk. DOI: http://dx.doi.org/10.2139/ssrn.4497621

[118] Ross, Anderson, and Tyler Moore. 2006. The Economics of Information Security. DOI: https://doi.org/10.1126/science.1130992

[119] References of Technology and Information Documentation. 2023. Correspondence between controls in ISO/IEC 27002:2022 and controls in ISO/IEC 27002:2013. Retrieved December 28, 2023 from http://www.itref.ir/uploads/editor/d3d149.pdf

A APPENDICES

A.1

Table A.1: Overview of the contents of each Function of NIST CSF (NIST, 2018)

Function	Contents
Function 1: Identify	Develop an organisational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
Function 2: Protect	Develop and implement appropriate safeguards to ensure delivery of critical services.
Function 3: Detect	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
Function 4: Respond	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
Function 5: Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Table A.2: Overview of the contents of each clause of ISO/IEC 27001 (ISO, 2013).

Clause	Contents
Clause 5: Information security policies	Developing an effective governance framework through development and review of policies.
Clause 6: Organization of Information Security	Developing organisational roles for Information Security and controls for mobile devices and remote access.
Clause 7: Human Resource Security	Ensuring HR Security through the employee's lifecycle
Clause 8: Asset Management	Protection of assets through asset inventory, classification, and adequate protection mechanisms.
Clause 9: Access Control	Deals with controlling access to business resources and ensuring employees are aware of their responsibilities.
Clause 10: Cryptography	Defining a policy on the application of encryption.
Clause 11: Physical and Environmental Security	Enforcing physical protection of business assets.
Clause 12: Operations security	Control changes to IT facilities, install anti malware, taking regular back-ups, maintaining, and monitoring logs, software installation, and manage vulnerabilities.
Clause 13: Communications Security	Maintaining security in the transfer of information between parties.
Clause 14: System acquisition, development, and maintenance	Enforcing requirements for secure software engineering principles during development.
Clause 15: Supplier relationships	Define policies and procedures for external supplier contracts and agreements. Monitor and audit the service provided.
Clause 16: Information Security Incident Management	Ensuring adequate response and recovery from security events and lessons learnt from past events.
Clause 17: Information security aspects of Business Continuity Management	Defining, testing, and updating the business continuity and resilience plans.
Clause 18: Compliance	Identifying regulatory obligations to external authorities like regulators and addressing external audits.

Table A.3: Overview of the contents of each Technical Control Theme of UK Cyber Essentials (NCSC, 2023)

Technical Control Theme	Contents
Technical Control Theme 1: Firewalls	Ensure that only safe and necessary network services can be accessed from the Internet.
Technical Control Theme 2: Secure Configuration	Ensure that computers and network devices are properly configured to • reduce the level of inherent vulnerabilities. • provide only the services required to fulfil their role.
Technical Control Theme 3: User Access Control	Ensure user accounts: • are assigned to authorised individuals only. • provide access to only those applications, computers and networks actually required for the user to perform their role.
Technical Control Theme 4: Malware Protection	Restrict execution of known malware and untrusted software, to prevent harmful code from causing damage or accessing sensitive data.
Technical Control Theme 5: Security Update Management	Ensure that devices and software are not vulnerable to known security issues for which fixes are available.

B.1

Table B.1: Sample form mapping to ISO 27001 and the NIST CSF

			MAPPING	
Number	Question	Form	ISO	NIST
1	Do you back up critical data at least once a week?	ProRisk, 2019	A.12.3 Backup	PR.IP-4: Backups of information are conducted, maintained, and tested
2	Are you PCI compliant, if applicable? If not applicable, leave blank.	ProRisk, 2019	A.18.1 Compliance with legal and contractual requirements	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
3	Do you enforce a policy of auditing and managing computer and user accounts?	ProRisk, 2019	A.9.2 User access management	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes
4	Do you have an established policy for checking the background of job candidates prior to their being offered employment?	MPR, 2018	A.7.1 Prior to employment	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
5	Is your computer system firewall protected?	MPR, 2018	A.13.1 Network security management	PR.PT-4: Communications and control networks are protected

The above table shows example mappings for questions from sample proposal forms. For example, Question Number 1 would be mapped to A.12.3 Backup which falls under Security Clause 12: Operations Security of the ISO 27001 and Security Category 2: Protect of the NIST CSF which contains the PR. IP-4: Backups of information are conducted, maintained, and tested subcategory.

