NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Insurance Risk and Finance Research Centre
Nanyang Business School

NTU Singapore Cyber Risk Management project

Key observations to enhance cyber resilience

March 2018

Authored by Caitríona Heinl, Associate Fellow, NTU Cyber Risk Management Project. For further information, please contact d-irfrc@ntu.edu.sg

Nanyang Business School, 50 Nanyang Avenue, Singapore
www.ntu.edu.sg

Foreword

Professor Shaun Wang

Director,
NTU Cyber Risk Management Project

Cybersecurity has become increasingly important since our economy is highly dependent upon digital information and communication, becoming even more inter-connected through complex networks. Nanyang Technological University Singapore (NTU) is hosting a Cyber Risk Management Project (CyRiM), which is supported by the Monetary Authority of Singapore, the Cyber Security Agency of Singapore, and leading global companies (Aon, Lloyd's, MSIG, SCOR, and TransRe in collaboration with the Geneva Association and Verizon).

The CyRiM project aims to bring technology and business approaches together to promote innovative risk management solutions and insurance products for specific industry sectors. It is developing a Singapore Cybersecurity Framework by combining quantitative and qualitative aspects, and making public policy recommendations that support risk management and insurance solutions to cybersecurity.

In the spirit of engaging diverse stakeholders in a meaningful dialogue, CyRiM organised a series of roundtables to discuss the key challenges that organisations are facing including a lack of data and expertise as well business tools to achieve cyber resilience.

While regulation and compliance requirements are driving most of the activities, they also come with a cost. Like many other economic activities, one size does not fit all, and thus, a business approach is required. A price or value (quantification) of cyber risk exposure and cybersecurity measures that are taken is essential to drive effective and efficient cybersecurity.

Organisations should take a holistic view of their cybersecurity investment and cyber hygiene. There is a role for insurance in raising awareness and nudging firms to take actions. Furthermore, insurers should step up to fill the data void through data sharing.

The NTU CyRiM roundtable discussions were lively and stimulating. Many new perspectives and insights were gained throughout these discussions. Looking ahead, the CyRiM project foresees the need for a new risk management industry to emerge in order to address the multi-facets of the digital economy, to enhance resilience of the eco-system, and to facilitate coordination among various stakeholders and regional governments.

I would like to thank Caitríona Heinl for convening the CyRiM policy group and compiling this report. I would also like to thank the working group participants for their input and support.

Professor Shaun Wang, Director, NTU Cyber Risk Management Project

Introduction

It is a well-documented concern that cyber threats are imposing costs on global economies, while challenging public confidence in institutions, governance and norms. [1] Although cyber defences have been improving in recent years, the cybersecurity community currently believes that nearly all information and communication networks and systems will be at risk for years. [2] Moreover, there is a visible increase in the levels of complexity across risks. [3] Greater interdependence across different infrastructure networks is further increasing the scope for systemic failures, whether from intentional cyber attacks, software glitches, natural disasters, or other causes.[4] As the so-called fourth industrial revolution intensifies networks' interconnectivity and reliance on each other, there is a need for information sharing – for instance, critical infrastructure such as utility providers may understand their own systems well but be less certain about the resilience of the systems to which they are connected.[5]

In order to address these types of difficulties, the global cyber community has identified a key challenge – there is a need to not only address cybersecurity failures in systems and organisations from a technical perspective but to also apply societal, institutional and economic analyses. [6] Current research gaps identified by decision-makers in Europe and Asia therefore include the search for optimal investment in information security, risk management and cybersecurity insurance.[7] In short, this field is considered to be more challenging for the insurance industry and decision-makers since these technology issues are dynamic in nature whereas other insurance areas, such as house insurance, are more static in nature.

Governments accept that there is space for either improvements or alternatives to current institutional and governance frameworks (market driven as well as national and international regulatory) with a view to improving cybersecurity. [8] However, some

[1] Daniel R. Coats, Director of National Intelligence, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence, 11 May 2017.

