NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE | Nanyang Business School

NTU Cyber Risk Management project (CyRiM): Roundtable series on optimal governance and regulatory structures to enhance resilience

Roundtable one session report

Prepared by Caitríona Heinl, Research Fellow, NTU Cyber Risk Management project, 7 September 2017

Project introduction

The NTU Cyber Risk Management project (CyRiM) held the first roundtable of this series on governance structures on 24 August 2017. An interdisciplinary working group of national experts was convened under Chatham House Rules to first examine the state of the field.

The discussion opened with an introduction to the group about the nature of the CyRiM project and NTU's lead as a provider of independent thought leadership. The Director of the project, Professor Shaun Wang, outlined the project's objectives. PWC Singapore is working with the CyRiM project on this part of the project's goals that relate to governance structures in order to provide additional thought leadership from an insurance and industry perspective.

Research Fellow, Caitríona Heinl, clarified that this is a collaborative project between industry, academia and government. This type of collaboration is aligned with many of the recommendations within the global cyber policy community whereby the insurance industry should ideally work closely with the cybersecurity industry. In particular, some of these recommendations call for the type of quantification research that is being examined within the CyRiM project workstreams in order to identify better measurements and robust indicators. It is envisaged that this work should further assist the public policy community in its decision-making by providing more concrete evidence given that many of these types of indicators are deficient at the moment.

Roundtable objectives

The overarching objective of this set of roundtables is to explore the gap that has been identified in Singapore (and elsewhere) whereby the governance and regulatory structures related to cyber risk management and insurance are not sufficient enough to enable both an effective insurance market and enhanced resilience.

The first session aimed to bring a diverse group of experts together at national level in Singapore in order to kick-start this process by examining key debates in a collaborative fashion. The theme of this first session focused on the current state of the field by examining the following: 1) "Framing the discussion: Current strategic thinking on cyber insurance and the future development of an effective cyber insurance market"; and 2) "Overview discussion: Relevant national market and regulatory structures in Singapore". Experts in other jurisdictions have pointed to the importance of bringing such a group of experts together over a period of years in order to jointly analyse this field and ultimately achieve successful outputs. For these reasons, the CyRiM project team emphasise that this is a process, which seeks to be collaborative and engaging so that the opinions of different stakeholders are taken into account. Thus, key deliverables of this process include building such a community of interest and producing a set of public policy recommendations.

A number of overarching themes were identified through consultations in advance of the working group meeting. It is hoped that the group would then build on these themes and identify additional gaps and questions that should be addressed going forward as part of a roadmap for this work in Singapore.

Framing the discussion: Current strategic thinking on cyber insurance and the future development of an effective cyber insurance market

The breadth of cyber risk

The discussion began with mention of the wide spectrum of cyber risk which can comprise state actors and national defence issues at one extreme, the consumer level at the other extreme, and businesses somewhere in between. Moreover, when discussions are held they can range from the very technical to public policy and regulation. A group member asked what role business can play, especially with the expected implementation of the draft Cyber Security Bill in Singapore. In New York, for instance, new regulations have been introduced for the financial sector and there is a lot happening across this wide spectrum. This begs the question – where do we start?

It seems that there is additional difficulty in this area given that the term "cyber risk" is so wide - in other words, the types of risks and losses are very broad. In the opinion of one group member, this means that it is not possible to seek a product by saying, "I want to purchase cyber risk cover", particularly with the many components of cyber risk. Real third party liability is quite extensive too and the price cannot be agreed. A key problem currently is the extensiveness of products available. Insurers are trying to scope out the basis of what is comfortable and the rest is left behind. In this participant's view, the model must mean that all components of risk become insurable.