B.2

Table B.2: Correspondence between controls in ISO/IEC 27002:2022 and controls in ISO/IEC 27002:2013

ISO/IEC 27002:2022 Control identifier	ISO/IEC 27002:2013 control identifier	Control name
5.1	05.1.1, 05.1.2	Policies for information security
5.2	06.1.1	Information security roles and responsibilities
5.3	06.1.2	Segregation of duties
5.4	07.2.1	Management responsibilities
5.5	06.1.3	Contact with authorities
5.6	06.1.4	Contact with special interest groups
5.7	New	Threat intelligence
5.8	06.1.5, 14.1.1	Information security in project management
5.9	08.1.1, 08.1.2	Inventory of information and other associated assets
5.10	08.1.3, 08.2.3	Acceptable use of information and other associated assets
5.11	08.1.4	Return of assets
5.12	08.2.1	Classification of information
5.13	08.2.2	Labelling of information
5.14	13.2.1, 13.2.2, 13.2.3	Information transfer
5.15	09.1.1, 09.1.2	Access control
5.16	09.2.1	Identity management
5.17	09.2.4, 09.3.1, 09.4.3	Authentication information
5.18	09.2.2, 09.2.5, 09.2.6	Access rights
5.19	15.1.1	Information security in supplier relationships
5.20	15.1.2	Addressing information security within supplier agreements
5.21	15.1.3	Managing information security in the ICT supply chain
5.22	15.2.1, 15.2.2	Monitoring, review and change management of supplier services
5.23	New	Information security for use of cloud services
5.24	16.1.1	Information security incident management planning and preparation
5.25	16.1.4	Assessment and decision on information security events
5.26	16.1.5	Response to information security incidents
5.27	16.1.6	Learning from information security incidents
5.28	16.1.7	Collection of evidence
5.29	17.1.1, 17.1.2, 17.1.3	Information security during disruption
5.30	New	ICT readiness for business continuity
5.31	18.1.1, 18.1.5	Legal, statutory, regulatory, and contractual requirements
5.32	18.1.2	Intellectual property rights

ISO/IEC 27002:2022 Control identifier	ISO/IEC 27002:2013 control identifier	Control name
5.33	18.1.3	Protection of records
5.34	18.1.4	Privacy and protection of PII
5.35	18.2.1	Independent review of information security
5.36	18.2.2, 18.2.3	Compliance with policies, rules, and standards for information security
5.37	12.1.1	Documented operating procedures
6.1	07.1.1	Screening
6.2	07.1.2	Terms and conditions of employment
6.3	07.2.2	Information security awareness, education, and training
6.4	07.2.3	Disciplinary process
6.5	07.3.1	Responsibilities after termination or change of employment
6.6	13.2.4	Confidentiality or non-disclosure agreements
6.7	06.2.2	Remote working
6.8	16.1.2, 16.1.3	Information security event reporting
7.1	11.1.1	Physical security perimeters
7.2	11.1.2, 11.1.6	Physical entry
7.3	11.1.3	Securing offices, rooms, and facilities
7.4	New	Physical security monitoring
7.5	11.1.4	Protecting against physical and environmental threats
7.6	11.1.5	Working in secure areas
7.7	11.2.9	Clear desk and clear screen
7.8	11.2.1	Equipment siting and protection
7.9	11.2.6	Security of assets off-premises
7.10	08.3.1, 08.3.2, 08.3.3, 11.2.5	Storage media
7.11	11.2.2	Supporting utilities
7.12	11.2.3	Cabling security
7.13	11.2.4	Equipment maintenance
7.14	11.2.7	Secure disposal or re-use of equipment
8.1	06.2.1, 11.2.8	User endpoint devices
8.2	09.2.3	Privileged access rights
8.3	09.4.1	Information access restriction
8.4	09.4.5	Access to source code
8.5	09.4.2	Secure authentication
8.6	12.1.3	Capacity management
8.7	12.2.1	Protection against malware
8.8	12.6.1, 18.2.3	Management of technical vulnerabilities
8.9	New	Configuration management
8.10	New	Information deletion
8.11	New	Data masking
8.12	New	Data leakage prevention
8.13	12.3.1	Information backup
8.14	17.2.1	Redundancy of information processing facilities
8.15	12.4.1, 12.4.2, 12.4.3	Logging
8.16	New	Monitoring activities
8.17	12.4.4	Clock synchronization
8.18	09.4.4	Use of privileged utility programs
8.19	12.5.1, 12.6.2	Installation of software on operational systems
8.20	13.1.1	Networks security
8.21	13.1.2	Security of network services
8.22	13.1.3	Segregation of networks
8.23	New	Web filtering
8.24	10.1.1, 10.1.2	Use of cryptography
8.25	14.2.1	Secure development life cycle
8.26	14.1.2, 14.1.3	Application security requirements
8.27	14.2.5	Secure system architecture and engineering principles
8.28	New	Secure coding
8.29	14.2.8, 14.2.9	Security testing in development and acceptance
8.30	14.2.7	Outsourced development
8.31	12.1.4, 14.2.6	Separation of development, test and production environments
8.32	12.1.2, 14.2.2, 14.2.3, 14.2.4	Change management
8.33	14.3.1	Test information
8.34	12.7.1	Protection of information systems during audit testing
8.31	12.1.4, 14.2.6	Separation of development, test, and production environments

