MVP

The Importance of Risk Appetite in Risk Assessment

The effects of risk management on small to medium enterprise and attitudes towards risk and risk management in New Zealand.

Katherine McConnell

Minimum Viable Protection Ltd,

Auckland, New Zealand

9 November 2020

Abstract

Through many years of experience in the Information Technology and the Cyber Security space, the team at Unisphere Solutions Ltd have identified cyber risk management and compliance as an area most New Zealand mid-sized businesses struggle to comprehend and manage effectively. With the long-term goal of simplifying such a process and providing a more consumable approach to this targeted audience, Unisphere developed their proprietary Minimum Viable Protection (MVP) methodology. While there are some tools available on the market today, the focus of these appears to be on risk assessment frameworks and management, with a lack of understanding risk appetite as a prerequisite.

Keywords: Cyber Security, Information Security, Risk Appetite, Risk Tolerance, Risk Assessment, Risk Management, Risk Framework, Small to Medium Enterprise (SME), New Zealand

1. Introduction to Digital Technologies and Cyber Security

Digital Transformation has become a buzz word for New Zealand (NZ) businesses as a rapid global shift toward technological change is underway [1]. As digital technology moves from being an assistant to business operations to a critical enabler of the global economy and increasingly popular e-commerce, digital infrastructure complexity increases and with it, the intricacies of cyber and information security [2, 3]. The NZ Government's [4] most recent cyber security strategy update stipulates that while NZ should take full advantage of the opportunities presented by engaging online, there must be a means to protect against cyber threats.

Advances in technology are becoming increasingly accessible and commonplace to average people such as Internet of Things (IoT) or Smart devices in homes and businesses, Artificial Intelligence (AI) and other cognitive technologies embedded in everyday activities, cloud computing, and the arrival of 5G cellular networks [2]. As technology makes such advances and allows for innovation, threats are proliferated in conjunction with those that already exist, increasing the breadth and scope of those associated risks. In the context of such changes, the requirement is passed to businesses to also rapidly adapt, as vulnerabilities tend to materialize abruptly, rather than develop gradually [5].

Cyber security is recognised as one of the top 3 global risks [3] with Small to Medium Enterprises (SMEs) being the object of attackers in approximately 72% of all data breaches [6] and with threat actors able to strike wherever they desire [2], and becoming progressively more brazen, there is the potential for the frequency and scale of attacks to intensify. With such diversity, it is unrealisable to articulate cyber security risk and while the government proactively reinforced the importance of cyber security in 2017, Symantec reported that in 2019 59% of individual New Zealanders had experienced some form of cybercrime costing $1.3million total in financial losses and an average of 4.3 hours dedicated to resolving the incident [7]. The same report formulated from 2017 survey data indicated the average loss for a New Zealand SME was $19,000 as a result of data breach, with 48% of respondents having suffered an attack in the past 12 months. Furthermore, 45% of those affected suffered downtime, 41% incurred expense by inconvenience, 29% suffered the need to repeat work and the associated costs and 12% suffering data loss [8]. Aura [9] saw a 10% increase in the number of businesses subjected to cyber-attacks between 2018 and 2019 with 47% of organisations being targeted comprising of staff levels between 100-199 employees. A quarter of respondents in this category also do not believe that senior management view cyber security as a key concern.

SMEs account for 97% of all businesses in New Zealand and 18% are reported to have no internet security [8]. With numerous emergences of high-profile information security incidents stirring awareness and fears, it is vital to recognise the importance of information security in achieving operational goals as well as the attention this sector is gaining from regulators [10]. Information is no longer being viewed as a tool, but rather a valuable asset for a business producing intrinsic economic value and considered in parallel to an organisation's cyber security rating [3]. In the current world climate in wake of the onset of the global Covid-19 pandemic, a hasty shift to remote working by unprecedented numbers of workers highlights the extension of a company's network far exceeding physical infrastructure. Therefore, challenges relating to cyber security are reaching beyond direct technology risks through continual evolution and adaptation in a cumulative effect, encompassing more than operations, services and data underpinned by digital technology [2].

2. Defining Risk and Risk Assessment

Risk is an ever-present factor to any operation regardless of size and thus the assessment and management of any risks relating to that specific business, organisation, industry, or sector must be undertaken [1]. According to the International Organisation for Standardization (ISO) [11], risk refers to uncertainty of outcomes in relation to objectives and the effect or deviation from the expected, be it positive or negative in consequence. The capricious nature of risk also necessitates the consideration of individual perception which reflects the values, requirements, and beliefs of all stakeholders and their attitude toward risk itself. Risks may focus on

various aspects and be applied at diverse levels in relation to the organisation's objectives and business strategy.

Information Technology (IT) and cyber risk refers to risks associated with the technological assets owned, and digital ventures undertaken by an organisation. Digital assets may include information and communication systems, services, hardware, software, and infrastructure. This type of risk may be seen as an unwanted electronic event that exposes the business to disruption or monetary loss, and the impact such an event has. Similarly, cyber risk may also be viewed as an exploitation of a potential vulnerability from any source of threat, the probability of this occurrence and the resulting adverse consequences. Information security refers to the confidentiality, availability, and integrity of data stored in information systems and the risks associated could include data theft or leak, intentional or unintentional disclosure of sensitive information, restriction of access and destruction or modification of data [12, 13].