[2] Daniel R. Coats, Director of National Intelligence, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence, 11 May 2017.

[3] World Economic Forum "The Global Risks Report 2017", 12th edition, Insight report, 2017, executive summary.

[4] World Economic Forum "The Global Risks Report 2017", 12th edition, Insight report, 2017, p.7.

[5] World Economic Forum "The Global Risks Report 2017", 12th edition, Insight report, 2017.

[6] European Commission, Horizon 2020 Work Programme 2016-2017: Secure societies – Protecting freedom and security of Europe and its citizens, European Commission Decision C (2017) 2468 of 24 April 2017, p. 66.

[7] European Commission, Horizon 2020 Work Programme 2016-2017: Secure societies – Protecting freedom and security of Europe and its citizens, European Commission Decision C (2017) 2468 of 24 April 2017, p. 66.
See also: Singapore NTU Cyber Risk Management project (CyRiM).

[8] European Commission, Horizon 2020 Work Programme 2016-2017: Secure societies – Protecting freedom and security of Europe and its citizens, European Commission Decision C (2017) 2468 of 24 April 2017, p. 66.

stakeholder reports still express uncertainty about the likely impact of insurance – in other words, whether these cyber insurance measures will result in a positive scenario where due diligence and minimum security standards are required or lead to risk transferring strategies.[9]

The NTU Singapore Cyber Risk Management project (CyRiM) aims to inform this public discourse. The project focuses upon ways to improve risk-based information security investment, societal resilience to cybersecurity risks through more effective institutional and incentive structures as well as challenges to the status of information security economics models. [10] CyRiM is an industry-government-academia research endeavour, which is supported by the Monetary Authority of Singapore (MAS), the Singapore Cyber Security Agency (CSA), and leading global insurance companies.

A core project premise is that robust cybersecurity solutions will most likely also require a business approach. This is especially the case since organisations may need financial or business incentives to take necessary actions individually and collectively. In this context, cyber insurance is expected to play an important role in the growing cybersecurity industry. The CyRiM project is thus developing a theoretical framework for economic analysis that should enable the optimisation of cybersecurity investment by firms and customised insurance policy. The project aims to support Singapore ambitions to become an industry centre of excellence on cyber risk.

The CyRiM project identifies two main growth areas for innovative cyber insurance products. First, a baseline insurance product for SMEs and other large organisations in order to incentivise the implementation of baseline cybersecurity measures. The basic concepts of cyber insurance need to be adapted to allow increased engagement with clients in order to ensure that they implement cybersecurity. Ideally, this should be cost-effective and inexpensive. Insurance companies should assist companies in this endeavour – otherwise, it is argued that such companies may not implement these measures. This approach is perhaps attractive to government stakeholders as a means to incentivise firms to increase their security posture. The second growth area is cyber insurance with specialised high-limit coverage for key infrastructure operators and high-value assets. The customised insurance policy should be optimised and underwritten with top underwriting expertise. Such specialised insurance products may be a good fit for an insurance market, which can be applied to specialised industry sectors and key infrastructure.

The project recognises the importance of policy relevance, and thus aims to engage with the policy communities to provide independent thought leadership on key questions. This should ultimately assist by informing the project's findings and lead to a more robust set of policy recommendations to

[9] Europol, Internet Organised Crime Threat Assessment (IOCTA), 2016, p.41.

[10] European Commission, Horizon 2020 Work Programme 2016-2017: Secure societies – Protecting freedom and security of Europe and its citizens, European Commission Decision C (2017) 2468 of 24 April 2017, p. 66. These three policy impacts are outlines as core aims of this H2020 call.

reduce risk, enhance cyber resilience and support the effective development of a cyber insurance market in Singapore. This is important given the apparent gaps in strategic thinking vis-à-vis cyber insurance in Singapore and beyond.

