Bulletin

Cyber incident cost estimates and the importance of building resilience

Vol. 84, No. 2, February 2020

RESERVE BANK
OF NEW ZEALAND
TE PŪTEA MATUA

Reserve Bank of New Zealand *Bulletin*

Subscribe online: www.rbnz.govt.nz/email-updates

For back issues visit: www.rbnz.govt.nz/research-and-publications/reserve-bank-bulletin

ISSN 1177-8644

Cyber incident cost estimates and the importance of building resilience

Aria Zhang, Rosie Collins, Cavan O'Connor-Close

Non-technical summary

Cyber resilience is the ability to withstand, contain, and rapidly recover from a cyber incident by anticipating and adapting to cyber threats and other relevant changes in the environment.

With the development of digitalisation, the financial sector enjoys more opportunities to improve customer experience and drive efficiency. The flip side is an increasing exposure to cyber risk due to ever-evolving cyber threats, the contagion effects of cyber incidents, a shortage of cybersecurity professionals, and increasing outsourcing to third parties. These developments pose both ongoing and new challenges for firms as they must constantly invest in maintaining their desired level of cyber resilience.

Cyber risk imposes costs upon the financial sector, not only for financial institutions but also for their customers and the financial system as a whole. These costs include both direct costs from financial loss and indirect costs such as reputational damage and the opportunity cost from foregoing more productive investment.

A good understanding of these costs is important in order to raise general awareness and to inform decisions around the management of cyber risk. Estimating these costs, however, is not easy. The fast-evolving nature of cyberattacks, a lack of historical data and the difficulty of quantifying the adverse impact on customer confidence and financial stability all mean that robust and reliable cost estimates are difficult to establish. This article draws on two internationally recognised methods to shed more light on the potential cost that cyber risk poses to the banking and insurance sectors in New Zealand. The first method is a bottom-up approach that uses firm specific data from abroad which is then extrapolated to New Zealand. The second method uses top-down analysis, linking the cost of cyber incidents to GDP. Both methods rely on historical survey information, assumptions and expert judgment, and neither method takes into account extreme events that have a low probability but are still plausible, i.e. black swan events. There are also some definitional discrepancies to contend with.

While it is important to bear those caveats in mind, the two methods produce remarkably similar results for New Zealand. The estimated average cost of cyber incidents is likely to be around NZD 104 million per annum for the banking industry and NZD 38 million for the insurance industry. To put this cost in context, it is the equivalent of 2-3% of annual profits for the banking and insurance industries. While that may sound manageable, these are annual costs and the cumulative impact over a five- or ten-year horizon would be significant. The top-down method uses a slightly different sector categorisation and produces an estimated annual loss for the financial and insurance services sector of between NZD 80-134 million. Moreover, according to the VaR (value-at-risk) method, in any given year there is a five percent chance that the costs could rise beyond NZD 2 billion for the banking industry, and more than NZD 300 million for the insurance industry, equivalent to 34% (25%) of the annual net profits for banks (insurers).

Notwithstanding the need for caution when interpreting these estimates, i.e. they should not be taken as literal point estimates, the analysis presented here shows that the financial cost from cyber incidents is real and has the potential to be significant. Additional costs that have not been captured by the two approaches used in this article include the loss of confidence in the financial system, the resulting impact on innovation and the adoption of new technological developments, and the diversion of resources away from productivity-enhancing investment. Managing cyber risk and building cyber resilience should be of importance to the financial sector as well as its regulators. The Reserve Bank's recent announcement to take a more proactive interest in this area should be read in this context[1].

1 See Financial Stability Report, November 2019 (RBNZ, Nov 2019).

Introduction

Digital technology is evolving at an unprecedented speed. Digitalisation and "everything moving online" bring new opportunities for businesses, but also increase the attack surface for criminals interested in exploiting the system's cyber vulnerabilities. In addition, the likelihood of spontaneous technology failures increases, heightening the risk of partial or full disruptions to the critical systems that underpin the day-to-day workings of the financial system. As a result, the financial sector is facing increasing threats from cyberattacks. The Bank of Bangladesh robbery saw USD 81 million stolen from the central bank in 2016; the infamous WannaCry scam of May 2017 affected over 200,000 users in 150 countries.

Although New Zealand's financial system has been relatively undisturbed by high profile cyberattacks to date, it would be naive to interpret this as a signal that New Zealand's financial system is not a target of cyberattacks. Figure 1 shows an increasing number of cyber incidents reported to the national Computer Emergency Response Team, New Zealand (CERT NZ). The financial sector is at disproportionate risk to systemic attacks relative to other sectors; more cyberattacks target the financial services sector than any other industries internationally (Ponemon Institute, 2018). In 2018, more than 60% of cyberattacks on New Zealand organisations targeted firms in the financial and insurance services sector (CERT NZ, 2019).