In order to qualify risk, assessments must be undertaken in order to appropriately treat and manage risk for a particular organisation. This process offers insight and recognition of key business strategies, goals, processes, assets, and data retention [1] as well as offering the provision of sufficient information to enable effective decision making in the presence of uncertainty [14]. The assessment process is followed by risk treatment through the implementation of controls and appropriate countermeasures, which arguably cannot be performed effectively and economically without understanding of risk in an individualised set of circumstances, such as to a particular business [15]. These controls are intended to modify risk exposure to what is deemed to be an acceptable level or magnitude [5]. There are many risk treatment options and some may include increasing risk capacity, or retaining known, existing risk through informed decision making or adversely, risk avoidance by ceasing or not commencing activities which may increase risk. Further risk treatment options include reduction of risk through the application of controls or risk transferral whereby another party assumes the risk by outsourcing services or purchasing insurance policies. It is important to note that by treating risk, there is the possibility of introducing further risk to the ecosystem and that there is always expected to be some level of residual or unidentified risk, commonly known as retained risk that an organisation must bear [11].

The process of risk assessment begins with the election of an established risk management framework. These frameworks are foundational repositories of components developed by global standards authorities to guide organisations through the risk assessment, management, and monitoring process. Once selected, the chosen framework is then used to develop a risk management plan encompassing the preferred approach, timeframes, and resources to be applied to management, monitoring, and review. Initially, an organisation must establish internal and external parameters that must be considered when managing risk in order to establish a baseline context and provide criteria by which risk must be measured centred around organisational objectives, international standards, governing law, and organisational policies. Risk assessment refers to the recognition and evaluation of the risks applicable to a particular organisation and the nature of those risks by way of further analysis to identify the source and cause of events that may ensue and their potential outcomes [11].

3. Risk Appetite & Risk Appetite Statements

In financial economics, the risk-reward theory dictates that in order for businesses to achieve success, a threshold of calculated risk must be assumed [16]. If risk is to be realistically managed, clear margins must be established as a part of this strategy within the process of risk assessment using the concepts of risk appetite and risk tolerance [15] and was introduced by The Committee of Sponsoring Organisations of the Treadway Commission (COSO) in their Enterprise Risk Management Integrate (ERMI) framework in 2004 [16].

Often incorrectly used interchangeably with risk tolerance, risk appetite refers to the level of risk an organisation considers acceptable and is prepared to engage in or retain, whereas tolerance refers to the spectrum of absolute minimum or maximum risk a company can withstand [17, 16, 18]. Ramamoorti and Stover [16] recommend both

qualitative and quantitative measures be used for greater coverage. These two elements are intrinsically linked and set quantified boundaries for an entity's risk [19, 20].

Risk tolerance develops naturally once risk appetites are established and both should be documented in a risk appetite statement that aligns with company goals and aims to lower residual risk and improve performance objectives in a meaningful and future-focussed manner. Therefore, board members and key managers should assume the responsibility of outlining both risk appetite and risk tolerance [20]. These statements are also used to provide direction toward compliance and may be referenced to assist those making business critical decisions to ensure operation within the set limits [19, 15]. Within the guidelines, a risk appetite trigger may also be incorporated as an escalation point. Activation of this trigger would occur when an organisation's risk profile is perceived to be pushing these thresholds and must be referred to a higher forum such as a risk committee or the board itself. It is also critical to review the thresholds, as they may fluctuate over time and any breach of the parameters should immediately prompt their reassessment [18, 21].

Cyber security and consequently cyber risk management has shifted from being segregated as a technical IT issue into a wider business issue. External stakeholders and regulators hold the expectations that organisations should have formalised risk appetite statements both at a departmental level and companywide [3, 15], therefore the discussion surrounding cyber risk management are moving into the board room and falling on the shoulders of the senior executives. Development of these risk appetite statements will be subjective based on the industry, operating methods, management values, company culture, strategic objectives, and legal or regulatory compliance requirements [3, 21], hence similar risks may be viewed differently across a range of businesses. Boardroom discussion and decision making is recommended by Crowe Harworth [20] rather than a "tick-box activity" to gain greater value from the exercise. During the statement development, a series of questions relating to each sector or type of risk should be considered including the nature of the perceived risk, the level of exposure the business is currently subject to, where limitations should be set and the general attitude toward risk taking. Organisations whose focus is central to regulatory compliance and business stability may have a lower propensity to take risks in contrast to those who are focused on rapid growth and actively seek to engage in riskier actions [21].

Following development by the board, clear communication of the risk appetite statement in common language, specific to the organisation is imperative to ensuring companywide understanding and actions taken according to the standards set by the board [21, 18]. With the cornerstone of the risk appetite framework now in place, managers, key decision makers, and the security team are empowered to make risk intelligent decisions that fall within the scope of the company's risk appetites [20, 22, 21]. Facilitating good risk management culture and communication also allows information to both cascade down through an organisational hierarchy and equally feed "risk messages" back up to the key risk managers and board members [18]. Clear communication eliminates any disparity between the reality of the scale of the risks being taken and any assumptions made by the board and inevitably achieve optimal calibration [22, 18]. Devoid of proper governance through a risk appetite statement and framework, rash decisions and excessive risk-taking may permeate the business, leading to undesirable consequences [18].