Source: [119] (http://www.itref.ir/uploads/editor/d3d149.pdf)

*New applies to controls that are new to ISO 27001:2022 and were not available in the ISO 27001:2013 version.

C.1

Table C.1 Full mapping of forms with UK Cyber Essentials

		Technical Control Themes		TC Theme 1	TC Theme 2	TC Theme 3	TC Theme 4	TC Theme 5
				1	1	1	1	1
Form ID	Insurer	Year	Country					
PF1	360 Underwriting Solutions	May-20	Australia	○	●	○	●	○
PF2	Absolute Insurance Brokers	Mar-18	United Kingdom	●	○	●	●	●
PF3	AIG	Jun-17	United Kingdom	●	●	●	●	●
PF4	Allianz	Dec-18	United Kingdom	●	●	●	●	○
PF5	Ascent	Mar-20	United Kingdom	●	●	●	●	●
PF6	Aust Brokers Corporate Cyber Insurance	Mar-21	Australia	●	●	●	●	●
PF7	Aust Brokers SME Cyber Insurance	Nov-17	Australia	●	●	○	●	●
PF8	Berkley Insurance Company	Mar-20	Australia	○	○	○	○	●
PF9	Brooklyn Underwriting	Jan-20	Australia	●	●	●	●	●
PF10	CFC Underwriting Limited	Mar-19	United Kingdom	●	●	○	●	●
PF11	CHUBB	Jun-17	United Kingdom	●	○	○	●	●
PF12	DUAL	Aug-20	Australia	●	●	○	●	●
PF13	Emergence	Apr-20	Australia	●	●	○	●	○
PF14	Global Re Broking Solutions Ltd	Jan-18	United Kingdom	●	●	●	●	●
PF15	Great American Insurance Group	May-18	United States	○	○	●	○	○
PF16	Hiscox Insurance	Mar-19	United Kingdom	●	●	○	●	●
PF17	Liberty Specialty Markets	Sep-17	Australia	●	○	○	●	●
PF18	London Australia Underwriting	May-20	Australia	●	●	●	●	●
PF19	MPR Underwriting (Crime & Cyber Crime Insurance)	Mar-18	United Kingdom	●	○	○	○	○
PF20	MPR Underwriting (Cyber Incident Response and Insurance)	Mar-18	United Kingdom	●	●	●	●	●
PF21	At-Bay	Feb-20	United States	○	●	○	●	○
PF22	Marsh	Mar-19	Australia	○	●	○	○	●
PF23	MFL Professional Insurance Brokers	Mar-17	United Kingdom	●	○	○	○	●
PF24	Miller	Jul-18	United Kingdom	●	●	●	●	●
PF25	NIG	May-18	United Kingdom	●	●	●	●	●
PF26	NMU	Jul-17	United Kingdom	●	○	○	●	●
PF27	OBF Insurance Group Ltd.	Oct-18	United Kingdom	●	○	●	●	●
PF28	ProRisk	Aug-19	Australia	●	●	○	●	○
PF29	QBE Insurance	May-16	United Kingdom	●	○	●	●	●
PF30	Routen Chaplin	May-17	United Kingdom	○	○	○	○	○
PF31	Royal & Sun Alliance Insurance	Mar-17	United Kingdom	●	○	●	●	●
PF32	SURA TECHNOLOGY RISKS	May-20	Australia	●	●	●	●	●
PF33	TDC Specialty Insurance Company	Nov-17	United States	●	●	●	●	●
PF34	TK SPECIALTY RISKS PTY LTD	Aug-19	Australia	●	○	○	●	●
PF35	Tokio Marine HCC	Mar-17	United Kingdom	●	●	●	●	○
PF36	Travelers Insurance Company Limited	Jan-19	United States	●	●	●	●	●
PF37	AmTrust Financial Services	Sep-16	United States	●	○	●	●	○
PF38	AXIS Insurance	Oct-20	United States	●	●	●	●	●
PF39	Beazley Insurance Company Inc.	Nov-17	United Kingdom	●	●	●	○	●