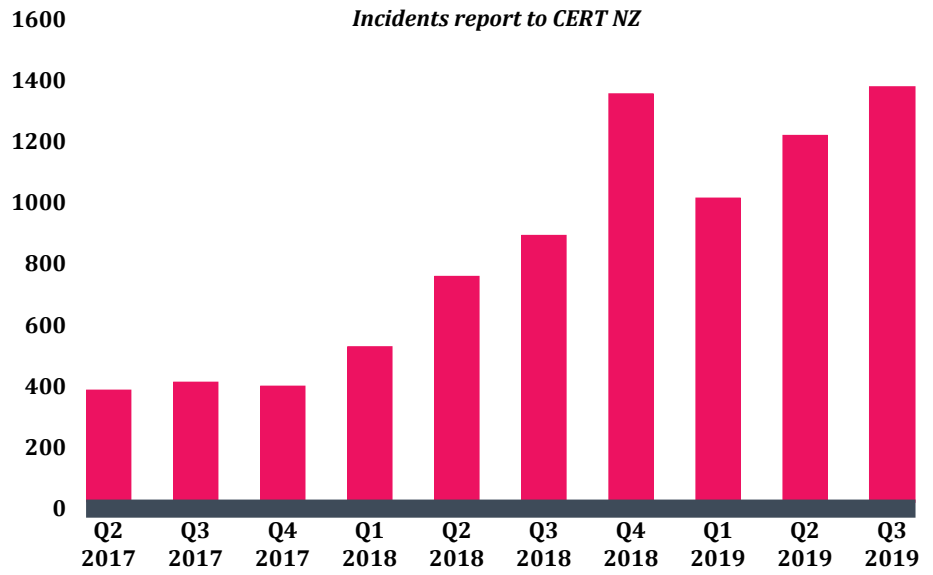


Figure 1 Number of incidents reported to CERT NZ by quarter (Source: CERT NZ, 2019).

Firms, of course, have their own interest in maintaining the smooth operation of their services and they will be alert to any reputational damage that could result from being the public victim of a large-scale cyber incident. It is therefore in their interest to invest in some form of cyber risk preparedness, without the need for regulatory coercion. However, it is not obvious that the decisions firms make in order to protect themselves (private benefits) are necessarily always and fully aligned with what is good for society at large (social benefits). Underinvestment by one firm could have an impact on other players in the system, and firms may lack the trust and confidence to share information with each other in a fully

transparent manner even when doing so would enhance the protection and preparedness of all system participants (coordination problems). Within firms, there could be communication challenges which in turn may be exacerbated by an inadequate understanding of cyber risk among the board members and senior managers. The impact of things going wrong, however, will be felt much more widely than just at the level of the individual firm.

The Reserve Bank has been monitoring cyber risk developments for a number of years[2] and has recently announced[3] an evolution in its policy stance towards taking a more proactive interest in improving the cyber resilience of the financial sector in New Zealand. This paper sheds light on the importance of cyber resilience to financial stability and is structured as follows. Part 1 introduces the concept of cyber resilience, highlights the key risk factors and examines the importance of cyber resilience; Part 2 discusses the challenges involved in estimating the potential costs of cyber risk; Part 3 quantifies the cost of cyber risk for the banking and insurance industries in New Zealand, using two different methods; Part 4 concludes.

1. Definition, challenges and importance of cyber resilience

1.1 What does cyber resilience mean?

Cyber resilience is the ability to withstand, contain, and rapidly recover from a cyber incident by anticipating and adapting to cyber threats and other relevant changes in the environment (Financial Stability Board, 2018). A cyber incident occurs when the cybersecurity of an information system or the information the system processes, stores and transmits is threatened, or when security policies or standards are violated. These include, but are not limited to, attempts to gain unauthorised access to a system or its data; unwanted disruption or denial of services; the unauthorised use of a system for the processing or storage of data; application or database failure, etc. Cyber incidents have proven to have serious implications for both firms and the wider financial system. Data breaches, financial losses, costly recovery processes, unauthorised access to commercially sensitive information, and brand damage are just some of the potential consequences of cyber incidents. These effects can contribute more broadly to the data integrity and confidence losses that can undermine the soundness and efficiency of the financial system.

A cyber resilient firm will develop and test its capacity to prepare for and respond to cyber incidents via investments in their cybersecurity knowledge, detection and response systems, and governance protocols. The recommended approaches to achieve this vary significantly, but typically most experts emphasise a holistic, systems-based view of risks and data assets (Gray & Mee, 2018). There is also a heavy emphasis on developing response and recovery capabilities within a firm, rather than simply a detection and preparation-based focus to build resilience (Gracie, 2014) (BIS, 2018).