4. Attitudes to Risk in New Zealand

Grant Thornton [23] conducted a survey investigating business risk in New Zealand covering 2015-2016 which indicated the focus for senior managers and board members relating to risk. The respondents ranked risk in order of priority and the top three results showed 79% determining reputational risk to be their primary concern, followed closely by 69% for cyber risk and 43% for regulatory risk. Compared to the prior 12-month period, 73% stated that their efforts in relation to cyber security had been amplified, with similar results echoed across multiple sectors and only 1% noting a fall in cyber risk investment. By comparing which tools were used to conduct risk management from 2012 to 2015, as shown in Table 1 below, a notable increase can be seen in the uptake of software use, event analysis,

quantitative analysis, external advisories, and the use of risk appetite statements [23].

	Public sector		Private sector		Not for Profit sector	
	2012	2015	2012	2015	2012	2015
Software	44%	53%	38%	68%	7%	43%
Key risk indicators	58%	55%	65%	73%	61%	71%
Quantitative analysis	27%	58%	37%	61%	14%	43%
Event analysis	84%	91%	87%	96%	79%	100%
External advisers	52%	72%	60%	66%	36%	86%
Organisational risk profile	84%	81%	71%	82%	57%	57%
Risk appetite statement	-	45%	-	57%	-	29%

Table 1 Comparison between 2012 and 2015 of tools used to manage organisational risk.

It was noted across all sectors from the survey results that smaller organisations are less likely to utilise risk management software and that those who use these tools often place a high value on risk management. Twice the number of respondents compared to the previous survey employ quantitative techniques and most often in conjunction with the use of risk management software. Additionally, 68% of companies utilised ongoing external support with 11% stating that they no longer do, and 6% were considering this option. Overall, 49% of these organisations now have a formal risk appetite statement but only 41% use risk reporting against tolerance levels. With the private sector respondents being more likely to hold a risk appetite statement it is interesting to note that the public sector was more likely to use active reporting against risk appetite values [23].

5. Challenges to Implementing Risk Management

5.1 Risk Frameworks

There are an abundance of standards and frameworks, which in itself provides the challenge of deciding which is most relevant to a particular organisation as a starting point. Additionally, these frameworks appear to be more complementary reading to develop an individualised internal framework, rather than an instructional or easily applied practical solution [5]. Developing a holistic internal framework based on one of these established frameworks presents added complexity to the risk assessment process and can seem disconcerting to those lacking in risk management experience [24]. If a suitable internal framework can be discerned, the subsequent challenge lies with implementing the strategy, regardless of how polished it may be. This struggle is encountered by many organisations and is described by Crowe Horwath [20] as "the tactical element of risk appetite: the cusp between strategic vision and implementation," and as such, may require further revisions of processes to enable strategy execution. The lack of directives stems from the unwillingness of regulatory bodies to detail the expectations of a risk appetite framework and there are few explicit examples in existence for companies to follow, which may in turn contribute to the lack of inclination of these associations to provide ordinances on risk appetite [18].

Many organisations treat risk management as merely a tick-in-the-box, rules-based compliance exercise to meet supervisory requirements and fail to recognise the value of embedding risk appetite ideas during strategy development. By taking this minimalist approach, they are unwittingly undermining the potential robust market growth that could be achieved by taking a more comprehensive and risk inclusive approach to business strategy [25]. The pitfall of implementing the controls detailed in these frameworks include a lack of regard for the risks they actually address, and vague or insufficient comprehension may lead to a false sense of security. This approach may also hinder the ability to swiftly identify a new or unexpected threat when it is presented and take the appropriate rapid action. It makes far greater sense to instigate a risk and value based cyber security model [2]. Organisations should work to understand their control frameworks and challenges applicable specifically to them in greater detail to overcome these tribulations. Only then will they be able to decide on the best initiative and controls to invest in and make acceptable choices regarding competing projects. All this must be taken under consideration whilst continuing to evolve rapidly to keep pace with the everchanging threat landscape [26].

5.2 Lack of Knowledge or Expertise in Cyber Risk

It is surmisable to say that knowledge of a risk is necessary to argue its existence and similarly any associated risk with a particular vulnerability. In all cases there, is invariably an inability to identify all possible and potential risks for any given

situation or environment due to possible unknowns, often leaving some aspect overlooked, therefore making absolute identification and analysis impossible [2, 5].

The revisions made by COSO to their ERM framework in 2017 aptly reflected the emerging complexity and pace of risk evolution in the global business environment and the importance of risk consideration in relation to strategy performance and development [16]. The ability to defend against potential cyber-attacks relies on a solid foundational knowledge of information security and familiarity with the range and scope of potential threats and vulnerabilities in relation to an organisation in order to develop a sound cyber security strategy and minimise undesirable effects. This will then enable the prioritisation of the manner in which to defend against such risks with appropriate coverage of as many areas as possible. In many cases, particularly in small to medium enterprises, this skillset is lacking [24] and with such diversity of environments and correlated threats, it is expected that there will be variation in cyber security outcomes across organisations. Oppliger [5] also notes that there is an imbalance between the theory and practice of information security, as suggested by Crowe Howarth [20] in relation to strategic vision and implementation.

Even with in depth research from approved sources, information security and risk management are reliant on the experience and perspective of the individual formulating the plans and conducting the assessments. Dependence on human expertise coupled with the lack of stability in the evolutionary threat landscape and the continual introduction of new assets into an environment can render these activities prone to error or the use of misidentified parameters. Furthermore, operating with incomplete information requires experts to employ a best guess as to the severity of cyber threats at the individual's discretion [24, 27].