An informal platform was therefore established for a range of experts in a neutral forum to examine core issues and promote more informed decisions about risk and insurance. This is a meaningful contribution because the majority of attention in this subject area often seems to emanate from the insurance community. Garnering input from the global cyber policy communities, government, industry and research institutes should help to provide critical thought and public debate to establish the policy foundations for these economic and risk assessment frameworks, including how they might be applied in Singapore. The work of this group also informed the development of the CyRiM quantification framework. The working group established for this research endeavour comprises thought-leaders and stakeholders from different disciplines. A series of informal closed-door roundtables were held in the latter half of 2017 and three session reports were produced. [11] A research seminar was then held in February 2018 with Dr. Ulrik Franke of RISE SICS (Swedish Institute of Computer Science) to discuss the cyber insurance market in Sweden. Research materials were provided by the CyRiM team and fellow group members in advance of each meeting.

The United States Department of Homeland Security and Organisation for Economic Cooperation and Development (OECD) have held similar discussions. This report highlights key insights captured within these roundtables in order to provide recommendations for next steps. The working group was invited to provide additional suggestions and further feedback before publication.

The work of this group is significant given a threat landscape wherein cyber criminals are currently the most active threat actor in cyberspace, responsible for at least two thirds of registered incidents. [12] They often operate in an environment that is high profit-low risk, which means that developing cost-effective security measures that act as a disincentive for attacks and cyber criminal activity could be beneficial.[13] The World Economic Forum has, for instance, called for better private sector involvement and business solutions to counter cyber threats. [14] The Global Commission on Internet Governance (GCIG) specifically recommends that governments work with the cybersecurity industry and the insurance sector to explore funding routes and capacity building efforts that can assist SMEs in managing digital security risk for the benefit of all.[15]

[11] These reports can be accessed at: http://irfrc.ntu.edu.sg/Research/cyrim/Pages/Roundtable.aspx

[12] European Union Agency for Network and Information Security (ENISA), "ENISA Threat Landscape Report 2016: 15 Top Cyber Threats and Trends", January 2017.

[13] European Commission, Horizon 2020 Work Programme 2016-2017: Secure societies – Protecting freedom and security of Europe and its citizens, European Commission Decision C (2017) 2468 of 24 April 2017, p. 66.

[14] World Economic Forum, 2015.

[15] Centre for International Governance Innovation and Chatham House, "Global Commission on Internet Governance: One Internet", Chapter: Reducing Crime in Cyberspace, 2016, p.66.

Moreover, to address volume crimes, some law enforcement reports note that investing resources in prevention activities may be more effective than investigation of individual incidents.[16] The GCIG thus recommends that governments draft legislation for mandatory public reporting of high-threshold data breach details. [17] The group is clear that despite current limitation, risk markets can play a major role in building resilience among individual and business users, therefore recommending that businesses purchase cyber insurance to cover the liability costs of successful breaches of their systems.[18] Nonetheless, guided by the 2015 Allianz guide to cyber risk, European law enforcement reiterates that making use of cyber insurance should not result in ignoring IT security, acknowledging that the insurance industry could be an important player in setting the baseline for adequate levels of security.[19] Given such concerns about risk transferring strategies, it would be beneficial if focus within the insurance industry gravitates toward incentivising due diligence and minimum security standards. It is even hoped that future research should consider relevant market sector specificities, validating such models with relevant actors from these sectors.[20]

A central question and current research gap is how decision-makers, law enforcement, regulators, market operators and insurance companies can implement such findings.[21] The World Economic Forum notes that the extent to which the benefits of emerging technologies are maximised and the risks mitigated will depend upon the quality of governance - the rules, norms, standards, incentives, institutions and other mechanisms. [22] Cyber insurance vendors may be persuasive in promoting best practice in the corporate sector - for instance, cyber premiums can be expected to be higher if best practices are not followed like health or vehicle insurance premiums that are affected by what a policyholder does or does not do. [23] In order to address such research disparities that are pervasive globally, the CyRiM roundtables sought to examine gaps in Singapore where the governance and regulatory structures for cyber risk management and insurance are not yet robust enough to enable an effective insurance market and enhanced resilience.