1.2 Challenges for achieving cyber resilience

In practice, it can be difficult to achieve cyber resilience for a number of reasons. One is the constantly evolving nature of technology and cyber threats, which has been likened by some experts to dealing with an “entire new category of storm” every few months (Myles, Lee, Thomas, & Meager, 2015). Exponential advances in technology rapidly increase the number of attack surfaces available for an adversary to exploit, leading to the unprecedented growth of new cyber vulnerabilities (McCallam, Frazier, & Savold, 2017).

2 See The Reserve Bank, cyber security and the regulatory framework (Fiennes, 2017)

3 See Financial Stability Report, November 2019 (RBNZ, Nov 2019)

Another issue is the unpredictable nature of contagion effects following a cyber breach. Even a simple attack can have unintended and cascading effects that are difficult to control for and hard to predict (Healey, Mosser, Rosen, & Tache, 2018). Attackers have an advantage in that they only need to be successful once; whereas cyber defenders must constantly maintain vigilance across the entire technology estate. This gives an advantage to the attacker, who can write one attack and then direct it to multiple firms, or spend months intruding the system of one specific firm (Myles, Lee, Thomas, & Meager, 2015).

The ever-evolving and highly contagious nature sets cyber risk apart from other more conventional operational risk. A chronic shortage of cybersecurity professionals worsens the problem when dealing with the challenges of cyber resilience. According to some estimates, there could be 3.5 million job openings worldwide in this field by 2021 (Herjavec, 2019). The shortage amplifies the cost of cyber resilience and knowledge management, increases staff turnover, and bids up the cost of good expertise. Introducing new talent within a limited timeframe to meet rapidly growing demand for expertise may lower the quality of staff entering the field overall (Deloitte, 2019).

An increasing number of firms have been outsourcing their ICT (information and communications technology) operations to dedicated cybersecurity firms or software companies in recent years (Herjavec, 2019). Microsoft (2018) estimates 75% of infrastructure for firms will be under third-party control by 2020. This has the effect of concentrating market power with relatively few cybersecurity firms, as well as concentrating risks within a sector that lies beyond the immediate remit of prudential regulators like the Reserve Bank.

1.3 Cyber resilience is crucial to maintaining financial stability

Financial stability is affected when cyber incidents lead to disruption to system usability, market confidence or data integrity. The 'always on' nature of the financial market puts heavy reliance on the timeliness and quality of financial data to maintain investor confidence (Myles, Lee, Thomas, & Meager, 2015). If a cyber incident compromises the availability, integrity, or confidentiality of this data, then it can lead to panic and flow-on effects that lead to instability in the financial system. Figure 2 depicts this process, showing that the impact of a cyber incident will depend on how substitutable a network is, whether there is a loss of market confidence, and the extent to which data integrity is compromised (Office of Financial Research, 2017).

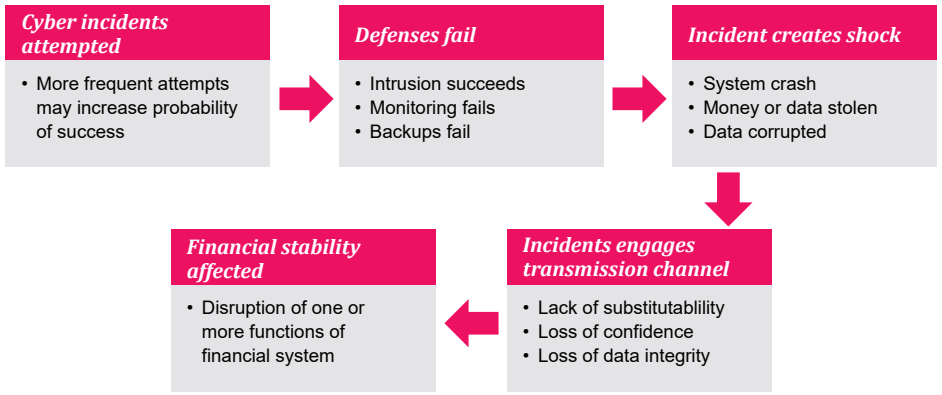


Figure 2 How an Attempted Cyber Incident Could Affect Financial Stability (Source: Office of Financial Research, 2017).

Given the complexities and the breadth of cyber threats, banks, non-bank deposit takers, insurers and financial market infrastructures, who keep money flowing around the economy and hold important financial data for customers, must have an increasing degree of readiness to respond to cyber incidents quickly and cohesively. A high level of cyber resilience is fundamental to the everyday functioning of the financial system in this increasingly digital climate.

2. *Challenges of estimating the cost of cyber risk*

Cyber resilience is important for the financial system in New Zealand, not only because of its disruptive threats to a sound and efficient financial system but also because of the disproportionate vulnerability of the financial sector to cyberattacks. An estimation of the costs these risks carry for financial institutions (FIs), their customers, and the wider financial system is useful in establishing the value of cyber resilience for the financial sector. This section discusses the composition of costs related to cyber incidents and estimates the cost of cyber risk for the financial sector in New Zealand.