Interdisciplinary

A group member proposed that having the right people involved in the process is important, such as the group of experts convened during this roundtable where there is representation from government, academia and industry. This therefore enables the right balance, which can help to identify what needs to be done, rather than making presumptions. Collective input will be more beneficial. Building a community of experts is key and this should also help to identify end deliverables. Another participant echoed this sentiment, observing that having a diverse group and individuals from different disciplines is important in order to garner varying viewpoints. This participant further felt that the group should be as open as possible in order to identify the best results and ideas, emphasising that this is very important to Singapore as a country. In other words, the group should aim to be objective and put personal agendas aside.

Initial brainstorming

Some key issues identified through an initial brainstorm with the working group members in order to clarify why this subject is important to their disciplines included the following: 1) Parties have insurance on a global basis and Singapore is no exception if a breach occurs elsewhere in terms of when a response is needed; 2) Some banks are being increasingly asked by customers (primarily corporates, but some individuals) for assistance given their perceived expertise in cybersecurity. Thus, the banking industry would like to provide more support but there are industry frustrations with the general status of unpreparedness and the weakest link in chains. This means that any progress by regulators and the insurance industry which will help to change this status quo for the better will be helpful, especially where there are regular IoT incidents; 3) Where public policy is concerned, there is keen interest in understanding the nexus between cybersecurity legislation and

the adoption of cyber insurance and how this relates to cyber resilience (and publicising it); 4) There seems to be a lack of preparedness from the insurance sector (across most insurers and not just underwriting); 5) There is space to understand the potential business implications and opportunities in how cybersecurity regulation and the insurance industry develop. This includes discussing the experience of experts working with the insurance industry in other countries and regions like Europe; 6) It is not clear what would happen when disputes start occurring in this space in Singapore. What can therefore be done ahead of time to ensure that dispute resolution is effective?; 7) How can insurance companies themselves be insured and protected from attack since they too are popular targets on account of the data they hold; 8) How can effective products be developed to sell to customers from a business perspective where their exposure to digital risk is increasing?; and 9) Cyber insurance is an integral part of dealing with cybersecurity risk. Given the principle of risk management, then one will accept, mitigate or transfer risk. It was felt, however, that there has not been enough discussion in Singapore about transferring risk. A key question is how can cyber insurance grow in the country, especially on account of its status as a financial centre - this requires deeper attention at a faster pace.

What can Singapore do better?

The discussion then gravitated towards the status of this field in Singapore vis-à-vis other jurisdictions. A participant explained that, in his view, thinking on this subject is so far rather advanced in Singapore, particularly since the Cyber Security Bill is quite ambitious. A key question though is how this will translate for businesses, including banks and owners of critical infrastructure. The United States Department of Homeland Security (DHS) held a similar exercise over a period of three years with insurance companies (these workshop findings were provided to the group in advance of the roundtable). However, this process hit a roadblock and does not seem to have progressed any further. The OECD is also holding discussions to examine these questions. This participant felt that this is a reminder of how much can be achieved in Singapore, perhaps even achieving more than the United States has been able to so far. Based on his observations, CyRiM project efforts require speaking to lots of stakeholders and the project is in the process of building an evaluation framework that allows different stakeholders to engage rather than speak across eachother, and to help organisations such as corporate clients of large banks to buy insurance. A key question, in his mind, is whether current cyber insurance is meeting customer demands and needs. To which the group seemed to provide a resounding no –what could therefore be done differently?

Market forces vis-à-vis regulation

Another group member observed that this then means that the question is whether this market can mature to the state that is required without injects of regulation and control. Another participant felt that market forces could exert sufficient pressure for insurers to modify their products without the need for regulation. On this point, another felt that although the Singapore Cyber Security Bill will be a boost for corporates to take action, they will be so entangled with auditing, compliance, and risk management that it is unclear whether they will have time to listen to insurance companies – unless an insurance product can help them to perform their obligations. Otherwise, it becomes even more challenging for these corporates.