Further challenges are faced by organisations in terms of resourcing in the sense that they face a number of limitations. It may be difficult to secure and retain specialised security and risk specific staff members or rather knowledge of these areas may be scattered across the organisation, rather than within a focussed group or individual. Companies are then forced to outsource these requirements and rely heavily on vendors and their management, with no means to monitor or oversee the work or controls put in place by them. Lack of disclosure of operation by these third parties or in-house documentation creates further complications and risks.

In some instances, the focus of a risk framework may focus too heavily on identification and protection rather than detection and response and as impermeability is impossible to achieve, as highlighted by Coden et al, this creates further vulnerabilities. Operations are put under immense pressure with the modern nature of threats and resources are often pushed past their limits, causing process breakdowns resulting in voluminous backlogs. The key causes are the lack of knowledge of assets, limited knowledgeable resources, insufficient tools and technologies for management and monitoring and incompatibilities between humans and the technologies provided. Security culture within an organisation also has a key role to play in reducing operational stress in that if risk and cyber security awareness and their associated responsibilities permeate all levels of the organisation rather than falling on the shoulders of the board, this builds resilience and enhances cyber posture. However, this element is often missing and all risk and cyber responsibility land squarely with the CIO or CISO [27, 26].

5.3 Lack of Standardized Measures

Although there has been a surge in the emphasis of importance of cyber risk, risk is often considered to be intangible as most are drawn from real world observations and individual experiences and do not come with a standardised unit of measure or value. This is due in part to the many considerations that must be taken when assessing them. The constant progression of threats, changing nature of an environment and factors such as human error create difficulty when attempting to determine accurate values [24, 16].

Most institutions will determine their own set of risk metrics in accordance with their chosen base framework to express and utilise the results of risk analysis. The results may then be ranked and prioritised as used as a tool to assist in making risk informed business decisions. Choosing accurate risk metrics is critical to ensuring the results are viewed as valuable [14]. Crowe Howarth

[20], Johansen and Rausand [14], and Ramamoorti and Stover [16] all agree that there is a need to provide standardised risk metrics or measures for cyber security risks but also acknowledge that very little development has been undertaken in this area. Additionally, guidance to aid in the interpretation surrounding the choice of risk metrics is a further recommendation from Johansen and Rausand [14] following on from their work in 2012 [28]. Due to the fact that most risk metrics fail to capture a full spectrum of outcomes, Ramamoorti and Stover [16], Johansen and Rausand [14] and a team at Oliver Wyman [29] suggest choosing a wide-ranging, balanced set of metrics that will better represent all aspects of risk and asset value with graphical representation to accompany the results.

Common practice for defining risk appetites uses a qualitative scale of low, medium, and high and are assigned such values through the intuition and experience of the individual performing the assessment to come to a reasonable judgement [21, 6]. Qualitative assessments methods may be useful for mapping abstract concepts, however it does not allow for risk calculation formulas to be applied, as it does not deal with numerical data, but rather presents the results as a description [14, 30, 21]. The results may then be separated into acceptable and unacceptable categories according to stakeholder vision. A variety of risk management methods for both qualitative and quantitative methods are available through several frameworks and academic proposals as shown in Table 2 below [3].

Qualitative Methods
The IT Infrastructure Library (ITIL)
Control Objectives for Information and Related Technology (COBIT)
ISOC/IEC 27005:2011 and 3100:2009
Information Security Forum (ISF) Simplified Process for Risk Identification (SPRINT) and Simple to Apply Risk Analysis (SARA)
Operational Critical Threat and Vulnerability Evaluation (OCTAVE)
NIST Special Publication 800-53 and 800-37
Consultative, Objective and Bi-functional Risk Analysis (COBRA)
Construct a platform for Risk Analysis of Security Critical Systems (CORAS)
Business Process: Information Risk Management (BPIRM)
Quantitative Methods
Information Security Risk Analysis Method (ISRAM)
Central computer and Telecommunications Agency Risk Analysis and Management Method (CRAMM)
BSI Guide- RuSecure- Based on BS7799 Standard
Cost-of-Risk Analysis (CORA)

Table 2 Qualitative and quantitative risk management methodologies [3]

There are greater benefits to be realised by performing quantitative risk appetite analysis, which connects numerical measurements with monetary value of assets [21]. However, many organisations shy away from this deep dive into their risk exposure and fail to link solid risk evaluation with strategy formulation [30, 29]. This in part is related to the aforementioned challenges, and the difficulties in applying current risk equations under real world conditions rather than in a simulation or lab setting [5].

There is also currently no universally accepted taxonomy for assigning value to digital goods and services relating to market value or costs. Ruan [3] proposes the solution through their work in cybernomics, a play on cyber economics. The standard equation for calculating impact of risk is the likelihood multiplied by the projected consequences, and as a mathematical equation, it requires values to be assigned to each parameter [19, 14]. Probability may be calculated subjectively determined by an analyst's degree of belief which can leave a degree of uncertainty. Consequence relates to harm to any assets, humans, or the environment under scrutiny [14].

A selection of harmful events should be included in the risk analysis based on the threats under consideration and their potential outcomes as well as the type of system or application being assessed. This equation is intended to indicate an estimation and directional views surrounding the level of risk rather than a result or absolute certainty and can be applied to a variety of scenarios to raise awareness in relation to cyber exposure. Once the results can be communicated throughout the organisation, an increase in transparency and discussion may be facilitated to increase cyber resiliency and moves the responsibility of risk from being solely with the IT team [29].

