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 three session report: **Good practices and sector case studies**

Written by Caitríona Heinl, Associate Fellow, NTU Cyber Risk Management Project

The third roundtable of the NTU CyRiM policy series was held on 21 November 2017 in Singapore. Driving questions about good practices and challenges in other jurisdictions were furnished to the working group in advance of the meeting. The first set of these questions follows a similar framework to the second roundtable where questions were split under four broad themes identified in initial group discussions. Time was allocated at the beginning of the session to allow the working group to raise any discussion points based on their analysis of the Roundtable two session report.

Theme One: Identify good practices and challenges in other jurisdictions under the following framework

1) Questions related to data and information sharing
2) Governance and legislative issues
    - For example, market forces vis-à-vis regulation - are these initiatives regulatory or industry driven in other jurisdictions?
    - Are there examples of regulations elsewhere that are already successful in driving cyber insurance?
    - Issues related to product liability; and breach notification.
3) Role of education
4) Risk transfer
    - Role of the insurance industry.
    - Are these countries promoting the uptake of cyber insurance?

The group was informed that jurisdictions could include larger countries such as the United States, United Kingdom, Australia, Republic of Korea and Japan. Countries in the Asia region are particularly noteworthy for developments in Singapore. Models in smaller countries such as Israel, the Netherlands, Estonia, Switzerland and Sweden could also be considered since their size means that they may face similar challenges as Singapore. Developments in regional bodies like the EU may have significant good practices and challenges applicable to the Singapore market. The group was asked to consider what within these frameworks could likely work (and not work) in a country like Singapore? Lastly, how can these frameworks work most effectively so that they may enhance cyber resilience both nationally and globally, thus strengthening global cyber stability?

Theme Two: Case studies - Consider how recommendations may apply to specific sectors

1) Financial sector: What are the unique characteristics in the financial sector that should be taken into account?
2) SME sector: What more should be done in the SME sector?
3) Smart Nation/Smart grid: The working group examined the financial and SME sectors at some length in previous CyRiM roundtables. What about the smart grid and programmes unique to Singapore such as the Smart Nation programme?

Theme Three: Application - Relevance and discussion surrounding the CyRiM project quantification framework

The Director of CyRiM, Professor Shaun Wang, presented the findings of his recent publication entitled "Knowledge Set of Attack Surface and Cybersecurity Rating for Firms in a Supply Chain" (November 3, 2017, latest version updates are available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3064533). The publication was furnished in advance of the meeting to facilitate group discussion on the public policy implications of these findings in order to garner practical group feedback for the CyRiM project.

Theme One: Identify good practices and challenges in other jurisdictions

1) Questions related to data and information sharing

A brief (non-comprehensive) overview of a number of initiatives was provided by group participants which is outlined below. In short, the EU General Data Protection Regulation (GDPR) is very specific as compared to other initiatives such as NIST in the United States. Group members observed that the EU GDPR and Network and Information Systems (NIS) Directive have transposed requirements for comprehensive risk assessments into the obligation for organisations to conduct data protection audits and privacy impact assessments (PIAs) in many instances. Insurers may expect applicants to reduce or limit their breach risk through implementing encryption, engaging in security audits, and deploying specific technical, administrative or other security enhancements. Australia recently introduced a critical information infrastructure (CII) law which has very strict requirements for CII and critical infrastructure assets for incidents, perhaps even the strictest requirements. Whereas in Japan, most regulation comes from ministry guidelines rather than single top-down legislation.

United States	• **Cybersecurity Act 2015** encourages private operators to share information about attacks while maintaining confidentiality, privilege and immunity from liability and anti-trust laws. Only defensive, not offensive, security measures are allowed. • **National Cybersecurity Protection Act 2014** directs the DHS National Cybersecurity and Communications Integrations Center to collect and share information about risks and incidents with the public and private sector. • **Federal Cybersecurity Enhancement Act 2016 and Federal System Modernization Act of 2014 (FISMA)** directs the DHS to implement intrusion assessment plans for federal authorities. • **Gramm-Leach-Bliley Act 1999** for the financial sector requires that integrity of data is ensured and notifications of breaches of customer information. • **Health Insurance Portability and Accountability Act (HIPAA)** provides similar provisions for healthcare organisations. • **Electronic Communications Privacy Act (ECPA)** prohibits third parties from intercepting or disclosing communications without authorisation.
EU	• **General Data Protection Regulation (GDPR) 2018** requires operators and controllers to notify data breaches to competent authorities in 72 hours and to individuals if there is a risk to their rights. • **NIS Directive** requires EU Member States to impose security requirements and notification obligations on their national essential service providers (both public and private) in sectors such as transport, banking, financial markets, health and water supply. It also requires Member States to introduce penalties for failures.