From a banking industry perspective, a participant felt that they are baffled by risk assessment already, especially since they cannot even benchmark their own capabilities vis-à-vis any other peer group. He does not feel that the industry can do this and yet they must do risk assessment. While there is smart actuarial data and patterns can then be identified so it can be built like this from the ground up, how to measure organisations' posture and risk in relation to cybersecurity is still challenging. There is not even a mature model. Another expert asked whether there is hesitancy because completing a risk assessment form is such a difficult task or is it because they are trying to

take their own steps to prepare for the risk as they undertake and apply for insurance? In other words, what is the main obstacle that is causing companies to take a step back? One answer provided is that there is a level of ignorance and this means there is uncertainty about good or bad steps. A participant proffered that this seems to be consistent with feedback from insurers too, in other words it is not so much that the product is good or bad but that they just do not know. Moreover, third party risk was raised as an issue of concern given that the smallest weakness, which may not be met on a risk assessment, could apparently mean exposure to third party risk (and this can be exploited).

From an insurance perspective, it seems that cyber risk is still relatively new and as insurers "we don't know what we don't know". Moreover, it is felt that there is insufficient data so how can insurers provide pricing when they do not know themselves – historically, insurers relied on data for events that happened but at the moment that data is not available. This means, from the participant's standpoint, that the data needs to be built up slowly before reasonable pricing and cover is established. Another group member felt that in conducting a market survey, insurers' questions were intelligent regarding the sort of coverage that would be needed. In fact, she felt that it was easier to understand than health insurance. Nonetheless, there are still many gaps in understanding from both the insurance and consumer side.

A key question identified is how the right proportion between market and regulatory drivers can be established.

Product liability

A key concern raised within the discussions is that while examining products for consumer insurance, the model for product liability is not in the first place even formed. This "flow back problem" (drawing comparison with the auto-industry) is part of the problem. On this point, from a vendor perspective, regulation drives the adoption of cybersecurity policies but most are based on compliance. This does not meet the real risks of attacks though. They, too, see this as a key challenge where there should be insurance products that cover risks that are beyond solely focusing on compliance. From the position of a vendor, this is a large gap, whereby regulation drives compliance but there is still this void that technology, vendors, and regulators must fill. Currently, we are at the stage of filling this void. Citing the Petya ransomware and the Ukrainian company responsible for software development, this member asked whether there is a single approach to deal with that risk.

Another participant disagreed with this opinion explaining that compliance is not the sole driver for SMEs, rather fear drives this part of the economy. However, other group members did not necessarily agree with this position.

In relation to compliance, another participant felt that this is a weakest link game - if you know that you are complying to a certain standard, attacks then decrease to a certain extent. For example, Singapore makes sure that Windows XP is not running in the country and because nobody has this exposed technology, it then makes the insurance process clear. The percentage of known flaws can be given so that one can have the level of the degree and processes which minimises underlying risk. It is inevitable that everyone will be exposed to those new vulnerabilities that appear. Another participant similarly posited that this can never be 100 per cent – everything could be done the right way, from every perspective such as compliance, technology, processes, people and resources. Nevertheless, this can make a big difference to the nation state when it comes to dealing with the 80 to 90 per cent base.

A key question then is how resilience could be increased through insurance by overcoming some of these limitations?

Overview discussion: Relevant national market and regulatory structures in Singapore

This part of the roundtable discussions continued to explore the current state of legislation and regulatory frameworks in Singapore. The objective was to highlight further key gaps and possible solutions for analysis during the next roundtable which aims to more deeply explore these questions.

Breach notification
An expert outlined that in Singapore most industries are not subject to mandatory breach reporting. Consequently, in his opinion, the typical corporate response is to not report any incidents. This means that there is a tendency to see lower levels of incidents than what actually occurs. Nonetheless, this will change shortly and he feels that when these declarations begin to be made there will be reaction from those whose data has been breached - they will demand to know how such corporates are going to fix this problem. Currently, those who are affected may not even be aware since they are not being told. Breach notification may, in his opinion, be a game changer.