PF40	Corvus Insurance	Mar-21	United States	○	●	●	○	○
PF41	G & M International	May-18	United States	●	●	●	●	●
PF42	HSB	Mar-20	United States	●	●	●	●	●
PF43	Tokio Marine HCC	Jan-21	United States	○	●	●	●	●
PF44	Ando insurance	Oct-21	United Kingdom	●	●	●	●	●
PF45	Travelers Insurance Company Limited	May-20	United Kingdom	●	●	●	●	●
PF46	BGi.uk	Jul-17	United Kingdom	●	●	●	●	●
PF47	Professional Insurance Agents Ltd	Apr-19	United Kingdom	●	○	○	●	●
PF48	Optimum Specialty Risks	Apr-21	United Kingdom	●	●	●	●	●
PF49	Axis Capital	Nov-21	United States	●	●	●	●	●
PF50	Apex Insurance Brokers	Dec-19	United Kingdom	●	●	○	●	○
PF51	Hartford Steam Boiler Inspection and Insurance Company	Jun-20	United States	●	●	●	●	●
PF52	The Hanover Insurance Group, Inc.	Feb-17	United States	●	●	●	○	○
PF53	United States Liability Insurance Company	Dec-21	United States	●	●	●	●	●
PF54	CFC Underwriting Limited (for SMES)	Sep-17	United States	○	○	○	○	○
PF55	ATC Insurance Solutions Pty Ltd	Dec-22	Australia	●	●	●	○	●
PF56	Nova Casualty Company	Apr-18	United States	●	●	○	●	●
PF57	Cowbell Cyber Inc	Feb-23	United States	○	●	○	○	○
PF58	Biz Lock	Dec-21	United Kingdom	●	●	○	●	○
PF59	Corvus Insurance	Jan-23	United States	●	●	●	●	○
PF60	The Hartford	May-22	United States	●	●	○	●	●
PF61	Beazley Insurance (BREACH RESPONSE)	Feb-23	United States	●	●	●	○	●
PF62	Distinguished Programs	Apr-20	United States	●	○	●	●	○
PF63	Arch Insurance Company	Sep-18	United States	●	○	●	●	●
PF64	CM&F Group	Oct-19	United States	○	○	○	●	●
PF65	CRC Insurance	Apr-19	United Kingdom	●	○	○	●	●
PF66	Biz Lock	Dec-21	United States	●	●	●	●	●
PF67	The Doctors Company	Aug-17	United States	●	○	○	●	●
PF68	Beazley Insurance (Beazley InfoSec)	Jun-18	United States	●	●	●	○	●

Colour Coding					
○ **Does not contain any control**	11	21	27	14	18
● **Contains all controls**	57	47	41	54	50
Total Forms	**68**	**68**	**68**	**68**	**68**
Percentage of forms not containing controls	16%	31%	40%	21%	26%
Percentage of forms containing controls	84%	69%	60%	79%	74%
Total	100%	100%	100%	100%	100%

