Monetary Authority of Singapore

Cyber Risk Surveillance: A Case Study of Singapore

MAS Staff Paper No.57

February 2020

Cyber Risk Surveillance: A Case Study of Singapore*

By

Joseph GOH, Heedon KANG, Zhi Xing KOH, Jin Way LIM, Cheng Wei NG, Galen SHER, and Chris YAO[1]

February 2020

*This paper describes research in progress by the author(s) and are published to elicit comments and to encourage debate. The views expressed in this paper are solely those of the authors and do not necessarily represent the view of the MAS, its Board of Directors, or MAS management, and the IMF, its Executive Board, or IMF management. This paper is also published as IMF Working Paper 20/28.

JEL CLASSIFICATION NUMBER: E44, G01, G21, G22, G28.

KEYWORDS: CYBER RISK; FINANCIAL INNOVATION; FINANCIAL INSTITUTIONS; SYSTEMIC RISK; STRESS TEST

[1] The authors gratefully acknowledge comments and suggestions from Antoine Bouveret, Christopher Wilson, Dan Nyberg, Daniel Wang, Edward Robinson, Ibrahim Ergen, Martin Čihák, Rosemary Lim, Tan Yeow Seng, Ulric Eriksson von Allmen and Vincent Loy while retaining responsibility for any errors or omissions. The authors are grateful to Stephanie Ng for excellent research assistance and participants at the MCM Quantm Seminar at the IMF for their useful comments.

ABSTRACT

Cyber risk is an emerging source of systemic risk in the financial sector, and possibly a macro-critical risk too. It is therefore important to integrate it into financial sector surveillance. This paper offers a range of analytical approaches to assess and monitor cyber risk to the financial sector, including various approaches to stress testing. The paper illustrates these techniques by applying them to Singapore. As an advanced economy with a complex financial system and rapid adoption of fintech, Singapore serves as a good case study. We place our results in the context of recent cybersecurity developments in the public and private sectors, which can be a reference for surveillance work.

CONTENT PAGE

Tables

1. MOTIVATION

1.1 Prominent cybersecurity incidents have raised the public profile of cyber risk.[2] The most notorious cyberattacks globally were WannaCry and NotPetya. The WannaCry ransomware attack of May 2017 affected computer systems in more than 150 countries (Reuters, 2017). Possibly the most destructive cyberattack ever, NotPetya cost at least US$10bn (Wired, 2018). Although not aimed at the financial sector, these attacks affected banks, ATM networks and card payment systems. The most well-known cyberattack in Singapore breached the confidential data held by a system of healthcare providers known as SingHealth (Straits Times, 2018).

1.2 Financial services are becoming increasingly digitalised, broadening the attack surface[3] for possible cyber events. Financial institutions are relying more on digital assets, introducing new entry points into their networks and digitising tasks and processes. These strategies require financial institutions to weigh cyber risks against the benefits of efficiency and customer experience. Financial services are the fourth most-digitised sector of the economy (Gandhi and others, 2018), and therefore highly exposed to cyber risk. The financial services sector also owns a lot of sensitive personal information, which explains why it is consistently one of the most highly targeted economic sectors for data breaches (Verizon, 2017-19). At the same time, external threats to financial institutions are rising with the volume of internet traffic, the number of its connected devices and the falling cost of launching large-scale cyberattacks (Cambridge Centre for Risk Studies, 2019).

1.3 Cyber risk can have systemic consequences for financial intermediation. A cyber event could lead to a run[4] on the deposits of a bank or to claims against an insurer. Traditionally, supervisors have treated cyber risk as a type of operational risk subject to microprudential supervision. However, an attack on a systemically important financial institution, a central counterparty,[5] or a major ATM network, the corruption of data of upstream providers on which financial contracts are based, or the disruption of critical third-party providers like global software providers or cloud computing services, could all have systemic implications. Cyberattacks could also target several financial institutions at the same time. Systemic effects can be exacerbated by financial and

[2] The definition of cyber, cyber risk, cyber incident and cybersecurity used here follows the lexicon published in FSB (2018).

[3] The attack surface is the set of characteristics of an information system that permit an adversary to probe, attack, or maintain presence in it. This definition is taken from the glossary of the National Initiative for Cybersecurity Careers and Studies, available at: https://niccs.us-cert.gov/about-niccs/glossary.

[4] Deposit insurance may not prevent a large-scale run of depositors seeking to avoid having their deposits frozen or their account information corrupted.

[5] Including a central bank and financial market infrastructure.

technological links between firms, concentrations, common exposures and second-round confidence effects. The possibility for systemic impacts on financial intermediation creates financial stability risks, which more national authorities are recognising (OFR, 2017; MAS, 2018; Bank of Canada, 2019).

1.4 Cyber risk could even be macro-critical, meaning that it could contribute to macroeconomic fluctuations, without necessarily triggering a financial crisis. The Council of Economic Advisers (2018) estimates that malicious cyber activity costs the U.S. economy between 0.3 and 0.6 percent of GDP in a typical year, but that the costs of a downside scenario could be several multiples greater. Under the downside scenario of a cyberattack on a national power grid, key infrastructure and amenities such as fuel supply, water supply, hospitals, public transportation, ports, railways, airports and communication services could be affected. Lloyds and Cambridge University (2015) estimate that a localised power outage in the U.S. lasting two weeks would cost two percent of GDP and affect various economic aggregates, including public and private consumption, labour productivity, imports and exports. Cybersecurity is becoming seen as a matter of public health and safety and national security (WEF, 2016; New York Times, 2019). While it remains to be seen whether cyberattacks could disrupt the functioning of fiscal or monetary policy, or whether cyber risk could lead to balance of payments stresses in a country, the IMF World Economic Outlook has recently added cyberattacks to its list of the main risks to global growth.[6]

1.5 Public agencies with a mandate for macroeconomic and financial stability have a responsibility to assess cyber risk levels, but policymakers may be daunted by the lack of data and tools. The International Telecommunications Union (ITU) produces a Global Cybersecurity Index, which is useful for cross-country comparisons, tracking progress over time, and identifying areas for improvement.[7] However, it applies to whole economies, leaving open the question of how to assess and monitor cyber risk in financial sectors.

1.6 Several studies have provided a useful assessment of the impact of cyber risk on the financial system. Kamiya and others (2018) examine the drivers of the likelihood and severity of data breaches among financial and non-financial firms using a sample of 188 such incidents between 2005 and 2014. Bouveret (2019) estimates the tail quantiles of the distribution of direct losses (i.e., value-at-risk) from 341 cybersecurity incidents affecting financial institutions between 2009 and 2017. Some work is required to customise and apply these methods to monitor cyber risk to the financial

[6] See, for example, the discussion in IMF (2019d).

[7] In the latest ITU index, Singapore ranks sixth globally and first in the Asia Pacific region.

sector of a given country. Santucci (2018) lists processes and frameworks for cyber risk management,[8] but the only measurement methodology appears to be cyber value-at-risk.[9]

1.7 Limited data availability is a key challenge to assessing and monitoring cyber risk.[10] Few datasets are publicly available, given the confidentiality of cybersecurity incidents. The novelty of cyber risk means that existing datasets provide short time series for analysis. Except where regulations require it, financial institutions are reluctant to disclose cybersecurity incidents, given potential regulatory or legal sanctions. Reporting is not standardised currently, so financial institutions' estimates of direct losses may not be comparable.[11] Indirect losses, including reputational effects, are difficult to quantify and can take time to materialise. Data may also become obsolete quickly, given the rapid pace of change in the information technology (IT) sector.

1.8 This paper offers simple analytical techniques and data sources for policymakers to assess and monitor cyber risk in the financial sector as part of their regular surveillance operations. It draws on the experience of Singapore given its significant commitment to building capabilities in this area.[12] Despite the above challenges, we find that some data and methods are readily available to analyse cyber risk. Key indicators can be collected and tracked, event studies can be conducted, survey estimates can be requested, statistical models estimated in other contexts can be applied in data-poor environments, and quantitative results can be presented in a standardised format. This quantitative work complements more qualitative ongoing work on cyber risk surveillance approaches and policy frameworks for the financial sector (e.g., BCBS, 2018; FSB, 2017-18; IMF, 2019b; Kopp and others, 2017).

1.9 The rest of the paper is structured as follows. Section 2 further motivates surveillance of cyber risk through transmission channels of cyber events to the

[8] The author lists the Information Risk Assessment Methodology (IRAM), Risk IT, Factor Analysis of Information Risk (FAIR), the National Institute of Standards and Technology (NIST) cybersecurity framework and cyber value-at-risk (CyberVaR).