Graphical representation of risk may be utilised to communicate risk more easily across an organisation. COSO's ERM framework leads auditors to favour a risk matrix to display and rank and organisations areas of risk, risk tolerance and risk appetite. This table can be used to identify each risk, define a range for the consequences based on scenarios and indicate the likelihood of their occurrence [11, 16]. To identify a spectrum of threats leading to a hazardous event and the resulting consequences, a bowtie diagram may be employed as show in Figure 1 [14]. Other reporting tools include a risk heatmap which are useful for presenting both qualitative and quantitative measures as demonstrated in Figure 2 below and are commonly used throughout all industries [16]. Once risk appetite and tolerance scores have been established, actual risk impact deduced from the performed analysis may be depicted using a spider graph to show whether the impact will fall within the acceptable limits. The example shown in Figure 3 uses financial, compliance, operational and reputation impacts as their chose parameters.

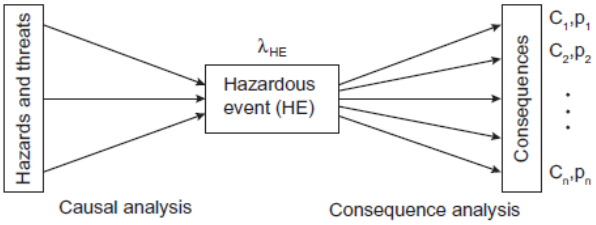

Figure 1 Bowtie diagram used to map scenario and consequences of hazardous events [16]

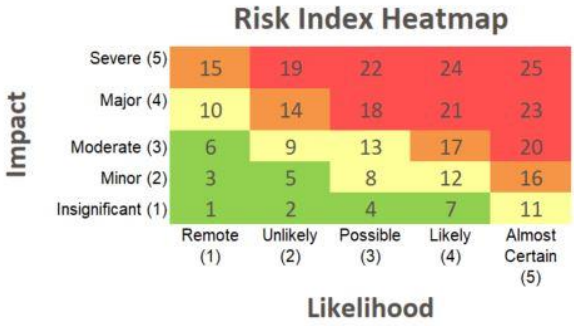

Figure 2 Example of a cyber risk heat map to indicate severity of risk in a graphical manner [31]

Figure 3 Spider graph depicting actual impact in orange and specified tolerance in blue [31]

5.4 Budgetary Restrictions

A hinderance to effective cyber security strategy is a lack of budget to completely cover all possible vulnerabilities in a system or environment. 75.5% of CISO's have disclosed that this is one of the foremost challenges faced by most organisations and it is therefore a requirement that compromises must be made [24].

Due to recent events, shareholders and board members are acutely more aware of and sensitive to any hint of financial mismanagement or lack of corporate governance. Coupled with pressure from regulatory bodies, senior management are being driven toward taking risk management more seriously [25]. Following effective decision-making strategies is crucial to efficient investment in cyber security resources, which is enabled through knowledge of an organisations risk appetite and strategies. Investments may only be made within the means of the organisation and in the case of smaller businesses, these budgetary restrictions may further undermine the ability to conduct proper risk assessment [24, 6]. Deloitte [18] and Sir David Walker as cited in Crowe Horwath [20] suggests that dedicated risk committees be established to tackle the voluminous task of risk management, however this function may only be possible in a large corporation, rather than a small to medium sized enterprise.

Ruan [3] argues that economics is the social science of studying human behaviour in relation to resource scarcity, the allocation of those limited

resources and how a choice in alternatives is determined. Therefore, in any scenario where the budget is fixed, it will become an "economic optimization problem," such as what is being faced by organisations with strained resources.

SMEs are an attractive target to malicious actors as they are often heavily restricted in financial investment in cyber security [24]. Cyber security is not often prioritised until there is a major breach [26] and CEO's who are risk averse may be sceptical about investing in exploration of new capabilities of information security technologies [27]. To achieve optimal information security and economic stability, the cost of the security controls must be considerably lower than the predicted losses due to any breach or disruption at a minimum. It may be less costly to accept some level of risk than apply excessive security controls outside of the minimum requirements and budget for a particular organisation [3]. In order to maximise the benefits to an organisation in relation to a given budget, companies must be able to effectively quantify their risk to determine Return on Investment (ROI) and Net Present Value (NPV) [24, 3, 26]. There is a current lack of consistent measurement methods and there is also no current data set that adequately demonstrates cyber risk in terms of the likelihood of economic loss, by which to base any comparison on for organisations undergoing similar assessments [3].

6. Why a Risk Appetite Assessment Tool is Necessary

The modern business climate is volatile in nature and requires organisations to develop a thorough understanding of their risk profile and their relationship with risk appetite [16]. Cyber security risks should be considered, planned for, and controlled in the same manner that any other business risk [1]. Risk appetite is a valuable element in the risk assessment process as the foundation for effective decision making around the use of technology in an organisation, but its influence is often underappreciated.

The early 2000s have seen significant global financial crises that have highlighted failures in risk management strategies whereby a failed articulation of risk appetite and tolerance has resulted in significant over or under investment in cyber security solutions and subsequent business failure or loss [21, 16]. Small and medium businesses are constantly exposed to a variety of security risks that may result in decreased revenue, increased expenditure, or interruption to normal business operation. In some cases, the severity of the impact experienced by such loss may cause a business to fail altogether. While it may be instinctual to business owners to be aware of these risks, proper risk management may reduce the possibility of an undesirable event occurring, or decrease the impact experienced as a result of the occurrence [32].