Table C.2 Full mapping of forms with ISO 27001

				ISO 27001:2013													
				S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16	S17	S18
			Security Control Categories	1	2	3	3	4	1	2	7	2	3	2	1	2	2
Form ID	Insurer	Year	Country														
PF1	360 Underwriting Solutions	May-20	Australia	○	◐	○	◐	○	●	○	◐	◐	○	○	○	○	◐
PF2	Absolute Insurance Brokers	Mar-18	United Kingdom	○	◐	○	◐	○	●	○	◐	◐	○	○	○	○	○
PF3	AIG	Jun-17	United Kingdom	●	●	●	◐	◐	●	●	◐	◐	○	●	●	●	●
PF4	Allianz	Nov-19	United Kingdom	●	◐	◐	◐	◐	○	○	◐	●	○	◐	○	○	◐
PF5	Ascent	Aug-16	United Kingdom	●	◐	◐	◐	◐	●	○	◐	◐	◐	●	○	◐	●
PF6	Aust Brokers Corporate Cyber Insurance	Mar-21	Australia	●	●	◐	◐	◐	●	○	◐	●	○	◐	●	◐	●
PF7	Aust Brokers SME Cyber Insurance	Nov-17	Australia	○	●	○	◐	◐	●	○	◐	◐	○	◐	○	◐	●
PF8	Berkley Insurance	Mar-20	Australia	○	○	◐	○	○	○	○	◐	○	○	○	○	◐	◐
PF9	Brooklyn Underwriting	Jan-20	Australia	○	◐	●	◐	◐	●	○	◐	◐	○	◐	○	◐	◐
PF10	CFC Underwriting	Jun-20	United Kingdom	○	●	◐	◐	◐	●	○	◐	●	○	○	●	○	◐
PF11	CHUBB	Jun-17	United States	○	◐	○	○	○	●	○	◐	◐	○	○	●	○	◐
PF12	DUAL	Aug-20	United Kingdom	○	◐	○	◐	◐	●	○	◐	◐	○	●	●	◐	●
PF13	Emergence	Apr-20	Australia	●	●	◐	◐	◐	●	○	◐	◐	○	○	○	●	●
PF14	Global Re Broking Solutions Ltd	Jan-18	United Kingdom	●	●	◐	●	◐	●	◐	◐	◐	○	●	●	●	●
PF15	Great American Insurance Group	May-18	United States	○	◐	◐	○	◐	●	○	◐	○	○	◐	●	○	●
PF16	Hiscox Insurance	Mar-19	United Kingdom	○	●	◐	◐	◐	●	○	◐	◐	○	●	○	◐	●
PF17	Liberty Specialty Markets	Sep-17	Australia	●	◐	○	◐	○	●	○	◐	●	○	◐	○	◐	●
PF18	London Australia Underwriting	May-20	Australia	○	●	◐	◐	◐	●	○	◐	●	○	◐	○	◐	●
PF19	MPR Underwriting (Crime & Cyber Crime Insurance)	Mar-18	United Kingdom	○	◐	◐	○	○	○	●	◐	◐	○	●	○	○	○
PF20	MPR Underwriting (Cyber Incident Response and Insurance)	Mar-19	United Kingdom	●	●	●	◐	◐	●	○	◐	●	○	◐	●	◐	●
PF21	At-Bay	Feb-20	United States	○	●	◐	◐	◐	●	○	◐	◐	○	◐	○	○	●
PF22	Marsh	May-20	Australia	●	○	◐	◐	◐	○	○	◐	○	○	◐	○	○	◐
PF23	MFL Professional Insurance Brokers	Mar-17	United Kingdom	●	◐	○	◐	○	●	○	◐	◐	○	◐	○	○	●
PF24	Miller	Jul-18	United Kingdom	●	○	◐	○	◐	○	○	◐	●	○	◐	○	◐	○
PF25	NIG	May-18	United Kingdom	●	●	◐	◐	◐	●	◐	◐	●	○	○	○	●	●
PF26	NMU	Jul-17	United Kingdom	○	○	○	○	○	○	◐	◐	◐	○	○	○	○	○
PF27	OBF Insurance	Oct-18	United Kingdom	●	●	◐	◐	◐	●	◐	◐	●	○	◐	●	◐	◐
PF28	ProRisk	Aug-19	Australia	○	○	○	○	◐	○	○	◐	◐	○	○	○	◐	○
PF29	QBE Insurance	May-16	United Kingdom	●	●	◐	◐	◐	●	○	◐	●	○	●	●	◐	●
PF30	Routen Chaplin	May-17	United Kingdom	○	◐	○	◐	○	●	○	○	○	○	○	○	○	◐
PF31	Royal & Sun Alliance (RSA) Insurance	Mar-17	United Kingdom	●	◐	◐	◐	◐	●	○	◐	◐	○	◐	○	◐	◐
PF32	Sura Technology Risks	May-20	Australia	○	◐	◐	◐	◐	●	○	◐	◐	○	○	○	○	◐
PF33	TDC Specialty Underwriters	Nov-17	United States	●	●	●	◐	◐	●	○	◐	◐	○	●	●	◐	●
PF34	TK Specialty Risks	Aug-19	Australia	○	◐	○	○	○	○	○	◐	◐	○	○	○	○	◐
PF35	Tokio Marine HCC	Mar-18	United Kingdom	○	○	◐	◐	◐	●	○	◐	◐	○	○	○	◐	●
PF36	Travelers Insurance	Jan-19	United States	●	●	◐	●	◐	●	○	◐	◐	○	●	●	●	●
PF37	AmTrust North America	Sep-16	United States	●	○	◐	◐	◐	●	◐	◐	◐	○	○	○	○	◐
PF38	AXIS Insurance	Oct-20	United States	●	●	◐	◐	◐	●	○	◐	●	◐	●	●	●	●
PF39	Beazley Insurance	Nov-17	United Kingdom	●	◐	◐	◐	◐	●	○	◐	◐	○	◐	●	◐	●