[9] FAIR is also a cyber value-at-risk method. It is a proprietary method developed by the Open Group, a global consortium of organisations (Jones and Tivnan, 2018).

[10] This view appears, for example, in Oliver Wyman (2019) and Santucci (2018). BCBS (2018) notes the lack of established data and the immaturity of resilience metrics. The need to enhance data collection is mentioned in Afonso and others (2019).

[11] Direct losses may include costs of identifying a cyberattack, notifying customers, forensic investigation, data recovery, compensating customers (e.g., with free credit score monitoring), public relations, and legal costs.

[12] Singapore is also a leader in this area based, for example, on the ITU cybersecurity index rankings (see footnote 6).

financial sector. Section 3 describes some analytical approaches, including tools and data, for monitoring and analysing cyber risk in the financial sector. The regulatory approach by the MAS and efforts by financial institutions to deal with the cybersecurity threat in Singapore are introduced in Section 4. These approaches can serve as a checklist for those with responsibility for surveillance of cyber resilience and for other jurisdictions seeking to improve their institutional arrangements. Section 5 concludes and provides directions for future work.

2. FINANCIAL STABILITY IMPLICATIONS OF CYBER RISK[13]

2.1 This section presents the broad framework for considering financial stability risks posed by cyber events. We first provide a brief introduction of the different types of cyber events and their risk transmission channels before discussing a simple approach for determining how systemically impactful different cyber events can be. By focusing on system-wide financial implications of cyber events, this framework can complement existing risk analyses which tend to focus more on operational risks that cyber events pose from an entity-level perspective.

A. Microprudential Risks Posed by Cyber Events

2.2 Cyber events can be broadly categorised into three types, based on the harm that they inflict: theft, disruption, and damage.[14] Theft-related cyberattacks extracts items that are valuable to the perpetrator, such as funds, monies, customer credentials, intellectual property or market-valuable information. Disruption-related cyberattacks can disrupt business functionality or degrade the availability of transactions or communications. Websites or servers, and internet-based businesses are examples of business functionalities that can be disrupted. Finally, a cyberattack can also affect data integrity, or damage system hardware or software or other equipment.[15]

2.3 Successful cyberattacks can cause financial institutions to experience various microprudential risks, namely solvency, liquidity, market, operational, legal, and/or reputational risks (Figure 1). When an individual bank incurs significant monetary

[13] This section is based on Box C in the Financial Stability Review published by the MAS in November 2018.

[14] Cyber events are often related to but can be unrelated to cyberattacks: for example, software updates or natural disasters can lead to the crystallisation of cyber risk through business disruptions without any nefarious intent (Bouveret, 2018). However, they often occur upon a cyberattack that targets financial institutions or the financial system. The section mainly focuses on financial stability implications of cyber events that are associated with cyberattacks.

[15] 'Damage' is used here to mean physical damage (to data integrity, software or hardware) as opposed to pecuniary losses.

losses or loses access to the payments system in which interbank transactions take place due to a cyberattack, its capital buffers can be drawn down and it could face possible technical defaults from inability to receive and make payments. A bank can experience a deposit run and a liquidity shortage if a cyberattack undermines customers' and counterparties' confidence in the institution.[16] A cyberattack on critical financial market infrastructure, or corruption of time-sensitive market data can potentially cause financial institutions to suffer market losses due to adverse market movements or erroneous trading decisions. Lastly, legal and reputational risks associated with successful cyberattacks could also lead to a further erosion of confidence and create knock-on impacts on a financial institution's solvency and liquidity positions. These cyber events could also accentuate the existing vulnerabilities in the banking system.

2.4 The microprudential implications of cyber events for insurers differ slightly from that of banks. Other than risks posed by direct cyberattacks on themselves, insurers are exposed to underwriting losses arising from the provision of affirmative or non-affirmative (silent) cyber insurance coverage for clients. While affirmative cyber insurance explicitly cover losses arising from cyberattack events, non-affirmative (silent) cyber coverage refers to insurance policies that provide implicit, unintended coverage. For example, a cyberattack can cause the malfunction of cooling systems that can result in hardware overheating, thus leading to a fire that can be claimed under a fire insurance policy—these policies provide non-affirmative (silent) cyber insurance coverage. Claims arising from these exposures, if significant, can impair the solvency and liquidity positions of insurance companies.

B. Systemic Risk Transmission Channels of Cyber Events

2.5 Beyond posing microprudential risks for individual entities, cyber events can also propagate these risks through the entire financial system and cause systemic risks[17] through three broad transmission channels, namely risk concentration, risk contagion, and erosion of confidence, as shown in Figure 1.[18]

[16] Duffie and Younger (2019) provide a contrarian view, arguing that cyber incidents are unlikely to lead to deposit runs, given that large U.S. banks' liquid assets are enough to cover their wholesale funding obligations due within one month.

[17] Systemic risk is defined as the risk of disruptions to the provision of financial services, which is caused by an impairment of all or parts of the financial system, with serious negative consequences for the real economy (IMF-FSB-BIS, 2016).

[18] Several studies have noted the possibility of cyber risk having systemic implications. The Institute of International Finance (2017) has investigated possible cyberattack scenarios that could lead to systemic outcomes, and the resulting impact on affected financial institutions and the entire financial system. The World Economic Forum (WEF) (2016) describes the financial risks as well as potential systemic impact associated with a cyber event that disrupts payment, clearing and settlement arrangements. The Office of Financial Research (2017) suggests three channels through which cyber

- Risk concentration: a cyberattack on a key financial market infrastructure, third-party service provider, or a systemically important financial institution could mean a loss of services that cannot be easily and promptly substituted.

- Risk contagion: a cyberattack on a financial institution could lead to difficulties that spill over to other financial institutions, given the highly interconnected nature of the financial system.

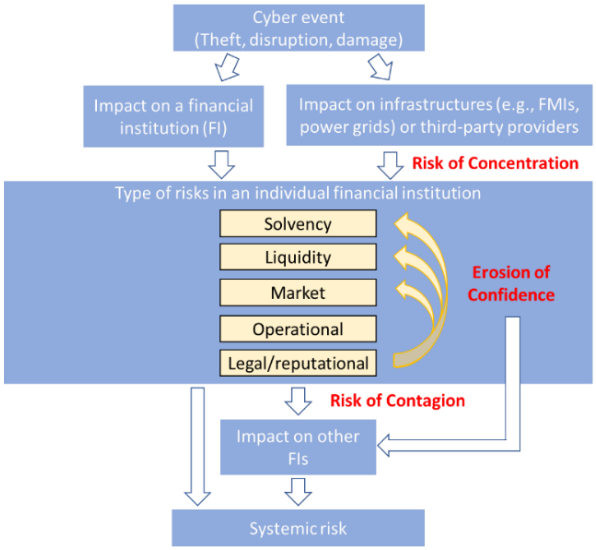
- Erosion of confidence: a widespread attack could trigger an erosion of confidence across several financial institutions or the financial system.

2.6 Risk concentration arises when cyberattacks are launched on financial market infrastructures or entities that the financial system is heavily reliant on for its daily functioning and operations. Examples of such critical financial market infrastructures include payment and settlement systems, trading platforms, central securities depositories, and central counterparties. The disruption of critical financial market infrastructure would hamper market transactions and expose market participants to liquidity and solvency risk.[19] Similarly, the disruption of material infrastructures such as power grids, telecommunications networks and IT infrastructures (e.g., cloud providers or internet service providers) could cause a large disruption to the provision of financial services and negative consequences for the real economy. The shift in recent years to greater adoption of technology in the provision of financial services could also result in increased reliance on a few common key third-party entities that provide proprietary technology solutions. These critical service providers could come under direct cyberattack themselves and propagate risks to their institutional clients from the financial sector.

events can threaten financial stability—(i) lack of substitutability (of a service), (ii) loss of confidence in a financial institution or the financial system, and (iii) loss of data integrity. This contrasts with earlier literature which argued that almost all cyber risk is microprudential and that a cyberattack could only lead to a systemic crisis if it were timed impeccably to coincide with other non-cyber events that undermine confidence in the financial system and the authorities (Danielsson, Fouché, and Macrae, 2016).

[19] For this reason, the Committee on Payments and Market Infrastructures and the Board of the International Organisation of Securities Commissions have issued guidelines on the recoverability of the operations of such financial market infrastructures in response to a cyberattack (CPMI-IOSCO, 2016).

Figure 1. Cyber Risk and Systemic Risk: Transmission Channels



Sources: MAS; and IMF.

