Incentive model for managing cyber risk in the supply chain

By

Denny Wan

Student ID: 31014356

A thesis submitted to Macquarie University
for the degree of Master of Research
Department of Computing
November 2019

Supervised by

A/Prof Christophe Doche (Department of Computing)

Professor Pavel Shevchenko (Department of Actuarial Studies and Business Analytics)

Examiner's Copy

Abstract

Competition has transformed many economic processes, from manufacturing to financial services, into complex supply chains. Entities along these chains specialise in core processes in which they have a competitive advantage, measured by their ability to manage the process risk at the lowest cost. Outsourcing of non-core processes does not relieve these entities from the associated regulatory compliance obligations and other liabilities. The rapid rise in financial liabilities from cyber-attacks, from record fines to class action settlements, demands a better understanding and handling of these outsourcing arrangements.

Unfortunately, our limited understanding of the rapidly evolving nature of cyber-attacks and the difficulty of quantifying cyber risk present a challenge in managing liability from cyber risks. The traditional compliance-based approach does not offer an assurance of security, with an increasing number of organisations suffering major data breaches despite being certified.

This research explores an alternative approach in building an incentive driven risk-sharing approach to minimise preventable data breaches. It focusses on improving cyber resilience at the source of risk. An incentive model ontology leveraging quantification techniques is presented to identify the key elements in the incentive model. This approach has been validated through the APRA CPS 234 and a cyber insurance use case.

Statement of Originality

I certify that the research presented in this thesis is original work carried out by the author. The work has not been presented for a higher degree to any university or institution other than Macquarie University, and contains no material previously published or written by any other person except where due reference is made in the text.

Wai Ming Denny Wan

24th November 2019

Acknowledgements

I would like to thank my supervisors for accepting my application, to explore this emerging area of managing cyber risk in a supply chain context. This research has produced insights and breakthroughs with tangible and measurable economic benefits validated through two specific use cases under a collaboration research arrangement with relevant industry sectors.

This particular area was not an area of focus for the University at the time of my application. I am grateful to my supervisors in making time to understand and assess the merit of my research proposal. This interest evolved from a simple desire to better understand cyber insurance pricing strategies from a supply chain risk management perspective. Their support and guidance helped me to transform the research focus into the development of an incentive model as a sustainable and scalable risk management methodology penetrating the rigid boundaries along a supply chain. They have also been supportive of my successful application for an Australian Commonwealth Scholarship which helped to ease my financial burden.

I also want to acknowledge the tremendous support my family has provided to me. To my wife, Rowena, thank you for keeping my spirits up when I was feeling distressed. To my sons, Rickey and Hamish, thank you for helping around the house when I was busy and for your moral support.

Finally, I want to thank the industry research partners, Agile Underwriting and HESTA Super Fund. To James Crowther, General Manager - Emerging Risk Agile Underwriting, thank you for your humour and war stories with brokers and policyholders. To Michael Collins, General Manager – Information Security HESTA, thank you for our shared passion in the FAIR framework and your confidence in my research in exploring a new paradigm in integrating risk appetite into cyber risk management.

Contents

List of Figures

List of Tables

1. Introduction

This chapter begins with an overview of the current threat landscape, exploring to what extent cyber-attacks are preventable and the impact from the changing regulatory landscape. It then explores unique security management challenges and opportunities in the supply chain. It draws on lessons learnt from the cyber insurance industry which recommended the strategy of improving cyber resilience at the source of risk.

Cyber risk is recognised as a material business risk which impacts business investment decisions and the valuation of a business. Gartner forecast more than USD$124 billion would be spent on cyber security controls worldwide in 2019 [1]. This is a significant investment in the global economy. However, despite this level of investment, large data breaches continue to be reported in the news.

Cyber security investment is often driven by company security policies and regulatory compliance obligations [2] such as the Payment Card Industry Data Security Standard (PCI DSS) [3] or the National Institute of Standards and Technology Cyber Security Framework (NIST CSF) [4], in order to improve the maturity of the security program. But compliance with security standards, assurance and audits does not guarantee security [5]. There are many factors contributing to these security gaps, such as incompatibility between the compliance frameworks [6] and current business processes, resulting in user resistance [7].

A phenomenon known as a ‘moral hazard’ [8] sees some business entities actively decrease their cyber security investments when covered by insurance. This difficulty is not unique to cyber insurance, being a common challenge for the industry at large [9]. In order to combat this, some insurers utilise incentive programs, such as offering premium discounts to subsidise the deployment of information security technology solutions. This aids in the management of cyber security by reducing the expected frequency of preventable data breaches, thus reducing the claim payment under the associated cyber insurance policies [10]. Unfortunately, an incentive program based on exclusively discounts can become expensive, limiting the scalability of such incentive program.

1.1 The Cyber Threat Landscape

This section explores aspects of the cyber threat landscape which are relevant to the development of the incentive model approach. An incentive program is effective against opportunistic, financially motivated attacks because attackers predominantly look for easy targets. An opportunistic attack can be foiled by raising the difficulty of attacking through implementing stronger security controls or by minimising the value of a successful attack to the attacker. This defence strategy works because the attacker is either unwilling or unable to increase their attack effort. They can also be discouraged if they expect the reward for their effort will be reduced, simply moving on to other more profitable victims. Opportunistic attacks are also known as non-targeted attacks because the victims are randomly selected.

In contrast, victims and their information assets in targeted attacks are chosen for specific reasons. Targeted attacks can be financially motived but are more commonly politically motivated. These attackers are willing and capable of increasing their attack efforts in the face of increased security controls. There have been many high-profile cyber-attacks attributed to a form of targeted attack known as "Advance Persistent Threat" (APT) campaigns [11], believed to be launched by nation-state attackers such as Iran, China, North Korea and Russia [12]. There is a perception that defence against targeted attacks is futile without equally sophisticated and advanced information security tools and expertise. Hence, cyber insurance presents itself as one of the most reliable forms of protection against potential financial losses from cyber-attacks. However this perception is being challenged under a number of current court cases covering some large cyber insurance claims. A notable example is the case of "Mondelez vs Zurich" for loss attributed to the NetPetya. The claim is being denied on the grounds that NetPetya is a cyber weapon created by a nation state. Therefore the attack is considered "An Act of War" which is excluded under the Property Insurance policy the claim is lodged [13]. This type of claim is also known as silent cyber [14] where the cyber insurance coverage is not explicit. Insurance and reinsurance marketplace Lloyd's of London is to mandate that all policies clearly state whether they will provide affirmative coverage for cyber risks. From January 1, 2020, Lloyd's underwriters will be required to clarify whether first-party property damage policies affirm or exclude cyber cover [15].

1.1.1 Are Cyber-Attacks Preventable?

The massive data breach suffered by Equifax in 2017 exposed the Personal Identifiable Information (PII) [16] of 145.5 million people. Analysis has shown that even basic preventative security controls are effective in defending against targeted attacks and controlling associated damage.

The first question is to ask if this attack was commercially motived by organised crime to monetise PII. Monitoring of various markets in the dark web [17] by many cyber security analysts for over a year did not undercover any evidence of the availability of the stolen PII for sale. This led to the conclusion by some commentators that the attack was launched by a state-sponsored hacker for espionage [18].

The second question is to ask if the attack was preventable. According to the US Government Accountability Office (GAO) Report 18-559 [19], the breach stemmed from a failure to enforce defence measures against weaknesses in identification and detection of attacks, as well as segmentation of access to databases and data governance. The investigation confirmed that the attackers remained in the network for 76 days, extracting data from 51 databases without being detected. The attacker exploited a known vulnerability (Apache Struts Web framework CVE-2017-5638) [20] on the Equifax Online Dispute Portal to establish a foothold in the network. There was evidence to suggest that the attacker uncovered this vulnerability through network scanning across the Internet. Once the attackers established a foothold, they leveraged the other weaknesses in the network to launch attacks against other servers allowing them to exfiltrate the targeted PII dataset.

Report 18-559 confirmed that the Equifax data breach was preventable as failures in enforcing preventative security controls allowed the attack to be successful. The question was why weren’t these preventable measures enforced? Was it due to budgetary constraint, technological failure or lack of corporate security culture? The judgement handed down from a recent class action lawsuit against Equifax concluded that the company misled the public and regulators on their effort to maintain good security [21]. There were also several flaws in their security culture identified in the judgement. For example, the portal used for managing credit disputes used the default username and password of “admin” and “admin” respectively.

The business impact on Equifax from the data breach has been immense. Equifax reached a settlement totalling USD$650M [22], covering the consumer class action fines from several regulators including the Consumer Financial Protection Bureau, the Federal Trade Commission and 48 states, plus the District of Columbia and Puerto Rico. The former CEO, Richard Smith, also resigned after backlash over the data breach [23]. In March 2019, Standard & Poor (Atlanta-based credit bureau) downgraded Equifax's credit rating from stable to negative [24] reflecting the possible fallout from the 2017 data breach. Moody's also downgraded its outlook on Equifax citing the breach in May 2019.

The lack of security culture was clearly an important factor contributing to Equifax's investment decision in not enforcing these preventative controls. This concern was noted by US Senators Warren and Cummings [25] when they released the GAO report [19]. It is clear that prevention is better than a cure. An effective way to improve cyber resilience is to invest in readiness for handling cyber incidents. The process of developing an incident response plan (discussed in chapter 5) draws focus on the weakness in the current cyber security processes and helps to develop better prevention measures. By preventing or minimising incidents, it reduces the total financial loss and recovery cost to the organisation. This change in attitude was noted in the GAO report where Equifax's public filings post-breach reiterated that the company took steps to improve security and notify affected individuals.

Clearly regulatory controls are insufficient to develop an effective security culture that does more than pay lip service to compliance. Equifax operates in a highly regulated industry as evident from their massive regulatory fine. They were also subjected to public scrutiny through their public filings. Hence this research explores an alternative approach in cultivating a constructive security culture through the development of an incentive program.

Companies often operate in environment where the regulators can impose heavy fines or suspend licenses from entities failing compliance checks. These disciplinary actions can directly lead to collapse. Despite this, there is often little incentive to improve security beyond demonstrating compliance. Unfortunately, many compliance frameworks such as PCI DSS are rigid, with limited scope for risk-based decision making to improve the cost effectiveness of controls. For example, a vulnerability patch policy might demand that all high priority (as ranked by the vendors or based on Common Vulnerability Scoring System (CVSS)) [26] based score patches are applied within a week regardless of the sensitivity of the data and other applications running on the server. This could result in an Internet facing server being exposed with a lower priority exploitable vulnerability remaining unpatched for an extended period. It should be noted that CVSS is not designed to be a risk metric and is often misused for this purpose. CVSS scores omit information pertaining the potential exploit victims' context. Researchers and managers in the industry have long understood that the severity of vulnerabilities varies greatly among different organizational contexts. Therefore the CVSS scores provided by the national vulnerability database (NVD) alone are of limited use for vulnerability prioritization in practice [27]. Jacob et al. showed vulnerability management could be improved through better exploit prediction [28]. This approach took into consideration the sensitivity of the workload, the availability of publicly available exploit tools and the history of active exploitation in the Internet. This methodology is expected to produce a targeted patching strategy, increasing the effective protection coverage of exploitable servers from active threats by diverting patching efforts from servers less likely to be exploitable. Notably this prioritisation approach is still not risk-based patching because it does not take into account the consequences of exploitation.

The risk-sharing model is a cost-effective and innovative approach which is well suited to managing cyber risks in supply chains. This is because entities along the chain are regulated by a contractual relationship which limits their control on other entities along the chain. There is often no obviously applicable security compliance framework for suppliers. Security management attributes present in the contract are often undefined or minimal giving room for individual interpretation. When security attributes are not explicitly specified in the contract and do not materially influence the contract price, they create an opportunity for fair and equitable negotiation. The negotiation must be conducted on the merit of mutual benefits. This is where the incentive model ontology can provide clarity and structure for the negotiation.

In a cyber insurance context, the incentive program creates an environment for risk-sharing between the risk owner (insurer) and the risk manager (the policyholder). In a generic supply chain context, the risk owner is the organisation which outsources its business processes to a downstream supplier. This supplier becomes the new risk manager. Research has shown that an incentive program with a risk-sharing feedback mechanism can lead to a genuine reduction in the frequency of accidents. One study of the effects of premium discounts on worker's compensation under a risk-sharing model based in the form of a "no claim bonus" scheme showed evidence of a genuine risk reduction [29]. The statistically significant reduction in claim rates could not be accounted for from under-reporting of such incidents.

This research has developed an incentive model ontology and analysis method, covered in chapter 3, as a structured process to develop an incentive program to foster a risk-sharing collaborative environment between the risk owner and risk manager. The cost in running the incentive program could be categorised as a preventative security control measure, as the cost of transferring the risk management responsibilities through the supply chain is often not priced. The investment decision can be modelled using optimisation strategies based on Cyber Risk Economics principles, since improvements in security help to minimise fraud and financial loss for all entities along the supply chain. When the incentive program is implemented as a pricing signal, it can be easily applied through the supply chain. This is because pricing signals have no intrinsic dependence on technology, unlike contemporary supply chain risk management approaches built on top of blockchains which can suffer from fragility [30].

While a supply chain is designed to transfer processes to entities with the lowest cost, it should be noted that liabilities for the transferred processes remain with the risk owner. Therefore, risk owners must rely on their suppliers to manage these risks and liabilities on their behalf. The incentive model is designed to protect and enhance these symbiotic relationships based on the principle of risk-sharing between these consumers and suppliers. The risk-sharing model reflects an awareness amongst these organisations that poor security controls degrade the quality of the supply chain. Lower quality exposes all organisations to some level of financial loss. For example, a weak user identity management process in a financial services supply chain enables identity theft resulting in the creation of fake credit card accounts. These fake accounts can be used to commit fraudulent transactions leading to financial loss by merchants and banks issuing the credit card.

Finally, there is scepticism on the effectiveness of an incentive driven security management program when regulatory driven regimes such as PCI DSS [3] failed to prevent large scale data beaches against their customers' credit card information. For example, when Target US suffered a massive data breach in 2012 [31] against their credit card database, the company was already certified to be PCI DSS compliant at the time. There is a perception that no security program can defend against well-resourced and persistent attackers such as a nation-state sponsored adversary. This research acknowledges this scepticism. An incentive driven security program is not designed to defend against well-resourced persistent attackers in targeted attacks. Incentive driven schemes are designed to minimise lapses in preventative security controls and are most effective against opportunistic attacks such as ransomware attacks. These lapses occur because resources have been diverted to other business priorities or overruled to reduce business costs. They reflect the lack of focus in the corporate security culture.

1.1.2 The Changing Regulatory Landscape

Cyber risk is now recognised as a business risk because of the financial losses from business interruptions, regulatory fines and class actions associated with cyber events. Investors must be fully informed of the cyber security posture of companies to support informed investment decisions. For example, Verizon Business successfully demanded a USD$350 million discount [32] from Yahoo from the sale of its business in 2017. The discount was based on Yahoo's failure to disclose two known data breaches in 2013 and 2014 during their negotiations. In contrast, Slack voluntarily disclosed its cyber liability [33] during its Initial Public Offering (IPO) in 2019. This disclosure did not harm its IPO prospects with its share price trading over 50% above the issue price. The class action against Capital One in relation to their recent data breach was estimated to be USD$600M [34]. As a result, the US Security and Exchange Commission (SEC) issued a commission statement [35] in 2018 demanding that regulated entities (publicly listed companies in the US stock exchanges) include their cyber risk disclosure in their annual filing. In the Australian context, the Australian Prudential Regulation Authority (APRA) Prudential Standard CPS 234, which came into force on 1st July 2019, demanded the business boards of regulated entities ensure that their information security capabilities are commensurate with the size and extent of the threat against their information assets, to enable continued sound operations.

However, Gordon et al. [36] did not find any significant correlation between the share prices of companies and their public disclosure of data breaches after studying a 2002-2007 sample of 31 cyber-incidents. Hilary, Segal and Zhang [37] made similar observations and found no evidence of longer term abnormal returns. They also failed to find an impact on executive employment from data breaches but found empirical evidence of a modest increase in cyber-risk disclosure.

On the other hand, cybersecurity breaches have a demonstrably negative impact on bystander (i.e., non-breached) firms in the same industry, affecting the valuation of all firms in the industry. This is referred to as the investment contagion effect. This impact can be offset by the disclosure by bystander firms of their levels of cybersecurity preparedness [38].

The commercial demand for assessing the cyber resilience of companies might be shown by the joint venture between Moody and Team8 in Israel announced in May 2019 [39]. They provide services to assess company defences and preparedness for cyber-attacks in comparison to other businesses and over time. The identified initial use cases for this service included companies engaging in mergers and acquisitions (M&A) or purchasing cyber insurance policies. Moody said the new cyber rating product was not integrated into its credit ratings service yet. However, the assessment of the cyber health of companies has had an impact on their credit ratings in the past.

1.2 Aim

This research aims to develop an alternative risk management strategy based on an ***incentive driven risk-sharing approach to minimise preventable data breaches***.

1.3 Methods

A thorough literature review, covered in chapter two, was conducted to evaluate existing incentive models to minimise preventable data breach incidents in supply chains.