	• **Review of ePrivacy Directive and Telecom Package in progress.** Both Acts require operators providing public communication networks and telecom service providers to ensure security and notify incidents.
Germany	• **German IT Security Law 2015** requires private and public infrastructure operators to implement minimum information security standards as well as reporting obligations for suspected attacks.
France	• **The Military Programming Law** obliges operators of information systems in critical infrastructure to submit reports on cyber attacks to the governmental agency ANSSI.
Australia	• **The Security of Critical Infrastructure (open to public consultation) 2017** requires certain entities relating to a CI asset to provide information on the asset and to notify in 30 days if certain events occur in relation to this asset.
Japan	• **Act on the Protection of Personal Information (APPI).** No obligation to notify data subjects or data authorities in the event of a data security breach. However, there are various guidelines from government ministries, some of which stipulate notifying the affected data subjects and authorities.
Republic of Korea	• The Personal Information Protection Act (PIPA) became effective on 30 September 2011. • The Act on Promotion of Information and Communication Network Utilisation and Information Protection, the 'IT Network Act', regulates the collection and use of personal information by IT Service Providers, defined as telecommunications business operators.
Hong Kong	• The Personal Data (Privacy) Ordinance (Cap. 486) ('Ordinance') regulates the collection and handling of personal data. The Ordinance has been in force since 1996 but was significantly amended (notably as regards direct marketing) in 2012/13.

Another participant noted that the size of some large banks is nearly ten per cent of the population of a small country like Singapore. Such a large percentage is a material subset of the population. When discussing data and the data that a bank might strive to obtain about itself, it is close to 100 per cent as they attempt to know everything possible about their own entity. It is felt therefore that for insurance, it should be mandatory to know the full inventory of what you are getting. Data and the threat are global in nature, emanating from absolutely anywhere. This means that all data from any location should be considered good. Restricting it could mean that vital information is missed. This type of thinking should apply in the inventory side – this does not include privacy content data since it is not vital to know, only where the data is and that it is valuable. In short, for collection and scope one should try to understand everything you have in terms of inventory. One of the weakest links is an entity's legacy and it is considered more valuable to try to understand this as a risk element than trying to deal with triage. Before getting to any risks, it is good to understand how

valuable your data is and this is one of the ways a large bank might approach it (although while it is an ideal objective, it is very hard to achieve 100 per cent).

From a government perspective on data collection, this can be viewed based on what is the purpose of the collection. Since the group is, in this case, discussing cyber insurance this means that if data is collected for insurance then it is important to understand the data set exactly required to build the business capability. While the earlier group discussion mentions the need for data for defence, this recommendation would mean a rather different set of requirements. If the business model is such that an entity knows it is very well protected then the insurance model might include providing rebates of lower premiums. If this is the type of model that is trying to be created, then it makes sense to collect this type of data. However, if one only wants to understand an incident and whether sufficient resources were allocated for an insurance claim, it will depend upon what it is that you are trying to do with this data collection.

One challenge is that if you do not fully, 100 per cent know what you have, then the risk is always the bit you do not have which exposes everything. For example, CSA is looking at issuing guidance for SMEs and one of the first things organisations should do is that they must know what they have. Thus, a model could be that a company knows what it has and can provide this to an insurance company as a list and so the company then has some type of assurance. By knowing what it has, it helps an insurance company to know the coverage. However, one participant noted an analogy could be drawn whereby some might insure the driver and others might insure the car which means the model can develop in different ways.

It was felt that in terms of the mechanics and protocols, a lot of these are quite standard with well-known exceptions such as STIX in the United States and TAXII protocols that work well. Many work well such as STIX whereas a different set is being considered in Europe and the WEF. It is still more important though to know what data is being collected and to then determine what is needed. However, determining why this data is being collected is a major challenge. There are significant concerns about compliance with GDPR, for instance, where one significant obstacle is identifying the defining purpose for why data is being collected. It seems that everyone has different criteria when making this decision and these criteria are not clearly defined. This means that a data leakage could be either important or unimportant but by whose definition and criteria? It is therefore felt that determining who decides that you really need to collect that data and by what criteria is one of the first problems to be solved. The data protection authorities in Europe are apparently uncertain about this too.