2.7 Risk contagion effects can also arise due to the high degree of interconnectedness within the financial system. For instance, impairment of business activities in a systemically important financial institution can curtail its ability to process transactions and post margins to its counterparties, resulting in heightened liquidity and solvency risks among multiple financial institutions. The failure of a highly interconnected and systemically important financial institution can cause multiple counterparty failures and trigger a 'domino' effect across the entire financial system.

2.8 Finally, the confidence effects of a cyber event can create systemic risks for the financial system. The impact of a loss of confidence can be difficult to estimate and predict and would depend on the length and severity of the damage or disruption caused by the cyberattack. Furthermore, while financial institutions can mitigate the direct loss impact of a cyber event through capital and liquidity buffers, an erosion of confidence can create a self-fulfilling chain effect that can overwhelm their existing buffers or contingency measures. For instance, an initial round of deposit withdrawals due to a cyber event can weaken a bank and further erode confidence, eventually culminating in a bank run with mass withdrawals. Given the potential outsized impacts of this transmission channel, measures such as coordinated crisis communications and effective contingency plans would be required to help maintain confidence during crises and minimise the likelihood of systemic outcomes.

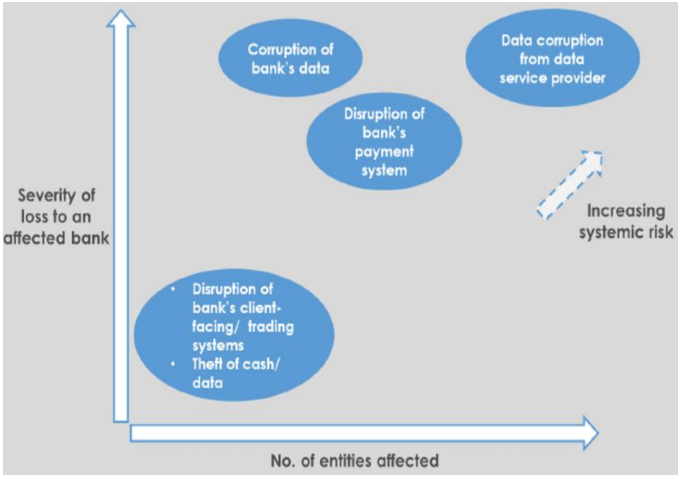
2.9 Although the three channels described above are largely similar to the way traditional financial shocks are transmitted through the financial system, a key difference lies in the speed of materialisation of risks within the financial system. The impact of a cyber event on a financial institution can quickly cause problems to

materialise within the entity and transmit these to the rest of the financial system much faster than traditional forms of risks. Another key difference is that a cyberattack at multiple non-systemic but (technologically) connected financial institutions could spill over to large systemically important financial institutions, even if the direct financial contagion from non-systemic firms would be limited. It is thus pertinent that policymakers develop a deeper understanding of the impact and transmission channels of cyber events and respond in a timely manner to minimise the risk that an event leads to systemic risk.

C. Systemicity of Cyber Events

2.10 An accurate assessment of systemic risk impact of a cyber event would require both an understanding of the nature of different cyber events and identification of the relevant risk transmission channels. Figure 2 below provides an example of an approach to differentiate and assess the systemicity of different types of cyberattacks. For instance, theft and disruption-related cyberattacks are likely to place pressure on financial institutions' liquidity and solvency buffers and the adequacy of these buffers would influence whether financial institutions would propagate these shocks to their counterparties and contribute to systemic outcomes. Post-crisis, the buildup of buffers among financial institutions is likely to help mitigate theft and disruption-related impacts and lower the likelihood of systemic outcomes from these types of cyberattacks.

Figure 2. Systemic Risk of Various Cyber Events



Sources: MAS; and Cambridge Centre for Risk Studies

2.11 Conversely, cyberattacks involving data damage can result in higher systemic risk. Financial institutions are particularly vulnerable to data damage, given the importance of data integrity in the financial sector. The financial impact of data damage could be significant, with indirect effects, such as loss of clients and reputational risk, likely to be more material than direct effects (recovery and litigation costs). The loss

of confidence in the data damage event could be very severe, especially if data manipulation has gone undetected for a prolonged period. This is because its impact would have propagated to a wider group of financial institutions, and any rectification would take an extended period.

3. ANALYSIS OF CYBER RISK TO FINANCIAL INSTITUTIONS

3.1 This section describes some approaches, including tools and data, for monitoring and analysing cyber risk in the financial sector. It illustrates how they can be applied, focusing on Singapore as a case study. Other approaches, like on-site inspections, penetration testing and thematic reviews, are also identified in the *Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector* published by the G-7.

A. Reinterpreting Traditional Risk Analyses as Cyber Risk Analyses

3.2 Traditional solvency stress tests, liquidity stress tests and contagion risk analyses already capture some aspects of cyber risk to financial institutions. For example, solvency stress tests already simulate a situation where asset prices decline sharply. A cyber event, particularly a form of fraudulent market manipulation, could be the source of this fall in asset prices. Liquidity stress tests already simulate a situation where depositors withdraw from an individual bank and where banks are also forced to sell or lend their assets at discounted prices to meet such cash requirements. A cyber risk event, possibly including a loss of reputation, could be the source of this liquidity stress. Contagion risk analyses, based on networks of bilateral exposures between financial institutions, simulate a cascading transmission of credit and liquidity risk between institutions. A cyber event, leading to a loss of confidence in a bank, for example, could be the source of the initial bank failure that causes domino effects via the interbank network.

3.3 Therefore, cyber risk to financial institutions can be assessed to some extent by the resilience of those institutions to traditional solvency, liquidity and contagion risks. In the Singapore context, a comprehensive set of risk analyses were published following the 2019 Financial Sector Assessment Program (IMF, 2019c). Since staff concluded that the financial system would remain resilient under adverse macroeconomic conditions, this implies that the buffers are also adequate for mitigating the impact of cyberattacks, even in the absence of a direct appraisal of cyber risk and resilience.

B. Key Indicators

3.4 Indicators on cyber risk in the financial sector are useful for assessing risk. These could be based on data of past incidents, investments, ratings or time to address risks. They are analogous to the idea of financial soundness indicators, applied to cyber risk.

3.5 Data on **cybersecurity incidents** can be analysed by agencies tasked with monitoring financial stability. In many countries, a mandatory reporting framework for breaches of customers' confidential information is already in place. Official cybersecurity operations centres often collect data on cyber events. The frequency of events can be monitored through time, as well as in the distribution of events across types of financial firm. For example, Figure 3 illustrates the rising frequency of cybersecurity incidents internationally,[20] which could reflect a combination of more frequent incidents and improved detection of incidents.[21,22] In Singapore, cyberattacks on financial institutions have primarily targeted securities firms and banks (second panel of Figure 3) and only one, thus far has led to a direct pecuniary loss. Most of the cyberattacks in Singapore were aimed at causing business disruptions like distributed denial of service (DDoS) attacks and website vandalism. Nevertheless, there have also been incidents of ransomware and attacks on third-party providers (including providers of cloud services and productivity and marketing software). Of course, many cybersecurity incidents do not incur losses while others can incur large losses, so frequencies of events only provide partial information. If data on financial losses are available, then the total value of losses can analogously be tracked over time and across types of financial institutions.[23]

3.6 Other indicators can also be monitored:

- **Resources allocated** to cybersecurity can be measured in headcount and proportion of the IT budget. PWC (2014) finds that firms allocate 4 percent of their IT budget to cybersecurity; in Singapore, the Cyber Security Agency (CSA) recommends 8 percent (CSA, 2018).

[20] Given the confidentiality of the Singapore data, this method is illustrated with published data for Canada.

[21] Indeed, Chart 10 in Bank of Canada (2019) shows that more past cybersecurity incidents are being discovered each year.

[22] It could also in principle reflect an increasing number of reconnaissance attempts by attackers e.g., port scanning activities.

[23] Losses can take time to materialise and can be difficult to measure. Therefore, distributions of losses need to be complemented by frequency distributions.

- Private sector firms (e.g., BitSight) produce **cybersecurity ratings** for financial institutions that can be monitored.[24]

- Financial institutions often collect information on the **time they take** to patch vulnerabilities, replace end-of-life software or detect malicious activity on their networks. A typical benchmark is to apply patches for critical vulnerabilities within 15 days and for high vulnerabilities within 30 days.[25]

- Financial institutions also collect information on the **numbers of devices** with installations of outdated software.