PF40	Corvus Insurance	Mar-21	United States	○	○	○	○	◐	●	○	◐	◐	○	○	○	○	○
PF41	G & M	May-18	United Kingdom	○	●	○	◐	◐	●	○	◐	◐	○	○	○	◐	◐
PF42	HSB	Mar-20	United States	●	●	◐	◐	◐	●	○	◐	◐	○	◐	●	◐	●
PF43	Tokio Marine HCC	Jan-21	United States	●	●	◐	◐	◐	●	○	◐	●	○	○	○	○	◐
PF44	Ando insurance	Oct-21	United Kingdom	●	●	◐	◐	◐	●	○	◐	●	○	◐	●	◐	●
PF45	Travelers Insurance Company Limited	May-20	United Kingdom	●	●	◐	◐	◐	●	○	◐	●	○	●	●	●	●
PF46	BGi.uk	Jul-17	United Kingdom	●	●	●	◐	◐	●	○	◐	◐	○	◐	○	●	●
PF47	Professional Insurance Agents Ltd	Apr-19	United Kingdom	○	◐	○	○	○	●	○	◐	◐	○	○	○	◐	◐
PF48	Optimum Speciality Risks	Apr-21	United Kingdom	○	●	◐	○	◐	●	○	◐	●	○	○	●	●	●
PF49	Axis Capital	Nov-21	United States	●	◐	◐	◐	◐	●	◐	◐	●	○	●	●	●	●
PF50	Apex Insurance Brokers	Dec-19	United Kingdom	○	◐	○	◐	○	●	○	◐	◐	○	○	○	○	◐
PF51	Hartford Steam Boiler Inspection and Insurance Company	Jun-20	United States	●	●	◐	◐	◐	●	○	◐	◐	○	◐	●	◐	●
PF52	The Hanover Insurance Group, Inc.	Feb-17	United States	●	●	◐	◐	◐	●	◐	◐	◐	○	◐	●	◐	●
PF53	United States Liability Insurance Company	Dec-21	United States	●	◐	◐	◐	◐	●	●	◐	◐	○	◐	●	◐	◐
PF54	CFC Underwriting Limited (for SMES)	Sep-17	United States	○	○	○	○	○	○	○	○	○	○	○	○	○	○
PF55	ATC Insurance Solutions Pty Ltd	Dec-22	Australia	○	●	○	○	◐	●	○	◐	◐	○	○	○	○	●
PF56	Nova Casualty Company	Apr-18	United States	○	◐	○	○	◐	○	○	◐	◐	○	◐	●	○	◐
PF57	Cowbell Cyber Inc	Feb-23	United States	○	●	◐	○	◐	●	○	◐	●	○	◐	●	●	○
PF58	Biz Lock	Dec-21	United Kingdom	○	◐	○	○	◐	○	○	◐	●	○	○	○	○	○
PF59	Corvus Insurance	Jan-23	United States	○	◐	◐	○	◐	●	○	◐	●	○	○	○	○	◐
PF60	The Hartford	May-22	United States	○	◐	○	○	◐	●	○	◐	◐	○	○	○	○	◐
PF61	Beazley Insurance (BREACH RESPONSE)	Feb-23	United States	●	○	◐	◐	◐	●	○	◐	◐	○	◐	●	◐	●
PF62	Distinguished Programs	Apr-20	United States	●	○	◐	◐	○	●	○	◐	◐	○	◐	○	○	◐
PF63	Arch Insurance Company	Sep-18	United States	○	○	○	○	○	●	○	◐	◐	○	○	○	○	◐
PF64	CM&F Group	Oct-19	United States	○	○	○	○	○	○	○	◐	○	○	○	○	○	◐
PF65	CRC Insurance	Apr-19	United Kingdom	●	○	◐	◐	○	●	○	◐	◐	○	○	●	○	◐
PF66	Biz Lock	Dec-21	United States	○	●	○	○	◐	○	○	◐	●	○	○	○	○	○
PF67	The Doctors Company	Aug-17	United States	●	◐	◐	○	◐	●	○	◐	◐	○	○	○	○	◐
PF68	Beazley Insurance (Beazley InfoSec)	Jun-18	United States	●	○	◐	◐	◐	●	○	◐	◐	○	◐	●	◐	●