The rest of the thesis is the result of my research. Chapter three covered the development of an incentive model ontology and analysis process for creating an incentive program consistent with an organisation's risk appetite. The model was built on the Open Group FAIR (Factor Analysis of Information Risk) Cyber Risk Quantification framework [40] and identifies risk factors and preventative security controls to improve cyber resilience. This represents a structured approach to develop an incentive program which takes into consideration the limitations in a supply chain, the applicable regulatory environment and liability frameworks. A hypothetical debt collection agency is used to illustrate how to apply the model to shape the handling and protection of PII [16].

The model was then validated via two use cases in a commercial setting, the "APRA CPS 234 Compliance Template" and the "Dynamic Excess for Cyber Insurance", discussed in chapters four and five. Chapter four discusses a research project collaboration with HESTA which aimed to develop an APRA CPS 234 compliance template. The focus was on third party service provider management and the dimensioning of materiality considerations. The compliance process is a two-phase process, commencing with an effort to quantify organisational risk appetite and risk tolerance to define applicable risk metrics in financial terms. These metrics were then to be used in Phase Two to guide the development of incentive programs for managing service provider compliance with CPS 234. The metrics connect the information security risk program with the Enterprise Risk Management (ERM) program, by aligning the measurement and prioritisation between these programs. Phase One activities are completed. Phase Two will be undertaken as part of another research project.

Chapter five discusses a research project collaboration with Agile Underwriting to develop an incentive program for cyber insurance policyholders to improve their cyber resilience. This was achieved by encouraging policyholders to develop their incident response plans. Constructive and positive feedback from brokers and policyholders was collected as evidence of the efficacy of this incentive-based approach.

Lastly, chapter six explores an extension to the implementation of the incentive model leveraging telematic technology and parametric insurance concepts to provide continual measurements in cyber resilience. CyberMetrics measurements were introduced to support the real time, continual measurements of the effectiveness of security controls targeted by the incentive program. A mathematical model of the expected business benefits was then conducted. To date, there has not been a commercial implementation of this model to validate its effectiveness.

2. Literature Review

The goal of the proposed incentive program was to minimise preventable data breach incidents through the implementation of preventative controls. Consequently, a narrative literature review was conducted, exploring any previous attempts to create an incentive model for minimising preventable data breach incidents. While no existing models were identified, it was evident that future models needed to optimise investments in cyber security controls. This review identified an opportunity to focus on improving cyber resilience at the source of risk to optimise cyber security investments.

The study of the optimal investment level in preventative cyber security controls is a key focus in Cyber Risk Economics (CRE) [41]. This is facilitated through the standardisation of cyber risk taxonomy, which provides a consistent understanding of the terms and concepts used in the analysis. This chapter also explores the global efforts to standardise cyber risk taxonomy such as the “Cyber Insurance Exposure Data Schema V1.0” and ISO 27102 for Cyber Insurance [42]. The Factor Analysis of Information Risk (FAIR) [40] supports this effort by providing a structured approach for quantifying cyber risk. A practical research application of these concepts is examined in the CRE program initiated by the U.S Government Department of Homeland Security (DHS). Lastly, an understanding and quantification of risk appetite is essential to calculate the financial metrics for designing an incentive program.

2.1 Optimal Cyber Security Investments

Cyber Risk Economics (CRE) is the study of an economic management approach for determining the optimal investment for protecting a set of information assets. The basic economic principle is that the investment should not exceed the expected loss. This is also the principle underpinning cyber insurance as a risk transfer mechanism where the insurance premium outlay should cover the expected financial loss, the administrative cost of the insurance policy and profit margin for the insurer. Ehrlich and Becker developed a theory of demand for insurance [43]. Their analysis concluded that a fair price of market insurance encourages an expenditure on self- protection and minimising the risk from “moral hazard” [8]. The incentive model developed in this research represents a different approach in constructing a fair price without offering policy premium discount.

The economic approach provides the language and framework to communicate the business value of security investments as calculated by “Value at Security Risk” (V@SR). Hulthén [44] suggested transforming this calculation into a Return On Security Investment (ROSI), a business term which is more familiar with the management and funding bodies to convey the importance and relevance of sufficient investments in information security. This approach allowed management to understand, compare and evaluate security risks and their economic consequences with risks generated by other sources, strategies or investment decisions. It offered a more rational basis for security investment decisions. His analysis, as with most research in CRE, assumed a risk neutral company which treats all forms of losses and investments to be of equal importance and assesses them based only on their financial impact. Gordon and Loeb [45] modelled the optimal investment in information security by estimating the expected net reduction in financial losses at a different levels of investment into security controls. Their model assumed that the organisation can influence the vulnerability of an information asset (by improving resilience through appropriate investments) but cannot invest to reduce the threat.

Their model stated three assumptions, A1 – A3, on $S(z, v)$, denoting the probability that an information set with vulnerability v will be breached given investment z. These assumptions can be summarised as thus:

- A1: If the information set is completely invulnerable, it consequently would not warrant any investment in security, being perfectly protected.
- A2: If there are no security investments, then the probability of a data breach is equivocal to its inherent vulnerability.
- A3: Increasing one’s security investments will reduce data breach risks faster than linear rate.

Boundary conditions A1 & A2 represents the extreme scenarios of perfect security and insecurity. Condition A3 modelled the situation where an increase in the level of security investment is expected to result in decreasing rates of return. Their analysis showed that an optimum investment level should not exceed 37% ($\approx 1/e$) of the expected loss. However, they did not assert that these probability functions could accurately reflect real world security systems. Critically, the core conclusion was that optimal investments into information security are individualised and quantifiable, with a key balance between over- and under-investing.

Other research explored alternative designs for these classes of breach probability functions. Willemson [46] proposed an alternative breach probability function $S^{III}(v,z)$ where the vulnerabilities could be completely eliminated beyond a certain level of investment b , allowing the losses to decrease to 0 and then stay at 0 with his model resulting in an optimal investment of 50% of the expected loss. To illustrate the value of b, Willemson provided an example of hiring a hitman to eliminate a potential threat. The cost of hiring the hitman (the security investment) will completely eliminate the threat and perhaps is less costly than the potential harm to the victim.

Unfortunately, investment metrics and optimisation strategies are still not widely adopted in industry. A survey by Moore et al. shown an overwhelming number of CISOs and boards do not calculate return on investment (ROI) or other outcome-based quantitative investment metrics; instead, they opt for process based frameworks such as NIST and COBIT to guide strategic investment decisions [47].

While the study in cyber risk economics is maturing, there currently exists a big gap between these theoretical economic models and the realities of the market. This has resulted in different risk assessment and insurance premium pricing approach between insurers. A study of over 100 insurance policies shown consistency on loss coverage and exclusions of insurance policies [48]. But there is a surprising variation in the sophistication of the equations and metrics used to price premiums. This is the result of different cyber risk pricing model adopted by insurers. A review of 24 self-assessed cyber insurance proposal shown a basis toward malware management at the expense of a balanced cyber risk management program based on established information security frameworks [49]. This might be because the insurer insurers consider these controls more effective at mitigating the risk they are liable for, instead of a balanced program based on the economic models. On the other hand, some insurers see a market opportunity in providing comprehensive cyber risk management program to policyholder to comply with their regulatory obligations [50].

2.2 Standardisation of Cyber Risk Taxonomy

The previous section explored some earlier risk models used for cyber risk economics research which were flawed due to a lack of reference to real world information security control systems and loss event definitions. This section explores the effort to create a common terminology to support research and modelling in cyber security investments.

Cebula and Young [51] published a detailed overview of a taxonomy for operational risks in four main categories:

i. Action of People
ii. Systems and Technology Failures
iii. Failed Internal Processes
iv. External Events

The taxonomy is mapped to the controls and specific threat categories in NIST SP 800-53[52] and the Generic Threat Profiles under the 'Operationally Critical Threat, Asset, and Vulnerability Evaluation' [53] method developed by the Software Engineering Institute in Carnegie Mellon University.

Peters, Shevchenko and Cohen conducted a comprehensive survey of risk taxonomies [54], including the FBI's Internet Crime Complaint Center (IC3) classification of different types of cyber events. The taxonomy mapped them to the Basel II/III's banking regulation categorisation of events, such as cybercrime in financial organisations. This mapping is useful for conceptualising the types of insurable losses from cybercrimes.

Moreover, the Cambridge Centre for Risk Studies published the 'Cyber Insurance Exposure Data Schema V1.0' [55] in early 2016. The goal of the schema was to:

i. Provide a standardised approach for identifying, quantifying, and reporting cyber exposure
ii. Enable the development of models for cyber risk that will be applicable to multiple users
iii. Facilitate risk transfer to reinsurers and other risk partners whilst risk sharing between insurers
iv. Provide a framework for exposure-related dialogues for risk managers, brokers, consultants, and analysts

The schema can be used to support cyber security assessments as a method of standardising exposure reporting and integrating a schedule of policies from different insurance companies. In addition, the International Organisation for Standardization published 'ISO 27102

Information Security Management - Guidelines for Cyber-Insurance' [42] in 2019 to provide guidance for:

i. Considering the purchase of cyber-insurance as a risk treatment option to share cyber-risks
ii. Leveraging cyber-insurance to assist in the managing of the impact of a cyber incident
iii. Sharing data and information between the insured and insurer to support underwriting, monitoring and claims activities associated with cyber insurance policies
iv. Leveraging an Information Security Management System (ISMS) when sharing relevant data and information with an insurer

The standard defines cyber risks that can be covered under a cyber insurance policy, as well as incorporating a generic risk assessment that the insurer can conduct in the underwriting process. Importantly, this standard explains how to leverage the ISMS published under the ISO 27001 Standard to produce data, information and documentation that can be shared with an insurer.

2.3 Improving Cyber Resilience at the Source of Risk

Minimising preventable data breach incidents is an important priority for insurers in managing claim exposure for cyber insurance. The research report "Advancing Accumulation Risk Management in Cyber Insurance" [56] published by the Geneva Association, a global insurance think tank, identified the man-made nature of cyber-attacks, the rapid spread of malware via the global Internet and the lack of historical claim data as key underwriting challenges in estimating the expected loss for cyber risk. These considerations have a cumulative impact on the potential claim exposure from a single large-scale cyber security incident. The recent June 2017 NotPeyta ransomware attack was estimated to have caused a USD$10 billion loss [57] to the global economy. The Wannacry malware unleashed a month prior was estimated to have caused USD$4 billion in loss to the global economy. The report recommended improving cyber resilience at the source of risk. In a supply chain, improving cyber resilience at the source of risk is an important strategy because of the delegation of risk management responsibilities through the outsourcing arrangement. The source of risk is consequently shifted along the supply chain under the transfer of the risk process.

In the case of these malware attacks, the source of risk is where the initial malware infection took hold. The focus of the incident response process was to contain the financial loss arising from the incident. Improvements could be delivered through phishing email security awareness training, a well-rehearsed incident response plan, reliable data backups and the restoration of infrastructure. The latter two approaches are discussed in the use cases covered in chapter 5 and 6.

2.4 Factor Analysis of Information Risk (FAIR)

Risk quantification is a key enabler in the study of CRE, providing the measurements required to make calculated decisions. It is the foundation of the DHS CRE program covered in the first research theme. However, the unwillingness of victim organisations to report data breaches and the difficulty of attributing financial losses to incidents both contribute to the difficulty in quantifying cyber risk [58]. In response, the Open Group published the Factor Analysis of Information Risk (FAIR) [40] standard as a globally recognised, open sourced framework for cyber risk quantification, offering a structured approach to break down risk scenarios and estimate the expected financial loss. The Incentive Model ontology developed under this research program, discussed in Chapter 3, is inspired by the FAIR methodology. This section provides an overview of the FAIR framework, exploring key building blocks in the taxonomy. The discussion serves as a foundation for the next few chapters and case studies. It also covers important discussions on data collection techniques and calibration. The FAIR framework is well suited for estimating cyber risk in emerging research areas such as the smart grid cyber threat [59], IoT network [60] and exploitations in mobile devices [61].

The FAIR Risk Language taxonomy is depicted in Figure 2.1:

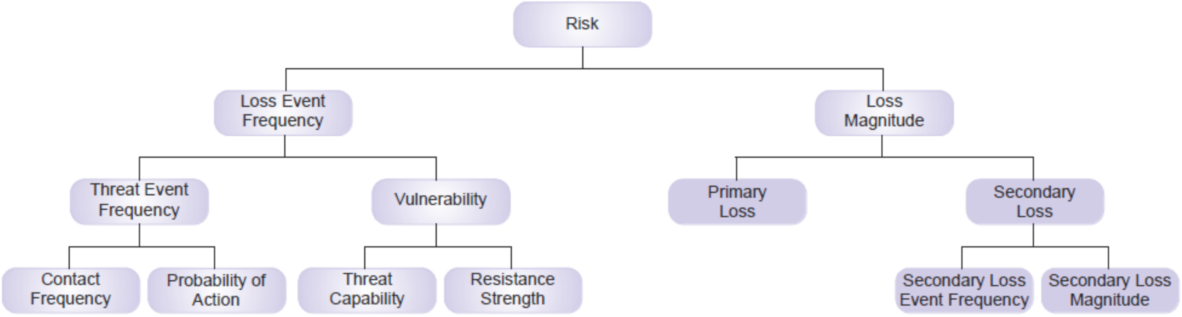


Figure 2.1 - The FAIR Risk Language taxonomy [62]

Risk is defined as the potential financial loss against an asset resulting from successful attacks. The expected loss can be calculated by multiplying the Loss Magnitude (LM) by the Loss Event Frequency (LEF). LM and LEF are conceptual tools for breaking down the risk scenario and are often not directly measurable. LM can vary significantly amongst the same type of loss event, depending on business conditions during the incident. For example, a denial of service attack against an online merchant during the Black Friday and Christmas shopping season would result in a significantly higher LM than during the rest of the trading year. Because LEF and LM might not be directly measurable, the FAIR taxonomy breaks down these building blocks further into their respective sub-components as shown in Figure 2.1 above. These sub-components are examined in detail in the following sections.

2.4.1 Loss Event Frequency (LEF)

LEF is broken down into Threat Event Frequency (TEF) and vulnerabilities. This breakdown recognises that not all attack (threat) events are successful and result in financial losses. The probability of a successful attack is represented by the vulnerability index of the asset. Therefore, LEF can be calculated by multiplying LEF by the vulnerability index.

2.4.1.1 Threat Event Frequency (TEF)

LEF is further broken down into “Contact Frequency” (CF) and “Probability of Action” (PoA) by the threat actors. These parameters can vary significantly at different sources of risk. CF is a “necessary but not sufficient” pre-condition for launching a successful attack which is a result of the need to provide reliable and consistent services to customers. The significance of this can be conceptualised through imagining a retail outlet, which is required to offer direct public access to their store front. This requirement can expose the store to attempted after-hours break-ins. Security screens and other anti-theft devices such as reinforced glass panels could be deployed to reduce opportunities of contact with the thieves. But these measures would impact the aesthetic design of the store and cost money. An alternative strategy would be to remove merchandise from the display windows after trading hours to reduce the “Probability of Action” (PoA). Potential thieves may be discouraged from attempting the break-in due to the uncertainty of the potential rewards. Another common strategy is to put the cash till right by the front door to confirm that no cash is kept on the premises.

2.4.1.2 Understanding vulnerability

The concept of vulnerability is often associated with the priority of software patches assigned by the vendor or based on an industry score such as the CVSS score. However, the FAIR framework breaks down the concept of vulnerability into “Threat Capability” (TCap) and “Resistance strength” (RS), to provide further clarification for mitigation options. This section examines limitations in the vulnerability scoring system and explains the FAIR approach.

The Australian Cyber Security Centre Essential Eight [63] best practice guide recommends patching all vulnerabilities rated with ‘extreme risk’ within 48 hours. PCI DSS V3.2 Requirement 6.2 mandated the installation of critical patches within one month of release. Requirement 11.2 required the Approved Vendor Scan identify and remediate any vulnerabilities scored greater than or equal to a CVSS score of 4.0. While these vulnerability scoring systems are commonly used to underpin patching policies, they can result in Internet facing servers retaining exploitable vulnerabilities due to lower priority scores remaining unpatched for an extended period. Jacob et al. [28] recommended an alternate strategy to improving vulnerability remediation through prediction of the likelihood of exploitation. This strategy takes into consideration the sensitivity of the workload, the accessibility of publicly available exploit tools and the history of active exploitation in the Internet. This methodology is expected to produce a targeted patching strategy which increases the effective coverage of protection of exploitable servers from active threats by diverting patching efforts away from servers less likely to be exploitable.

Under the FAIR framework, vulnerability is measured by the amount that TCap exceeds RS. It might be helpful to conceptualise RS as the difficulty faced by the attacker in overcoming the security controls. Both measurements have been normalised to a maximum value of 1 to simplify the calculation process. This vulnerability model is more suited for estimating the cost-effectiveness and optimal investment level of security controls.

2.4.2 Loss Magnitude

Loss magnitude is broken down into the primary and secondary loss categories, spanning six forms of loss as follows:

1. Productivity loss: Losses resulting from an operational inability to deliver products or services

2. Response costs: Losses associated with the costs of managing an incident
3. Replacement costs: Losses resulting from an organisation having to replace capital assets
4. Competitive Advantage loss: Losses resulting from intellectual property or other key competitive differentiators that are compromised or damaged
5. Fines and judgements: Fines or judgments levied against the organisation through civil, criminal, or contractual actions
6. Reputational damage: Losses resulting from an external stakeholder perspective that an organisation's value has decreased and/or that its liability has increased

Primary loss occurs directly as a result of the threat agent's action upon the asset, resulting in losses in productivity, response costs and replacement costs. The other three forms of loss only occur as Primary Loss when the threat agent is directly responsible for those losses (e.g. Competitive Advantage loss occurring when the threat agent is a competitor, Fines and Judgments when the threat agent is filing charges/claims, etc.).