- Financial institutions can measure the proportion of staff that have completed security **training courses**. Some institutions perform regular phishing exercises on their own staff, measuring and tracking the proportion of staff that passes the tests.

- Indices for monitoring can be constructed from **predictive models** that provide early warning of unusual activity. These can be constructed by applying statistical techniques to analyse network traffic data or firewall logs.

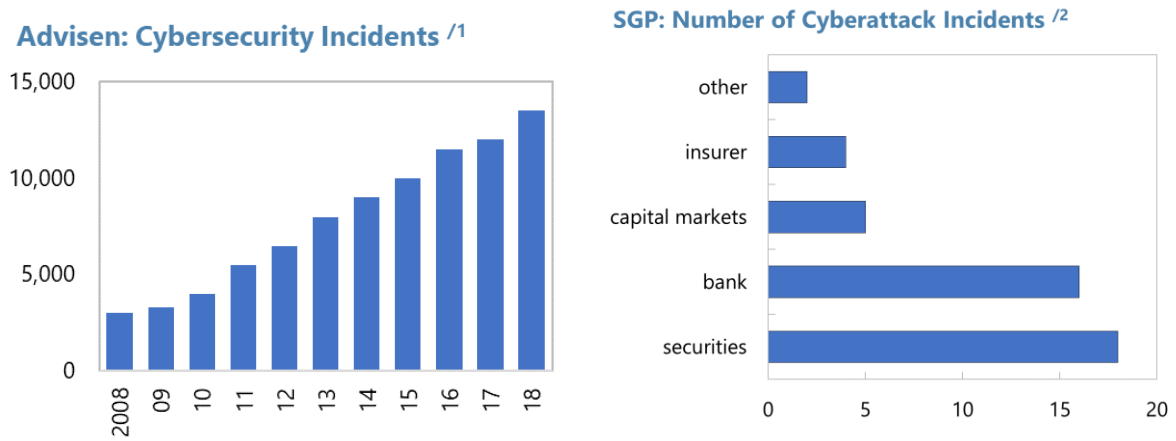
- **Internet searches** for the cybersecurity of specific financial institutions can be monitored through time, for example using Google Trends (Redscan, 2019).

3.7 BCBS (2018) lists other indicators that firms themselves monitor. These include number of times malware or websites were blocked, numbers of online directories containing stakeholder information, numbers of and ratings from penetration tests, numbers of unknown devices on networks. The appendix gathers some of the potential indicators from this subsection into template examples for regulators and financial institutions.

[24] BitSight scores companies and CIIs on a scale of 250-900 based on 4 categories of data: compromised systems, security diligence (e.g., access points, website security, patching speed, server software), user behaviour (secure file sharing, exposed staff credentials) and public disclosures (media reports of incidents).

[25] These deadlines are mandated for the information systems of federal agencies in the United States (DHS, 2019).

Figure 3. Frequency of Cybersecurity Incidents (number of events)



Sources: Bank of Canada (2019) and MAS. Notes: 1/ Number of cybersecurity incidents from international data collected by Advisen and are approximately transcribed from the Bank of Canada's 2019 Financial System Review. They refer to those that have or could have resulted in substantial financial losses. 2/ This chart refers to the number of cyberattack incidents that occurred in the Singapore financial sector between 2014 and November 2018. The only cyberattack that led to a direct pecuniary loss occurred at a capital markets intermediary. Therefore, the distribution of losses across sectors in Singapore would have a 100 percent weight on the capital markets sector.

C. Monitoring Risk Without Cybersecurity Incident Data

3.8 If cybersecurity incident data are available, models of the likelihood and severity of incidents can be estimated, as described in the following subsection. However, even if such data are not available, published models that were estimated in other contexts can be applied to the jurisdiction of interest. For example, studies like Kamiya and others (2018) provide formulae that can be used to estimate the likelihood of a cyberattack on a firm or the fall in stock price that would result from a hypothetical cyberattack on a firm if it were to occur. These formulae are coefficients of regressions estimated on publicly available data. To apply a formula to a given firm, one only needs to calculate some firm-specific variables like size, Tobin's *q*, stock return, leverage and asset intangibility as inputs.[26] These calculations can be updated in real time, as firm-specific variables change. One caveat of such approaches is that estimates will be affected by the sample selection bias that underlies any dataset on which these formulae are based.

3.9 Another useful analytical technique in the absence of data are questionnaires, which could be a self-assessment or a tool for the regulator to gain information from financial institutions (possibly within the supervision process). Healey and others (2018) provide examples of questions.

[26] Models that include fixed effects require extra care, because the estimated firm-specific fixed effects from the old context would not be applicable to the firms in the new context. If the model is first-differenced, then these fixed effects would be eliminated. Then the first-differenced model can be used to track increases or decreases in (but not the level of) the likelihood or severity of loss.

D. Data Sources, Event Studies and Value-at-Risk

3.10 Datasets are also available for bespoke analysis on cyberattacks, and we provide below two examples of studies that were conducted using these datasets.

3.11 Kamiya and others (2018) used data published by the Privacy Right Clearinghouse (The PRC), for their **event study** analysis. The authors use a sample of 188 cyberattacks that led to data breaches on U.S. financial and non-financial firms between 2005 and 2014. The authors find that median stock returns fall by 50 basis points and value-weighted stock returns fall by 76 basis points on a cyberattack, both of which estimates are statistically significant. The authors also control for other asset pricing factors, but it is unclear whether these are correlated with incidents of data breaches.

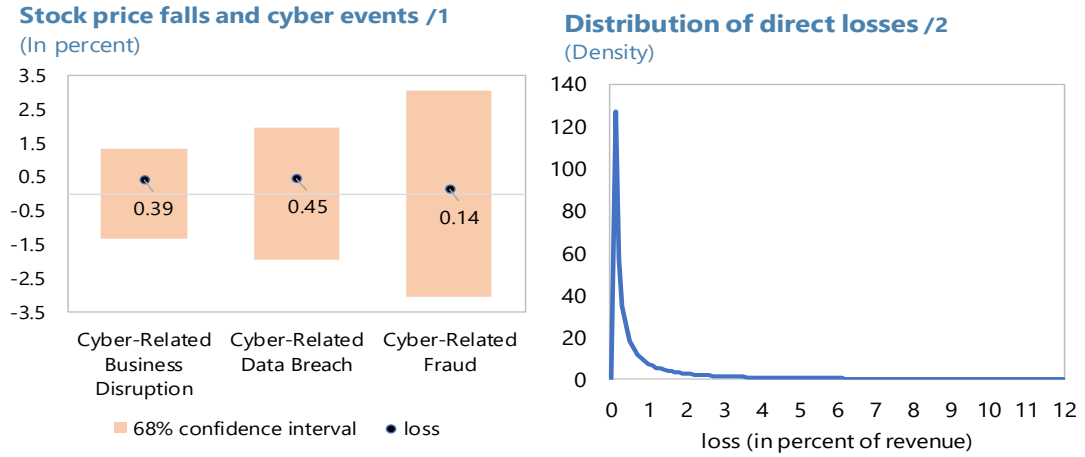
3.12 We analysed a subset of 341 cyberattacks pertaining to financial institutions worldwide using news stories data compiled by the Operational Riskdata eXchange Association (ORX).[27] An event study approach suggests that financial firms' stock prices fall by 45 and 39 basis points on days of cyberattacks leading to data breach or business disruption respectively (first panel of Figure 4).[28] The loss on data breaches is similar to the 50 basis points found by Kamiya and others (2018), whose coverage is slightly different.[29] Incidents of cyber-related fraud have had much smaller effects. Nevertheless, the wide confidence bands in Figure 4 suggest that these losses are difficult to distinguish from normal stock market volatility.

[27] Besides compiling similar data from news stories, ORX also collects data on cybersecurity incidents (data breaches, fraud and business disruption) from its members and shares the data with them.

[28] The stock price falls are measured around the day on which the cyberattack was first made public. A more thorough analysis could use abnormal returns from an asset pricing model, but the appropriate model for an international dataset is uncertain.

[29] Kamiya et al (2018) use data on U.S. events only and include attacks on non-financial firms.

Figure 4. Severity of Cyberattacks



Source: Authors' calculations based on ORX and Bloomberg data.
Notes: 1/ The loss is calculated as the natural logarithm of the fall in the price from the day before the cyber event is published in the media to the day after it is published. The 68 percent confidence interval is a one-standard deviation confidence interval, based on the standard deviation of losses across events of a given type. 2/ The loss in percent of revenue is the ratio of the direct losses of all an organisation's events in a given year in ORX to that organisation's gross revenue of the previous year. The density is the lognormal density whose first two central moments (in logarithms) match those of the (logarithm of the) underlying data.