If there is too much data, it can become overly complicated and so it is considered very important to define from the outset what must be collected, for what reason and at which level. A participant explained that in a competitive environment that not many organisations are willing to share information though. For example, in the case of financial institutions, while the FS-ISAC is established to share information, an entity may sometimes withhold sensitive data such as indicators of compromise even where it could be helpful for the wider community. It was thus suggested that one model which works for sharing information means that every company subject to a breach is mandated to disclose by payment forensics investigators (PFIs) with licences (which is similar to what the Singapore government is trying to achieve). Within five days of the start of an investigation, a disclosure about what happened is made to a merchant, providing immediate information about indicators of compromise and merchant exposure therefore allowing for collective measures from the payment card brands as well as the banks. Nonetheless, this is niche model and other models need to evolve. Other factors are important such as who creates the environment for data sharing; what is the context for contributors; and what are the protections surrounding collection and protection.

Another participant interpreted this section in a different manner. They interpreted this to mean data breach information that has already gone and it is not a question of choice. Instead, it is a case of what has already been leaked or a system breach even if data has not been leaked. This means that from an insurance perspective there are two sides to consider. The first side is known breaches, which encourage individuals to purchase insurance. If everything is kept quiet like the current situation then people do not feel threatened and do not therefore feel a need for insurance. For instance, when CEOs in other countries are asked whether it is possible to sell cyber policies or insurance, the answer is often no. Although there is attention on this area, there is not a real sense of threat. Thus, it is suggested that information related to an information leak or breach enables people to understand the real nature of the risks.

The other side is underwriting. This comprises determining the cost of the breach and how much it costs to repair the damage. From an underwriting perspective, it is possible to provide quotations without lots of detailed information. When there is not enough information, a view is taken that they might reduce the limits they are prepared to underwrite. Where there is more information, one can be more aggressive since it is easier to be clearer about the level of risk, what can therefore be offered and the desired premium to charge. The role of mandatory breach notification is therefore considered important, especially if this market is going to develop so that people protect themselves properly and insurance can be provided to cover where damage has already been done.

The next question to then consider is who should own the data? It was suggested that this information should be available to everyone, either through a government agency or an insurance association to collect the information, keep it confidential and make it available for insurance companies to use from an underwriting point of view. In terms of analysis, insurance companies should do their own analysis. While government bodies can conduct a certain amount of analysis to understand risk within their own countries, from an insurance perspective it is up to insurance companies to do their own analysis in order to form their own view about what they are prepared to insure. This raises another question about the right price. Ideally, the more data there is, the better it is to determine the best price. However, there is no perfect price and as long as there is enough information, the price can be calculated.

2) Governance and legislative issues

This section opened with an observation that legislating to collect data would be rather harsh and even if such legislation is in fact implemented, there must also be a benefit – for example, benefiting from others' data because of the obligation to share information. This is considered to be difficult though. For instance, it may not be in the interests of every organisation to share negative information about their own enterprise. One participant examined what is covered by insurance companies and what is not insured such as revenue loss, concluding that an entity would most likely want to keep this part under wraps from customers to avoid negative repercussions. The question then is how can one get around this?

When considering other jurisdictions, it is noted that in many countries, government and regulators are driving developments in this space. In other words, the insurance industry is being driven by government regulation rather than market forces. In the United States, for example, the group previously observed that once legislation was implemented, insurance sales rose. However, it is still not clear whether the cyber insurance industry is mature enough to deliver products that address the needs of the market. This includes whether SMEs are even aware that they need cyber insurance. Nonetheless, the group finds that once legislation in place, while it may not be directly enforcing cyber insurance, where it identifies some use for companies they will suddenly seek insurance. In addition, the power of the insurance industry to cause behavioural change should not be

underestimated once it decides to apply rules. Other countries in the Asia Pacific region apparently promoting the uptake of cyber insurance include Hong Kong, which is most likely pushing for key industries rather than across sectors. One member noted that there seems to be more active marketing of cyber insurance in Hong Kong than in Singapore.