On the other hand, secondary loss occurs as a result of secondary stakeholders (e.g., customers, stockholders, regulators, etc.) reacting negatively to the primary event. One may think of it as fallout from the primary event. An example would be customers taking their business elsewhere after their personal information had been compromised or due to frustration experienced as a result of frequent service outages. Because only a small portion of primary loss events lead to secondary loss events, it is useful to calculate the Secondary Loss Event Frequency (SLEF) and Secondary Loss Magnitude (SLM).

2.4.3 Collecting Expert Estimation using PERT Distribution

Collecting expert estimation is an important milestone among the six steps of the FAIR analysis process (Figure 2.2).

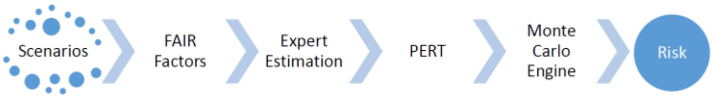


Figure 2.2 – The FAIR Analysis Process [64]

Experts are risk process owners with operational experience in the risk process and have a good understanding of the nature of the identified risk factors. They are not expected to have any formal training in risk analysis which helps in minimising perceived biases in the risk model.

Additionally, they are well aware of the potential opportunities available to threat agents to launch attacks.

Unfortunately, translating this operational knowledge into predictions of Threat Event Frequency (TEF) is not a straightforward process, challenging even experts with sophisticated cyber security skills and training in statistical methods. The FAIR analysis process eases this problem by using the PERT distribution to capture these inputs. The PERT distribution belongs to a family of continuous probability distributions, PERT (a, b, c), characterised by three probability parameters: minimum (a), most likely (b) and maximum (c). The PERT distribution is an effective modelling tool to capture expert opinions [65] where it is difficult to obtain data to accurately determine the uncertainty of all the variables [66] [67]. PERT distribution does not assume heavy tail, producing a simple and clean distribution representing the approximation from expert estimates as an input to Monte Carlo simulation. This characteristic is particularly suited for cyber risk management where the requirement is to produce accurate but not exact estimation to support strategic decisions such as prioritisation of investment decisions.

2.4.4 Calibrating Expert Estimates

The FAIR framework embeds the calibration process developed by Hubbard from his research in Applied Information Economics (AIE) [68] to improve accuracy and consistency from expert estimates. Hubbard observed that most people tend to over or under value their estimates. The concept of being “90% confident” of an event occurring often leads to these estimation errors due to encouraging a lack of vigour in the estimation process.

Hubbard proposed a simple “Clarification Chain”:

1. If it matters at all, it is detectable/observable
2. If it is detectable, it can be detected as an amount
3. If it can be detected as a range of possible amounts, it can be measured

Hubbard expanded his measurement methodology, using the “calibration process” to transform “expert estimates”, typically in the form of discrete distributions, into Confidence Intervals (CI) as a continuous distribution. Hubbard hypothesised that people have good instincts on the probability of events occurring given their experience. The problem is the language of “probability” and statistics. Hubbard advocated the “Spin the Dial” approach to help experts to overcome this language barrier. The approach is depicted in Figure 2.3:

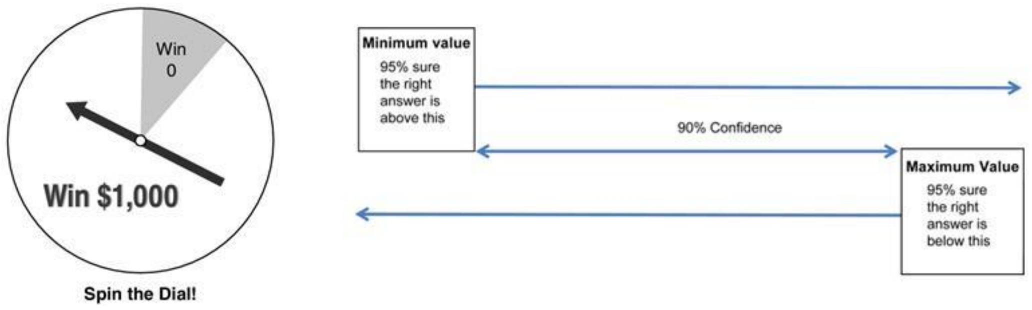

Win
0
Win $1,000
Spin the Dial!
Minimum value
95% sure the right answer is above this
90% Confidence
Maximum Value
95% sure the right answer is below this

Figure 2.3 –Hubbard’s calibration process [69]

Under this approach, the expert is given absurd estimates for the PERT distribution such as a maximum of 100 successful ransomware attacks per day. He found that incentivising the experts with a hypothetical $1,000 reward for making a correct estimate had an observable benefit in improving the accuracy of their estimates. The estimation process was repeated with increasingly defined estimation criteria, until experts no longer felt confident of winning given their 10% chance of being right, with their estimates being summated to form the “90% Confidence” interval.

2.5 DHS CRE Program

The United States Department of Homeland Security (DHS) Science and Technology Directorate (S&T) established a Cyber Risk Economics project in 2018 to support research into the business, legal, technical and behavioural aspects of the economics of cyber-threats, vulnerabilities and controls [41]. The focus of the research was to evaluate:

i. Investment into cybersecurity controls (technology, regulatory, and legal) by private-sector, government and private actors
ii. The impact of investments on the probability, severity and consequences of actual risks and the resultant cost and harm
iii. The value of the correlation between business performance measures, evaluations of cybersecurity investments and impacts; and
iv. Incentives to optimize the investments, impacts and value basis of cyber-risk management

The research strategy was divided into 6 themes, covering 12 areas (Figure 2.4). It identified that the general lack of understanding and effective assessment of cyber risks by leaders in the economy represented a fundamental challenge in managing cybersecurity risks. Consequently, investment decisions were made exclusively on qualitative risk measurements, using previous breach events as a proxy measure of risk. The current practice focusses disproportionally on vulnerabilities instead of risk (i.e. suffering a financial loss), undervaluing the consequences of cyber incidents for external entities like suppliers, customers and the public. It observed that cyber risk metrics are often framed in qualitative or operational terms (e.g. the number and timeliness of systems patched) but are rarely quantified using traditional financial measures that guide investment decisions in other areas of risk, such as the Return On Investment (ROI).

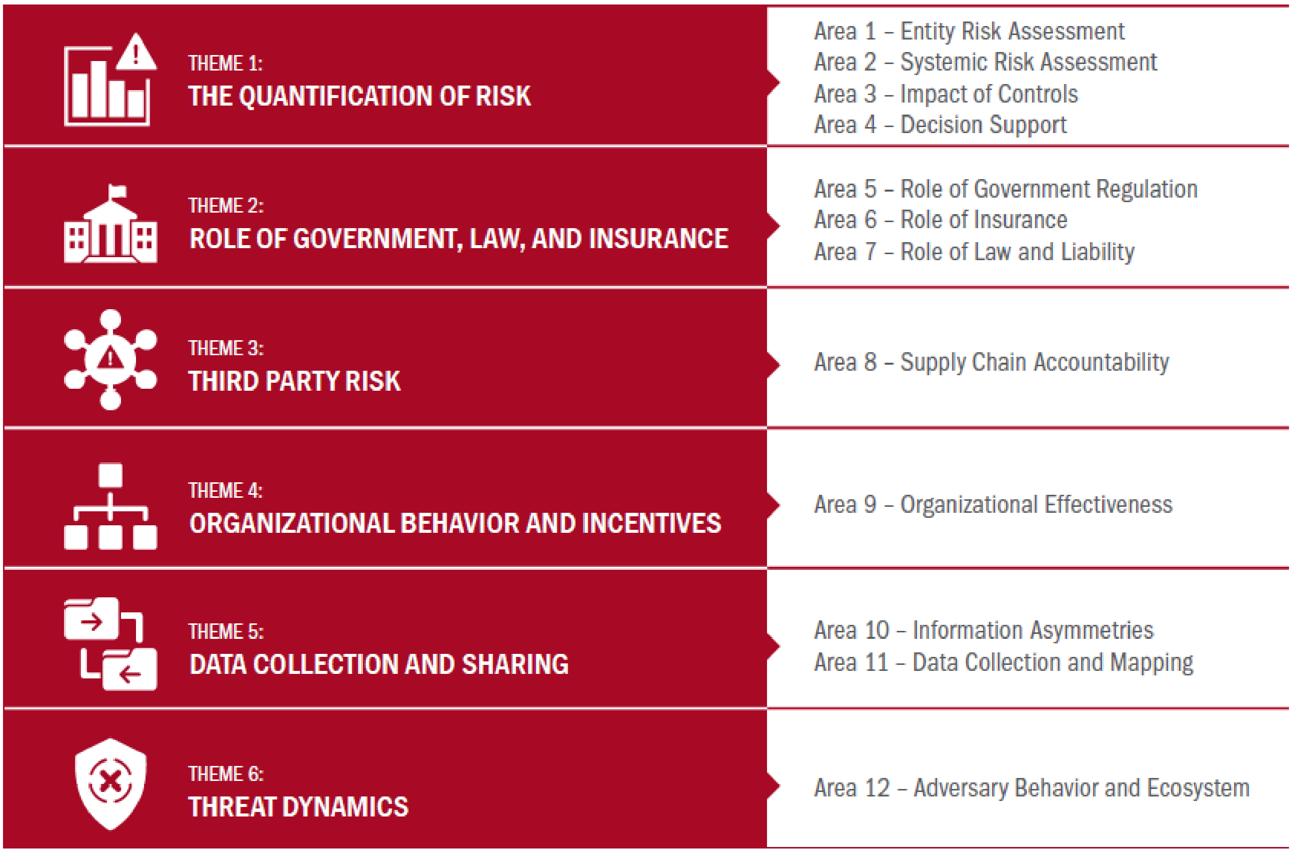

THEME 1:
THE QUANTIFICATION OF RISK
Area 1 – Entity Risk Assessment
Area 2 – Systemic Risk Assessment
Area 3 – Impact of Controls
Area 4 – Decision Support
THEME 2:
ROLE OF GOVERNMENT, LAW, AND INSURANCE
Area 5 – Role of Government Regulation
Area 6 – Role of Insurance
Area 7 – Role of Law and Liability
THEME 3:
THIRD PARTY RISK
Area 8 – Supply Chain Accountability
THEME 4:
ORGANIZATIONAL BEHAVIOR AND INCENTIVES
Area 9 – Organizational Effectiveness
THEME 5:
DATA COLLECTION AND SHARING
Area 10 – Information Asymmetries
Area 11 – Data Collection and Mapping
THEME 6:
THREAT DYNAMICS
Area 12 – Adversary Behavior and Ecosystem

Figure 2.4 - 2018 CYRIE Capabilities Gaps Research Strategy [41]

Research area 3 focussed on supply chain risk management. Some of the research topics include modelling incentives and mechanisms for up and down stream suppliers to cooperate in improving cyber security and quantifying how coordination costs factored into shared security contexts.

Research area 9 focussed on organisational effectiveness, including how incentives at the organisational level got translated into individual cyber risk-reducing behaviour; and identifying individual incentives that could lead to better organisational performance.

2.6 Risk Appetite

The risk appetite of an organisation defines the boundary of their risk management framework and provides guidance on the appropriate level of investment in security controls. The Bank of International Settlements guidance on ‘Principles for Sound Management of Operational Risk’ [70] provides some concrete examples of the application of risk appetite to the operational risk management. The challenges of mapping high level risk appetite statements to operational risk management thresholds were discussed in ‘Operational Risk Appetite’ [71]. The paper explored the process of propagating risk appetite statements from the business board to the operational decision-making levels of the organisation.

The Institute of Risk Management (IRM) paper ‘Risk Guidance Paper Appetite & Tolerance’ [72] identified the following principles for developing a risk appetite:

i. It can be complex and should not be oversimplified for the sake of simplicity
ii. It needs to be measurable. Otherwise the statement may become empty and vacuous. Shareholder value or 'Economic Value Added' may be a good starting point. Relevant and accurate data is vital to ensure this process is subject to the same level of data governance as routine accounting data
iii. It is not a single fixed concept but consists of a range of appetites for different risks which might vary over time
iv. It should be developed in the context of an organisation's risk management capability, which is a function of risk capacity and risk maturity
v. It takes into account different views at strategic, tactical and operational levels
vi. The control culture of the organisation at the operational level should be balanced against the propensity to take risks at the strategic level

The IRM case study on risk appetite statements [73] extracted from the annual reports of major companies explores how effective these six principles have been when applied and the lessons learned.

2.6.1 Acceptable Risk

There is no perfect security solution. Investments in security capabilities can be expected to minimise but not eliminate expected losses. The cost effectiveness of these investments is expected to level out with increasing levels of investment as shown in Figure 2.5 below:

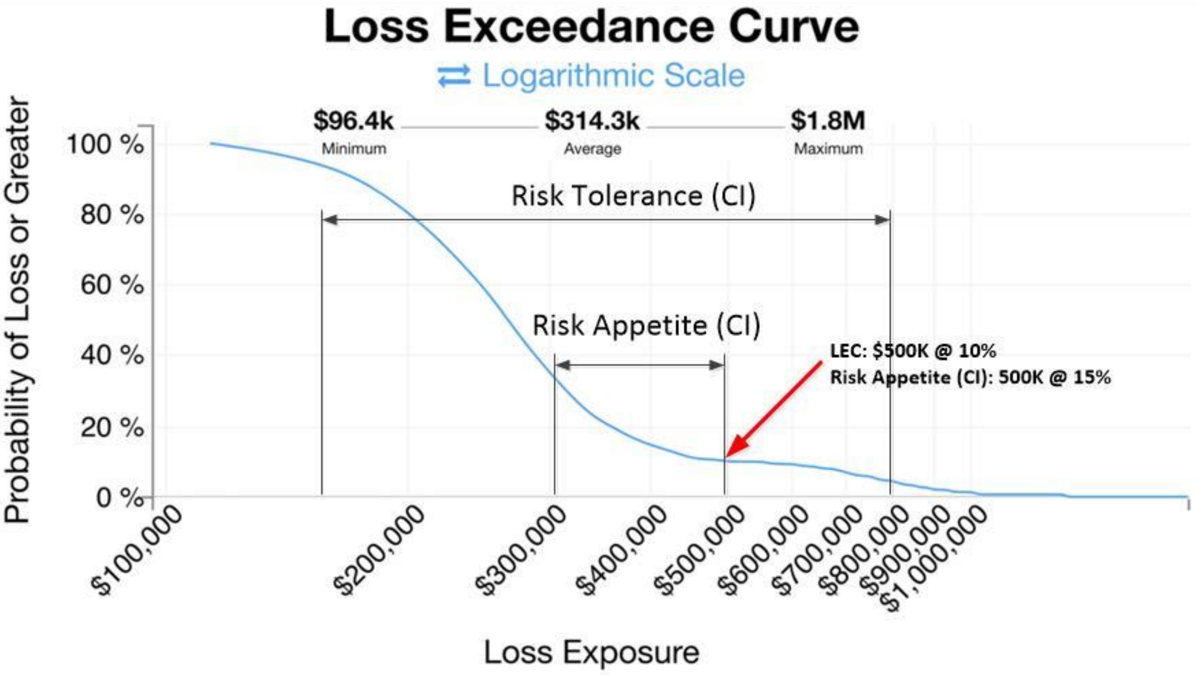


Figure 2.5 - Dimensioning residual risk against risk appetite and risk tolerance limits

The Loss Exceedance Curve (LEC) represents the residual risk [74] after security controls have been applied. If the level of residual risk is within the risk appetite, the security control is sufficient and is a part of normal business practices.

Risk appetite statements are high level business statements such as “we will not expose more than x% of our capital to losses in a certain line of business”. These high-level statements can be broken down into two key parameters: risk appetite and risk tolerance. Risk appetite represents the limit for "acceptable risks" under normal operating conditions. Risk tolerance defines the maximum acceptable deviation from the risk appetite. If the expected loss exceeds the risk tolerance, other risk transfer or mitigation strategies should be deployed to reduce the expected loss. Taken together, these two parameters serve as guard rails to protect the business from exposure to extreme risks which can reduce profitability and even lead to failure of the organisation.

To determine whether the security capability is sufficient, the risk appetite and risk tolerance levels should be compared against the LEC of the treated risk process after applying security controls. To facilitate such a comparison, the risk appetite and risk tolerance levels must be expressed in the equivalent LEC format by solicitating risk appetite input from key risk stakeholders and quantifying these inputs using the FAIR methodology. The Australian Government Department of Finance issued a ten-step guideline on how to define risk appetite and tolerance [75]. The process involves interviewing senior executives to define the risk appetite statement and Subject Matter Experts (SMEs) to build and refine risk tolerance statements. These inputs capture the targeted risk range (risk appetite) and operational limits (risk tolerance).

To simplify visual representation, the approved risk appetite and risk tolerance CI, expressed as loss magnitude and probability value pairs, are marked against the LEC in Figure 2.5. If these CI value pairs are greater than the expected losses at the corresponding part of the LEC, the solution is acceptable. For example, in Figure 2.5 the probability of suffering a $500,000 loss is 10%. The risk appetite estimated a 15% probability of suffering this level of loss. Therefore, the residual risk level is acceptable. It can be concluded from this calculation that the information security capability is commensurate with the size of the threat.