Colour Coding														
○ Does not contain	34	15	23	22	17	13	58	2	6	66	30	41	30	10
◐ Partially contains	0	25	40	44	51	0	7	66	42	2	26	0	27	26
● Contains all controls	34	28	5	2	0	55	3	0	20	0	12	27	11	32
Total Forms	**68**	**68**	**68**	**68**	**68**	**68**	**68**	**68**	**68**	**68**	**68**	**68**	**68**	**68**

Percentage of forms not containing all	50%	22%	34%	32%	25%	19%	85%	3%	9%	97%	44%	60%	44%	15%
Percentage of forms partially containing	0%	37%	59%	65%	75%	0%	10%	97%	62%	3%	38%	0%	40%	38%
Percentage of forms containing all	50%	41%	7%	3%	0%	81%	4%	0%	29%	0%	18%	40%	16%	47%
Total	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %

Table C.3 Full mapping of forms with NIST CSF

				Security Functions	Function 1	Function 2	Function 3	Function 4	Function 5
					6	6	3	5	3
Form ID	Insurer	Year	Country						
PF1	360 Underwriting Solutions	May-20	Australia	○	◐	◐	○	○	
PF2	Absolute Insurance Brokers	Mar-18	United Kingdom	○	◐	◐	○	○	
PF3	AIG	Jun-17	United Kingdom	◐	◐	◐	◐	○	
PF4	Allianz	Nov-19	United Kingdom	◐	◐	◐	○	○	
PF5	Ascent	Aug-16	United Kingdom	◐	◐	◐	○	○	
PF6	Aust Brokers Corporate Cyber Insurance	Mar-21	Australia	◐	◐	◐	○	○	
PF7	Aust Brokers SME Cyber Insurance	Nov-17	Australia	◐	◐	◐	○	○	
PF8	Berkley Insurance	Mar-20	Australia	○	◐	○	○	○	
PF9	Brooklyn Underwriting	Jan-20	Australia	◐	◐	◐	○	○	
PF10	CFC Underwriting	Jun-20	United Kingdom	◐	◐	◐	◐	○	
PF11	CHUBB	Jun-17	United States	◐	◐	◐	○	○	
PF12	DUAL	Aug-20	United Kingdom	○	◐	◐	◐	○	
PF13	Emergence	Apr-20	Australia	◐	◐	◐	○	○	
PF14	Global Re Broking Solutions Ltd	Jan-18	United Kingdom	◐	◐	◐	○	○	
PF15	Great American Insurance Group	May-18	United States	◐	◐	◐	○	○	
PF16	Hiscox Insurance	Mar-19	United Kingdom	◐	◐	◐	◐	◐	
PF17	Liberty Specialty Markets	Sep-17	Australia	◐	◐	◐	○	○	
PF18	London Australia Underwriting	May-20	Australia	◐	◐	◐	○	○	
PF19	MPR Underwriting (Crime & Cyber Crime Insurance)	Mar-18	United Kingdom	◐	◐	○	○	○	
PF20	MPR Underwriting (Cyber Incident Response and Insurance)	Mar-19	United Kingdom	◐	◐	◐	◐	○	
PF21	At-Bay	Feb-20	United States	◐	◐	◐	○	○	
PF22	Marsh	May-20	Australia	◐	◐	◐	○	◐	
PF23	MFL Professional Insurance Brokers	Mar-17	United Kingdom	◐	◐	◐	○	○	
PF24	Miller	Jul-18	United Kingdom	◐	◐	◐	○	◐	
PF25	NIG	May-18	United Kingdom	◐	◐	◐	○	○	
PF26	NMU	Jul-17	United Kingdom	○	◐	◐	○	○	
PF27	OBF Insurance	Oct-18	United Kingdom	◐	◐	◐	○	○	
PF28	ProRisk	Aug-19	Australia	○	◐	◐	○	○	
PF29	QBE Insurance	May-16	United Kingdom	◐	◐	◐	◐	○	
PF30	Routen Chaplin	May-17	United Kingdom	○	◐	○	○	○	
PF31	Royal & Sun Alliance (RSA) Insurance	Mar-17	United Kingdom	◐	◐	◐	○	○	
PF32	Sura Technology Risks	May-20	Australia	◐	◐	◐	○	○	
PF33	TDC Specialty Underwriters	Nov-17	United States	◐	◐	◐	○	○	
PF34	TK Specialty Risks	Aug-19	Australia	◐	◐	◐	○	○	
PF35	Tokio Marine HCC	Mar-18	United Kingdom	◐	◐	◐	○	○	
PF36	Travelers Insurance	Jan-19	United States	◐	◐	◐	◐	○	
PF37	AmTrust North America	Sep-16	United States	◐	◐	◐	○	○	