2.1 The composition of costs

For FIs, costs incurred in cyber incidents can be direct or indirect. *Direct costs* are relatively easy to identify and include immediate tangibles like investigation fees, costs of legal assistance, the costs of customer notification, and immediate business recovery costs. The indirect costs are less tangible. They could include reputational damage (loss of customers or discounts required for future products or services), future investments in better cybersecurity systems, and any increases to insurance premiums that arise after the incident. Opportunity costs, which encompass what could have been invested somewhere else rather than on cybersecurity, are also counted as indirect costs. Evidence shows around 90% of the total costs of cyber incidents are indirect costs (Deloitte, 2016).

The costs of cyber incidents incurred for an FI can also extend to its customers and the financial system. For customers, cyber incidents can bring about direct costs like the loss of financial or intellectual assets, or indirect costs due to factors like a personal information breach or business disruption. More broadly, the financial system will bear costs when a cyber incident has spillover effects (World Economic Forum, 2016). These costs capture the loss of confidence, system delays, and loss of data integrity that arise from this disruption. Cyberattacks against financial market infrastructures and systemically important banks are more likely to impose costs on the financial system due to their highly interconnected characteristics. These broader effects, though likely significant, are inherently unpredictable and difficult to estimate.

2.2 Difficulties in estimating the cost

Estimating the costs of cyber incidents can be difficult for a number of reasons.

Firstly, costs are likely to be ***underestimated*** due to the unavailability of comprehensive and robust data. Companies affected by cyberattacks may be unwilling to report the attacks, or may report prematurely without fully acknowledging the indirect costs associated with the breach. Indirect costs borne because of a third-party breach are also harder to predict (Ponemon Institute, 2018).

Secondly, some of the costs are ***difficult to quantify***, especially for the larger scale impacts on financial stability and consumer confidence. For example, losses associated with reduced investment or consumption due to heightened uncertainty can be significant, but hard to evaluate. Cyberattacks could also slow the pace of innovation by reducing the expected return to innovators and investors. The opportunity costs arising from a failure to take full advantage of information technology may also have long-term impacts that are difficult to estimate.

Thirdly, costs continue to ***increase*** as more business functions move online, more people connect to the internet globally, and more crucial services are provided by third parties. The unprecedented rate of digitalisation means historical data may not effectively indicate future trends. We do not observe a simple growth pattern in the field of cyber risk.

3. *Estimated costs of cyber risk for banking and insurance industries*

Despite the challenges discussed above, some methods have been developed by international bodies to estimate cyber risk-related costs. We apply two of these approaches to evaluate the cost of cyber risk in the banking and insurance industries in New Zealand. The first is a bottom-up method using the ratio between the cost of cyber risk and total income obtained from empirical data. The second is a top-down method, based on the ratio between the cost of cyber risk and GDP. It is worth noting that these estimation methods are only able to provide a rough idea of the potential cost, considering the highly uncertain nature of cyber incidents, the lack of sufficient historical data in New Zealand, and the limitations of the existing methods for cyber risk cost estimation.

3.1 Estimation using a bottom-up method

An industry-based method, developed by Deloitte and the World Bank Forum, has been used since 2013 to track cyber events in the Netherlands. The method is based on granular data collected from a range of corporations across different industries that track the types, levels and frequencies of cyberattacks, the types of assets attacked and the profiles of the attackers involved. The values derived are also supplemented by judgements made by a range of industry experts. Box A provides a more in-depth description of the method.

The basic process establishes a relationship between costs related to cyber incidents and the total income of an industry. It produces two measures; the ***expected loss value*** for every $1 billion of income in the industry, and a ***Value at Risk*** (VaR) measure which estimates the upper range of losses in a given time frame (in this case, over a year) at the 95% confidence level. This means in some extreme but still plausible scenario of cyber attacks, there is a 5% chance the cost could be higher than the estimated VaR.

Table 1 shows the ratios of cyber risk loss to total income and ratio of the VaR to total income for key industries in the Netherlands.

Table 1 Ratio between the cyber cost and the total income of an industry

Sectors	Expected loss to total income (%)	Cyber VaR to total income (%)
Banking	0.4	7.7
Insurance	0.4	3.3
Asset Management & Pensions	0.2	0.7
Public Sector	0.7	8.5
Utilities	1.1	14.8

Source: Dealing efficiently with cybercrime: Cyber value at risk in the Netherlands (Deloitte, 2017).