2.6.2 Acceptable Losses

Taking acceptable risk is essential to sustaining profitable earnings in a competitive market. Without taking risks, profits will be squeezed out by price competition. Outsourcing and other supply chain arrangements offer organisations opportunities to transfer risk at a better price than they can manage themselves. This allows organisations to focus on managing risks which give them a competitive advantage.

Therefore, both risk appetite and risk tolerance are inextricably linked to performance of the business over time. These parameters, represented by the 95% CI estimates, are overlaid on the LEC in Figure 2.5. If the probability of the expected loss is within the estimated risk appetite CI limits for the organisation, it would be reasonable to conclude that security capability is commensurate with threats. Otherwise, the security controls should be reviewed and improved to reduce the expected loss, lowering it to within the risk appetite CI. Similarly, if the CI estimate for the risk tolerance has been exceeded, other risk transfer mechanisms such as cyber insurance should be considered in order to narrow the gap.

The dimensioning of the insurance coverage limit is illustrated in Figure 2.6. Investment in cyber risk management programs is designed to minimise preventable cyber-attacks. The expected reduction in financial loss should cover the Risk Appetite CI range. Residual risk can be transferred to an insurer through a cyber policy representing the risk boundary between "MUST RETAIN and "CAN TRANSFER".

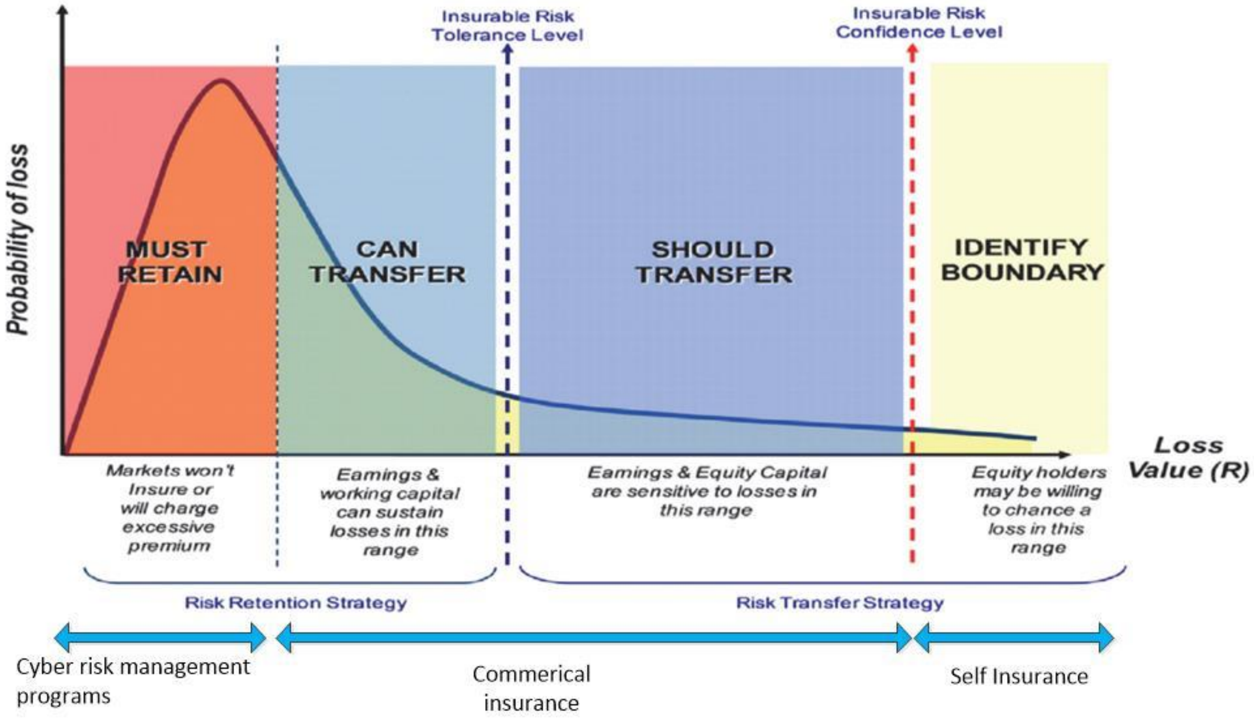

Insurable Risk Tolerance Level
Insurable Risk Confidence Level
Probability of loss
MUST RETAIN
CAN TRANSFER
SHOULD TRANSFER
IDENTIFY BOUNDARY
Loss Value (R)
Markets won't Insure or will charge excessive premium
Earnings & working capital can sustain losses in this range
Earnings & Equity Capital are sensitive to losses in this range
Equity holders may be willing to chance a loss in this range
Risk Retention Strategy
Risk Transfer Strategy
Cyber risk management programs
Commerical insurance
Self Insurance

Figure 2.6 – Dimensioning cyber insurance limits [76]

The transferred risks should cover the Risk Tolerance CI range. The incentive program developed under this research program is designed to moderate the transferred risks particularly in a supply chain context where the policyholder does not have direct control of the risk process such as an outsourced authentication service.

3. Incentive Model Ontology

This chapter describes a structured approach for developing incentives to minimise avoidable data breach incidents. Key building blocks in the incentive model ontology (Figure 3.1), are discussed. A case study featuring a hypothetical debt collection agency is used to illustrate how this ontology could be utilised to develop an incentive program to minimise PII exposure.

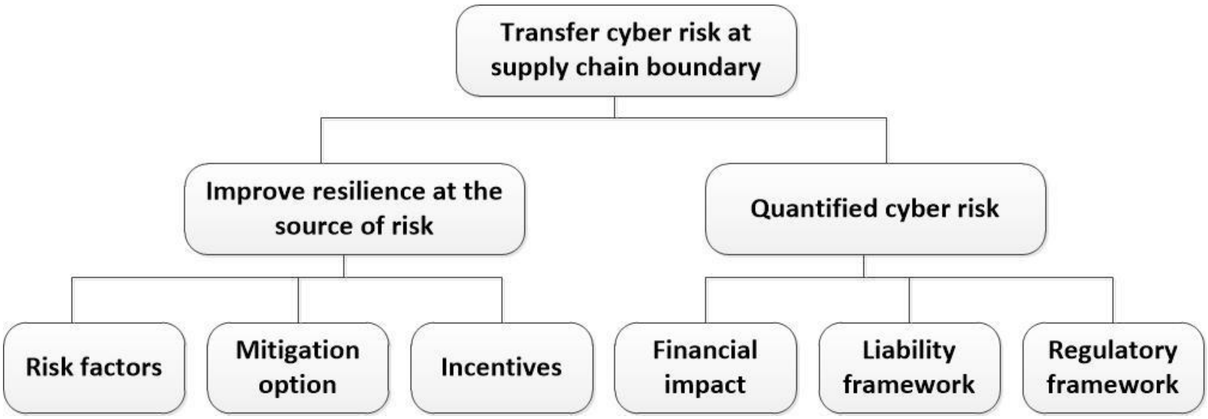


Figure 3.1 – Incentive model ontology

The incentive model empowers the risk owner to regain control of the risk process being transferred to other entities along the supply chain. However, such programs must be designed judiciously as an incorrectly designed incentive program could have the unfortunate effect of encouraging undesirable behaviours.

The incentive model is developed under a five step process discussed in section 3.1 and is applied to a hypothetical debt collection agency in section 3.3.

3.1 Incentive Model Analysis Process

This section discusses the five steps of the incentive model's analysis process depicted in Figure 3.2 below.

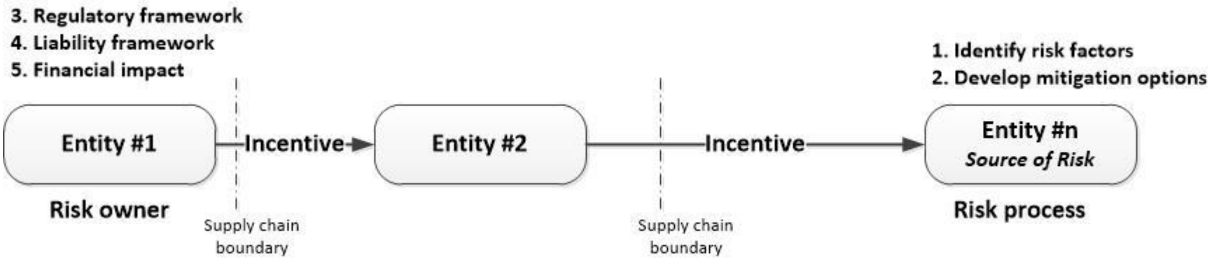


Figure 3.2 – Incentive model analysis process

The five steps in the incentive model analysis process are:

1. Identify risk factors
2. Develop mitigation options
3. Identify applicable regulatory framework
4. Explore liability framework
5. Estimate financial loss from risk materialisation

1. Identify risk factors

The operating environment of the transferred risk process should be analysed using the FAIR framework to identify the risk factors. The newly created operating environment of a freshly transferred risk process could be different from the designs and assumptions applied by the risk owners to the original environment. For example, there are likely to be a much broader set of threat communities targeting large service providers such as IT outsourcers or cloud service providers. The higher concentration of highly skilled staff in a large service provider environment can expose the environment to a higher risk from insider threat. The attack against Capital One by a former Amazon Web Services (AWS) engineer highlighted this form of risk [34]. The decision by Capital One to host their infrastructure in AWS exposed their data to a unique and new vulnerability which did not exist in their private data centre.

2. Develop mitigation options

The list of identified risk factors provides an analysis context to examine the range of mitigation options. The balance between the FAIR factors of “Contact Frequency” vs “Probability of Action” and “Threat Capabilities” vs “Resistance Strength” are a rich source of inspiration for developing mitigation options. Risk owners should examine the process and technology controls available in the operating environment of the transferred risk process to identify mitigation options. These options might not be available in their native operating environment before the transfer. The implementation of these mitigation options might demand a change in the design and optimisation of the risk process, impacting the user experience and process cost. For example, a transferred risk process might only support a specific brand of hardware token for user authentication. This might require the risk owner to bear the cost of acquiring and distributing the new set of hardware tokens to their users and to provide users with appropriate training.

3. Identify applicable regulatory framework

The risk owners must examine the impact of the transferred risk process on the set of applicable regulatory framework on the risk process. The risk transfer process does not relieve the risk owner of their compliance and regulatory obligations. A common challenge is data sovereignty when data resides in a different jurisdiction (such as in the US or EU) exposed to different law enforcement regimes and subpoena rules.

4. Explore liability framework

Liability is commonly associated with the secondary loss category under the FAIR framework discussed in section 2.4.2. The number of stakeholders involved in a transferred risk process can increase significantly. This can be due to the sharing of data processing platforms in the transferred risk process. For example, data subpoena orders by law enforcement agencies against other tenants in the shared infrastructure can unintentionally expose a risk owner's data set. This could violate the 'European Union General Data Protection Regulation' (EU GDPR) [77] provision which demands that data owners seek consent from their customers before sharing their personal data. This can be an expensive and time-consuming process. Risk owners should make provisions against these conceivable circumstances such as encrypting all data at rest to prevent it from being readable when it is subpoenaed without their consent. This might increase outsourcing costs and compound the management process. It is an investment optimisation decision which can be examined under CRE principles.

5. Estimate financial loss from risk materialisation

The FAIR framework can be applied to estimate potential financial losses based on the output from the analysis in the previous sections. This estimate identifies boundaries on the investment and ongoing operating costs required to establish and administer the incentive scheme. The total cost of the incentive scheme should not exceed the estimated financial loss. Modelling of the benefits from an incentive scheme is discussed further in chapter 6 for the CyberMetrics use case.

3.2 Bankruptcy of AMCA

This section reviews the impact from a recent data breach which led to the bankruptcy of a debt collection agency and class action against its client. It demonstrates the need for prudent management of cyber risk in a supply chain.

Medical billing firm, the American Medical Collection Agency (AMCA), filed for bankruptcy in June 2019 after suffering a massive data breach [78], exposing the personal information of nearly 20 million Americans. AMCA provided debt collection services to several large medical diagnostics service firms. AMCA's expertise was in collecting high volumes of receivables with very small balances. It collected Personally Identifiable information (PII) including name, home addressees, social security number, bank account information and credit card information. It received notification from its acquiring bank that a disproportionate number of credit cards that at some point had interacted with its web portal were later associated with fraudulent charges.

In response to this discovery, its four major clients including LabCorp, Quest Diagnostics, Conduent Inc and CareCentrix Inc terminated their service contracts. In addition, VISA and Mastercard demanded significant remediation actions and security upgrades in addition to imposing fines. The company incurred USD$3.8m in notification costs, USD$2.5m in legal costs and USD$0.4m on incident response before it collapsed. It was also exposed to at least three lawsuits from plaintiffs in New York. The company concluded that it could not afford these massive costs and declared bankruptcy.

The collapse of AMCA also led to class actions against some of its major clients. A class action lawsuit against LabCorp was filed on June 13 in the U.S. District Court in Kansas City, Kansas. The lawsuit alleged that the medical diagnostic company failed to monitor its billing and collections vendor affecting 7.7 million of its customers and violated HIPAA by failing to protect its consumers' data. Unfortunately, the medical diagnostic company did not have a list of the consumers affected. It is clear from this case that it is in the interest of consumers (such as LabCorp) in a supply chain to properly manage the information security postures of their suppliers. Outsourcing a service does not dilute or remove the obligation of the consumer to protect their information.

The bankruptcy of AMCA and the resulting class action against LabCorp firmly underlined the importance of investing in preventative security controls. Because of the ongoing bankruptcy procedure and class action, detailed analysis of the attack has not been made public. Therefore, it is not known whether the attack was targeted and whether it could have been averted through preventative security controls. But AMCA noted in its bankruptcy filing that evidence showed the company was hacked as far back as August 2018, a full 6 months before the data breach was discovered in March 2019. This showed that the information required to discover the attack was available to the firm but was not actioned for want of preventative detection processes. This consideration will add weight to the class action alleging negligence on the part of LabCorp by failing to monitor the security posture of AMCA as a service provider. If LabCorp had an incentive program in place with AMCA, it might have been a useful defence against the class action by demonstrating due diligence.

3.3 Modelling PII Management in a Debt Collection Agency

This section provides an overview on the operating model of a hypothetical debt collection agency called ABC and demonstrates how to apply the five step incentive model analysis process discussed in section 3.1. The developed incentive program is shown in Figure 3.3. This incentive program is designed to discourage debt collectors from selling PII to criminals.

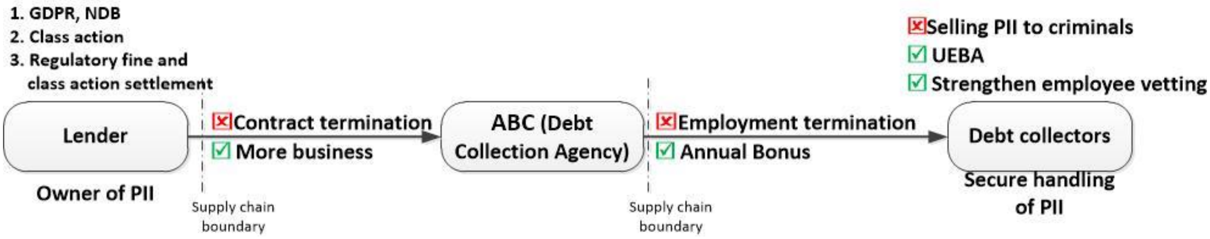


Figure 3.3 – Incentive model against insider threats

This paragraph provides an overview of the operating model of a debt collection agency. The agency collects outstanding debts on behalf of lenders such as banks. Debt collection is a time-consuming process which must comply with regulations for the management of consumer credits. PII of debtors, including full name, address and date of birth, are passed from the lender to the debt collection agency. PII is used to establish contact with the debtor and confirm their identify. If the debtors' contact details are changed due to relocation, job change or simply to avoid contact from the lender, a private investigator might be engaged to track down the debtors in order to serve the debt reminder notices.

Enforcement of court orders to recover debt against property and other assets owned by debtors requires debt collectors to present PII to proof the debtor's ownership of the targeted asset and their liability under the debt obligation.