While some felt regulations truly drive the market, others remain sceptical that regulation does in fact make a difference. They explain that, in their experience, CISOs may have minimal compliance requirements where there is no legislation or regulations and even if there are guidelines, they are only a tick-in-the-box to meet minimal requirements. This means there is a gap because security is only as strong as the weakest link and some industries can be used as launch pads for attacks on other industries. Thus, in the case of Singapore, while 11 CI sectors are identified under regulations, many other sectors are not included.

Another member noted that regulations are required to overcome short-term thinking where reporting and sharing data has a long-term benefit. The group felt that anonymising collection would be helpful, which is apparently the principle followed in practice. From a government perspective, there has not been much input from the insurance industry for the current Cyber Bill in Singapore. If the industry finds that these recommendations are a way to help then it should lobby Government and provide input, particularly since current thinking only covers mandatory reporting for CII incidents due to sensitivities about other sectors.

One question posed included how the Government can do mandatory reporting anonymously and how can this be achieved because of the trust issue. It was suggested that perhaps insurance companies could be trusted because there must be a payout, which is a benefit, and so the breach data can be aggregated by an insurance company anonymously. While CII cannot escape because of investigation, what about the rest of the market? There currently seems to be a soft approach because of an unwillingness to come across too strongly in non-CII sectors. Nonetheless, if industry feels there is an important need for the Government to move in that direction, it is possible (even where no industry is currently doing so). It was noted that the CyRiM project members did provide input to the recent CSA and PDPC consultations, which included good input from the insurance industry and recommendations to focus beyond CIIs.

One member noted that it could be possible for an insurance company to do the disclosure and that could become part of the policy that data is collected directly which could make sense for small companies. In other words, there is a contract with the smaller company submitting data and regulations on aggregating such data in order to deal with the weaker links of these smaller parts of the market while CIIs will have the best defences in any case. Legislation in the United Kingdom is regarded as good practice on active cyber defence controls. Eighty per cent of attacks can be safeguarded by active defence so that government takes a stronger role for all industry across all sectors. It is felt that, at a minimum, active cyber defence controls should be in place for most attacks and the remaining 20 per cent can be tackled with regulations and other initiatives. For active cyber defence in the United Kingdom, the scale of government involvement is outlined, including what it can do when working with large telcos, IT companies across industry sectors, what they can contribute and what government can do to help these companies to protect the nation against mass and scaled attacks (not only on CI sectors but across sectors). Australia is trying to adopt this approach and the United Kingdom is strongly advocating it as good practice.[1] It was

[1] For more information, please see

a) https://www.ncsc.gov.uk/news/ncsc-rolls-out-free-and-easy-steps-improve-public-sector-cyber-security-0

b) https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk:

noted, however, that this works in the United Kingdom on account of Directors' negligence and personal liability clauses. In order to protect themselves, Directors must be very clear about their defensible position. This link to individual liability supports the success of these initiatives by ensuring that a company Board must ask questions such as "what is the preventative position for cyber risk"?

Another member felt that the issue for the insurance industry collecting data is not necessarily the insurance claim. It is the primary responsibility of Directors to look after their company and ideally they should not need insurance if they have taken the right security measures in the first place (using the lock the doors analogy). The insurance side should only kick in when everything else fails, in other words the risk transfer part for the measures that did not work. The house insurance analogy is useful to show that if certain types of locks are purchased, discounts in premium are provided since all parties benefit. This should, by extension, be a logically similar approach for cyber protection. However, there may be a certain amount of attacks that do not cause loss of data or breaches which should be reported but do not reach the insurance company. This means that this issue can feel somewhat circular and thus exemplifies why government action and legislation on reporting may be essential (ensuring that if reporting is to occur, that the form of government body is a safe institution for the collection of data).

When the group considered whether any other insurance model went through a rapid maturation of risk assessments and premium discounts, the general experience in the insurance industry has been a realisation they got it wrong in the early stages and more data was needed to then figure out best practice. Generally, insurers do this themselves rather than through legislation. This is a gap raised in a recent ENISA report which identifies variation in the ways insurance companies work and the lack of standardisation or harmonisation [ENISA, "Commonality of risk assessment language in cyber insurance: Recommendations on cyber insurance", November 2017]. Nevertheless, there is no harmonisation across other risks either.