These ratios are calculated based on empirical data collected in the Netherlands. Unfortunately, we lack the data to calculate the ratios for New Zealand. However, using the ratios provided above, we can instead derive an estimate for the banking and insurance industries in New Zealand. To verify comparability, we use international metrics to assess the usefulness of the Netherlands in comparison to New Zealand. The Digital Adoption Index (DAI) for New Zealand is 0.71 in 2016, compared to 0.84 for the Netherlands. This reflects that New Zealand is less digitalised compared to the Netherlands. If we make an assumption that digitalisation increases the vulnerability of a system to cyber incidents because of a corresponding increase in attack vectors, then we can also assume that cyber incidents are likely to be positively correlated with a higher DAI score to some extent. In terms of cybersecurity, the Global Cybersecurity Index (GCI) for New Zealand in 2018 was 0.789 whereas it was 0.885 for the Netherlands. A lower score indicates that New Zealand is relatively less prepared for cyber incidents than the Netherlands, and thus more vulnerable to attacks.

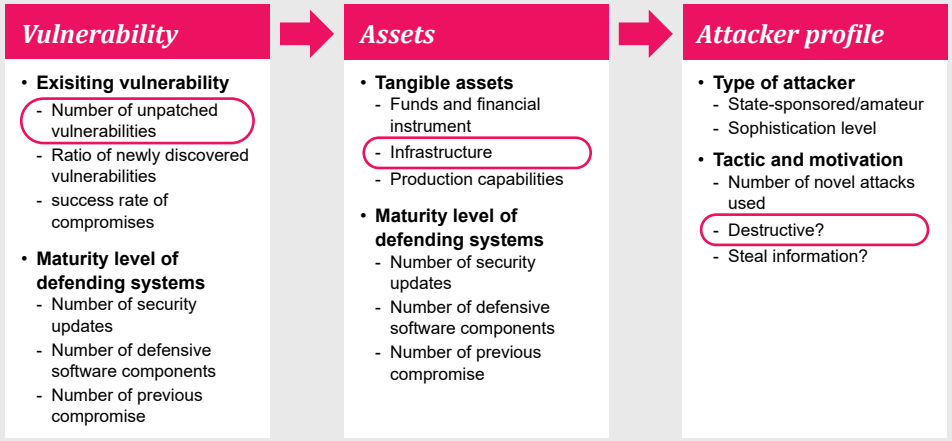
Box A

Estimating cyber value-at-risk (VaR)

Deloitte and the World Economic Forum developed a model for quantifying cyber cost, and introduced the concept of cyber value-at-risk (VaR) (World Economic Forum, 2015). Cyber VaR considers three components of cyber risk for an organisation: its vulnerability, its assets, and the profile of its potential attackers.

1. Vulnerabilities take into consideration the number of unpatched systems inside an organisation; the number of previous compromises it has experienced; the maturity level of its defending systems as defined by the number of security updates applied; the number of defensive software components installed on the network; and the network typology and infrastructure.
2. Assets includes tangible assets and intangible assets. The former typically includes funds and financial instruments; infrastructure; production facilities; and financial losses incurred through temporary business disruption; complete business interruption; and regulatory fines. The latter includes intellectual property; customer or employee data; and a company's reputation.
3. Attacker profiles look at the type of attackers; whether they are amateurs, state-sponsored, or a part of organised crime rings; their motivations; and the sophistication of the attacks.

The three categories of factors set the foundation of the method. The biggest challenge of estimating cyber VaR is that it requires a large set of real-world historical data regarding the frequency and severity of cyber risk events. Deloitte utilised this method using real-world data to estimate the cyber cost for different industries in the Netherlands (Deloitte, 2016).



For example, a bank was attacked by a group of state-sponsored attackers when it had a certain number of unpatched legacy systems, thus causing the disruption of its internet service infrastructure for two hours. The bank should then record the impact (direct and indirect cost associated with the event) and categorise the impact to the certain type of asset from the certain type of attack under the certain level of vulnerability. By collecting the historical data of cyber attacks on certain information assets, the bank can estimate the probability of a certain type of cyber incident and the cost associated with the incidents. The total VaR of the bank can, therefore, be obtained by aggregating all types of cyber incidents. The bank can adjust the estimation when there is a change in its vulnerability or the maturity of its defence system, for example, by decreasing the use of legacy IT systems that are no longer supported by service updates.

The cyber VaR method has limitations due to historical data availability, unidentified software vulnerability, and the limited risk scenarios it supports (Ruith & Spataru, 2016). Despite this, the model is still useful for obtaining insights.

We can combine the effects of susceptibility to cyber incidents with the effects of cyber resilience to compare New Zealand with the Netherlands. Table 2 reflects this, giving an overall effect measure for New Zealand of 0.90 compared with 0.94 for the Netherlands. We interpret this as reasonable evidence for using the ratio obtained from the Dutch datasets to estimate cyber costs for New Zealand's own financial system.