Compliance driven risk management may hold benefits in that there may be notable improvements in corporate governance, however this method is more suited to those environments that wish to solely achieve control and stability, rather than supporting profitable and sustainable growth [25]. There are numerous products to assist with risk management against a risk framework however, risk appetite and tolerance do not appear to be a consideration and assessment tools for these parameters seem to be unaccounted for [21, 25].

As an attempt at risk management, companies will often establish standards, policies, processes, procedures, and controls to safeguard valuable assets. The more formal risk management process, at the present time, acknowledges the importance of risk appetite and tolerance on risk treatment but does not include these valuations as a step. There are also no clear guidelines as to how establishing these limits should be carried out and how they should then be used in risk-based decision making. Companies are not often willing to share their methodologies with other parties interested in undertaking such assessments when they inevitably face the need to perform these calculations [21].

This gap in the risk assessment tool set has left an opportunity to develop a cross-industry solution to benefit businesses wishing to pursue in-depth risk assessments for the first time or to utilise and unify existing appraisal and review processes [20, 21]. Although risk appetite may be viewed differently by individuals, a systematic means of calibrating risk limits may be indispensable to those with lesser experience commencing cyber risk assessments to coach them through the initial process [16].

7. Conducting Risk Appetite Assessments

7.1 Steps to Articulating Risk Appetite

Head of Risk at Charterhouse Risk Management Jill Douglas stated that although the risk appetite statement is considered to be the most difficult aspect of any risk management implementations, a set of well-defined and measurable tolerances is fundamental to any risk framework and the cycle as a whole.

Communicating risk appetite allows for swift reaction when faced with both challenges and opportunities [20]. In order to carry out risk appetite assessments, Hakkala and Virtanen [21] affirm that firstly both tangible and intangible assets must first be identified to understand the scope. Following this, regulatory and legal requirements must be considered that may affect a particular asset or the organisation, which will assist with the third step of asset valuation on a three or five step appraisal scale. Lastly, threats and vulnerabilities must be identified in relation to the assets [21].

Deloitte [22] and Oliver Wyman [25], argue that the first step is to formulate a risk appetite scale in accordance with the objectives an organisation wishes to achieve to communicate quantitative parameters taking into consideration requirements and concerns of stakeholders. Oliver Wyman [25] then goes on to insist that embedding the first stage of risk appetite within the culture of an organisation is key to its success and a comparison of actual versus desired risk should be conducted and risk trigger limits should be ascertained to create an escalation tree.

Merrit [17] includes the cornerstones of information security which are confidentiality, integrity, and availability (CIA) in the first stage, which is to isolate relevant loss types. Secondly, a set of measurable thresholds should be determined for each loss type in terms of magnitude and frequency considering tolerance for each over a twelve-month period. The final stage is to look at the actual risk and compare it to the given risk appetite to begin thorough analysis. Both CERT NZ [1] and Groves [15] similarly claim that defining categories of risk should be the first stage. Groves [15] provides the specific examples of key classes for banks which are strategic, reputation, credit, interest rate, liquidity, price, operational and compliance. CERT NZ [1] offers a more general list comprised of operational, reputational, financial, and technical and suggests that considering the impact of these risks, they could then be rated qualitatively into low or minimal impact, medium or recoverable damage and high or lasting damage.

7.2 Risk Appetite Categories

To carry out risk appetite assessment, there are areas of risk which are more applicable to cyber security for businesses. In order to cover a range of business and industry types while providing standardisation, these categories should be taken a high level, such as those outlined by CERT NZ [1] with Merrit [17] emphasising the need to incorporate CIA when evaluating risk appetite. Gillion [13] indicates that the target of malicious actors is often personal and financial information which is categorised as Personally Identifiable Information (PII) and would fall within all three tenets.

Businesses deal with varying classifications of data and different businesses will be using different types across differing levels and this will influence their risk profile and therefore their risk appetite. Confidential data is highly sensitive information that is collected for an explicit purpose. In the event such data was disclosed, tampered with, or lost significant harm to both business operations, regulatory compliance and their reputation may result. Companies that collect and retain significant volumes of PII will likely have a lower risk appetite in the interest of providing the utmost protection and security. Private or internal information should be restricted to need to know access as unauthorised disclosure, modification or loss will also result in detriment to the business and must be guarded in the interest of privacy. Public data is that which can be made available to the public without the risk of loss or disadvantage to the organisation [21].

There may be variations in regulatory risk by geographical location under different governmental laws and regimes. This may also be noticeable at an organisational level depending on the hierarchy system in place [20]. The Privacy Act 1993 has undergone revisions and the new Privacy Act 2020 comes into effect on the 1st of December 2020 in an effort to make privacy

protections more robust. Promoting risk management strategies and encouraging early intervention as well as the addition of further regulatory stipulations surrounding reporting, cross-border protections, access to information and penalties that may be enforced due to non-compliance. The new Act also allows the Privacy Commissioner more control in the ability to issue compliance notices, prompting an organisation to begin or cease certain activities, make judgements on formal requests for access. The Privacy Commissioner also the right to disclose to the public any business that has suffered a data breach under the new reporting scheme where the incident has been deemed to cause or potentially cause serious harm to any individual [33].

It is conceivable that such an action may also cause an impact to a business's reputation. To expand on the cross-border protections mentioned in the Privacy Act 2020, it is essential to comply with the regulations of both the originating country and the destination of any data being transferred across geographical locations. It is important to understand the implications of risks when engaging in partnerships with countries that fall under strict regulations such as the European Union (EU) and the General Data Protection Regulation (GDPR) that is under enforcement with its members. In some cases, sanctions may prevent data moving across borders altogether. Should an organisation be found to be in breach of applicable regulations, they may be subjected to hefty fines which would impose a financial impact on the business [21, 13].