In response to a question as to whether legislation would break the model in the way insurance works such as the freedom to decide how to assess or discount, one expert could not think of another example where this has occurred before. In their opinion, the reason is most probably because other risks did not evolve as quickly and in such a complicated manner nor did they have such huge implications as cyber. This is a very specific type of risk and all other types of risks evolved over many years. The only equivalent could be Director and Officer (D&O) insurance where many argue that the current status of cyber is where the D&O field was ten years ago with professional indemnity insurance. Nevertheless, the scale of potential losses in this field are still in a different league which makes this is a unique area and different to other risks faced by the insurance industry in the past. Even where there is legislation that mandates D&O insurance, it is still different given the scale in the field of cyber. For example, a Director may be held responsible for several people following a failed M&A or equivalent, but thousands as well as the general public could be affected in cyber.

Is there then a counter-argument that market forces should decide this so that where insurance companies have lax minimum requirements, they will begin to raise their standards following events? Some members felt that this could, and possibly should, happen but while insurance companies are going through that period they offer very limited cover which may not be sufficient.

---

c) https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/NCSC%2010%20Steps%20To%20Cyber%20Security%20NCSC.pdf

d) https://www.ncsc.gov.uk/guidance/10-steps-executive-summary

In relation to the financial sector, it is felt that guidelines issued by MAS are important, particularly since they may often reflect future legislation. These are considered helpful especially in an area that is changing rapidly to allow the regulator to signal companies as much as possible. Thus, instead of legislation, guidelines would be very welcome, in fact critical, where government could develop voluntary guidelines for companies (such as six items that tackle 80 per cent of the risk).

For other sectors, however, one participant noted that guidelines, such as the NIST framework, exist but organisations are not taking action. The group noted that this framework is not specific enough for SMEs and the language is too complicated. Australia has a data essentials scheme which is good if taken seriously. However, research apparently shows that it is not being used by small, large or even government organisations. Only a minor proportion is doing so and this shows that in addition to guidelines there is still a need for some type of enforcement, unless market forces can drive this instead. One member felt that unless this becomes a unique comparative advantage for a company, they are not hopeful about the effectiveness of guidelines. Their effectiveness will depend on who issues them and even then a push will still be needed. On the other hand, another member explained that where guidelines and initiatives such as cyber essentials schemes are integrated that the industry would begin to take a concerted approach, whether through insurance or business contracts. This will eventually scale. The United Kingdom is providing good practices to surmount these challenges. In the United States, while legislation kick-started the purchase of cyber insurance, it is becoming increasingly market-driven. For example, SMEs may require insurance in order to obtain contracts. Smarter SMEs are also asking how they should be protected. In short, this model started with legislation and it then became more market-driven. Guidelines are thus not useless and it is better to have them to avoid a vacuum. Market forces could be the push that is still needed behind guidelines exemplified by smaller companies needing insurance if they are to bid for a contract. This nudge can start with a cohesive government strategy across sectors.

In addition, products can eventually be measured against guidelines, thus enabling feedback into devices. While a guideline might not make sense to a consumer of insurance, it can tell manufacturers how to potentially measure these criteria. Although, this is a rough measurement, manufacturers can then market these products with this value proposition.

Regarding the use of cyber essentials schemes, some issues were raised such as 1) Would this increase costs in the supply chain and if so, is this trade-off worthwhile; and 2) Should these criteria be imposed on your supply chain for day-to-day efforts? There is concern that there will be a big difference between medium and large companies as compared to SMEs. For instance, this will be a pure cost for SMEs whereas it would offset the costs of larger companies because it will mean less monitoring and supervision of technology adoption. While an element of this could be a way forward, difficulties with implementation of these schemes in the United Kingdom were highlighted. The vast majority of companies declare that they have met these standards but there is no check. The way in which they are implemented incentivises the certifying authority to only conduct a paper exercise without a corresponding increase in security. How then can these companies be brought to a higher standard? They argue that there is only so much that they can do and it is likely that the EU GDPR implementation in 2018 will act as a stick so that companies must provide honest declarations. In addition, there are problems with the current system of subsidising cyber essentials through the lottery system. Some feel that the current limitations of these schemes mean there is no real added value at this point (although it also means that there may not be real cost increases for SMEs). Nonetheless, if it is important to make a real difference, there will be cost issues and will companies that are part of the supply chain be agreeable to this additional cost? If so, this is a useful finding. Moreover, if companies were willing to pay such additional costs, why are they not doing so already? It would be helpful to identify what is currently impeding this situation. One member explained that, currently, if a large company requires an SME to complete a 20-30 page form they will just sign off where there is nothing underpinning the form.