Table 2. DAI and GCI Index of New Zealand and the Netherlands, 2018

Sectors	Likelihood of being attacked (DAI)	Readiness of defending attacks (GCI)	Overall effect (DAI / GCI)
New Zealand	0.71	0.79	0.90
Netherlands	0.84	0.89	0.94

Source: DAI is extracted from www.worldbank.org; GCI is extracted from www.itu.int

Having verified that the financial sectors in New Zealand and the Netherlands are broadly comparable, we then need to make three key assumptions. First, we assume that the banking and insurance industries in New Zealand have tangible and intangible assets similar to their peers in the Netherlands. Second, we assume that the potential direct and indirect costs of each type of cyber incident are similar between the two countries. The third assumption is that the threat environment is also similar in the two countries.

An estimate of the cost of cyber incidents is obtained by applying the ratios shown in Table 1 to the income of the banking and insurance industries in New Zealand. As shown in Table 3, the annual expected loss for cyber incidents in the banking and insurance industries is about NZD **104 million** and NZD **38 million** respectively. This is equivalent to approximately 2 to 3% of net profit for the banking and insurance industries every single year. The cumulative cost impact over, for example, a five- or ten-year horizon is substantial, particularly when considering the opportunity cost from not being able to use this portion of the profits more productively in addition to the direct financial loss.

Moreover, the estimated VaR at the 95% confidence interval exceeds NZD **2 billion**. This means that there is a 5% chance that the cost could be higher than NZD 2 billion for the banking industry, and more than NZD 300 million for insurance industry. These numbers are equivalent to 34% of the net profits for banks and 25% of the net profits for insurers in a given year.

Table 3. Annual expected value loss and Value at Risk of cyberattack

Sectors	Total Income (NZD, m)	Expected Value Loss (NZD, m) [of net profit]	VaR (NZD, m) [of net profit]
Banks & NBDT	26,094	104 [2%]	2,009 [34%]
Insurance	9,394	38 [3%]	310 [25%]
Subtotal		142	2,319

Source: the Reserve Bank Income Statement Survey and New Zealand Insurer Data Collection (RBNZ 2019).

It is worth noting that these figures are based on a set of assumptions which include the assumption that historical data are a guide to the future and losses follow a normal distribution (bell-curve). They do not effectively capture the potential losses from more extreme events. 'Black Swan' or 'Dragon King' events, defined as meaningful outliers of unique origin, refer to unusually extreme events that were unpredictable, even when examining the far right tail of the loss distribution (Sornette, 2009). In such events, the total loss will not be proportional to the cost of any historically observed cyberattacks and is likely to affect financial stability in more unpredictable ways (Eling & Werner, 2016), as shown in Figure 3. As pointed out by Eugene Ludwig (2019), it is important for the whole financial sector to be aware that cyber risk is among the most critical tail risk issues we are facing today, and "these tails risks must be vigorously addressed" (p. 3).

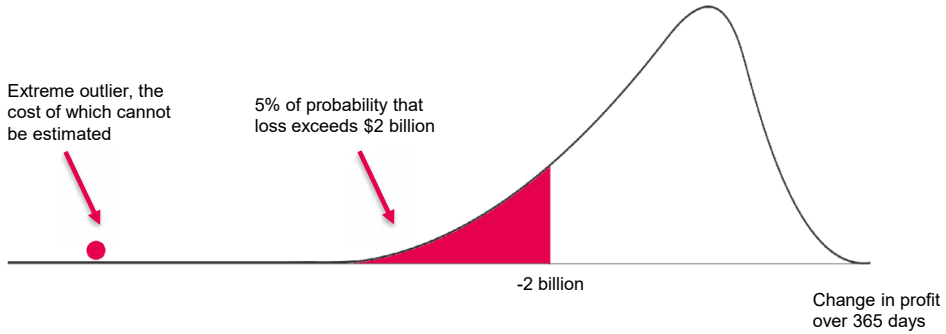


Figure 3 A skewed distribution of Value at Risk from Cyber Incidents, with extreme outlier events

Another limitation of the estimation is that the analysis is for stand-alone organisations. Spillover effects from one FI to another have not been taken into account. Therefore, the estimation may not fully reflect the adverse impact of cyber risk on the financial system as a whole.

3.2 Estimation using a top-down method

A second method helps test the plausibility of the findings obtained with the first method. We adopt a top-down approach developed by McAfee in 2013, using updated estimates of global cyber risk costs from 2018. These costs reflect the survey information from various countries in each major region globally as well as estimates made by cybersecurity officials on losses suffered due to cyber incidents. Expected losses are then estimated as a percentage of GDP in each country. The losses for countries in East Asia and Pacific region were estimated to be between 0.53% and 0.89% of GDP in 2018 (McAfee, 2018). By comparison, European countries that have the highest rates of digital adoption by region have a slightly narrower range, lying between 0.79% and 0.89% of GDP. We use the Asia-Pacific band to estimate a range for New Zealand, based on the financial and insurance services sectors' annual contributions to GDP.