Core questions were identified through CyRiM consultations ahead of the working group meetings. The first group discussion explored the current state of the field in order to frame the discussions on strategic thinking on

[16] Europol, Internet Organised Crime Threat Assessment (IOCTA), 2016, p.13.
[17] Centre for International Governance Innovation and Chatham House, "Global Commission on Internet Governance: One Internet", Chapter: Reducing Crime in Cyberspace, 2016, p.62.
[18] Centre for International Governance Innovation and Chatham House, "Global Commission on Internet Governance: One Internet", Chapter: Reducing Crime in Cyberspace, 2016, p.66.
[19] Europol, Internet Organised Crime Threat Assessment (IOCTA), 2016, p.41.
[20] European Commission, Horizon 2020 Work Programme 2016-2017: Secure societies – Protecting freedom and security of Europe and its citizens, European Commission Decision C (2017) 2468 of 24 April 2017, p. 66.
[21] Ibid.
[22] World Economic Forum "The Global Risks Report 2017", 12th edition, Insight report, 2017.
[23] Centre for International Governance Innovation and Chatham House, "Global Commission on Internet Governance: One Internet", Chapter: Reducing Crime in Cyberspace, 2016, p.66.

cyber insurance and the future development of an effective cyber insurance market. This first session further explored national market and regulatory structures in Singapore.

The next meeting continued the discussion on national market and regulatory structures in Singapore. This analysis was divided into driving questions under four broad themes, namely 1) Questions related to data; 2) Legislative issues; 3) The role of education; and 4) Risk transfer. The final meeting examined good practices and challenges in other jurisdictions using a similar framework to previous roundtables by examining questions related to data and information sharing; governance and legislative issues; the role of education; and risk transfer. The group then focused on the applicability to specific sectors such as the SME sector and Singapore's Smart Nation programme (the group previously discussed the financial sector). The group also considered the application of the evolving CyRiM quantification framework. The framework under development was informed by group insights in 2017. This group discussion provided a further opportunity to obtain stakeholders' input on the public policy implications that could arise.

Key Observations

This section outlines key CyRiM working group findings which fall under the following headings: 1) Defining cyber risk; 2) The significance of insurance; 3) Establishing the right proportion between regulatory and market drivers to foster an efficient cyber insurance ecosystem; 4) Issues related to data; 5) Education and awareness-raising; 6) Product liability and supply chain risk; 7) NTU CyRiM quantification framework; 8) SMEs; and 9) Regional harmonisation.

Defining cyber risk

Given the broad types of risks and losses, there is a wide spectrum of cyber risk. The many components of cyber risk means that it is very difficult to seek "cyber risk" cover. A key problem is the extensiveness of available products.

Cyber insurance is an integral part of dealing with cyber risk. Given the principle of risk management, an entity will accept, mitigate or transfer risk. However, insufficient discussion has been held in Singapore about risk transfer.

There is no mature model when it comes to measuring organisations' risk in relation to cybersecurity. If a CyRiM project objective is to develop a framework on the meaning of risk and loss to understand the process of risk transfer, traditional risk is static compared to cyber risk which is highly dynamic. How then can a framework be developed to provide reasonable protection while ensuring that insurers are not over-exposed? Past risks have not evolved as quickly and in such a complicated way as cyber. Nor, have they had such major implications as cyber where the scale of potential losses is in a different league to other risks faced by the insurance industry.

The significance of insurance

Both government and industry representatives would like to explore whether (and how) resilience could be increased through insurance.

Insurance could be the closest alternative to government regulation, where it could become a tool to enhance cybersecurity and incentivise entities. Key sectors, such as the financial sector, are frustrated about the level of unpreparedness and weak links across the supply chain. Any progress that can be made by government and the insurance industry to change this situation is therefore encouraged. The ability of the insurance industry to cause behavioural change should not be underestimated.