The flow of PII in the debt collection process is depicted in Figure 3.4:

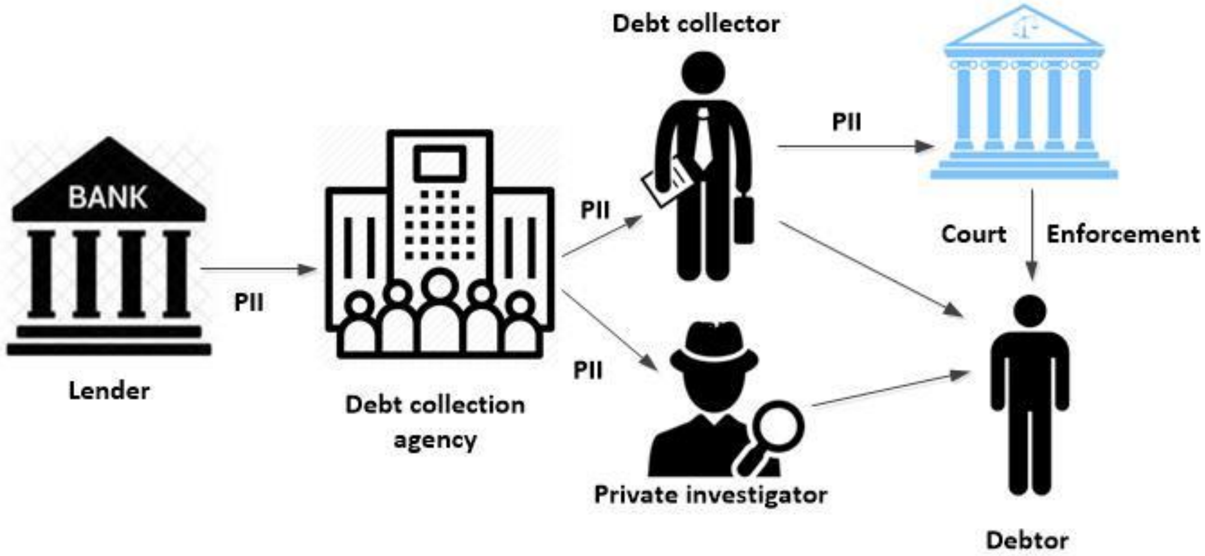


Figure 3.4 - Handling of PII in the debt collection agency supply chain

PII might be captured in printed form or stored electronically on the laptop or mobile phone apps used by debt collectors and private investigators. The debt collector and private investigator can be contractors of the debt collection agency. In this case, they are responsible for the secure handling of PII provided to them.

Secure handling of printed information is dependent on the security practice of the individual debt collector and investigator. There have been many reported incidents where printed PII information is simply discarded in unsecured trash bin due to the lack of secure document disposal bins in the office. Printed documentation might be discarded insecurely whilst out of the office for convenience. Similarly, laptops might not be protected by strong disk encryption. As a result, a lost laptop can potentially expose the PII for all debtors.

3.3.1 Estimating LEF

The Incentive Model analysis process begins with an examination of the four potential sources of risk for the handling of PII in the supply chain scenario depicted in Figure 3.4 above:

1. Handling of PII at the agency level

2. Handling of PII by debt collectors
3. Handling of PII by private detectives
4. Provision of PII to the court system

To illustrate this analysis process, we decided to simplify it through only demonstrating the handling of PII by debt collectors, although the analytical process should be repeated on the other sources of risk. The identified risk factors for debt collectors are presented in Table 3.1:

Table 3.1 – Risk factors for PII handling by the debt collectors

Risk Scenario	**Asset**	**Threat Community**	**Threat Type**	**Effect**
1	Debtor PII	Privileged insiders	Malicious	Confidentiality
2	Debtor PII	Privileged insiders	Malicious	Integrity
3	Debtor PII	Privileged insiders	Error	Confidentiality
4	Debtor PII	Privileged insiders	Error	Availability
5	Debtor PII	Privileged insiders	Error	Integrity

Insider threats are a constant problem, even for information security vendors with strong security control processes. For example, Trend Micro disclosed in November 2019 [79] that an employee used fraudulent means to gain access to a customer support database that contained names, email addresses, Trend Micro support ticket numbers and in some instances telephone numbers. Information on 68,000 customers was sold to tech support scammers to initiate fraudulent calls impersonating the security company's staff. Upon discovery of the attack, actions were immediately taken to ensure no additional data could be improperly accessed and the incident was reported to law enforcement for further investigation.

Debt collectors, as privileged users, might abuse their board access maliciously. In this case, the debt collector might sell PII records to organised criminals. Stolen PII can be used to commit identity fraud such as via the creation of false bank accounts or by blackmailing these debtors. This type of attack impacts the confidentiality of the record and is represented by scenario 1 in Table 3.1.

Debt collectors might also be asked by criminals to alter the amount of outstanding debt in order to defraud the lenders. Lenders may not detect this type of fraud because they don't always expect the complete recovery of outstanding debt on delinquent debtors. This type of attack impacts integrity of the record and is represented by scenario 2 in Table 3.1.

Human error is another likely source of attack from these privileged insiders. According to the Office of the Australian Information Commissioner (OAIC) 2019 Notifiable Data Breach (NDB) report [80], amongst the 245 notifications, 34% and 62% were attributed to human error and malicious attacks respectively, with the remaining 4% attributed to system faults. An example of human error might be debt collectors mistakenly emailing debt collection notices to the wrong person due to an error in the matching of the debtor's identity. Additionally, debtor email addresses might be accidentally exposed via a broadcast email. This is covered under scenario 3 in Table 3.1.

Worse still, a debt collector might accidentally delete a debtor's records, effectively writing off their debt. This is represented by scenario 4 in Table 3.1.

Finally, the debt collector might incorrectly alter a debtor's records, such as by changing their contact details during an update. This would prevent the debtor from receiving future reminder notices, resulting in the debt becoming delinquent and incurring further unnecessary late payment penalties. This is represented by scenario 5 in Table 3.1.

Threat actors can be discouraged from acting by the fear of being caught, the concept underlying the design of the "Probability of Action" control. This control can be achieved through access monitoring and training for debt collectors, highlighting the likelihood of inappropriate access being detected through the monitoring program. In the case of a debt collector colluding with organised crime to sell access to the PII database, they would be informed through their training that such illegal action could lead to the termination of their employment and potential jail time.

A simulation might proceed as follows. The hypothetical debt collection agency, ABC, conducted a workshop with their head of human resources, head of operations and head of the debt collector team to collect an expert estimate on loss event frequency. The team leaders were aware of three data loss incidents attributed to human error in the past year. Fortunately, the number of debtor records impacted were relatively small and the incident quickly detected and rectified. All impacted debtors were notified immediately. The investigations concluded that these incidents did not result in any material harm. Therefore, notification of these incidents to the OAIC under NDB was not required. No malicious activities were detected in the past year, but HR reported two incidents of inappropriate access in previous years with malicious intent. The debt collectors involved were terminated and the staff vetting procedure updated to identify potential fraudsters. The workshop agreed that the most likely probability is that one data incident could occur per year. The maximum frequency is 5 given the updated personnel vetting procedure and peer review procedure. The loss event frequency from this simulation is summarised in Table 3.2:

Table 3.2 – Loss Event Frequency estimation

LEF Minimum	LEF Most likely	LEF Maximum	Confidence
0	1	5	Moderate

3.2.2 Developing Mitigation Options

Analysis of the generic risk factors tabled in Table 3.1 produced several mitigation options in Table 3.3:

Table 3.3 – Mitigation options for identified risk factors

Risk Scenario	Threat Community	Threat	Threat Type	Mitigation option
1	Privileged insiders	Selling data to criminals	Malicious	1. Deploy UEBA 2. Strengthen staff vetting
2	Privileged insiders	Altering records	Malicious	Enforce granular user access control
3	Privileged insiders	Emailing the wrong recipients	Error	Conduct security awareness training
4	Privileged insiders	Accidentally deleting records	Error	Maintain reliable backups
5	Privileged insiders	Entering data incorrectly	Error	Instigate reliable data reconciliation processes

This analysis is driven by the review of the typical workflow for debt collectors and their standard operating environment. The two major threat types are malicious action or human error. Actions covered in risk scenario 1 and 2 (in Table 3.3), reflect the malicious intent of users, which can be difficult to detect using technology and whose actions might not show any warning signs. Contextualised analysis is required to draw insights and conclusions on these behaviours. A threat hunting exercise looking for unusual user activity patterns based on User and Entity Behaviour Analytics (UEBA) is an effective defence against malicious actions. Threat hunting is an active cyber defence approach wherein an analyst sifts through the network and system event logs to look for unusual patterns. Granular access control systems and regular user audits are effective in minimising unauthorised access attempts to alter customer records.

Genuine user errors, covered in risk scenarios 3 to 5 (in Table 3.3), are more readily detectable and preventable by technology and process-based controls. For example, security awareness training is the best approach to minimise the risk of data exposure due to user error in mailing protected information to the wrong recipients (scenario 3). Records deleted accidentally can be recovered from reliable and regular backup systems (scenario 4). Finally, data entry errors can be detected through data reconciliation tools (scenario 5).

3.3.3 Estimating Loss Magnitude

The loss estimation process is covered in step 3 to 5 in the Incentive Model analysis process discussed in section 3.1. The focus of the quantification process is to provide a fair and reasonable estimate on the expected financial loss. The three pillars of the quantification process are liability framework, financial loss and regulatory framework as depicted in Figure 3.5:

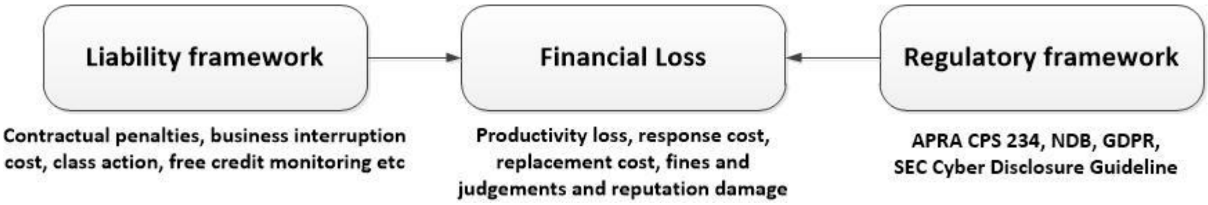

Liability framework
Financial Loss
Regulatory framework
Contractual penalties, business interruption cost, class action, free credit monitoring etc
Productivity loss, response cost, replacement cost, fines and judgements and reputation damage
APRA CPS 234, NDB, GDPR, SEC Cyber Disclosure Guideline

Figure 3.5 – Estimating financial loss under the incentive model

This is an important analytical step to calculate the funding for the incentive model. The total cost of the incentive scheme should not exceed the estimated financial loss. The six forms of loss discussed in section 2.4.2 were used as a guide to estimate the potential financial losses from these five risk scenarios. Under this simulation, one of ABC's lenders conducted an internal workshop with their legal, finance, operations and marketing teams to collect their estimates on the potential financial losses arising from these threat events. The applicable regulatory frameworks for this analysis were the EU GDPR and Australian NDB. Customer class action was the most likely source of liability. The legal and operations teams reviewed settlement records for previous class action cases for PII exposure and also consulted the findings in the IBM Ponemon Institute Cost of Data Breach [81] report to generate some basic estimates. These estimates are shown in Table 3.4:

Table 3.4 – Loss estimates associated with identified risk factors

Risk Scenario	**Threat Community**	**Threat**	**Threat Type**	**Financial loss**
1	Privileged insiders	Selling data to criminals	Malicious	\$250 / record
2	Privileged insiders	Altering records	Malicious	\$100 / record
3	Privileged insiders	Emailing the wrong recipients	Error	\$50 /record
4	Privileged insiders	Accidentally deleting records	Error	\$70 / record
5	Privileged insiders	Entering data incorrectly	Error	\$50 / record

3.3.4 Developing Incentives

An incentive scheme is most effective when it is designed to target a specific risk scenario. Under this simulation, ABC's lender decided to focus on risk scenario 1 after reviewing the loss estimates detailed above (Table 3.4) given the high expected financial losses. The objective was to discourage debt collectors from selling PII records to criminals. More business would be channelled to ABC if the agency agreed to implement an effective risk mitigation program and provided continual reports on the maturity of the program. The incentive scheme is depicted in Figure 3.3 at the beginning of section 3.3.

The incentive program was implemented at two levels. The lender threatened to terminate their contract with ABC if they failed to implement reasonable safeguards against risk. ABC also threatened to terminate the employment of any debt collector found to be selling PII records. Conversely, debt collectors practicing good security hygiene with the PII entrusted to them received an extra annual bonus.

In addition, ABC would be required to implement the UEBA system to monitor unusual user behaviour and access patterns to detect fraudulent activities. They would also be required to strengthen their user vetting process. The lender would subsidise these implementation costs through their promise to channel more business towards the agency.

4. APRA CPS 234 Use Case

This chapter covers a real-world application of this incentive model to build a compliance process for APRA CPS 234 standard by creating financial metrics on acceptable losses calculated based on risk appetite. The Australian Prudential Regulation Authority (APRA) is an independent statutory authority that supervises institutions across the banking, insurance and superannuation sectors and promotes financial system stability in Australia. APRA's information security standard 'Prudential Standard CPS 234 Information Security' [82] came into force on 1st July 2019. The standard demands that the business boards of regulated entities maintain an information security capability commensurate with the size and extent of threats to their information assets, ensuring their continued sound operation. When information assets are managed by a related party or third party, the APRA-regulated entity must assess the information security capabilities of that party. This is to assess if they are commensurate with the potential consequences of an information security incident affecting those assets.

During the public consultation process for the development of the APRA CPS 234, key challenges emerged for businesses to identify significant information security risks and appropriately manage their third-party service providers. The APRA CPS 234 made cyber risk a business problem because the business boards were responsible for maintaining their information security capabilities to facilitate sound operations. Consequently, information security risks had to be managed in the same manner as other enterprise risks such as credit risks, market risks and operational risks, whilst also being subjected to prudent financial investment disciplines such as Return on Investment (ROI) measures.

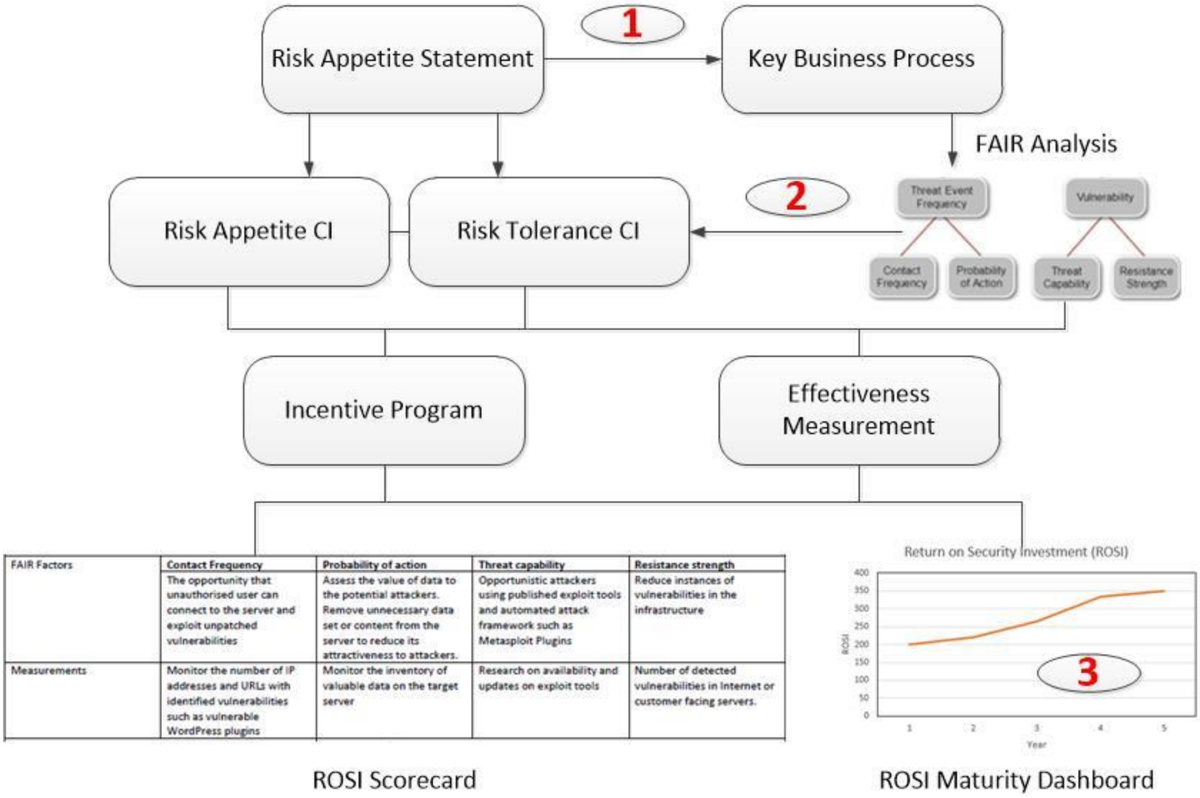
A two-phase approach has been developed to achieve compliance with the APRA CPS 234 standard. The first phase involves integrating information security risk management into the enterprise risk framework by quantifying organisational risk appetite and risk tolerance statements through leveraging risk quantification techniques discussed in chapter 3. The output from this phase is a set of information risk metrics (i.e. the financial losses associated with exposure of the PII records and identity fraud etc.) expressed in financial terms. In the second phase, the incentive model is applied to analyse service delivery from the selected service providers, identifying risk factors and preventable security measures in order to develop appropriate incentive models. Phase One will be explored below, while Phase Two will be expanded upon as part of another research project.

4.1 Research Validation

This chapter discusses a research collaboration project with HESTA [83] to develop a generic APRA CPS 234 Compliance template addressing Phase One requirements. HESTA is Australia's leading Health and Community sector industry superannuation fund with over 840,000 members and AUD$50B funds under management. The quantified risk appetite and risk tolerance levels could then be used to guide the development of the incentive program under Phase Two of the analysis process.

4.2 Building an APRA CPS 234 Compliance Template

This section describes a generic APRA CPS 234 compliance template (Figure 4.1), which ensures that the regulated entity's security capability remains commensurate with its threats.