From an insurance industry perspective, the absence of mandatory reporting means that there is an issue with the lack of data. There is, from this standpoint, also a lack of fear. With experience in developing a product to sell, CEO feedback is that a cyber policy will not sell currently because people are not yet frightened enough (this is in relation to whether a product should be embedded to automatically include cyber or as a cyber policy). If this is the case, then it is not worth it for the cyber insurance company. Moreover, many insurers currently speak about the wide gap between the type of exposure they have and premiums collected. The whole point of insurance is sharing, in other words collecting a bit from everyone and paying the odd policy for those who are unfortunately hit. In his mind, this is the key issue from an insurance perspective – there is a need for enough people to recognise that they need this insurance as well as enough reporting so that there is sufficient data in order to rate it. This will then allow for the development of a product to begin and the effective building of a fund (which for all other products has been done for the last 200 years).

The next issue, from an insurance perspective, is figuring out how much of a fund is actually needed. Even though it is possible to place limits in a policy based on a fair estimate (for a larger company those limits can be rather high), it is at the same time very hard to figure out what those limits should actually be. This means that a lot of focus within policies seems to surround services since there is little value in handing over a cheque after a cyber incident. There will still be a significant problem which means that services are an important part of the policy. In his opinion, these types of services such as, among others, forensics, legal, crisis management, dealing with the regulator, and PR, are key.

Costs
Another concern surrounded issues related to costs. During the consultation process on the draft Singapore Cyber Security Bill, it became clear that CIIs are concerned about extra work burdens and the associated costs. In particular, while some may be classified as CII in an industry, their competitors may not have a similar classification - does this then affect their competitive posture? It was suggested that a good outcome would be to explore whether the insurance industry can work towards assisting these players to meet these requirements while some of the costs of cyber

insurance could go towards tax credits. This, it was suggested, would support the entire industry and be good for the country.

Another group member felt that in terms of breach notification, it is not just a case of reporting the incident. The questions then begin to flood in and this can escalate rather quickly. From a government perspective, a way to consider this type of scaling up is not just from a cost standpoint. Instead, like health insurance, something has happened which needs to be fixed and how does one find the right doctors. Whereas another participant felt differently about this point explaining that the policies contained provisions for remediation costs, services and hotlines, among other services. This participant, however, did not see incentives whereby the correct technology is encouraged from the outset in order to prevent incidents. It was felt that currently preventative measures that corporates could deploy to help reduce the risk of an attack do not seem to be rewarded by, for example, a reduction in premium.

Another question raised is whether there is a standardised way to measure and assess in order to rank products or organisations? This could provide a framework that shows where one stands. The difference between two products is such that one product can force you to update security without any choice whereas the other product allows choice but you leave it until later. In this instance, it was suggested that the premium should surely be different. In order to make this work though, there would need to be pushback on the product side so that although the product could be chosen, it would have to flow back the entire way. From a risk management perspective, this means that consideration would need to be paid to how managing your business in this manner could affect the premium. It seems that in terms of knowledge though, not all insurers are able to do so at this juncture.

Scale and risk transfer

It was then suggested that scale is needed since without this it is not clear why any insurer would become involved. By way of analogy, fire insurance evolved in the United States following fires in San Francisco. Planning regulations were developed by the insurance industry because it could not continue to insure houses that were burning down. This provides an historic example of this type of process and a process that should happen with cyber. However, it was felt that it is too early at the moment and much development is still needed. For instance, third party risk is not clear yet and from a technical perspective, it seems that very few understand this area properly.

From a vendor perspective though, one problem that the industry often faces is that, for the most part, it is dealing with the unknown. To use the above analogy, this means that this is not in fact an issue of "fire protection" but rather one of innovation. For example, there could be 300,000 new samples per day and the damage could range from zero to hundreds of millions. Moreover, this is most likely from the weakest link in the supply chain that cannot be insured against – this is the problem. It was felt that an insurance policy cannot be developed out of the current situation where there are only two types of companies – those that have been breached and those who do not know that they have been breached.