It became apparent during the consultation process for the Singapore Cyber Security Bill that critical information infrastructure (CII) owners are concerned about additional work burdens and costs. Therefore, what is specifically needed to significantly change the current situation for insurers? Given government concerns about increasing costs, how can the right balance between costs and adoption be achieved? For example, the CyRiM project quantification framework is built on a cost-benefit analysis that identifies the right levels of investment in cyber and where investment is best placed to reduce

potential risk. There could beadditional value in exploring whether the insurance industry can assist such CII owners to meet their requirements.

Among other recommendations, one solution proffered is whether some of the costs of cyber insurance could go towards tax credits. This is one example of coordinated actions that could be taken to counter cyber incidents.

Currently, there does not seem to be incentives to encourage the correct technology from the outset, and some experts argue that preventive measures do not seem to be rewarded by, for example, reductions in premium. Nonetheless, some insurers explicitly offer premium discounts for a higher cybersecurity posture.

It is still not clear whether insurance can be used effectively as a tool to enhance resilience. Risk transfer should not mean that the risk is moved around without resolving the problem. Insurance companies can deal with residual risk for those risks that cannot be controlled where the client acted reasonably. In other words the "unknown unknowns" and unpredictability associated with the dynamic nature of cyber. Preventative measures must be taken and insurance is useful for what is not foreseeable. How then can incentives for cyber hygiene be increased through a combination of market driven and regulatory mechanisms? Ideally, there could be an expectation that insurers will make sure that basic standards are met and insurance can kick in where unknowns arise and best practice has been followed. However, recent experience in other countries such as Sweden shows that there has been no reduction of underlying cyber risk with insurance (although this is a small market which may yet mature).

In the United Kingdom, some insurance companies are using the Government's voluntary cyber essentials scheme, which aims to raise security standards, as a form of certification. This means that if a company uses the scheme, the insurance company will offer a premium discount. In Singapore, smaller companies may only take these types of actions if they can see the benefit. Government may therefore need to establish some form of benchmarking.

A number of problems are associated with the possible use of such certification schemes though. For example, businesses may see these standards as end goals rather than working beyond them, or they may be used for branding the business entity. There could, however, be value in such a scheme where insurers use it to assess the insurability of an organisation and calculate premiums accordingly.

Establishing the right proportion between regulatory and market drivers to foster an efficient cyber insurance ecosystem

Some experts feel that cyber insurance products, in their current form, are not meeting customer needs. There seems to be a clear gap related to the demand side, which requires future work.

In addition, it is not clear that the cyber insurance market can mature sufficiently without some regulatory intervention. It appears that the insurance industry is not mature enough to deliver products that meet the needs of the market.

Government regulation may be required to make cybersecurity standards mandatory rather than waiting for the insurance industry to develop them. In many countries, government regulation, rather than market forces, is driving the insurance industry. Voluntary guidelines could be particularly helpful given how rapidly this field changes, although an additional push from market forces may also be needed to support their effectiveness. The right nudge can start with a cohesive government strategy across sectors.

It is still not clear whether market forces could exert enough pressure for insurers to modify their products without the need for regulation. Even where demands can be made when purchasing an IT product that security guidelines are followed by a vendor, past experience shows that government must eventually become involved. In the United States, requirements for mandatory reporting caused an increase in the purchase of insurance but it is now becoming increasingly market-driven. However, the data derived from these reporting requirements has not been particularly helpful data for insurers to develop good products. It is not clear where data is being released in a manner that helps the insurance industry to develop products. While the implementation of the EU General Data Protection Regulation (GDPR) will change the European market and perhaps make it more similar to the U.S. market for individuals, it is not fully certain how the new regime will affect the cyber insurance market. In particular, it is not clear whether regulatory GDPR fines can be covered by insurance. A question that remains to be answered is how, or whether, this will affect markets in Asia.

There is also a need for structured data because currently the regulator has not yet figured out why the data is collected and what should be done with this collected data. The insurance industry could alleviate this situation by providing recommendations to government about how such information could be made available effectively.