Industry-wide benchmarking around business continuity plans, information sharing, and governance were raised as an option if there is no element of enforcement. It is not clear whether there are examples of this being done well. There are some systems which are supposed to achieve this and to aggregate the information to develop a scoring system similar to S&P ratings. However, benchmarks might work better for those customers who care about these ratings or have their own customers who care.

Lastly, while the legislation outlined in the first section highlights regulatory initiatives, rather than industry-driven actions, they can boost fast development of the cyber insurance market. And this in turn can have advantages beyond governmental regulation. In addition, the common feature of the main cyber security/data breach notification laws is that they set baseline security information requirements without making particular standards obligatory for industry. Such laws should in fact require higher cybersecurity resilience (including comprehensive risk assessments, data protection audits, privacy impact assessments), thus creating greater demand for cyber insurance coverage. In other words, government regulation results in an emphasis on meeting basic minimum standards, whereas insurance results in companies striving to adopt and improve upon best practices.

3) Role of education

Another member felt that cyber insurance is not an education provider and this should be kept separate, thus education on insurance could be useful. Even if cyber insurance companies are inadvertently educating by the fact that completing a policy is educational and increases knowledge through the requisite assessment.

4) Risk transfer

One member felt that cyber insurance is not a silver bullet to the many challenges companies, citizens and regulators face in cyberspace. Cybersecurity regulation on its own will likely result in insurance industry growth, but the interdependency between a growing cyber insurance market and enhanced cyber resilience of the nation is yet to be determined.

Mathematical risk-modelling is certainly an area to consider for the better balancing of costs and benefits of enhanced cyber protection. But ultimately, it is the development and evolution of the market and accompanying public-private cooperation mechanisms closing the gaps in capacity, knowledge or resources of different parties that will determine how resilient, responsive and flexible the country is going to be in dealing with cyber threats.

Theme Two: Case studies - Consider how recommendations may apply to specific sectors

1) SME sector

A member observed that the group seems to agree that many (if not most) SME owners do not see the necessity to ensure their security of supply chain factors, or establish even basic information security organisational and technical practices. The widespread belief that SMEs are too small to be attacked is in fact strengthened by their numbers, where each time a small proportion of SMEs is hit by a widespread malware outbreak. SMEs, often part of a critical supply chain, can destabilise major actors and larger companies which are crucial to national security.

SME inability to interpret technical threats, or incidents, as massive business risks, and the lack of capacity to respond to those, leads to greater vulnerability up and down the supply chain. Reducing

these risks through 'SME cyber certification' initiatives or more rigorous compliance in the procurement process of larger firms, creates its own set of challenges – being non-conclusive in the first case and prohibitive to competition in the latter. This is where cyber insurance may play a critical role in risk reduction by offering SMEs coverage for added-value technical services, such as incident response or digital forensics that would be too costly for most SMEs in-house. While SMEs will likely prefer standardised cyber insurance, the additional coverage for third-party liability, data restoration, litigation and other costs may help to create a more level field for SMEs supplying services to the largest enterprises and CIIs.

This is where a group member feels educating SMEs matters most - raising their cybersecurity and cyber insurance awareness, sharing knowledge on best practices and incentivising risk management approaches to cybersecurity among the smaller firms. Whether this should be driven by insurance companies themselves is an open question, and in Singapore the government continues to be the driving force of the wider awareness and adoption of good cybersecurity practices; including a range of existing initiatives (such as SMEs Go Digital).

Particularly in relation to SMEs, every risk cannot be prevented and there will always be a breach in which case insurance companies should make sure that there is quick prevention. Government similarly thinks that insurance has a role to play. In addition, moving SMEs to the cloud is recommended where cloud providers often have more capacity than governments in terms of protection. However, there is a need to reform the concept of split responsibility so that these providers take full responsibility for their service. Moving to this type of model needs more analysis, particularly since it is not enough to say that being on the cloud is sufficient given that there will still be residual risk. This means that there is still a need for insurance which should be addressed in future.

Another member felt that product liability issues have been under-discussed and a country can have a major impact on corporations (for example, recent developments in Germany and the EU). While Singapore may be a small country this does not mean that it cannot require standard product standards which can make a big difference on the overall risk position. At the end, it comes back to products and by way of example, is the cloud that Singapore SMEs use a standard that the Singapore government approves or a global standard?