It was suggested that it could be possible to build software to self assess and governments could perhaps even deploy such software (although this must be trusted since it too could end up as a vehicle for breach). A framework would be required to explore how this would work.

From a technical angle, a key question is how risk is transferred, especially where examining cyber risk management by looking at cyber insurance as a means to transfer risk. A group member posited that the point of using insurance to transfer risk is not clear (if one does not know how to transfer risk). Rather, the key word in this discussion is risk itself – there are many risks, even unknown

risks, and as an end user of a system or a system owner, you must know the risks that you face. If you want to transfer risk to a third party, you must then know what are the actual risks that they can help cover. There are thus two sides to consider: 1) From an operational angle, what are the potential losses that an end user is going to suffer as a result of the risk?; and 2) From an insurance angle, what is the compensation that can be given if a loss is suffered? In addition, what are the components that can be compensated? If an objective is to develop a framework on the meaning of risk and loss to understand this process of risk transfer, traditional risk is more static whereas cyber risk is highly dynamic, often updating a few times per day. The question is then how to develop a framework that provides reasonable enough protection and ensures that insurers are not overexposed. A group member felt these are the types of parameters that should be examined when it comes to gaps in strategic thinking. Moreover, what kind of data is in fact needed for cyber, assuming it will become available? Another member explained that the costs and severity of attacks are examples of the types of data needed, in other words loss data from an insurance standpoint. A goal though must be that it does actually reduce the risk, and this then links back to rewarding customers with reduced premiums for hardening their resilience.

From a government perspective, given the level of malware and vulnerabilities, the question then becomes how this could be staggered (is it even possible to do so)? Industry will generally say that 80 per cent of risk comes from certain key areas, which means that measures should be implemented by such key areas with a high probability of data being stolen. One question is whether there is a way to group certain measures to provide certainty that particular protections are in place? Then, if you are in the next level of an even higher risk group, there may be another set of measures that could be taken (as well as incentivised)? This takes into account that there will always be a level of risk that is too difficult, which regulators understand and they recognise that a company could not do anymore.

In terms of transferring risk, this is just moving it around without resolving the problem. This may be unsustainable. Moreover, from a homeland security standpoint, assuming that insurance does indeed work as a framework: if SMEs, for instance, transfer risk to insurance companies, then an attacker still wins if the target is large numbers of SMEs which transfer risk to insurance companies. This is because, in this case, while SMEs are not CII such an attack indirectly impacts the nation.

Significance of insurance: Market mechanisms vis-à-vis regulation

It was felt that in an ideal market, from a vendor perspective at least, insurance is the closest to regulation outside government regulation itself. It could help to define the rules of the game by reducing premiums for example. If the insurance industry could be used as a tool to enhance cybersecurity for all industries and to incentivise entities, this would be a good way forward. However, a key issue is whether this is in fact possible. Instead, government regulation may be needed that would make such cybersecurity standards mandatory rather than waiting for the insurance industry to develop them Thus, what is the most efficient way for a country like Singapore, which is small and dynamic and where regulations are often used as drivers?

Another group member further felt that for this to be successful, the right ecosystem would need to be built to enable insurance players. For instance, they are currently seeking data and breach notification requirements that would help to provide this data. So how can legislation such as mandatory breach notification achieve this so that insurers will then become more interested in covering the community? In Singapore, breach notification is only for CII whereas it is broader based and mandatory beyond CII under the EU General Data Protection Regulation (GDPR). Group members felt that such dichotomy between countries cannot continue. Thus, with breach notification, it should drive better cyber hygiene and there will then be a need for more cyber risk assessments which will provide data, and more purchase of cyber insurance.