Another concern is that while regulation can drive the adoption of cybersecurity policies, most are then based on compliance. This does not meet the real risks of attacks. Insurance products should therefore cover risks beyond a focus on compliance. In addition, outside the 11 CII sectors identified by regulations in Singapore, many other sectors are not included.

Examples of good practices in other jurisdictions include the minimum standards of the London markets. The insurance industry in Singapore should provide more input about its needs to the Government. For example, while mandatory reporting only covers the 11 CII sectors due to sensitivities about other sectors, the insurance industry might feel there is a need to cover additional sectors.

Issues associated with gathering data

1. Insufficient amounts of data

a) Pricing and underwriting:
Given the insufficient levels of data, it is not clear how insurers can provide reasonable pricing. On the other hand, some argue that there is often enough data. For example, the amount of losses from different types of incidents is

known and can be estimated within the financial industry. The nature of damage across sectors can be assessed for what should be insured, particularly where exploits or malware on the black market can be used to predict possible damages.

From an underwriting perspective, it is possible to provide quotations without lots of detailed information. Where there is not enough information, a view is taken that the limits for underwriting be reduced. Where there is more information, it is easier to be clearer about the level of risk, what can be offered, and the best premium.

In short, in an ideal world it is better to have more data in order to determine the right price. However, there is no perfect price. As long as some basic information is available, an insurer can calculate a price for insurance coverage.

b) Significance of breach notification from an insurance industry perspective: First, the absence of mandatory reporting means that there is a lack of data. There is a need for a certain level of reporting so that sufficient data can be used to rate insurance. In the United States, however, mandatory reporting requirements did not necessarily provide useful data for insurers to develop good products. In Singapore, breach notification is only for CII currently. However, this is broader based and mandatory beyond CII under the EU General Data Protection Regulation (GDPR).

Second, where breaches are not reported, this means that consumers are not concerned and thus not yet willing to buy cyber insurance. Even where there is much attention on cyber risks, there is not a tangible sense of threat among consumers. There is a need for people to recognise that they should consider cyber insurance as part of their overall cyber risk management.

Third, there is concern about associated compliance costs and whether they could be staggered.

2. Types of data required and the purpose of collection from an insurance perspective

Assuming data can be made available, there is a need to clearly identify the types of data that are required and the purpose for collection from an insurance perspective. For example, from an insurance perspective, if the model under consideration is such that a well-protected entity is due to receive a premium discount, then the relevant data could be data for defensive measures. If, however, there is a need to understand an incident and whether sufficient resources were allocated for an insurance claim, there could be different data collection requirements.

Current cybersecurity legislation in Singapore focuses primarily on systems log data for investigations but how does this help insurers establish the right pricing? Therefore, when discussing data collection (whether mandatory or not) it is important to very clearly identify the type of data needed. Government can then be informed and the right guidelines developed.

Another overarching goal should be that the data required does in fact reduce the risk. This links back to rewarding customers with reduced premiums for hardening their resilience.

3. How and by whom should data be collected?

There could be a role for a regulator to create databases from which shared anonymised data could be obtained. A number of recommendations in other countries include data repository centres where information on incidents might be shared to enable the insurance industry to develop better premiums and policies.

It is not clear how such a repository should be designed though. Currently, there seems to be two models under consideration, namely a public-private partnership or a government agency centre. An alternative model could perhaps be designed for industry to access available data. For example, an insurance association could possibly collect the data and make it available to insurance companies to assist the underwriting process. Insurance companies should conduct their own analysis in order to determine what they are prepared to cover.

Industry representatives consider all data, from any location, as valuable (except privacy content data). Restricting it could mean missing vital information. Moreover, one of the weakest links is an entity's legacy and there can be more value dealing with this than with triage.

An additional challenge is whether organisations are in fact willing to share information in a competitive environment.

Education and awareness-raising

There are numerous gaps in understanding both within the insurance industry and among corporates from the buyside.