3.13 Apart from event studies, such data can also be used to estimate the **value-at-risk** associated with cyber events, which is the largest loss that could be expected to occur with a given level of confidence. Bouveret (2019) uses ORX news stories data to estimate the value-at-risk of direct losses from cyber events, expressed in constant price U.S. dollars. To illustrate a similar approach with a slightly new application, the second panel of Figure 4 shows the (estimated lognormal) distribution of direct losses in percent of the organisation's revenues of the previous year.[30] The 95 percent one-year value-at-risk is then 4.7 percent of revenues, but it is subject to significant estimation uncertainty.[31] This estimate is in line with Bouveret (2019), who estimates

[30] In the analysis here, losses are aggregated to the firm—year level and matched to each firm's gross revenues of the previous year. The distribution we fit is therefore the distribution of yearly losses, in percent of revenues, directly. By contrast, Bouveret (2019) fits a distribution to the event-level losses in constant price U.S. dollars, and combines it with a calibrated Poisson random variable for the number of events in any given year, to simulate a compound distribution of annual (constant price U.S. dollar) losses. After deriving the dollar value-at-risk, external data is then used to express this estimated value-at-risk as a percent of net revenues. The author's approach might then overestimate the value-at-risk (in percent of revenues) if there is a positive correlation between nominal losses and income, as suggested by our data and certain results in Kamiya et al. (2018).

[31] The 68 percent bootstrapped confidence interval puts the (95 percent) value-at-risk between 1.6 and 9.8 percent of revenues. Part of the uncertainty comes from the difficulty in matching ORX data to Bloomberg data on revenues. Of the 102 events in the ORX news stories data with direct losses, only 21 events match to Bloomberg data on revenues. The greatly reduced sample size motivates the choice here of a simple lognormal distribution rather than the more flexible distributions considered in Bouveret (2019).

an analogous value-at-risk of 17 percent of net income,[32] which is about 2.5 percent of gross income for the firms in our data. Our value-at-risk is expected to be a bit larger because it is conditional on observing a (positive) loss, while Bouveret's (2019) is an unconditional estimate.

3.14 Again, every dataset on cybersecurity incidents is affected by sample selection bias and the results of analyses must therefore be taken with caution. Since most of the events in the PRC and ORX datasets are not systemic events for the financial sector, such estimates should also not be considered as estimates of the systemic risk from cyberattacks, which could be larger.

E. A Cyber Risk Assessment Matrix (Cyber RAM)

3.15 A Risk Assessment Matrix (RAM) is an analytical device commonly used in IMF surveillance to present the results of an assessment undertaken by staff.[33] A RAM is a table, where rows index downside scenarios and columns show the likelihood and severity of each. The same device can be used to present the results of an assessment of cyber risk, which could be the collective judgement of a group of experts or a summary of the results of a survey.[34]

3.16 Table 1 illustrates this presentational device based on a MAS-administered cyber stress test of 18 banks in Singapore in 2019. In the stress test, banks were asked to describe two severe cyber risk scenarios that they would be most vulnerable to. The first cyber risk scenario had to feature a direct cyberattack on the bank, while the second scenario had to feature a cyberattack on an external party (e.g., third-party service provider) on which the bank relies for its operations. In formulating these scenarios, banks could either reference known events, or come up with hypothetical ones that are unprecedented but plausible. Banks were also asked to provide (i) qualitative analysis of transmission channels; (ii) mitigating measures that could be taken in response to the cyberattack; and (iii) quantitative estimates of potential losses with and without the mitigating measures. The 'likelihood' shown in this table is based on the proportion of banks that identified the scenario, rather than on any expert

[32] The value of 17 percent comes from scaling up the average of 10 percent of net income by the ratio of the 95th percentile loss of US$167bn to the average loss of US$100bn (all of which appear on page 4 of that paper).

[33] A RAM appears in IMF Article IV reports. This RAM contains material risks, including potentially cyber risk, if it is material for the country in question. This RAM is explained in Box 5 of IMF (2015). The cyber RAM proposed here differs from this RAM in that it enumerates more material scenarios relating to cyber risk and excludes scenarios that are immaterial from a cyber risk perspective.

[34] A similar presentational device is proposed by Santucci (2018). The advantage of the cyber RAM proposed here is that it collects all scenarios into one table.

judgement. A column could be added to the table with information on banks' estimated losses under each scenario, to capture severity.

3.17 Specific types of cyber risk scenarios envisaged by banks in Singapore generally fall into three categories, theft of data or money, disruption of banks' IT or payment systems and damage/corruption of customer data, with banks indicating that they would be most affected by first two categories (money theft and IT system disruptions). The most typical cyberattack scenario is in the form of a phishing email which infects user workstations with malware, and subsequently spreads within the bank network to other systems, resulting in theft of data or money and disruption of services.

Table 1. Cyber Risk Assessment Matrix for Banks [1]

Scenario	Likelihood [2]	Security measures
Corruption of data from data service provider	0% of respondents	• Due diligence e.g. on service provider
Theft of data or money For example, ATM jackpotting: malware causes ATMs to dispense cash. Especially if malware is delivered to the centralised ATM software delivery system.	60% of respondents	• Access control • Multiple security devices (e.g., firewalls, intrusion prevention systems) • Regular security testing • Malware protection
Disruption of a bank's IT systems For example, DDOS attack: disruption to websites prevents customers from accessing internet and mobile banking applications. Customers would still have access to banking services at bank branches. A more severe example would be a disruption of a bank's own payment processing system.	60% of respondents	• Disaster recovery systems, including alternate site • Incident response plans
Corruption of customer data: a bank discovers that its customer data has been corrupted for three days. The affected data include demographics, transactions and account balances. Banking services are disrupted until data can be recovered.	20% of respondents	• Regular tape backups to enable data restoration

Disruption of third-party services Most important providers include: payments and clearing systems (public and private), telecommunications, utilities, printing	n.a.	• Due diligence • Third parties' contractual cybersecurity obligations • Business continuity measures, like alternate service providers

Source: Participating banks' responses to bottom-up stress test exercise.
Notes: 1/ This table is an application of the "Risk Assessment Matrix," as a presentational device, to assess cyber risk in the banking sector. The main text defines the interpretation of this table. The table should not be confused with the Risk Assessment Matrix of in the Singapore FSAP (IMF 2019a, 2019c), which covers all material risks to the whole financial system.
2/ The likelihoods reported in this table are based on the fraction of banks that identified the scenario as a significant risk to themselves, rather than on any expert judgement.

3.18 Banks indicate that adequate measures are in place to mitigate the attacks, including multiple layers of security controls, like strong data encryption, access controls, regular cyberattack simulations, and disaster recovery measures. Unsurprisingly, systemic cyber risk scenarios are relatively unexplored by individual banks. The cyber RAM can also include scenarios that were identified by policymakers, not only by financial institutions themselves.

F. Stress Tests on Cyber Risk in Singapore

3.19 Policymakers can obtain estimates of the likelihood and severity of cyberattacks by asking financial institutions to assess them using proprietary data. These estimates obtained are checked for reasonableness with simple validation checks and by comparing estimates across financial institutions. Such exercises also encourage financial institutions to allocate more resources to this area and develop their risk management practices. These tests could involve estimating losses from a prescribed scenario, identifying scenarios that would result in severe losses and estimating the coverage against cyber risk that financial institutions have written.

3.20 The MAS conducts stress tests and industry-wide exercises for financial institutions to assess their resilience to cyber threats from two complementary perspectives. While the focus of stress tests is on the adequacy of capital and liquidity buffers to weather the impact of cyberattacks, industry-wide exercises test their business continuity and crisis management plans to respond and recover from cyberattacks.

3.21 A cyber risk scenario was first introduced in the MAS' industry-wide stress test (IWST) in 2016 to attune participants to the microprudential implications of cyber risks. In the scenario, an international crime syndicate was assumed to have launched a

series of simultaneous hacking attacks on some of the financial institutions in the Asia region, including Singapore. The cyberattack resulted in loss of entire customer databases and a 24-hour system downtime for the banks' client-facing (including mobile and web-based) operational systems. The stress test results showed a somewhat smaller impact on banks than expected, and the estimated losses varied significantly across banks. This partly reflected the fact that some banks did not explicitly account for systemic impacts arising from financial contagion and confidence effects. Indeed, the few banks that considered systemic transmission channels (e.g., inability by affected counterparties to fulfil payment obligations and customer deposit withdrawals due to confidence effects) reported much larger losses than the other banks. In addition, banks were still building up expertise in quantifying the microprudential costs of cyber risks, and the exercise provided a valuable learning experience for both the banks and MAS.