It was suggested that there could be a role for the regulator to create those databases from which data could be obtained. Currently, there is an ongoing public consultation on the PDPA and points related to this roundtable discussion include the following: 1) Notifications to customers and the Personal Data Protection Commissioner about loss of information that is deemed to have an impact or put customers at risk. Guidelines will be issued (e.g. financial information); and 2) Notification for cases involving scale where more than 500 customers may be affected, even if this is not considered sensitive. The group was encouraged to submit their input through this consultation. It seems that mandatory breach notification was in fact considered when the PDPA was first passed but two issues arose at that time. First, concern about compliance costs, and second, how these could be staggered.

From a government perspective, prioritising key issues is important and identifying what is actually needed to significantly change the current situation for insurers. There is generally a government worry about costs increasing too much. If cost and adoption do not move at a certain rate together then the balance could tip to the detriment of companies. So how can this be staggered to achieve the right balance between costs and adoption? From a government perspective, insurance could be a key way - if it is done the right way in order to incentivise and increase cyber hygiene.

Another member felt that an additional level of regulation that could be applied is product certification for import and export. In other words, how far can a framework go so that it is not only dealing with the front end but also at the back end for issues such as product certification? The example of automotive product recall where products have not complied was cited. The idea is that this model could lift the base in terms of compliance and quality. In addition, action could be taken against a manufacturer who does not deliver on the product that is being sold. The draft Cyber Security Bill goes some way to achieve this by holding service providers to standards. However, it was felt that there could also be value in considering corrective measures for the insurance industry that even go beyond this (including national boundary corrective actions such as a framework that ensures product quality in the first place). On this point, from a vendor perspective, the size of the Singapore market may become an issue. While the insurance industry, as a global industry, may be able to introduce standards that will ultimately benefit Singapore, the size of Singapore means that it may not have such leverage on these products.

It was suggested that there is much to learn in terms of minimum standards from the London markets. Lloyds, for instance, has been looking at data and insurance, even if Singapore has done a lot on the regulation side. In addition, how can incentives for cyber hygiene be increased through a combination of market driven and regulatory mechanisms? The role of education in increasing cyber hygiene and perhaps helping to reduce the number of claims was also suggested.

Lastly, it was felt that the implementation of the draft Cyber Security Bill and PDPA will create enormous pressure on cybersecurity professionals. Companies are struggling globally to fill this gap and Singapore is no exception. It is unclear how the system should develop to fill this gap and supplement the supply of resources that are not there at the moment (and may not even be there in five or ten years). From a government perspective, there is sometimes a danger of "seeing ghosts" when new regulations come out, especially in new sectors. This is why these public consultations are important to reach out to all stakeholders. The next hurdle will be how these new developments can be operationalised.

Relevance to the CyRiM project quantification framework

In combining these discussions with the evolving CyRiM project framework, a short overview was provided. First, groups within the United States DHS and the OECD are discussing similar cyber

insurance issues. The CyRiM project has been focusing on developing a "Singapore framework" which is being discussed within this global community. From the group's discussions during the roundtable, it seems that there is a need to do the following: 1) Consider cyber insurance rather than traditional insurance; 2) Reduce risk; 3) Identify incentives; 4) Help corporations to meet compliance requirements in a meaningful way; and 5) Take cost concerns into account. The CyRiM project is currently built on a cost-benefit analysis that is a four-dimensional quantification framework. These dimensions are: 1) Threats (such as vendor data and input); 2) Vulnerability at corporate level; 3) Impact; and 4) Network effect. The project is building mathematical models and examining the data to calibrate them. While it is using a framework, this is conceptual and every firm is different which means that one size may not fit all. In addition, it has considered levels of investment in cyber such as investing more and in what specifically. It is currently exploring how this will reduce potential risk and loss. The thinking of this group session seems to align with what the project is developing in first scanning the environment and examining whether cyber insurance is fulfilling these roles (and why not). The project can also use this group's input to assist in developing this framework more effectively.