Table 4 shows a similar result to what we get using the bottom-up method. Especially, the upper range of the estimated loss (NZD 134 million) is quite close to what we obtained using the first method (NZD 142 million). Considering the exposure and disproportionate vulnerability of the financial sector to cyber risk, the estimation using the top-down method may also underestimate the cost for the financial sector. Nevertheless, the comparable results obtained from the different two methods support each other and indicate the estimation is reasonable.

Table 4. Estimated loss due to cyber risk for the Financial & Insurance services sector in New Zealand.

Sector	GDP	Ratio of cyber cost (%)	Estimated loss (NZD, m)
Financial & Insurance Services	15,079	0.53-0.89	80~134
All Industry	246,404	0.53-0.89	1,306~2,193

Source: Regional gross domestic product: Year ended March 2017 (Statistics New Zealand, 2018).

4. Conclusion

Cyber resilience is crucial in maintaining financial stability. This paper examines the concept of cyber resilience and estimates the potential costs of cyber risk for New Zealand's financial system. Depending on the method used, the indicative estimates show that the expected cost of cyber incidents for the banking and insurance industry is between NZD 80 and 140 million per year. There is a non-negligible chance that in any given year these losses could exceed NZD 2.3 billion for the banking and insurance sectors combined, or the equivalent of about 34% (25%) of the banking (insurance) sector's annual net profit. More extreme events have a low probability but are still plausible.

These cost estimates illustrate the importance of managing cyber resilience effectively, and support a more proactive interest by the Reserve Bank in this area. The specifics of how the new policy stance will translate into in practice is beyond the scope of this article, but an *a priori* assessment of the incentives acting on industry as well as the Reserve Bank seems to suggest that there is ample scope for collaboration with industry and other public bodies. Addressing cyber risk is a collaborative endeavour. No person is an island.

References

AIG. (2017). *Is cyber-risk systemic?*

Anderson, R., & Tyler, M. (2006). The economics of information security. *Science*, 610-613.

Andreasyan, T. (2018, 10 21). *UK financial sector unites for Financial Sector Cyber Collaboration Centre*. Retrieved from www.bankingtech.com: www.bankingtech.com/2018/10/uk-financial-sector-unites-for-financial-sector-cyber-collaboration-centre

APRA. (2018, November 7). *APRA finalises prudential standard aimed at combating threat of cyber attacks*. Retrieved from APRA.gov.au: www.apra.gov.au/news-and-publications/apra-finalises-prudential-standard-aimed-at-combatting-threat-of-cyber

APRA. (2019). *Prudential Standard CPS 234 Information Security*.

Bauer, J. M., & Eeten, M. J. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, 706-719.

BIS. (2018). *Cyber-resilience: Range of Practices*.

BoE & FCA. (2018, May 9). *Building the UK financial sector's operational resilience*. London. Retrieved from www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf

Central Bank of Ireland. (2016). *Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks*. Retrieved from https://centralbank.ie/docs/default-source/Regulation/how-we-regulate/policy/cross-industry-guidance-information-technology-cybersecurity-risks.pdf?sfvrsn=2

CERT NZ. (2019). *Quarterly Report: Data Landscape Quarter 2*. CERTNZ. Wellington: New Zealand Government. Retrieved from www.cert.govt.nz/about/quarterly-report/quarter-four-report-2018

CERTNZ. (2019, 03 18). *Christchurch tragedy-related scams and attacks*. Retrieved from Cert.govt.nz: www.cert.govt.nz/businesses-and-individuals/recent-threats/christchurch-tragedy-related-scams-and-attacks

CSA. (2019, 4 16). *Cybersecurity Act*. Retrieved from CSA.gov.sg: www.csa.gov.sg/legislation/cybersecurity-act#sthash.RkzG48ni.dpuf

CSA Singapore. (2019, May 9). *Cybersecurity Act*. Retrieved from csa.gov.sg: www.csa.gov.sg/legislation/cybersecurity-act

Deloitte. (2016). *Beneath the Surface of a Cyber Risk*. Retrieved from www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html

Deloitte. (2016). *Cyber value at risk in the Netherlands*. Retrieved from www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-cyber-value-at-risk.pdf

Deloitte. (2019). *The changing faces of cybersecurity*. Deloitte. Retrieved from www2.deloitte.com/ca/en/pages/risk/articles/the-changing-faces-of-cybersecurity.html

Eling, M., & Werner, S. (2016). What do we know about cyber risk and cyber risk insurance? *The journal of Risk Finance,* 474-491.

Federal Reserve Board. (2015). *FFIEC Cybersecurity Assessment Tool for Chief Executive Officers and Boards of Directors*. Retrieved from www.federalreserve.gov/supervisionreg/srletters/sr1509.htm

Federal Reserve Board. (2019, 4 16). *Information Technology Guidance*. Retrieved from Federal Reserve: www.federalreserve.gov/supervisionreg/topics/information-technology-guidance.htm

Fiennes, T. (2017). *The Reserve Bank, cyber security and the regulatory framework*. Wellington: RBNZ.