FAIR Factors	Contact Frequency	Probability of action	Threat capability	Resistance strength
	The opportunity that unauthorised user can connect to the server and exploit unpatched vulnerabilities	Assess the value of data to the potential attackers. Remove unnecessary data set or content from the server to reduce its attractiveness to attackers.	Opportunistic attackers using published exploit tools and automated attack framework such as Metasploit Plugins	Reduce instances of vulnerabilities in the infrastructure
Measurements	Monitor the number of IP addresses and URLs with identified vulnerabilities such as vulnerable WordPress plugins	Monitor the inventory of valuable data on the target server	Research on availability and updates on exploit tools	Number of detected vulnerabilities in Internet or customer facing servers.

Figure 4.1 – A generic APRA CPS 234 compliance template

The application of the template consists of three key steps:

1. The extraction of risk appetite statements applicable to the key business process to be protected

2. The quantification of the risk appetite and risk tolerance using the FAIR framework based on the selected risk appetite statements and the key business process
3. The performance of FAIR analysis on security capabilities. The measurement is compared against the quantified risk appetite and risk tolerance levels in order to assess whether capability is commensurate with the threats

Steps 1 and 2 comprise Phase One, while step 3 is implemented in Phase Two.

HESTA General Manager for Information Security, Michael Collins, stated “this approach to quantify risk appetite and risk tolerance could close the gaps in our current analysis framework”. Specifically, it helps in understanding and applying these high-level business statements for making operational and investment decisions to information security policies and projects. This business benefit represents the output of Phase One.

These steps integrate cyber risk management into enterprise management by using the measurement of reduction in financial loss as a common language. This language bridges the communications gap between the enterprise and cyber risk teams, enabling cyber risks to be managed consistently with other business risks and subjecting them to the same prudent financial management discipline based on ROI. These analyses provide the context to develop the effectiveness measurement metrics discussed in “Targeting cyber security investment – the FAIR approach” [84]. Moreover, incentive schemes represent a cost-effective way to manage a service provider’s security posture besides enforcing compliance. Incentive schemes targeting specific security metrics provide organisations with a meaningful degree of control over their service providers. The whitepaper ”Vendor Risk Management with Real Numbers” [85] explores this approach.

These risk processes are analysed using the Open Group FAIR methodology to extract potential risk factors and estimate their capacity to reduce potential financial losses. The “Know Your Customer” (KYC) [86] business process will be used to illustrate this three-step process. The risk processes include user identity management and authentication processes.

Step 1

The Enterprise Risk Management (ERM) and Information Security (infosec) team review the collection of risk appetite statements to identify statements applicable to the key business processes. For the KYC process, an applicable risk appetite statement might be:

> *Management is willing to accept non-exceptional operational risk event losses to a maximum of x% of revenue due to identity fraud.*

This risk appetite statement could influence the user identity solution for online banking channels. The user identification process is a key assurance process for Anti-Money Laundering (AML) compliance and a potential barrier to scaling these services. A tiered identity solution might be considered where a lower assurance level of the identity capturing process is tolerated for accounts with lower limits on the frequency and amount of transactions. For accounts with higher transaction limits, solutions with higher levels of assurance, such as an in-person verification process, might be mandated.

Step 2

The risk appetite statements selected in step 1 are then applied to the key risk processes to create the scenario for FAIR analysis. At this stage of analysis, security solutions are not considered in the modelling. In other words, this phase of the analysis measures the inherent risks of these processes. As suggested in the Department of Finance guidelines [75], to develop risk appetite, senior management such as the Chief Risk Officer, heads of line-of-business and operations teams are invited to provide expert estimates for the FAIR analysis. The FAIR methodology uses the PERT distribution to model expert opinions. The PERT distribution is well suited for this task because it only requires an estimate on the minimum, maximum and most likely values. It does not require a historical loss value for this phase of the analysis. The output from this analysis phase calculates risk appetite and risk tolerance Confidence Interval (CI) values as inputs for step 3. If risk appetite and risk tolerance levels are currently expressed in heatmap format, they can be converted into a CI format (expressed in the form of LEC) using this analysis step.

Step 3

This stage of analysis estimates the ability of the security controls to reduce potential financial losses from protected information assets in the key business process. The goal of this analysis step is to assess whether the organisation's information security capability is commensurate with their potential threats by comparing the residual risk (after applying the security controls) with the risk appetite CI.

For the KYC process, the information asset is the assurance level of the authenticity of the user identity. Failure in this control can expose the organisation to regulatory actions under their AML compliance obligations. If several security control options are available, the cost effectiveness of these options can be compared by estimating the Return on Security Investment (ROSI) for each option and their corresponding maturity profile.

The FAIR factor analysis and measurement metrics are summarised below.

Risk:				
Threat Analysis:				
Remediation:				
FAIR Factors	**Contact Frequency**	**Probability of action**	**Threat capability**	**Resistance strength**
Measurements				
Investment:		Loss Impact:		
Return on Security Investment: $\text{ROSI}=\frac{\text{Monetary loss reduction-Cost of the solution}}{\text{Cost of the solution}}$				

Figure 4.2 – ROSI Scorecard format

Most security controls require integration with business processes and infrastructure. These integration processes can take some time to mature. The maturity process can be tracked via the ROSI Maturity Dashboard shown in Figure 4.1. Appendix-H in APRA CPG 234 [87] (implementation guide for APRA CPS 234) also includes some suggestions on common information and metrics to be reported to the board. These are useful inputs for the composition of the scorecard and dashboard. Security controls with a lower ROSI but shorter time to mature might be preferred over other controls with higher ROSI but with a longer maturation time. This is because solutions with a shorter maturity cycle help to minimise expected losses.

4.3 The APRA CPS 234 Supply Chain

The APRA CPS 234 demands that regulated entities assess the compliance of their third-party service providers. The supply chain relationship is depicted in Figure 4.3. The regulated entity should identify all information assets being managed by the service provider and quantify their risk appetite and risk tolerance limits for these information assets under the first phase of the compliance template. The quantified limits should be applied to the incentive model analysis process to identify the applicable risk factors and mitigation options under the second phase of the compliance template.

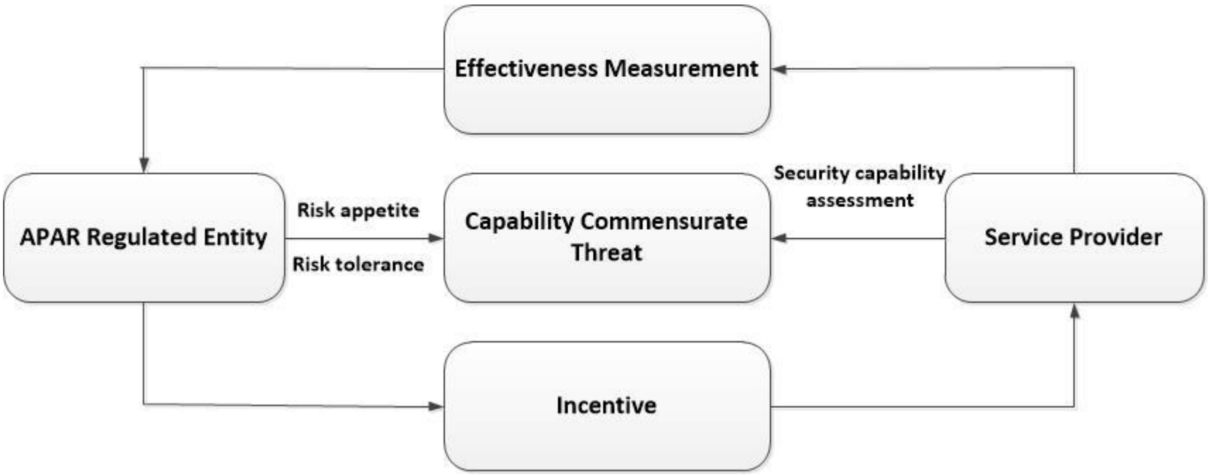

Effectiveness Measurement
Security capability assessment
APAR Regulated Entity
Risk appetite
Risk tolerance
Capability Commensurate Threat
Service Provider
Incentive

Figure 4.3 – The APRA CPS 234 supply chain

The situation is further compounded where nested supply chains involve other downstream suppliers and service providers as shown in Figure 4.4:

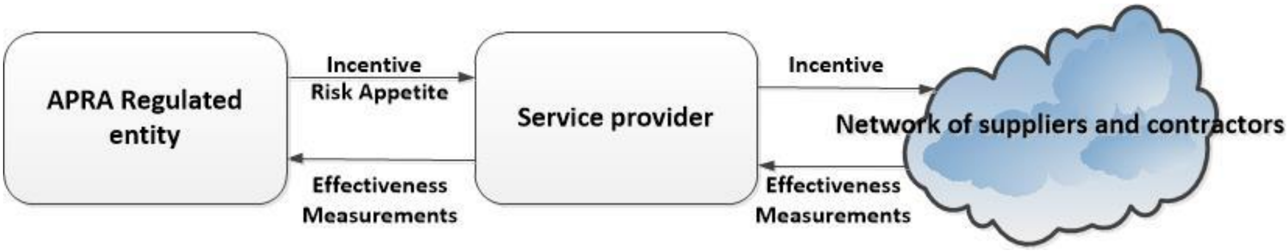

APRA Regulated entity
Incentive
Risk Appetite
Effectiveness Measurements
Service provider
Incentive
Network of suppliers and contractors
Effectiveness Measurements

Figure 4.4 – The arrangement of nested suppliers and service providers in a supply chain

The composition of the nested supply chain is often a guarded commercial secret which might expose the business model of the service provider and its cost structure. An incentive driven security management program creates a common shared interest and risk between the risk owner and nested suppliers. This approach is a more sustainable and scalable collaborative management approach.

5. Cyber Insurance Use Case

To improve the sustainability of the cyber insurance industry, insurers rely on policyholders to maintain basic information security hygiene to minimise avoidable data breach incidents. Insurance policies have the potential downside of encouraging policyholders to reduce their investment in risk controls or to take more risks as the loss from materialisation of insured risk is offset by the insurance payout. This is known as a "moral hazard" [8]. The development of an incident response plan is an effective way to focus policyholder attention on their information security practices. Additionally, an incentive program based on discounts can become expensive, limiting their scalability. This was confirmed in the feedback received from insurance brokers in the cyber insurance use case discussed in this chapter.

5.1 Research Validation

This chapter discusses a research collaboration project between Macquarie University and Agile Underwriting to develop a cost effective and sustainable incentive program to improve policyholder cyber resilience [88]. Agile Underwriting is a Sydney-based underwriting agency specialising in cyber insurance policies. According to their General Manager of Cyber Risk, James Crowther, empowering businesses to improve their cyber readiness is the most effective way to reduce their cyber risk exposure and accelerate their recovery from cyber attacks [88]. This collaborative project developed the 'dynamic excess' policy endorsement initially available under their CyberSelect policy. Policyholders are encouraged to take advantage of the data breach preparation and response guide published by the Office of the Australian Information Commissioner (OAIC) to improve their level of cyber readiness. The focus is on maintaining current documentation and developing co-ordinated cyber response plans within the organisation. Via a "Dynamic Excess Endorsement", Agile offers a financial incentive in the form of up to 50% of the policy excess paid back to the policyholder in the event that a claim is paid and the conditions of the endorsement are met.

The principle of "dynamic excess" is:

> ***The dynamic reduction of the claim excess (deductable) based on the quality of the incident response plan***

The operation of the scheme is as follows:

1. Policyholders are offered the optional “dynamic excess” endorsement under their CyberSelect policy
2. Policyholders who opt-in for this endorsement will submit a copy of their incident response plan and subsequent updates to Agile Underwriting for the record
3. When a cyber insurance claim has been lodged, the incident response team will then review the submitted plan to accelerate the response process. The quality of the plan will determine the claim reduction amount, dynamically.

The business benefits of this scheme are:

1. The incentive does not incur any upfront costs in the form of premium discounts
2. It avoids the upfront cost of engaging a cyber security expert to examine the quality of the incident response plan. The plan is only examined during a claim by experts in the incident response team
3. The net reduction in total insurance claims for business interruption due to an accelerated incident response process will more than outweigh the cost of offering a reduction in the claim excess

Importantly, the insurer is no worse off if the quality of the incident response plan is poor. The elimination of the upfront cost in premium discounts and proactive reviews of the incident response plan enable this approach to be financially sustainable and scalable.

After its first year of operations, Agile Underwriting’s broker community is slowing warming up to this new paradigm. Michael Joseph of Austbrokers Cyber Pro (ACP), a specialist Cyber Insurance Broker, commented “We are pleasantly surprised by the simplicity and effectiveness of this policy endorsement. We have examined several different approaches to help our clients to improve their cyber resilience and we believe this is one of the more effective incentives within the market to date. The common approach of subsidy through premium discounts is not financially attractive to us. It does not offer enough incentive to our client to take concrete steps. Leveraging the free Incident Response Template from OAIC under the NDB scheme makes a lot of sense”.

Jonathan McCoy, Director of Casobe & Co, said “Our team proactively educates our clients on cyber security issues and regularly reviews their cyber insurance cover to reflect their changing business environments…this policy endorsement is a concrete demonstration of our forward thinking and proactive approach in serving our clients. The board of our clients want to understand the value of its cyber insurance cover and our level of cyber resilience. This policy endorsement is an easy way to achieve these goals. It gives confidence to their board that we understand their business environment. It validated that our proactive approach in offering appropriate cyber insurance cover was successful, representing value for money.”

5.2 OAIC Incident Response Template

The OAIC is the Australian regulator for privacy and freedom of information. The Notifiable Data Breaches (NDB) [89] scheme, administered by the OAIC, demands that organisations or agencies subject to the Australian Privacy Act 1988 [90] notify affected individuals and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved. In the OAIC NDB 2019 [80] report for the first year of operation of the NBD scheme, the regulator received a total 964 notifications representing a 712% increase compared to the previous 12 months under the voluntary scheme. 60% of reported breaches were attributed to malicious or criminal attacks while human error accounted for 35%, covering 95% of the breaches as shown in Figure 5.1:

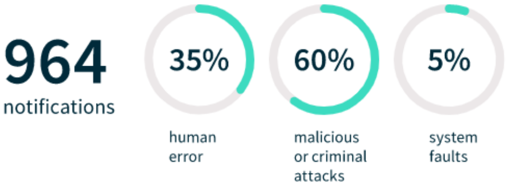


Figure 5.1 - Data breaches notified under the NDB scheme, 2018 to 2019 [80]

To improve incident readiness of these entities, the OAIC provides data breach response plan templates [91] which offer practical guidance on how to reduce the impact of a data breach, meet obligations under the NDB scheme and support individuals to reduce harm. It therefore makes sense for insurers to encourage policyholders to take advantage of these free templates to improve their incident response readiness. Improvements in readiness are expected to reduce the frequency of data breach events and total insurance claim amounts due to rapid containment of the impact from these incidents.

5.3 Design of the Incentive Program

The incentive scheme is designed to encourage policyholders to develop their incident response plan without the offer of subsidies through premium discounts. Through workshopping with the Agile Underwriting team, the “dynamic excess” incentive model can be used to expand upon the Incentive Model Ontology introduced in Figure 3.1. The resultant mapping is displayed below:

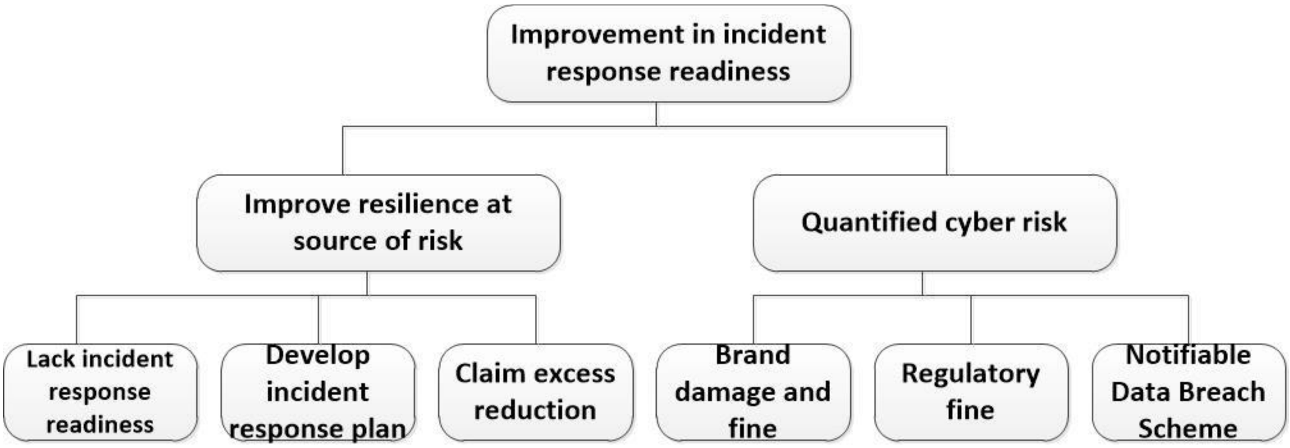

Improvement in incident response readiness
Improve resilience at source of risk
Quantified cyber risk
Lack incident response readiness
Develop incident response plan
Claim excess reduction
Brand damage and fine
Regulatory fine
Notifiable Data Breach Scheme

Figure 5.2 – Incentive model for “dynamic excess”

A lack of management of incident response readiness by policyholders increases the likelihood of a data breach against the policyholder, resulting in higher and more frequent claim payments from the insurer. The primary identified risk factor is the lack of an effective incident response plan. One mitigation strategy is to encourage policyholders to develop and test an effective incident response plan using the free templates from the OAIC. The incentive provided is a reduction in claim excess. The applicable regulatory framework is the Notifiable Data Breach (NDB) scheme. The primary liability arises from regulatory fines, financial impacts and brand damage.