3.22 Direct life and general insurers were likewise required to quantify the losses that they could potentially experience because of disruption to their operations under the same cyberattack scenario that was prescribed for banks. In addition, the scenario included disruption to 5 of the insurers' largest clients to whom they had provided affirmative cyber insurance coverage. For disruption of insurers' operations, insurers considered impacts from a decline in new business volume/termination of existing business and increase in operational and other costs arising from system remediation or compensation to policyholders. For disruption to clients to whom the insurers had provided affirmative cyber insurance coverage, the cyberattack was expected to trigger claim losses that exceed the limits of the cyber policies. The 2016 cyber stress test results suggested that insurers were not materially impacted by the scenario. No insurer failed the cyber risk scenario.

3.23 The MAS, in collaboration with the IMF, built on the 2016 exercise by conducting another stress test on cyber risk as part of the 2019 IWST and the Financial Sector Assessment Program (FSAP). As described above in the context of the cyber RAM, banks were asked to identify the most impactful direct and third-party cyberattack scenarios. This approach allowed MAS to explore the most dire cyber scenarios (for financial buffers and profits). It also facilitated MAS' understanding of the banks' identification of the relevant transmission channels and built up an internal inventory of cyber scenarios for future work. The 2019 approach, however, had the disadvantage of being more difficult to aggregate and compare results across banks.

3.24 As seen in Table 2, the results of the 2019 IWST bank cyber stress test were aggregated separately for scenarios relating to theft, disruption and damage as the banks had performed stress tests on different cyber scenarios. Banks estimated that they would be most affected by theft of funds and business disruption scenarios but would have ample capital and liquidity buffers to mitigate the impact of these

cyberattacks (Table 2). On average, banks estimated that losses from a direct cyberattack would amount to about 35–65 percent of quarterly net profits, depending on the cyber scenario type, and would cause the Capital Adequacy Ratio (CAR) and the Liquidity Coverage Ratio (LCR) to drop by 0.1–0.4 and 8.4–35 percent respectively. Indirect cyberattacks result in smaller losses of 20–50 percent of quarterly net profits and insignificant falls in the CAR and LCR. Results also suggest that confidence effects from cyberattacks are likely to impact banks more immediately through the customer deposit channel rather than credit demand. Banks expect most of the costs of these cyberattacks to reflect declines in future revenue due to reputational impact and other costs such as monies stolen, legal charges and marketing/public relations expenses.

3.25 As part of the 2019 IWST exercise, Singapore insurers were asked to measure their exposures to cyber risk through the affirmative and non-affirmative (silent) cyber risk coverage that they had written. Specifically, the MAS surveyed 17 direct general/composite insurers on the claims that would arise if their 10 largest clients of affirmative cyber coverage and their 10 largest clients of property and casualty insurance were victims of cyberattacks. In the scenario, sensitive data in the organisations' client-facing, back-end and backup systems were corrupted and stolen under a ransomware attack. The scenario prevented these organisations from resuming their operations using accurate and complete data for at least four weeks.

3.26 Direct insurers expected the claims from affirmative and non-affirmative (silent) cyber coverage to be manageable, mainly due to reinsurance arrangements in place. Insurers reported exposures of S$600 million and S$3.4 billion for affirmative and non-affirmative (silent) cyber coverage, respectively. Claims arising from these exposures amounted to S$1.8 billion, which were shared between the direct insurers and their reinsurers and could be offset against a release of technical reserves. The net losses reduced the aggregate CAR of these insurers by only three and two percentage points for affirmative and non-affirmative (silent) cyber coverage, respectively. Some insurers which participated in the cyber stress test exercise and had exposure to non-affirmative (silent) cyber coverage have since put in place risk mitigation actions, including inserting appropriate exclusion clauses in their contracts.

Table 2. Bottom-up Estimates of Banks' Losses from a Direct Cyberattack
(In percent)

	Direct Cyberattack			Indirect Cyberattack	
	Theft	Disruption	Damage	Theft	Disruption
Fall in demand for credit (in percent of credit)	0.4	0.1	0.1	0.2	0.1
Withdrawal of deposits (in percent of deposits)	1.7	1.9	1.1	5.1	3.9
Loss (in percent of quarterly profits)	65.2	44.4	36.4	20.4	50.7
Fall in CAR (in percentage points)	0.1	0.2	0.4	0.1	0
Fall in LCR (in percentage points)	9.5	35	8.4	1.6	3.6

Notes: Estimates reported here are without the banks' contingency measures. Estimates include assessment of the duration of the disruption, the affected computer systems and services. Methodology includes using historical transactions data, staffing and inventory costs, fines specified in regulation, reference to past incidents internationally and reference studies. No bank reported a damage-related scenario for indirect cyberattacks.

G. Analysis of Cyber Risks Posed by Outsourcing Relationships

3.27 A comprehensive analysis of cyber risks would need to also incorporate risks posed by financial institutions' outsourcing relationships. It is common for financial institutions to adopt outsourcing practices to enhance efficiency by tapping on third-party service providers with specialised expertise. However, outsourcing activities also expose firms to cyber risks associated with the IT security posture of their outsourcing partners. For example, cyber breaches at outsourcing partners could lead to disruption of outsourced services, leakage of sensitive customer information, or compromise of financial institutions' IT environments through the IT linkages that they have established with their partners. This creates a risk that needs to be monitored. Furthermore, concentration risk can arise if many financial firms rely on the same service providers, particularly if these outsourcing service providers are reputable and established in their areas of expertise.

3.28 In Singapore, the MAS regularly collects information on outsourcing arrangements of financial institutions. In particular, financial institutions are expected to maintain an updated register of all existing outsourcing arrangements and to submit this register to MAS at least annually or upon request. MAS uses the information in the registers to determine if there are any commonly-used service providers that may warrant closer scrutiny given potential concentration risks. The MAS recently

completed a review of concentrations of financial institutions to outsourcing providers. The review concluded that there are no significant operational linkages between major financial institutions and technology firms.

H. Mapping the Network of Financial and Cyber Exposures

3.29 The financial-cyber network map is an approach that regulators can use to analyse cyber risk exposures further (IMF, 2019b). Usually, interconnectedness of financial claims and obligations is measured independently of information and communications technology (ICT) interconnectedness. However, these connections can provide complementary information if combined. For example, two firms may not be directly connected, but may be connected through other firms by a combination of financial and ICT connections.[35] The connections can also signal contagion or concentration risks and firm-specific vulnerabilities that can inform microprudential supervisors.

3.30 Such a map is comprised of nodes and edges. The nodes include all financial institutions, critical information infrastructures and third-party providers. Therefore, the first step in constructing such a map is to identify these entities. The edges are the financial and ICT connections between entities. In turn, ICT connections could reflect actual or potential data flows between computer systems. Such data flows could be measured in terms of importance to the business[36] or simply by whether or not a connection exists. Financial exposures between financial institutions are typically collected in standard supervisory reporting templates. ICT exposures to third-party provides are sometimes collected as part of the approvals process for material outsourcing relationships. Information on other relationships must be collected separately or estimated.

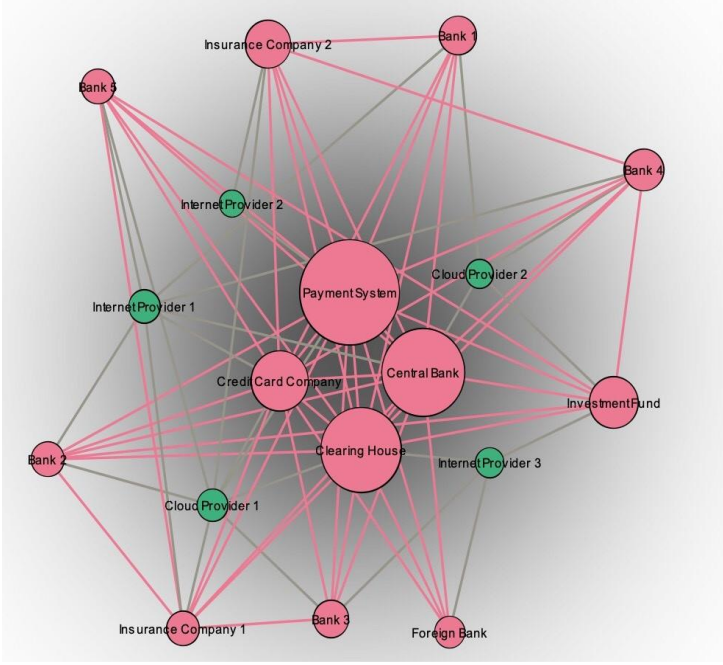
3.31 Once a dataset of all nodes and edges is established, it forms the (possibly weighted) adjacency matrix of a network that can be plotted as a network 'map' using standard software. Different colors could be used to distinguish financial and ICT connections.[37] Constructing such a map is ongoing in Singapore. Accordingly, the accompanying chart shows a stylised depiction (Figure 5).