For corporates (potential buyers of cyber insurance), there is a need to raise awareness about the importance of insurance and why it is needed. This is especially the case given the general unwillingness to buy cyber insurance due to a lack of tangible concern about cyber threats (arguably driven by the lack of breach notifications). Another problem is that the term "cybersecurity" can be too vague. Terminology used should be more specific to be relevant. Moreover, buyers often find cyber insurance is complicated and it must be made more accessible. It does not help that insurance companies do not always understand the nature of cybersecurity which can then impact the products they are selling as well as their ability to explain these issues to clients.

Corporates should be made aware that insurance should ideally place them in a better position after an attack or loss. They should also be made aware that insurance should not be a replacement for cyber hygiene. In addition, there is a risk that companies may only buy up to those limits imposed without first understanding whether these limits are enough for their industry or business.

For the purposes of education, a suggested framing for a proper cybersecurity posture requires a combination of both cyber hygiene and the purchase of insurance. This is particularly significant given the need for scale in order to develop an effective cyber insurance market. Furthermore, the SME sector especially needs education on these issues.

Government could possibly address these gaps. The insurance industry could assist in raising awareness among clients so that they understand which risks the client should deal with and where insurance should step in.

Product liability and supply chain risk

The right model for product liability has not been developed. Product liability issues should receive more attention.

It is recommended that an additional level of regulation could be applied for product certification for import and export. Corrective measures could be considered for the insurance industry that go beyond holding service providers to standards under the Singapore Cyber Security Bill. Guidelines should deal more closely with the supply chain for product manufacturers, including possible import and export legislation on products (while ensuring innovation can thrive).

There is a counter-argument however. Although the insurance industry is global in nature and it may be able to introduce standards that benefit Singapore, the size of a smaller country like Singapore means that it may not have this type of leverage on products.

Presenting evidence of an insurance policy does not seem to provide much confidence when buyers test third party suppliers' current practices. The security practices of the third party supplier are most important to the buyer.

Organisations can only see so far down the chain when making third party assessments. It is not clear to what extent a company should be insured and what premiums should be required when there is no idea about the extent of possible damage (for example, third party software). It is currently difficult to understand potential exposure. The NTU CyRiM project is thus working with Lloyds and the Cambridge Risk Research Centre on developing cyber loss scenarios.

In the financial industry there are guidelines for management of third party vendors and due diligence which some consider proof that guidelines can change the status quo. Risk can also be transferred contractually to vendors, which brings further clarity on how risk can be measured and what risk can be transferred.

NTU CyRiM quantification framework

The Singapore-based NTU CyRiM project has developed a quantitative framework for cyber risk. One project paper quantifies how a firm's cybersecurity investment affects the residual annual loss expectancy, which is closed related to the required insurance premium. [24] The quantification framework validates the assertion that insurance discount is justified for a better cybersecurity posture. The paper also highlights the potential benefit of collective spending by the private sector in countering the growth of cybercrime, for which insurers can play a role by facilitating such collective spending.

As part of the CyRiM quantification framework, another paper defines the knowledge set for an organisation regarding its cybersecurity attack surface, including known unknowns vs. unknown unknowns, and how the

[24] Wang, Shaun, Integrated Framework for Information Security Investment and Cyber Insurance (September 15, 2017). Available at SSRN: https://ssrn.com/abstract=2918674.

production frontier can be expanded by investments in data and expertise.[25] The CyRiM quantification framework also reflects the requirement for third party security rating where, by way of example, small firms should invest more to optimise the ecosystem (even if they do not have to invest as much on their own). One way to achieve this is through business incentives such as larger firms requiring a security rating or certification from smaller firms. Nevertheless, security rating does not help the ecosystem sufficiently unless this rating is very sharp.

With adequate testing, the Singapore-based quantitative framework can potentially enable insurers to offer analytical services as part of their product offerings.

The SME sector

Discussion seems to point to tailored industry-specific insurance, which requires further exploration. Different sectors will have different requirements and different levels of cybersecurity maturity. For example, given the financial industry's mature understanding of cyber risks, it could create its own list of what risk it would like to transfer or share with the insurance industry and thus enable better risk quantification and products.