The size of the company must also be considered in terms of revenue, headcount and in the case of cyber security, the number of devices owned by the organisation. Devices could include networking devices, endpoints, servers, IoT devices, printers, and mobile devices. This is necessary to individualise risk decisions and also to build a data set to perform comparative analysis when formulating budgets. As mentioned above, regulations can impose financial risk to an organisation in terms of fines, however there may also be considerable cost involved in bringing a business in line with regulatory standards. Recovery costs and business disruptions should also be considered when determining budget and the actual cost of a particular risk [13, 21].

A business's reputation can often be the difference between sustained success and ultimate failure. In an age of online presence and social media, the public perception of a company can change rapidly and views spread hastily [13]. Customers and shareholders have greater insight and awareness into company operations and if there is a perception that proper governance is not being undertaken to manage risk, it can be damaging to reputation. This pressure from external stakeholders is forcing organisations to develop formalised risk frameworks enabling sound decision making and the ability to justify these decisions [25]. Gillion [13] states that the greatest reputational damage is sustained through events such as data breach or theft and poor handling of an occurrence. Distributed Denial of Services (DDoS) attacks that disrupt customer facing websites and services and business operations may also create unfavourable, lasting judgements from stakeholders. Publicly reported security breaches may also influence a company's position in the stock market, as buyers respond negatively to these types of events based on the perception that security may not have been made enough of a priority [10].

As previously mentioned, it is vital to understand a business's attitude to risk to formulate their risk appetite. This is a key consideration and should not be discounted when dissecting risk categories and their implications. Organisations that require greater stability and control may determine that they are generally risk averse and devise their risk framework in accordance with this sentiment. Others that are focussed on rapid growth and development may be more willing to take greater risk to achieve these goals [26, 25].

8. Conclusion

It can be deduced from these findings that risk is a crucial element to the success or failure of any organisation. Cyber security risk in particular is becoming increasingly valid as the world moves towards a more digitized manner of conducting business, which presents its own unique set of risks to be qualified and quantified. Understanding risk is necessary to assist risk-driven decision making, communicate risk management and embed risk-aware culture throughout an organisation.

This surge in interest regarding formal risk management both at an organisational level and in academia still leaves risk appetite and tolerance establishment as a preliminary stage to risk assessment and management unacknowledged by major industry frameworks and standards. While there are many quick to suggest and call for better strategies for how to conduct risk appetite assessments and establish relevant thresholds, as well as simplifying the process of implementing a risk management framework, there are no established tools at this stage to assist businesses in carrying out risk appetite assessments.

Realistically, the development of an internal cyber risk framework in its entirety and the implementation of tasks outlined within followed by continual monitoring and revision involves in-depth experience in both cyber security and risk management. Many organisations find that they are lacking the relevant resources to carry out this governance and compliance exercise effectively and thus this exercise is avoided altogether. In turn this leaves the company exposed to unacknowledged risks and vulnerabilities that if exploited could have a severely damaging impact, and in the worst case, lead to business failure. If this barrier were removed and an easily consumable process could be established, more businesses would be likely to take up formalised risk appetite and tolerance assessments. This stepping-stone to understanding their risk posture will facilitate the beginnings of securing their organisation against threats to their business success.

References

[1] CERT NZ, "Cyber security risk assessments for business," n.d. [Online]. Available: https://www.cio.com/article/3211428/what-is-digital-transformation-a-necessary-disruption.html. [Accessed 5 August 2020].

[2] M. Coden, A. Holbrook, A. Schneuwley, S. Chan and C. Winters, "How to quantify cyber risks and optimize your cyber investments," 2020. [Online]. Available: https://www.linkedin.com/feed/update/urn:li:activity:6706687479896002560/.

[3] K. Ruan, "Introducing cybernomics: a unifying economic framework for measuring cyber risk," *Computers & Security,* vol. 65, pp. 77-89, 2017.

[4] New Zealand Government, "New Zealand's cyber security strategy 2019: Enabling New Zealand to thrive online," 2019. [Online]. Available: https://dpmc.govt.nz/publications/new-zealands-cyber-security-strategy-2019.

[5] R. Oppliger, "Quantitative risk analysis in information security management: a modern fairy tale," *IEEE Security & Privacy,* vol. 13, no. 6, pp. 18-21, 2015.

[6] A. Fielder, S. Konig, E. Panaousis, S. Schauer and S. Rass, "Uncertainty in Cyber Security Investments," *Computer Science and Game Theory,* pp. 1-17, 2017.

[7] Norton LifeLock, "2019 Cyber safety insights report - global results prepared by the Harris poll," 2019. [Online]. Available: http://now.symassets.com/content/dam/norton/campaign/NortonReport/2020/2019_NortonLifeLock_Cyber_Safety_Insights_Report_Global_results.pdf?promocode=DEFAULTWEB.

[8] S. Barker, "In-depth: Norton by Symantec explains how Kiwi SMBs lose $19,000 from cyber attacks," 2017. [Online]. Available: http://securitybrief.co.nz/story/-depth-norton-symantec-explains-how-kiwi-smbs-lose-19000-cyber-attacks.