6. CyberMetrics

CyberMetrics in this research report refers to a set of metrics measuring the level of cyber resilience. In this chapter, a simple CyberMetrics design covering two common backup system metrics is presented. These metrics are collected to measure the level of incident response readiness and resilience against cyber attacks. A loss model is presented showing how an insurer can embed these CyberMetrics elements in the claim deduction calculation as an incentive. The incentive program encourages insurance policyholders to invest in maintaining backup systems to meet or exceed these metrics in order to maximise claim payout and minimise expected losses from cyber attacks. In other words, this incentive program creates a collaborative environment between the insurer and policyholder

Section 6.1 describes the development of CyberMetrics in backup systems to protect against ransomware. It tables a mathematical model of the business benefit from the incentive program design. Section 6.2 applies these CyberMetrics values to a proactive cyber insurance scheme. Section 6.3 tables a practical and scalable architecture for the deployment of this strategy. Section 6.4 explains the development process of this CyberMetrics design using the FAIR analysis. Section 6.5 discusses how to apply the Incentive Model analysis method to develop an incentive program.

6.1 Ransomware Protection Incentive Program Design

The most effective protection against ransomware is to have current data backups. Two key metrics for quality of backup are Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO).

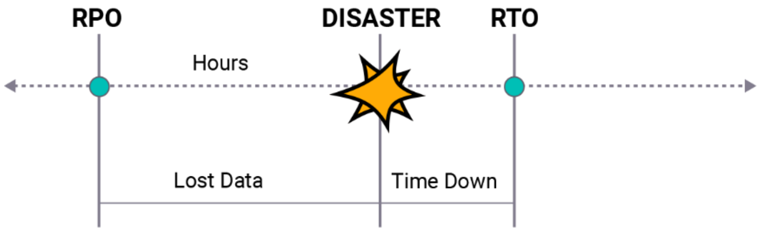


Figure 6.1 – Loss impact from PRO and RTO measured in units of time (i.e. hours)

- RPO measures the amount of data loss after the successful restoration of backup data. RPO is primarily determined by the frequency of backups, such as hourly intervals

- RTO measure the expected amount of time to complete the restoration process. RTO is largely determined by the volume of data to be restored and the capacity of the restoration system

Because data can be stored in different storage systems protected by different backup regimes, the calculation of RPO and RTO requires an accurate inventory of the protected data asset and operational characteristics of the associated backup infrastructure. Assume the protected information asset consists of *M* elements. Asset element *i* is protected by a backup system with backup characteristics of RPO(i) and RTO(i), both of which are measured in units of time. Data losses resulting from RPO(i) can be recovered by re-entering the lost data from transaction journals and offline documents at a cost of $D(i)$, measured at the rate of $/hour. The loss from business interruptions while waiting for data to be restored during the period RTO(i) is L(i), measured at the rate of $/hour. Variable Z is the expected loss from a single ransomware event against the set of protected *M* assets (1,...,M), given by:

$$Z = \sum_{i=1}^{M}\big(RPO(i)D(i) + RTO(i)L(i)\big) \qquad \textbf{(6.1)}$$

Moreover, the value of RPO(i) and RTO(i) might vary over time. These values can be monitored continuously via an Application Programming Interface (API) from the backup infrastructure. The expected loss from a single ransomware event against the set of protected *M* assets (1,...,M) at time *t*, denoted by $Z(t)$, is given by:

$$Z(t) = \sum_{i=1}^{M}(RPO(i,t)D(i,t) + RTO(i,t)L(i,t)) \qquad \textbf{(6.2)}$$

The asset owner can offer incentives to the backup infrastructure operator to adhere to the agreed value of these metrics in order to minimise the probability of loss exceeding the expected value. The expected loss against the set of *M* assets from *N* successful ransomware attacks at times $t_1,\dots,t_N$, during the insured period, denoted by Z_{Tot}, is given by:

$$Z_{Tot} = \sum_{j=1}^{N} Z(t_j) = \sum_{j=1}^{N}\ \sum_{i=1}^{M}(RPO(i,t_j)D(i,t_j) + RTO(i,t_j)L(i,t_j)) \quad \textbf{(6.3)}$$

6.2 A Proactive Cyber Insurance Scheme

Given the loss model Z_{Tot} discussed in equation 6.3, the insurer can include a variable recovery factor for each claim calculated based on a set of agreed CyberMetrics measurements. These measurements will be collected for the period covered by the claim.

The recovery portion of the claim (claim payment from insurer to the policyholder), denoted by $\alpha(t)$, is determined by K agreed CyberMetrics measurements as follows:

$$\alpha(t) = \frac{\sum_{i=1}^{K} CyberMetric_i(t)}{K} \tag{6.4}$$

Where $0 \leq CyberMetric_i(t) \leq 1$. That implies $0 \leq \alpha(t) \leq 1$.

Moreover, CyberMetrics measurements can be assigned with a weighting factor W_i such that $0 \leq W_i \leq 1$ draws attention to these specific controls. The weighted recovery portion, denoted by $\tilde{\alpha}(t)$ is given by:

$$\tilde{\alpha}(t) = \frac{\sum_{i=1}^{K} W_i \, CyberMetric_i(t)}{K} \tag{6.5}$$

For example, the CyberMetrics value for the RPO is given by

$$CyberMetric_1(t) = \frac{1}{M * MPRO(t)} \sum_{i=1}^{M} RPO(i, t) \tag{6.6}$$

where $MPRO(t) = max\big(RPO(1, t), \ldots, RPO(M, t)\big)$

Likewise, the CyberMetrics value for the RTO is given by

$$CyberMetric_2(t) = \frac{1}{M * MPTO(t)} \sum_{i=1}^{M} RTO(i, t) \tag{6.7}$$

where $MPTO(t) = max\big(RTO(1, t), \ldots, RTO(M, t)\big)$.

The expected loss to the asset owner after the claim recovery in the insured period given successful attacks at times, $t_1, \ldots, t_N$, can be found as

$$\acute{Z}_{Tot} = \sum_{j=1}^{N} \left(1 - \alpha(t_j)\right) Z(t_j) \tag{6.8}$$

It is in the interest of asset owners to maintain $\tilde{\alpha}(t)$ close to the target value of “1” to minimise annual expected loss. This is the primary incentive mechanism to encourage proactive management action.

6.3 Creation and Collection of CyberMetrics Measurements

CyberMetrics should be measurable and manageable by asset owners. But this is not always the case in a supply chain as asset owners transfer management control of the risk process through the supply chain arrangement. For example, a cloud-based backup process does not offer asset owners direct control of the RPO/RTP values. Asset owners might not have the necessary skills to design or interpret the CyberMetrics or have the necessary infrastructure to collect the measurements. This service can be offered by a new generation of CyberMetrics Managed Security Service Providers (MSSP) as depicted in Figure 6.2:

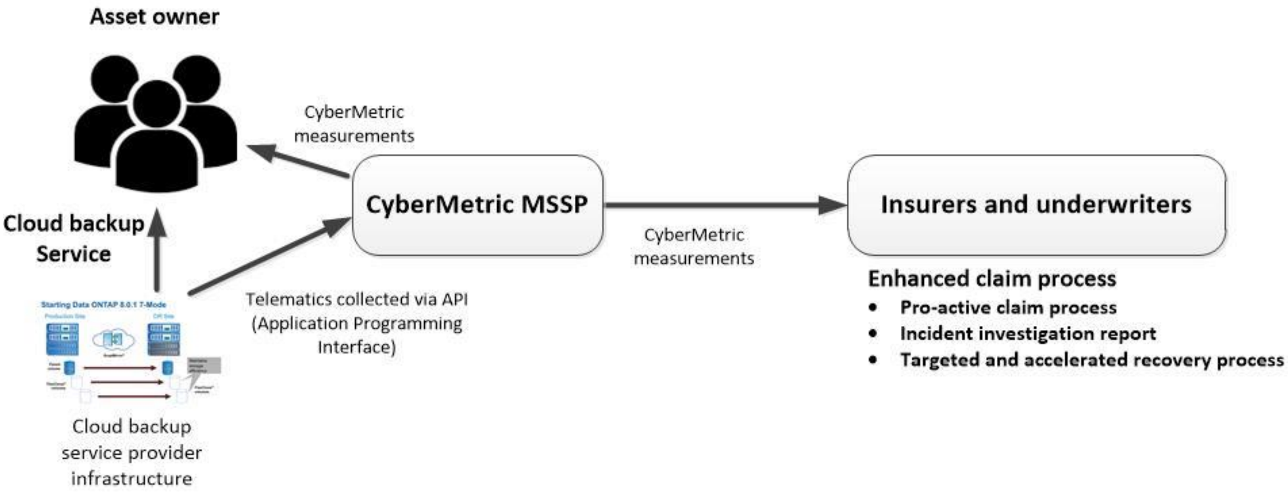

Asset owner
CyberMetric measurements
CyberMetric MSSP
Insurers and underwriters
Cloud backup Service
CyberMetric measurements
Telematics collected via API (Application Programming Interface)
Enhanced claim process
Pro-active claim process
Incident investigation report
Targeted and accelerated recovery process
Cloud backup service provider infrastructure

Figure 6.2 – CyberMetrics architecture

6.4 Developing the Incentive Model

In this section, the identified risk factors are mapped through the Incentive Model Ontology introduced in Figure 3.1. The resultant mapping is displayed below:

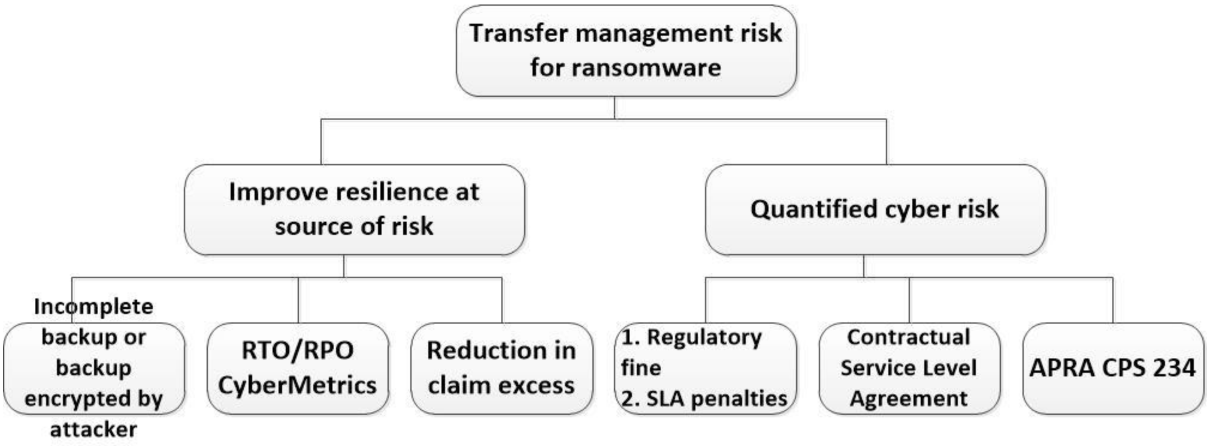

Transfer management risk for ransomware
Improve resilience at source of risk
Quantified cyber risk
Incomplete backup or backup encrypted by attacker
RTO/RPO CyberMetrics
Reduction in claim excess
1. Regulatory fine
2. SLA penalties
Contractual Service Level Agreement
APRA CPS 234

Figure 6.3 – Incentive model for RTO/RPO CyberMetrics

The key risk factors are incomplete backup, or the backup being encrypted by the attacker. The proposed mitigation strategy is to continually monitor key backup quality indicators such as RTO and RPO values. The incentive on offer is a reduction in claim excess. The applicable regulatory framework is APRA CPS 234 where the liability arises from contractual penalties in the Service Level Agreement (SLA) between regulated entities and backup service providers. Financial impact arises from regulatory fines and SLA penalties.

Equation 6.8 (page 47) represents the value of the incentive to the policyholder, reducing their total financial loss from successful ransomware attacks after insurance claims. The design of the recovery portion of the claim (claim payment from insurer to the policyholder), denoted by $\alpha(t)$ in equation 6.3 (page 46) and the weighted variant $\tilde{\alpha}(t)$ in equation 6.4, creates a collaborative environment between the insurer and policyholder in a supply chain relationship. The financial loss estimated through the quantified risk could be covered by the policyholder's insurance policy. The expected loss from the insurer's perspective sets the funding ceiling for the reduction in claim excess they can offer to the policyholder. Claim excess (or deductibles) for cyber insurance covers can be in the order of millions of dollars. From the policyholders' perspective, investment in improving the quality and consistency in their backup infrastructure is driven by the need to protect business processes, in addition to minimising deductions from insurance claim payouts. Policyholders need to model the incremental returns on investment from improving the backup system against the potential savings from a reduction in claim excess.

The research into this optimisation calculation is beyond the scope of the current research but remains a potential candidate for future research. For the purpose of illustration, consider the investment options of x1 … x4 such as

x1 = increase backup system capacity

x2 = increase frequency of incremental backup

x3 = using multiple remote and cloud based storage facilities

x4 = using offline storage such as Amazon Glacier

Investment	RPO	RTO	Analysis
x1	→	↑	Increase in backup capacity minimises the risk of failed backup when the backup media is full. It improves the Recovery Time Objective (RTO) by reducing the backup and restoration time.
x2	↑	→	Increase in backup frequency reduces the amount of data loss and requirement for data re-entry after a successful

			restoration process. It improves the Recovery Point Object (RPO) by reducing the amount of data loss.
x3	↑	↑	Leveraging multiple remote or cloud storage will help to reduce both RPO and RTO objectives by speeding up the restoration process and reducing the amount of effort in data re-entry.
x4	→	↓	Offline backup (such as AWS Glacier provides the highest level of resilience against ransomware which provides search and encrypt online backup channels.

Legend:

↑ - Increase

→ - no change

↓ - Decrease

The impact on increasing backup capacity is illustrated in figure 6.4. When the backup capacity is less than the backup data set size, there is an increase probably of failure in the backup process due to the backup media becoming full. This will result in an increase in RTO. Increasing the backup capacity will help to reduce RTO which underpins the CyberMetric 1 measurement. Similarly, the Return on Investment (ROI) in backup capacity will increase with backup capacity. The return is calculated from the reduction in recovery portion of the claim denoted by $\alpha(t)$ in equation 6.3 (page 46).

However, when the backup capacity exceeds the backup data set size, the additional capacity does not further reduce RTO as the backup and restore processes are no longer resource constrained. Similarly, further investment will lead to a reduction in ROI due to plateauing of the RTO value.

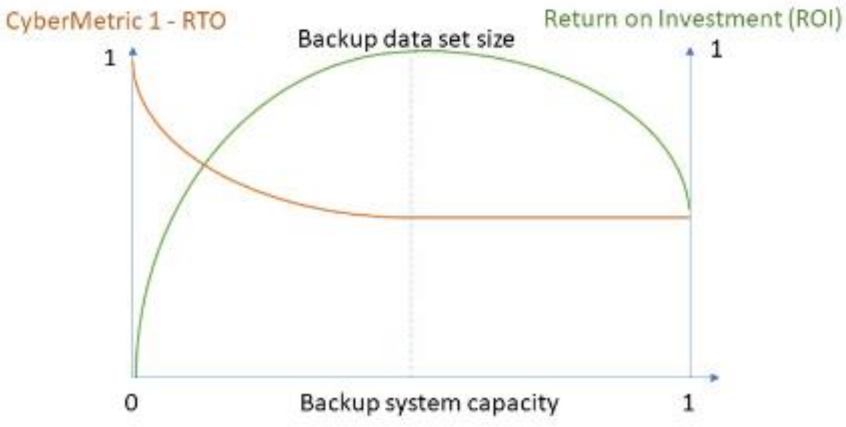


Figure 6.4 – Return of Investment from increasing backup capacity

7. Conclusion

This research explored the approach of using an incentive program to minimise preventable data breach incidents in a supply chain by targeting improvements in resilience at the source of risk. An incentive model ontology and analysis method are presented to guide the development of the incentive program. The incentive model was applied to three different use cases, namely the APRA CPS 234 Compliance Template, CyberSelect Cyber Insurance policy and CyberMetrics for ransomware defence. HESTA expressed the view that the APRA CPS 234 Compliance Template is a powerful way to apply risk appetite statements to guide the prioritisation of their cyber risk management program. Similarly, Agile Underwriting has collected positive feedback from their industry consultants, brokers and policyholders confirming the business value and effectiveness of “dynamic excess”, which has materially changed the security culture of their policyholders in their efforts to improve cyber incident response readiness. Finally, mathematical modelling of the potential benefits of the CyberMetrics use case has been provided, although no commercial pilot of the scheme was attempted.

8. Future Research

Phase Two of the compliance template is to be covered in an extension of the collaboration agreement with HESTA.

The CyberMetrics use case could be validated using a combination of software simulation and application to case studies through research collaborations with the industry. Elements in the CyberMetrics model can be expanded to cover different storage management architecture and cloud backup strategies. Some current research into Accumulation Risk modelling also focuses on large scale outages of cloud service providers. Some of these simulation approaches and analyses will provide a good starting point to extend this research.

Another important research area of CyberMetrics is the strategy for weight allocation to the different CyberMetrics elements exposed in equation 6.5. The CyberMetrics approach is well suited towards the current trend of parametric insurance. The weight allocation strategy is an important consideration for effectiveness and integrity in developing CyberMetrics programs.