Whereas, combining insurance with cybersecurity products and solutions beyond traditional insurance could be a game changer for sectors such as the SME sector where entities may not have the funds to invest in cybersecurity and lack adequate understanding of the threats. SMEs represent a large percentage of companies within the Singapore ecosystem. Cyber insurance could play an important role in risk reduction by offering SMEs coverage for technical services such as cyber hygiene solutions, incident response or digital forensics. They are often too costly in-house. It seems that many SME owners do not see the importance of ensuring the security of supply chain components, or establishing basic information security practices. SMEs are often part of a critical supply chain impacting the stability of larger companies and major actors crucial to national security.

Government regulation could be particularly helpful for this sector. In particular, awareness raising exercises could address the gap whereby SMEs may not be aware that they need cyber insurance. Government, rather than the insurance industry, might be better placed to continue driving awareness of good cybersecurity practices.

Regional harmonisation

Multinational corporations (MNCs) generally prefer standardised legislation and guidance across jurisdictions to avoid dealing with different legislative frameworks. Furthermore, deeper harmonisation could assist such companies to assess their group-wide risk across subsidiaries in different countries. Such harmonisation can also occur dynamically where, for example, a country like Singapore adopts and showcases good practices in the use of cyber insurance to enhance

[25] Wang, Shaun, Knowledge Set of Attack Surface and Cybersecurity Rating for Firms in a Supply Chain (November 3, 2017). Available at SSRN: https://ssrn.com/abstract=3064533.

cybersecurity. Nonetheless, competition remains among countries in the Asia region where differences in regulatory frameworks can sometimes equate to competitive advantages.

Other future developments could include guidelines from the regulator on cyber exposure for more responsible cyber insurance practices, like efforts pursued in the United Kingdom. Establishing the nature of what is covered is very important, and the OECD is also examining this issue. In the wake of scenarios such as the Equifax incident, there are concerns about public protection.

NTU Cyber Risk Management project core working group[26]

- Shaun Wang, Director, Cyber Risk Management project, Nanyang Business School, NTU
- Paul Faulkner, Executive Director, Chief Risk Officer, MSIG Holdings (Asia) Pte. Ltd
- Shea Leen Woo, Partner, Insurance Industry Leader, PWC
- Vincent J Loy, Managing Director, Accenture
- Bryan Tan, Partner, Pinsent Masons MPillay
- Oleg Abdurashitov, Head of Public Affairs, Asia Pacific Kaspersky Lab
- Caitríona Heinl, Research Fellow, NTU Cyber Risk Management project
- Professor Lam Kwok Yan, School of Computer Science and Engineering, NTU
- Vincent Teo, PWC
- Simon Lawrie, SVP Cyber Security Operations, Global Information Security, Bank of America Merrill Lynch, Merrill Lynch Global Services Pte. Ltd
- Meena Chandra, Assistant Director, Asset Management and Insurance Division, Monetary Authority of Singapore
- Asha Hemrajani, former Member of the Board of Directors, ICANN
- Benjamin Ang, Senior Fellow, CENS, RSIS, NTU Singapore
- Selwyn Scharnhorst, Director of Ecosystem Development, Cyber Security Agency of Singapore
- Grace Lim, Senior Casualty and Marine Underwriter, TransRe
- Kim Swan, Regional Regulatory and Compliance Manager, Asia Pacific, Lloyd's of London (Asia) Pte Ltd
- Jim Fitzsimmons, Director, Control Risks
- Ashish Thapar, Managing Principal, VTRAC Investigative Response, Verizon
- Chan Chi Ling, Strategist, Strategic Planning & Futures, Strategy Group, Prime Minister's Office Singapore

[26] Additional government and industry stakeholders participated in some, but not all, roundtables.

Nanyang Business School, 50 Nanyang Avenue, Singapore 639798
www.ntu.edu.sg