[9] Aura, "2019 Cyber security market research report," 2019. [Online]. Available: https://www.kordia.co.nz/aura-cyber-security-market-research-2019.

[10] C. Feng and T. Wang, "Does CIO risk appetite natter? Evidence from information security breach incidents," *International Journal of Accounting Information Systems,* vol. 32, pp. 59-75, 2019.

[11] International Organisation for Standardization, "ISO/Guide 73:2009(en) Risk management - vocabulary," n.d. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en. [Accessed 16 September 2020].

[12] A. Sardi, A. Rizzi, E. Sonaro and A. Guerrieri, "Cyber risk in health facilities: A systematic literature review," *Sustainability,* vol. 17, no. 12, 2020.

[13] K. Gillion, "Technology and business risks," in *The Routledge Companion to Accounting and Risk*, M. Woods and P. Linsley, Eds., Oxon, Routledge Abingdon, 2017.

[14] I. Johansen and M. Rausand, "Foundation and choice of risk metrics," *Safety Science,* no. 62, pp. 386-399, 2014.

[15] B. Groves, "What is your institutions risk appetite? How to identify and measure risk," 2020. [Online]. Available: https://www.whitlockco.com/institutions-risk-appetite-identify-measure-risk/.

[16] S. Ramamorti and R. Stover, "Risk consumption: Understanding the difference between risk appetite and risk tolerance can deter organisations from digesting too much risk," *Internal Auditor,* vol. 75, no. 2, p. 36, 2018.

[17] R. Merrit, "Define your company's appetite for risk with FAIR analysis," 2019. [Online]. Available: https://www.fairinstitute.org/blog/define-your-companys-appetite-for-risk-with-fair-analysis.

[18] Deloitte, "Risk appetite frameworks: how to spot the genuine article," n.d. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-appetite-frameworks-financial-services-0614.pdf. [Accessed 13 September 2020].

[19] LogicManager, "Risk appetite vs risk tolerance and residual risk," n.d. [Online]. Available: https://www.logicmanager.com/erm-software/knowledge-center/best-practice-articles/risk-appetite-risk-tolerance-residual-risk/. [Accessed 23 September 2020].

[20] Crowe Howarth, "Risk appetite and tolerance guidance paper," n.d. [Online]. Available: https://www.theirm.org/media/7239/64355_riskapp_a4_web.pdf. [Accessed 11 September 2020].

[21] A. Hakkala and S. Virtanen, "Risk appetite assessment algorithm - a starting point for small and medium size organisations for understanding information security requirements," Master of Science in Technology Thesis: Security of Networked Systems, 2020.

[22] Deloitte, "Five steps to developing a comprehensive risk framework," *The Wall Street Journal: Risk & Compliance Journal,* 5 Jan 2017.

[23] Grant Thornton, "Risk on the rise: a snapshot of business risk in New Zealand," 2016. [Online]. Available: https://www.grantthornton.co.nz/globalassets/1.-member-firms/new-zealand/pdfs/business-risk-survey-report-15-16.pdf.

[24] A. Fielder, E. Panaousis`, P. Malacaria, C. Hankin and F. Smeraldi, "Decision support approaches for cyber security investment," *Decision Support Systems,* vol. 86, pp. 13-23, 2016.

[25] Oliver Wyman, "What's your risk appetite?" n.d. [Online]. Available: https://www.oliverwyman.com/content/dam/oliver-wyman/global/en/files/archive/2011/Risk_Appetite_CRC_0705.pdf. [Accessed 10 September 2020].

[26] S. Ramachandran, N. Yousif, W. Bohmayr, M. Coden, D. Frankie and O. Klier, "A smarter way to quantify cyber risks," 2019. [Online]. Available: https://www.bcg.com/capabilities/digital-technology-data/smarter-way-to-quantify-cybersecurity-risk.

[27] C. Feng and T. Wang, "Does CIO risk appetite matter? Evidence from security breach incidents," *International Journal of Accounting Information Systems,* no. 32, pp. 59-75, 2019.

[28] I. Johansen and M. Rausand, "Risk metrics: Interpretation and choice," in *IEEE International Conference on Industrial Engineering and Engineering Management*, Hong Kong, 2012.

[29] W. Hedrick, J. Raman, T. Goyal, E. Woon and R. Lam, "Navigating cyber risk quantification," 2019. [Online]. Available: https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2019/aug/navigating-cyber-risk-quantification.pdf.

[30] Oliver Wyman, "What's your risk appetite?" [Online].

[31] A. Jones, "Stop seeing red: How to revamp your risk assessment process to free up more resources," n.d. [Online]. Available: https://www.erminsightsbycarol.com/revamp-risk-assessment/. [Accessed 9 October 2020].

[32] CPA Australia, "Risk management guide for small to medium businesses," 2009. [Online]. Available: https://www.cpaaustralia.com.au/~/media/corporate/allfiles/document/professional-resources/business/risk-management-guide-for-small-to-medium-businesses.pdf?la=en. [Accessed 15 September 2020].

[33] Ministry of Justice, "Key initiatives: privacy," n.d. [Online]. Available: https://www.justice.govt.nz/justice-sector-policy/key-initiatives/privacy/. [Accessed 16 September 2020].

[34] SAM for Compliance, "Experts in Standards Compliance and Cyber Security," n.d. [Online]. Available: https://www.samcompliance.co/. [Accessed 14 October 2020].

Minimum Viable Protection Ltd.

www.minimumviableprotection.com

info@minimumviableprotection.com

(09) 242 1418