Fiennes, T. (2017). *The Reserve Bank, cyber security and the regulatory framework*.

Financial Conduct Authority. (2018). *Cyber and Technology resilience: Themes from cross-sector survey 2017/2018*. London: Financial Conduct Authority.

Financial Stability Board. (2018, 11 12). *Cyber Lexicon*. Retrieved from www.fsb.org: www.fsb.org/2018/11/cyber-lexicon

FMA. (2019). *Cyber-resilience in FMA-regulated financial services*.

Friedman, S., & Eckenrode, J. (2018). *The state of cybersecurity at financial institutions*. Deloitte. Retrieved from www2.deloitte.com/insights/us/en/industry/financial-services/state-of-cybersecurity-at-financial-institutions.html

FSB. (2018, 11 12). *Cyber Lexicon*. Retrieved from www.fsb.org: www.fsb.org/2018/11/cyber-lexicon

Government Communications Security Bureau. (2018). *Cyber Threat Report 2017/18*. Wellington: National Cyber Security Centre.

Gracie, A. (2014). Managing cyber risk – the global banking perspective. *British Bankers' Association Cyber Conference*. London.

Gray, A., & Mee, P. (2018). *Large-scale cyber attacks on the Financial System*. Oliver Wyman. Retrieved from www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2018/march/Large-Scale-Cyber-Attacks-DTCC-2018.pdf

Healey, J., Mosser, P., Rosen, K., & Tache, A. (2018). T*he Future of Financial Stability and Cyber Risk*. The Brookings Institution. Washington DC.: THE BROOKINGS INSTITUTION. Retrieved 04 16, 2019, from www.brookings.edu/wp-content/uploads/2018/10/Healey-et-al_Financial-Stability-and-Cyber-Risk.pdf

HKMA. (2019, May 9). *Enhanced Compentency Framework for Banking Practitioners*. Retrieved from www.hkma.gov.hk: www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20190329e1.pdf

International Telecommunication Union. (2019). *Global Cybersecurity Index 2018*. Geneva. Retrieved from www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

International Telecommunications Union. (2018). *Global Cybersecurity Index*. ICT Applications and Cybersecurity Division. Retrieved 4 17, 2019, from www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Ludwig, E. (2019). Keynote address. *19th Annual International Conference on Policy Challenges for the Financial Sector*. Washington D.C.

McAfee. (2018). *Economic Impact of Cybercrime – No Slowing Down*.

McCallam, D. H., Frazier, P. D., & Savold, R. (2017). Ubiquitous Connectivity and Threats: Architecting The Next Generation Cyber Security Operations. *The 7th Annual IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems*. Hawaii, USA.

Moore, T., Dynes, S., & Chang, F. R. (2016). Identifying How Firms Manage Cybersecurity Investment. *Economics of Information Security*. Berkeley.

Myles, D., Lee, A., Thomas, Z., & Meager, L. (2015, 12 10). Cyber-attacks: Financial stability's newest threat. *International Financial Law Review*. doi:02626969

National Cyber Security and Communications Integration Centre. (2019, 4 16). *Related Resources*. Retrieved from www.us-cert.gov/related-resources

National Cyber Security Centre. (2019, May 9). *Working with CERT NZ*. Retrieved from ncsc.govt.nz: www.ncsc.govt.nz/about-us/working-with-cert-nz

Office of Financial Research. (2017). *2017 Financial Stability Report*. Washington: U.S. Department of the Treasury.

Ponemon Institute. (2018). *Cost of a data breach study: Global overview*.

RBNZ. (Nov 2019). *Financial Stability Report*.

Ruith, J., & Spataru, D. (2016). *The benefits and limits of cyber value-at-risk*.

Sornette, D. (2009). Dragon-Kings, Black Swans and the Prediction of Crises. *International Journal of Terraspace Science and Engineering*.

SWIFT. (2019). *Three Years on from Bangladesh: tackling the adversaries*. SWIFT. Retrieved 04 16, 2019, from www.swift.com/news-events/news/swift-report-shares-insights-into-evolving-cyber-threats#REPORT

Unisys Corporation. (2018). *A report on global results of the 2018 Unisys Security Index*. Unisys Corporation.

Warren, P., Kaivanto, K., & Prince, D. (2018, 12 21). Could a cyber attack cause a systemic impact in the financial sector? *Quarterly Bulletin* (2018 Q4). Retrieved from www.bankofengland.co.uk/quarterly-bulletin/2018/2018-q4/could-a-cyber-attack-cause-a-systemic-impact-in-the-financial-sector

World Economic Forum. (2015). P*artnering for cyber resilience: towards the quantification of cyber threats*.

World Economic Forum. (2016). *Understanding Systemic Cyber Risk*.