PF38	AXIS Insurance	Oct-20	United States	◐	◐	◐	○	○
PF39	Beazley Insurance	Nov-17	United Kingdom	◐	◐	◐	○	○
PF40	Corvus Insurance	Mar-21	United States	○	◐	○	○	○
PF41	G & M	May-18	United Kingdom	◐	◐	◐	○	○
PF42	HSB	Mar-20	United States	◐	◐	◐	○	○
PF43	Tokio Marine HCC	Jan-21	United States	◐	◐	◐	○	○
PF44	Ando insurance	Oct-21	United Kingdom	◐	◐	◐	◐	○
PF45	Travelers Insurance Company Limited	May-20	United Kingdom	◐	◐	◐	◐	○
PF46	BGi.uk	Jul-17	United Kingdom	◐	◐	◐	○	○
PF47	Professional Insurance Agents Ltd	Apr-19	United Kingdom	◐	◐	◐	◐	○
PF48	Optimum Specialty Risks	Apr-21	United Kingdom	◐	◐	◐	○	○
PF49	Axis Capital	Nov-21	United States	◐	◐	●	◐	○
PF50	Apex Insurance Brokers	Dec-19	United Kingdom	◐	◐	◐	○	○
PF51	Hartford Steam Boiler Inspection and Insurance Company	Jun-20	United States	◐	◐	◐	○	○
PF52	The Hanover Insurance Group, Inc.	Feb-17	United States	◐	◐	◐	◐	○
PF53	United States Liability Insurance Company	Dec-21	United States	◐	◐	◐	○	○
PF54	CFC Underwriting Limited (for SMES)	Sep-17	United States	○	○	○	○	○
PF55	ATC Insurance Solutions Pty Ltd	Dec-22	Australia	◐	◐	◐	○	○
PF56	Nova Casualty Company	Apr-18	United States	◐	◐	◐	○	○
PF57	Cowbell Cyber Inc	Feb-23	United States	◐	◐	○	◐	○
PF58	Biz Lock	Dec-21	United Kingdom	○	◐	◐	○	○
PF59	Corvus Insurance	Jan-23	United States	◐	◐	◐	○	○
PF60	The Hartford	May-22	United States	○	◐	◐	○	○
PF61	Beazley Insurance (BREACH RESPONSE)	Feb-23	United States	◐	◐	◐	○	○
PF62	Distinguished Programs	Apr-20	United States	◐	◐	○	○	○
PF63	Arch Insurance Company	Sep-18	United States	○	◐	◐	○	○
PF64	CM&F Group	Oct-19	United States	○	○	◐	○	○
PF65	CRC Insurance	Apr-19	United Kingdom	◐	◐	◐	○	○
PF66	Biz Lock	Dec-21	United States	○	◐	◐	○	○
PF67	The Doctors Company	Aug-17	United States	◐	◐	◐	○	○
PF68	Beazley Insurance (Beazley InfoSec)	Jun-18	United States	◐	◐	◐	○	○

Colour Coding					
○ **Does not contain any control**	14	2	7	55	65
◐ **Partially contains**	54	66	60	13	3
● **Contains all controls**	0	0	1	0	0
Total Forms	**68**	**68**	**68**	**68**	**68**
Percentage of forms not containing all	21%	3%	10%	81%	96%
Percentage of forms partially containing	79%	97%	88%	19%	4%
Percentage of forms containing all	0%	0%	1%	0%	0%
Total	100%	100%	100%	100%	100%

D.1

Table D.1: The percentage of coverage of each Function of the NIST CSF based on forms from the US (n=26) and the entire data set (n=68).

Coverage	None			Partial			All		
Form origination	US	Rest of the World	Variance	US	Rest of the World	Variance	US	Rest of the World	Variance
Function 1: Identify	23%	21%	2%	77%	79%	-2%	0%	0%	0%
Function 2: Protect	8%	3%	5%	92%	97%	-5%	0%	0%	0%
Function 3: Detect	15%	10%	5%	81%	88%	-7%	4%	1%	-3%
Function 4: Respond	85%	81%	4%	15%	19%	-4%	0%	0%	0%
Function 5: Recover	100%	96%	4%	0%	4%	-4%	0%	0%	0%