Bibliography

Reference List

1. Gartner. *Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019*. 2018; Available from: https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019.
2. Kolkowska, E. and G. Dhillon, *Organizational power and information security rule compliance.* Computers & Security, 2013. **33**: p. 3-11.
3. PCI SSC. *Payment Card Industry Data Security Standard*. 2019; Available from: https://www.pcisecuritystandards.org/pci_security/.
4. NIST CSF. *Cyber Security Framework (NIST CSF)*. 2019; Available from: https://www.nist.gov/cyberframework.
5. Duncan, B. and M. Whittington. *Compliance with standards, assurance and audit: does this equal security?* in *Proceedings of the 7th International Conference on Security of Information and Networks*. 2014. ACM.
6. Mattia, A. and G. Dhillon. *Applying double loop learning to interpret implications for information systems security design*. in *SMC'03 Conference Proceedings. 2003 IEEE International Conference on Systems, Man and Cybernetics. Conference Theme-System Security and Assurance (Cat. No. 03CH37483)*. 2003. IEEE.
7. Pahnila, S., M. Siponen, and A. Mahmood. *Employees' behavior towards IS security policy compliance*. in *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*. 2007. IEEE.
8. Khalili, M.M., P. Naghizadeh, and M. Liu. *Designing cyber insurance policies: Mitigating moral hazard through security pre-screening*. in *International Conference on Game Theory for Networks*. 2017. Springer.
9. Shavell, S., *On moral hazard and insurance*, in *Foundations of Insurance Economics*. 1979, Springer. p. 280-301.
10. Bolot, J. and M. Lelarge, *Cyber insurance as an incentivefor Internet security*, in *Managing information risk and the economics of security*. 2009, Springer. p. 269-290.
11. Chen, P., L. Desmet, and C. Huygens. *A study on advanced persistent threats*. in *IFIP International Conference on Communications and Multimedia Security*. 2014. Springer.
12. Minister for Foreign Affairs. *Attribution of Chinese cyber-enabled commercial intellectual property theft*. 2019; Available from: https://www.foreignminister.gov.au/minister/marise-payne/media-release/attribution-chinese-cyber-enabled-commercial-intellectual-property-theft.
13. Cook County Illinois County Department. *Mondelez vs Zurich court filing*. 2019; Available from: https://assets.documentcloud.org/documents/5759256/397265756-Mondelez-Zurich.pdf.
14. Secure Systems Innovation Corporation, *Silent Cyber Risk is Largest Inhibitor of Cyber Insurance Market Growth: Secure Systems Innovation Corporation.(DATABASE AND NETWORK INTELLIGENCE: SECURITY STUDY).* Database and Network Journal, 2018. **48**(2): p. 15.
15. Reinsurance News. *New Lloyd's mandate to require clarity on silent cyber coverage*. 2019; Available from: https://www.reinsurancene.ws/new-lloyds-mandate-to-require-clarity-on-silent-cyber-coverage/.
16. Schwartz, P.M. and D.J. Solove, *The PII problem: Privacy and a new concept of personally identifiable information.* NYUL rev., 2011. **86**: p. 1814.

17. Chertoff, M. and T. Simon, *The impact of the dark web on internet governance and cyber security.* 2015.
18. Kate Fazzini. *The great Equifax mystery: 17 months later, the stolen data has never been found, and experts are starting to suspect a spy scheme*. 2019; Available from: https://www.cnbc.com/2019/02/13/equifax-mystery-where-is-the-data.html.
19. Marinos, N. and M. Clements, *Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach.* United State Government Accountability Office, Report to Congressional Requestors, 2018.
20. NATIONAL VULNERABILITY DATABASE. *CVE-2017-5638 Detail*. 2018; Available from: https://nvd.nist.gov/vuln/detail/CVE-2017-5638.
21. *17-CV-3463-TWT*. 2019, NORTHERN DISTRICT OF GEORGIA, ATLANTA DIVISION. p. IN RE EQUIFAX INC. SECURITIES LITIGATION.
22. Stacy Cowley. *Equifax to Pay at Least $650 Million in Largest-Ever Data Breach Settlement*. 2019; Available from: https://www.nytimes.com/2019/07/22/business/equifax-settlement.html.
23. Stephen Gandel. *Equifax CEO pushed out after data hack getting nearly $20 million in bonuses*. 2019; Available from: https://www.cbsnews.com/news/equifax-data-breach-settlement-disgraced-former-ceo-getting-nearly-20-million-in-bonuses-after-the-hack/.
24. MARK SULLIVAN. *Why Equifax Still Gets An "A" Rating From The Better Business Bureau*. 2017; Available from: https://www.fastcompany.com/40471670/why-equifax-still-gets-an-a-rating-from-the-better-business-bureau.
25. Press Release. *Warren and Cummings Release New GAO Report on Major Failures by Equifax in Massive Cyber Breach*. 2018; Available from: https://oversight.house.gov/news/press-releases/warren-and-cummings-release-new-gao-report-on-major-failures-by-equifax-in.
26. Mell, P., K. Scarfone, and S. Romanosky, *Common vulnerability scoring system.* IEEE Security & Privacy, 2006. **4**(6): p. 85-89.
27. Fruhwirth, C. and T. Mannisto. *Improving CVSS-based vulnerability prioritization and response with context information*. in *Proceedings of the 2009 3rd international Symposium on Empirical Software Engineering and Measurement*. 2009. IEEE Computer Society.
28. Jacobs, J., et al. *Improving Vulnerability Remediation Through Better Exploit Prediction*. in *2019 Workshop on the Economics of Information Security*. 2019.
29. Rautiainen, R.H., et al., *Effects of premium discount on workers' compensation claims in agriculture in Finland.* American journal of industrial medicine, 2005. **48**(2): p. 100-109.
30. González, M.A., et al. *Challenging anti-fragile blockchain applications*. in *11th EuroSys Doctoral Workshop EuroDW'17*. 2017. Belgrade, Serbia.
31. Reuters. *Target Settles 2013 Hacked Customer Data Breach For $18.5 Million*. 2017; Available from: https://www.nbcnews.com/business/business-news/target-settles-2013-hacked-customer-data-breach-18-5-million-n764031.
32. Arjun Kharpal. *Verizon completes its $4.48 billion acquisition of Yahoo; Marissa Mayer leaves with $23 million*. 2017; Available from: https://www.cnbc.com/2017/06/13/verizon-completes-yahoo-acquisition-marissa-mayer-resigns.html.
33. Eduard Kovacs. *Slack Lists Cybersecurity Risks Ahead of Going Public*. 2019; Available from: https://www.securityweek.com/slack-lists-cybersecurity-risks-ahead-going-public.
34. Shruti Shekar. *Capital One hit with potential $600 million class-action lawsuit following data breach*. 2019; Available from: https://mobilesyrup.com/2019/08/14/capital-one-breach-potential-class-action-law-suit-600-million/.
35. Securities and E. Commission, *Commission Statement and Guidance on Public Company Cybersecurity Disclosures.* February, 2018. **26**: p. 2018.
36. Gordon, L.A., M.P. Loeb, and L. Zhou, *The impact of information security breaches: Has there been a downward shift in costs?* Journal of Computer Security, 2011. **19**(1): p. 33-56.

37. Hilary, G., B. Segal, and M.H. Zhang, *Cyber-Risk Disclosure: Who Cares?* Georgetown McDonough School of Business Research Paper, 2016(2852519).
38. Kelton, A.S. and R.R. Pennington, *Do voluntary disclosures mitigate the cybersecurity breach contagion effect?* Journal of Information Systems, 2019.
39. Press Release. *Moody's and Team8 Launch Joint Venture to Create a Global Cyber Risk Standard*. 2019; Available from: https://ir.moodys.com/news-and-financials/press-releases/press-release-details/2019/Moodys-and-Team8-Launch-Joint-Venture-to-Create-a-Global-Cyber-Risk-Standard/default.aspx.
40. The FAIR Institute. *WHAT IS FAIR? From a Compliance-based to a Risk-based Approach to Information Security and Operational Risk*. 2019; Available from: https://www.fairinstitute.org/what-is-fair.
41. Kenneally, E., L. Randazzese, and D. Balenson. *Cyber Risk Economics Capability Gaps Research Strategy*. in *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*. 2018. IEEE.
42. Internation Standard Organisation (ISO). *ISO/IEC 27102:2019 Information security management — Guidelines for cyber-insurance*. 2019; Available from: https://www.iso.org/standard/72436.html.
43. Ehrlich, I. and G.S. Becker, *Market Insurance, Self-Insurance, and Self-Protection.* Journal of Political Economy, 1972. **80**(4): p. 623-648.
44. Hulthén, R., *Communicating the economic value of security investments: Value at security risk*, in *Managing Information Risk and the Economics of Security*. 2009, Springer. p. 121-140.
45. Gordon, L.A. and M.P. Loeb, *The economics of information security investment.* ACM Transactions on Information and System Security (TISSEC), 2002. **5**(4): p. 438-457.
46. Willemson, J. *On the Gordon & Loeb model for information security investment*. in *The Workshop on the Economics of Information Security*. 2006. Robinson College, University of Cambridge, England.
47. Moore, T., S. Dynes, and F.R. Chang, *Identifying how firms manage cybersecurity investment.* Available: Southern Methodist University. Available at: http://blog. smu. edu/research/files/2015/10/SMU-IBM. pdf (Accessed 2015-12-14), 2015. **32**.
48. Romanosky, S., et al., *Content analysis of cyber insurance policies: How do carriers write policies and price cyber risk?* Available at SSRN 2929137, 2017.
49. Woods, D., et al., *Mapping the coverage of security controls in cyber insurance proposal forms.* Journal of Internet Services and Applications, 2017. **8**(1): p. 8.
50. Talesh, S.A., *Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses.* Law & Social Inquiry, 2018. **43**(2): p. 417-440.
51. Cebula, J.L. and L.R. Young, *A taxonomy of operational cyber security risks*. 2010, CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.
52. NIST, *Security and Privacy Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53 Revision 4)*. 2013, National Institute of Standards and Technology.
53. Alberts, C.J., et al., *Operationally critical threat, asset, and vulnerability evaluation (OCTAVE) framework, Version 1.0.* 1999.
54. Peters, G., P.V. Shevchenko, and R. Cohen, *Understanding cyber-risk and cyber-insurance*, Macquarie University Faculty of Business & Economics, Editor. 2018, Macquarie University: Sydney, Australia.
55. University of Cambridge Judge Business School, *Cyber Exposure Data Schema v1.0*. 2016, Cambridge Centre for Risk Studies.
56. Hofmann, D., S. Wilson, and R. Carter, *Advancing accumulation risk management in cyber insurance.* The Geneva Association, Tech. Rep, 2018.
57. Andy Greenberg. *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. 2018; Available from: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

58. Garg, A., J. Curtis, and H. Halper, *Quantifying the financial impact of IT security breaches.* Information Management & Computer Security, 2003. **11**(2): p. 74-83.
59. Le, A., et al., *Incorporating FAIR into Bayesian Network for Numerical Assessment of Loss Event Frequencies of Smart Grid Cyber Threats.* Mobile Networks and Applications, 2018: p. 1-9.
60. Park, M., et al. *Complex Network of Damage Assessment Using GMM Based FAIR*. in *2018 IEEE International Conference on Big Data and Smart Computing (BigComp)*. 2018. IEEE.
61. Park, M., et al. *FAIR-Based Cyber Influence Damage Assessment for Exploit in Mobile Device*. in *International Symposium on Mobile Internet Security*. 2017. Springer.
62. Hutton, A. and J. Jones. *The Openg Group FAIR Risk Taxonomy (O-RT), Version 2.0*. 2013; Available from: https://www2.opengroup.org/ogsys/catalog/C13K.
63. Australian Cyber Security Centre. *Essential Eight Explained*. Available from: https://www.cyber.gov.au/publications/essential-eight-explained.
64. Jones, J. and J. Freund, *Measuring and Managing Information Risk: A FAIR Approach*. 2014: Butterworth-Heinemann.
65. VOSE Software. *Distributions used in modeling expert opinion*. 2017; Available from: https://www.vosesoftware.com/riskwiki/Distributionsusedinmodelingexpertopinion.php.
66. Aunsmo, A., et al., *Stochastic modelling of direct costs of pancreas disease (PD) in Norwegian farmed Atlantic salmon (Salmo salar L.).* Preventive veterinary medicine, 2010. **93**(2-3): p. 233-241.
67. David Vose. *Modeling expert opinion*. Available from: https://www.vosesoftware.com/riskwiki/Modelingexpertopinionintroduction.php.
68. Hubbard, D. and M. Millar, *Modeling resilience with applied information economics (AIE)*. 2014, Technical Consortium, a project of the CGIAR.
69. Hubbard, D.W. and R. Seiersen, *How to measure anything in cybersecurity risk*. 2016: John Wiley & Sons.
70. Basel Committee on Banking Supervision. *Principles for the Sound Management of Operational Risk*. 2011; Available from: https://www.bis.org/publ/bcbs195.pdf.
71. PwC Financial Services. *Operational risk appetite*. 2014; Available from: https://www.pwc.com/gx/en/banking-capital-markets/events/assets/pwc-operation-risk-appetite.pdf.
72. Larry Rieger. *Risk appetite and tolerance: guidance for practitioners*. 2011; Available from: https://www.theirm.org/media/7239/64355_riskapp_a4_web.pdf.
73. The Institute of Risk Management. *Risk snapshot - Risk Appetite Statements*. 2017; Available from: https://www.theirm.org/media/6878/0926-irm-risk-appetite-12-10-17-v2.pdf.
74. Rachel Slabotsky. *Inherent Risk vs. Residual Risk Explained in 90 Seconds*. 2017; Available from: https://www.fairinstitute.org/blog/inherent-risk-vs.-residual-risk-explained-in-90-seconds.
75. Australian Government Department of Finance. *Case Study: Defining Risk Appetite and Tolerance*. 2016; Available from: https://www.finance.gov.au/sites/default/files/2019-11/case-study-defining-risk-appetite-and-tolerance.pdf.
76. Denny Wan. *A FAIR-Based Cyber Insurance Claim*. 2019; Available from: https://www.fairinstitute.org/blog/a-fair-based-cyber-insurance-claim.
77. European Union. *General Data Protection Regulation (GDPR)*. Available from: https://gdpr-info.eu/.
78. Brian Kreb. *Collections Firm Behind LabCorp, Quest Breaches Files for Bankruptcy*. 2019; Available from: https://krebsonsecurity.com/2019/06/collections-firm-behind-labcorp-quest-breaches-files-for-bankruptcy.
79. Trend Micro. *Trend Micro Discloses Insider Threat Impacting Some of its Consumer Customers*. 2019; Available from: https://blog.trendmicro.com/trend-micro-discloses-insider-threat-impacting-some-of-its-consumer-customers/.

80. Office of the Australian Information Commissioner. *Notifiable data breaches statistics (2019)*. 2019; Available from: https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/?start=0&year=2019.
81. Ponemon Institute. *IBM Ponemon Institute 2019 Cost of a Data Breach Report*. 2019; Available from: https://www.ibm.com/security/data-breach.
82. The Australian Prudential Regulation Authority. *Prudential Standard CPS 234 Information Security*. 2019; Available from: https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf.
83. Optus Macquarie University Cyber Security Hub. *MQ Uni Leading the Development of an APRA CPS 234 Compliance Template*. 2019; Available from: https://www.mq.edu.au/about/about-the-university/offices-and-units/optus-macquarie-university-cyber-security-hub/news-and-events/news2/news/mq-uni-leading-the-development-of-an-apra-cps-234-compliance-template.
84. Denny Wan. *Targeting Cybersecurity Investment - a FAIR Approach*. 2019; Available from: https://www.fairinstitute.org/blog/targeting-cybersecurity-investment-the-fair-approach.
85. Denny Wan. *Vendor Risk Management with Real Numbers'*. 2018; Available from: https://www.linkedin.com/pulse/vendor-risk-management-real-numbers-denny-wan/.
86. AUSTRAC. *Customer identification: Know your customer (KYC)*. Available from: https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/customer-identification-and-verification/customer-identification-know-your-customer-kyc.
87. The Australian Prudential Regulation Authority. *Prudential Practice Guide CPG 234 – Management of Security Risk in Information and Information Technology*. 2019; Available from: https://www.apra.gov.au/sites/default/files/cpg_234_information_security_june_2019.pdf.
88. Optus Macquarie University Cyber Security Hub. *Agile & Optus Macquarie University Cyber Security Hub Collaborate*. 2018; Available from: https://www.mq.edu.au/about/about-the-university/offices-and-units/optus-macquarie-university-cyber-security-hub/news-and-events/news2/news/agile-cyber-and-the-optus-macquarie-university-cyber-security-hub-collaborate/agile-and-optusmqcsh.
89. The Office of the Australian Information Commissioner. *About the Notifiable Data Breaches scheme*. 2019; Available from: https://oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme/.
90. The Office of the Australian Information Commissioner. *https://oaic.gov.au/privacy/the-privacy-act/rights-and-responsibilities/#OrgAndAgencyPrivacyActCovers*. 2019; Available from: https://oaic.gov.au/privacy/the-privacy-act/rights-and-responsibilities/#OrgAndAgencyPrivacyActCovers.
91. The Office of the Australian Information Commissioner. *Data breach preparation and response*. Available from: https://oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/.