2) Smart Nation/Smart grid

A member of the group observed in previous roundtables that there is some correlation with the current work of a World Economic Forum (WEF) working group and the CyRiM group. The WEF group has a similar framework to the approach that has evolved throughout the CyRiM policy discussions. This includes: 1) Governance and incident response; 2) Information sharing; 3) Role of the insurance industry; and 4) Liability.

The WEF working group similarly comprises participants from the insurance industry, public sector, technology companies and infrastructure providers brought together to consider building resiliency against risks, with particular emphasis on CI and the smart grid. The first workshop discussed guidelines on risk governance, incident response and the role of the insurance industry – questions similar to the work of the CyRiM group.

Key observations relevant to the CyRiM project include the following:

a) Information sharing

The WEF might experiment with a cross-border information sharing platform. However, there are some concerns around the design principles for this platform, which are similar to some of the questions discussed within the CyRiM session. For example, trust issues where it is not certain who

should be in such a community of interest; how should an information sharing platform be designed?; and what is the underlying architecture? The closest model could be a United States Department of Energy cyber fed model which is community-based for real-time sharing of threats. This is relevant given CyRiM discussions about the purpose of data sharing and what types of data would serve that purpose. The CyRiM discussions in this session seem to be more relevant to analytics for insurance and how premiums based on past incidents can be calculated whereas the WEF has been more focused on real-time dissemination of information to prevent further cyber threats from doing more damage. In addition, some design considerations include ownership and who should own such a platform given that this owner would decide what information is relevant, how information would be shared and permission to access information. The "poison in the well" phenomenon was also discussed whereby competitive corporate behaviour could sometimes lead to deliberately contributing misleading information. A question posed to the group is whether insurers could have access to such information sharing platforms and whether they would benefit from them.

b) Risk management
It was noted that two main ways to manage risks include standards and benchmarking. Key limitations for standards include 1) Enforceability and who will be responsible for such enforcement. If a State is responsible, there may be a high chance of enforcement but it is not certain if this is the case with industry associations (or similar initiatives). At the global level, should it be the WEF or a similar body?; and 2) Do standards motivate risk reducing behaviour? Whereas for benchmarking, there is a rating for different companies akin to a badge that says "cyber secure" and this could prevent further attacks by reducing attackers' incentives.

c) Liability
A question posed included how liability can be apportioned between the private and public sectors to ensure sustainability of CI. There are different frameworks such as the "waterfall approach" to liability where, in the first instance, the infrastructure provider is liable to the point of bankruptcy and there might be groups (in industry for example) that have pooled insurance funds. The public sector would be the last resort. However, it is contentious as to whether the public sector should be the last resort given recent past experience in the financial industry and the desire to prevent moral hazards.

Group discussion on the above observations noted that while there is support for global sharing platforms and there is space for insurance industry involvement, it is not clear in the foreseeable future whether institutions will share data. There are no other platforms, except security service providers (which do not share information since they collect information). There is scepticism as to whether there would be a platform between certain countries in the near future. Moreover, for the markets, would certain laws be breached by such sharing? Even though global platforms are important, it is felt that national legislation or industry standards are more important. Another member took a different view explaining that there is already much information sharing, albeit mainly on an informal basis between CERTs. A global platform could thus help. However, this would most likely be sharing information limited to a certain response and dealing with the threat.

It was noted that the only Asian WEF member countries are Japan, Singapore and India. Another obstacle highlighted is the challenge associated with different types of commercial interests. From a commercial perspective, there will be a desire to share the data set and to then produce one's own set that is better. Commercial value comes from that delta and the ability to respond faster than others. Data is also of commercial benefit so if a corporation is confident of its fast response time then it would not likely be hesitant to share as long as it provides you with more data. However, if a corporation has a slower response time this means that even if they can obtain the data they cannot respond fast enough in which case it does not hold the same value. Another issue is who is withholding data?

Theme Three: Application - Relevance and discussion surrounding the CyRiM project quantification framework

Professor Shaun Wang in his presentation to the group noted that the insights from the CyRiM policy group assisted by connecting this academic product to practical issues. This academic paper builds on the literature from leading scholars and while it does not specifically mention insurance, it will have application in insurance. The "knowledge set" is a new concept since it first aims to quantify a firm's level of knowledge of cybersecurity.