[35] No special technique is needed to combine financial and ICT exposures.

[36] One measure of the importance of data flows to the business is their size in bytes.

[37] The map can be seen as the graph of a two-layer network, where one layer depicts financial connects and the other depicts ICT connections.

Figure 5. An Example of a Financial-Cyber Network Map



Source: IMF (2019b)

4. APPROACHES TO CYBERSECURITY IN THE SINGAPORE FINANCIAL SECTOR

A. Regulatory Approach

4.1 As Singapore's central bank and financial regulator, the MAS works closely with the CSA to administer the Cybersecurity Act 2018 and oversee the cybersecurity of the financial sector. The MAS regards cyberattacks as a growing threat to the financial system and expects the increasing digitalisation of financial services to heighten cyber risk. The MAS has adopted a cybersecurity strategy with the following strategic elements.

Regulation and Guidance

4.2 The MAS sets minimum regulatory requirements and expectations on technology risk management (TRM) in Notices and Guidelines. Specifically:

- **The TRM Notice** obliges financial institutions to maintain minimum levels of availability, resilience and recoverability for their critical systems. Financial institutions are also required to implement IT controls to preserve confidentiality of customer information.

- **The Cyber Hygiene Notice** obliges financial institutions to implement a set of cybersecurity measures to mitigate common and pervasive cybersecurity threats. These include implementing network perimeter defence, malware protection, multi-factor authentication, timely patch updates, and establishing baseline configuration standards.

- **TRM Guidelines** recommend technology risk management practices, including those relating to cyber surveillance and security operations, cybersecurity testing, and protection of online financial services.

Supervision

4.3 The MAS verifies financial institutions' compliance with regulatory requirements and expectations through onsite inspections and off-site surveillance. Where there are areas of supervisory concerns, the MAS follows up with financial institutions to ensure that the concerns are addressed promptly and effectively. To anticipate and promptly respond to cyber risk, the MAS also monitors key financial institutions' cybersecurity strategy and changes in their risk management frameworks and controls.

Cyber Surveillance and International Co-operation

4.4 The MAS collects and analyses cyber threat information from various sources in its Financial Sector Security Operations Centre (FS-SOC). Relevant insights, distilled from the FS-SOC, are shared with financial institutions to build collective cyber situational awareness and resilience within the financial system. The MAS has also forged strong partnerships with the international community, including international standard-setting bodies to help shape cyber risk management standards.[38]

Competency Building and Industry Collaboration

4.5 To develop cybersecurity skills in Singapore, MAS has established a Cybersecurity Capability Grant to encourage international financial institutions to base their cybersecurity functions in the country.[39] This enables the deepening of cybersecurity operational capabilities in Singapore, like SOCs and cybersecurity centres of excellence. The MAS also partners with industry. The Association of Banks in Singapore (ABS) Standing Committee on Cyber Security (SCCS), formed in 2013, is a forum for the IT security heads of key financial institutions to discuss cyber threats

[38] The MAS is currently chairing the Financial Stability Board (FSB) working group on Cyber Incident Response and Recovery (CIRR), which aims to develop a toolkit to help financial institutions respond to and recover from cyber incidents effectively.

[39] Such functions include SOCs, fusion centers and centers of excellence.

and countermeasures. This committee has issued industry guidelines to raise cybersecurity standards, organised cybersecurity seminars to create greater awareness of cyber threats and conducted table top exercises to test response measures.

Cyber Security Agency (CSA)

4.6 The Singapore government established the CSA in 2015 to oversee Singapore's national cybersecurity functions. The CSA's mandate includes the protection of critical information infrastructures, strategy and policy development, security operations, and ecosystem development.

4.7 The Cybersecurity Act 2018 ("Act") requires owners of critical information infrastructures to implement a set of mandatory measures[40] to protect these systems against cyberattacks. The Act also requires owners to notify the CSA of cybersecurity incidents.

B. Efforts by Financial Institutions

4.8 Major financial institutions in Singapore adopt multiple layers of security mechanisms to mitigate cyberattacks, which reduces single points of failure in defences and addresses different attack vectors:

- **Predictive mechanisms** use data analytics and machine learning tools to analyse cyber threat intelligence and understand adversaries.

- **Preventive mechanisms** segregate internet browsing and email access on endpoint terminals to insulate the internal corporate network and prevent cross-contamination.

- **Detective mechanisms** monitor systems and endpoints to identify anomalies and suspicious activity, in some cases through dashboards with real-time metrics.

- **Respond and recovery mechanisms** in the form of cybersecurity exercises to test the ability to respond promptly to cyber threats and implement recovery plans.

4.9 Key financial institutions in Singapore have established their own SOCs to integrate the analysis of system and security events. These SOCs are equipped with

[40] Such measures include conducting regular audits and risk assessments and participating in exercises to validate response measures.

tools[41] to see into the IT operating environment and detect cyberattacks early. Some financial institutions also plan to establish cyber security fusion centres. These incorporate cyber intelligence gathering and analysis, security operations, security incident management as well as cyber forensics investigation, to identify and respond more proactively to advanced threats. Staff in SOCs undergo regular professional training.

5. CONCLUSIONS

5.1 Cyber risk poses a growing threat to financial stability, and public agencies will need to do more to better understand and assess its financial stability implications. This paper helps in this task by presenting data sources and methods for analysing cyber risk. These include key indicators that can be collected and tracked through time, event studies, value-at-risk, custom surveys, structured presentation via a cyber RAM and financial-cyber network maps. These analytical approaches are illustrated with applications to Singapore, and the appendix provides examples of templates for data collection. Even in the absence of cyber event data, this paper argues that models estimated in other contexts can be applied regularly in a given jurisdiction.[42] The quantitative results of the Singapore analyses, and descriptions of the public and private sector cybersecurity initiatives there, should provide a reference for surveillance work.

5.2 The (one-year, 95 percent) value-at-risk of 4.7 percent of gross revenues consumes a significant amount of the capital budget for operational risk (which in the Basel III standard includes cyber risk). The BCBS has recommended capital requirements for operational risk of about 11 percent of gross income for banks with gross income up to €1bn,[43] which is intended to cover unexpected loss from many sources besides cyber risk, and possibly at a higher level of confidence than 95 percent.[44] This suggests that for these banks, even just the 95th percentile of cyber

[41] Such tools include Security Information and Event Management (SIEM) solutions, network traffic inspection solutions, and security analytics tools.

[42] This idea is discussed in Section 3, subsection C. Of course, if cyber event data are available, then they should be used instead.

[43] More specifically, BCBS (2016) proposes that capital requirements grow with a "business indicator" at a rate of 0.11 per euro. In turn, the "business indicator" is an aggregate of income from interest, leases, dividends, services and financial trading. It is designed to be a proxy for exposure to operational risk, but ORX (2016) has shown that it is almost equal to gross income ($R^2 = 0.96$). For this brief discussion, the "business indicator" is assumed to be equivalent to gross income.

[44] BCBS (2016) is not explicit about the level of confidence underlying its formula for capital requirements. However, the advanced measurement approach to operational risk under the Basel II standard specified that capital for operational risk should be sufficient to cover 99.9 percent of one-year losses (BCBS, 2011).

risk consumes about two-fifths[45] of the capital budget for operational risk over one year. One final point to note is that our value-at-risk estimate is a measure of idiosyncratic rather than systemic risk because it is based on idiosyncratic events. However, by modifying the approach to allow for correlations between events across firms,[46] measures of systemic cyber risk can be derived.

5.3 However, many questions remain. For example, further work needs to estimate the size of systemic risk from cyberattacks to the financial sector. The papers cited here focus on firm-specific events, and financial institutions often do not internalise the implications of a cyber incident on systemic risk in the bottom-up stress tests for Singapore. Systemic losses could be larger but could also be somewhat offset by diversification effects. Another example relates to the potential selection biases in the datasets on cyber events. To overcome such biases, future analyses may find it useful to build in first-stage models of the selection process.

5.4 The financial-cyber network map is a recent idea that has yet to be applied in practice. When such data become available, specialised contagion risk models may need to be developed to analyse such data. For example, contagion could be modelled over a two-layer network, where one layer represents the financial links and the other layer represents the ICT links. Similarly, concentration analysis for outsourcing arrangements has been described here. In applications, such analysis needs to distinguish between concentration risk, and the desirable concentration that arises when many financial institutions use the same reputable third-party providers.

[45] Two-fifths here is calculated as the ratio of 4.7 to 11. Using 2.5 from Bouveret (2019) instead of 4.7, this drops to one-fifth. Therefore, the fraction is large, despite the caveats that our calculated value-at-risk applies to all financial institutions, not just banks, and is subject to substantial estimation uncertainty.

[46] Bouveret (2019) allows for such correlations.

REFERENCES

Afonso, G., Curti, F., McLemore, P. and A. Mihov. 2019 “Understanding Cyber Risk: Lessons from a Recent Fed Workshop.” Blog, Liberty Street Economics, Federal Reserve Bank of New York.

Bank of Canada, 2019, “Financial System Review”.

Basel Committee on Banking Supervision, 2011. “Operational Risk - Supervisory Guidelines for the Advanced Measurement pproach.” Bank for International Settlements, June.

Basel Committee on Banking Supervision, 2016. “Standardised Measurement Approach for Operational risk.” Consultative Document, March.

Basel Committee on Banking Supervision, 2018. “Cyber Resilience: Range of Practices.” Bank for International Settlements, December.

Bouveret, Antoine, 2019, “Estimation of losses due to cyber risk for financial institutions,” Journal of Operational Risk, 14(2) pp. 1-20.

Cambridge Centre for Risk Studies, 2019, “Cyber Risk Outlook.” Judge Business School, University of Cambridge. Prepared in collaboration with Risk Management Solutions, Inc.

Committee on Payments and Market Infrastructures, 2016. “Guidance on cyber resilience for financial market infrastructures.” Joint with the Board of the International Organization of Securities Commissions. June.

Council of Economic Advisers, 2018, “The cost of malicious cyber activity to the U.S. economy.” White House.

Cyber Security Agency of Singapore, 2018, “Singapore Cyber Landscape 2017.” ISBN: 978-981-11-7062-1

Department of Homeland Security, 2011. “Subject: Vulnerability Remediation Requirements for Internet-Accessible Systems.” Binding Operational Directive 19-02.

Danielsson, Jon, Morgane Fouche, and Robert Macrae, 2016, “Cyber Risk as Systemic Risk,” VOX CEPR Policy Portal.

Financial Stability Board, 2017. "Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices." October.

Financial Stability Board, 2018. "Cyber Lexicon." November.

Gandhi, P., Khanna, S. and S. Ramaswamy, 2016, "Which Industries are the Most Digital (And Why)?" Harvard Business Review, April.

Healey, J., Mosser, P., Rosen, K. and A. Wortman, 2018. "The Ties That Bind: A Framework to Assess the Linkage Between Cyber Risks and Financial Stability." Working Paper, Project on Cyber Risk to Financial Stability, School of International and Public Affairs, Columbia University. December, pp. 1-12.

International Monetary Fund, 2015. "Guidance Note for Surveillance under Article IV Consultations." May. (Washington: International Monetary Fund).

International Monetary Fund, 2019a. "Singapore: Financial Sector Stability Assessment." (Washington: International Monetary Fund).

International Monetary Fund, 2019b. "Cybersecurity Risk Supervision." Departmental Paper No. 19/15, Monetary and Capital Markets Department. (Washington: International Monetary Fund).

International Monetary Fund, 2019c. "Singapore: Technical Note on Financial Stability Analysis and Stress Testing." (Washington: International Monetary Fund).

International Monetary Fund, 2019d. "World Economic Outlook, April 2019: Growth Slowdown, Precarious Recovery." (Washington: International Monetary Fund).

International Monetary Fund, Financial Stability Board, and Bank for International Settlements, 2016, "Elements of Effective Macroprudential Policies." Available at: https://www.imf.org/external/np/g20/pdf/2016/083116.pdf

Jones, N. and B. Tivnan, 2018. "Cyber Risk Metrics Survey, Assessment, and Implementation Plan." Case no. 18-1246, The Homeland Security Systems Engineering and Development Institute, May.

Kamiya, Shinichi, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, Rene M. Stulz, 2018, "What is the Impact of Successful Cyberattacks on Target Firms?" NBER Working Paper No. 24409, National Bureau of Economic Research.

Kopp, E., Kaffenberger, L. and Jenkinson, N., 2017. "Cyber Risk, Market Failures, and Financial Stability." Working Paper no. 17/185, International Monetary Fund.

Lloyds and Cambridge University Center for Risk Studies, 2015. "Business Blackout: The Insurance Implications of a Cyberattack on the US Power Grid." Emerging Risk Report – 2015.

MAS, 2018, "Financial Stability Review".

Office of Financial Research, 2017. "Cybersecurity and Financial Stability: Risks and Resilience." OFR Viewpoint 17-01, February 15.

Oliver Wyman, 2019. "Navigating Cyber Risk Quantification. The Art and Science of Cyber Quantification Through a Scenario-Based Approach."

ORX, 2016. "Capital impact of the SMA. ORX benchmark of the proposed Standardised Measurement Approach." Available at https://managingrisktogether.orx.org/sites/default/files/downloads/2017/05/orxcapitalimpactofthesma1.pdf.

PricewaterhouseCoopers, 2014. "Managing Cyber Risks in an Interconnected World," September.

Redscan, 2019. "Cyber Security in Search: Analysis of Google Search Trends 2004-2019." Redscan Cyber Security Limited. Available at https://www.redscan.com/wp-content/uploads/2019/09/Redscan-Report_-Cyber-Security-In-Search_Sept19.pdf

Reuters, 2017, "Cyber attack hits 200,000 in at least 150 countries: Europol". May 14.

Santucci, L. 2018. "Quantifying Cyber Risk in the Financial Services Industry." Discussion Paper no. 18-03, Consumer Finance Institute, Federal Reserve Bank of Philadelphia.

The Straits Times, 2018, "Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack." July 20. URL: https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most

Verizon, 2017, "Data breach investigations report".

Verizon, 2018, "Data breach investigations report".

Verizon, 2019, "Data breach investigations report".

Wired, 2018, “The untold story of NotPetya, the most devastating cyberattack in history”. August 22.

World Economic Forum, 2016. “Understanding Systemic Cyber Risk.” White Paper, Global Agenda Council on Risk & Resilience, October.

APPENDIX I. EXAMPLES OF DATA REPORTING TEMPLATES

This appendix provides examples of templates that could be used to collect data from individual financial firms on their cyber risk exposure and cybersecurity practices. Note that these templates are stylised representations and should be tailored to each jurisdiction.

Annual budget for cybersecurity		number of full-time employee equivalents	spending (US$ '000)
Total budget for ICT	(1)		
of which, budget for cybersecurity	(2)		
= (1)/(2) x 100			

Board and senior management	
Are there Board members with expertise in cybersecurity?	yes/no
Does the Board receive training on cyber risk?	yes/no
Does the Board receive regular cyber risk reports from staff?	yes/no
If so, how many times per year?	
Does the firm's senior management designate an individual responsible for cybersecurity?	yes/no

Cyber hygiene practices	
Does the firm apply automatic security patches?	yes/no
Average number of days it takes to patch software vulnerabilities	
Does the firm use multi-factor authentication:	
for all administrative accounts?	yes/no
for all accounts with access to customer data?	yes/no
Does the firm use malware protection software?	yes/no
Does the firm maintain a list of its critical information infrastructures (CIIs)?	yes/no
Does the firm maintain a written set of security standards for each CII?	yes/no

Please list all cyber incidents that occurred this reporting period													
ID	earliest date of occurrence (yyyy/mm/dd)	date of detection (yyyy/mm/dd)	event type (breach, disruption or fraud)	cause (external, people, processes)	third party provider involved (yes/no)	number of records breached	estimated direct loss amount (US$ '000)	reported to law enforcement (yes/no)	insured (yes/no)	direct loss amount insured (US$ '000)	jurisdiction	business line	description
1													
2													
3													
…													

Please describe cyber risk scenarios that would have the greatest impact on your firm							
scenario number	description	direct loss (in US$ '000)	fall in deposits (percent)	fall in CAR (percent)	fall in LCR (percent)	mitigating actions	preventive measures
1							
2							
3							
…							

Monetary Authority of Singapore