The paper presents economic models of cybersecurity investments by a firm, first considering the cost-benefit to the firm itself, and then to the eco-system of a supply chain. It introduces a concept of a firm's *security knowledge set* of its attack surface, relative to the universe of threats. It proposes three classes of security production functions as the frontier curve of a firm's knowledge set. It distinguishes two types of security investments in acquiring data, information and expertise vis-à-vis deploying defence measures and detection tools, and derive formula for optimal allocations. It analyses cyber breach propagations between firms in a supply chain, and demonstrates that large firms requiring contractors to show security rating by third parties can be an effective way of reducing information gaps in a supply chain. It presents a model for the reliability (sharpness) of cybersecurity rating for firms, and shows how the perceived reliability of cybersecurity rating affects the incentives for firms to increase their security investments.

One graph was used to illustrate a knowledge set, which can expand or contract, depending upon the different types of knowledge of the firm about what it knows. Such knowledge includes every aspect and step of cybersecurity such as staff, system vulnerability, cyber defence and detection. The knowledge set is a relative concept where, for instance, a large bank has a very large knowledge set but an SME is much simpler. There can be benchmarking (for example, by type and size of the firm) of knowledge set whose elements in practical terms could be a practical guideline of what one should be doing. The knowledge set should be dynamic in nature. Thus, an important starting point is to quantify what is known by the firm and what should be known. Some of the mathematical curves show what action to take and how much risk is reduced.

The second main point in the paper is that it outlines two types of investment. First, investment in knowledge. Second, investment in action (such as detection or vulnerability, prevention tools or emergency response). For example, a firm can expand the knowledge set by hiring talent. After investing in knowledge, a firm can invest in concrete action. Another graph was presented. One of the axes quantifies where to invest and whether this is in knowledge or action. A mathematical result shows there is an optimal proportion to be invested in knowledge and action, and if this rule is not followed then the entire cybersecurity investment wastes a lot of money. This mathematical result is similar to the Nobel Prize Cobb-Douglas theory on optimal production.

Mathematical curves are proposed to quantify the reduction in cyber breach probability through investment in security measures. A CyRiM member reemphasised this key point about the starting point - that if nothing is done, then a cyber breach will surely occur given an attack. Well known academic papers previously started with zero investment but Professor Wang starts with some benchmark amount (if there is no investment, there is a probability of one of cyber breach given an attack). Without using a ratio to some benchmark for the quantification though, the security investment amount could go through the roof for large firms.

While this paper only outlines two dimensions of security (namely, prevention, detection), a third dimension from a security perspective (namely, incident investigation and response) can be

incorporated. Professor Wang observes that many firms are not benchmarking or investing along the frontier, and by using this model they could derive optimal level investment.

The second part of the discussion focused on the supply chain since the first part relates to one firm and this can be expanded to the supply chain. A simple example is such that one large firm has eight small firm contactors (the same approach can be applied to a more complex supply chain). For a large firm, the attack surface will increase with one additional contractor and even though this firm might know its own inventory, it does not know the contractors and this is a knowledge gap. Thus, it is important to quantify this gap when new contractors are added. Ways to improve the expansion of the knowledge set is to require more firms to have certification or rating. The paper reflects this requirement for third party security rating. By way of example, at the ecosystem level, small firms need to invest more – even if they do not have to invest as much on their own, to optimise the ecosystem they need to invest much more in cyber security. One way to achieve this is through business incentives such as larger firms requiring a security rating (certification) from smaller firms. This seems likely going forward because large firms will gradually ask for security rating.

The next level of discussion is then the mathematical model for security rating. A basic model called the Gaussian copula model can be applied by translating cyber breach probability into sigma value. This paper shows that unless the security rating is very sharp, the whole ecosystem is not helped very much by security rating. Thus, the sharpness of security rating must be improved. If this is done, then large firms can ask small firms for certification and can then show mathematically how the welfare of the ecosystem increases. These findings relate to earlier group discussions that some security rating does not really add much value which means there is a need for better quality in terms of how to rate companies overall.

While this academic framework is cutting-edge in academia, a key obstacle is how to translate the findings. Professor Wang made a number of proposals to consider based on the group discussions. The CyRiM project considers how to bridge the gap between the buy and sell side of cyber insurance. The buy side identifies that issues will be better managed for SMEs where there is a knowledge gap and benchmarking and incentives are used for this. It seems that hurdles so far include the fact that buyers are not convinced about the value of insurance, and that there is a need to both reduce risk and transfer it. This means there are two parts.

Next, while the paper does not touch upon this concept, in terms of application there could be value in proposing a standardised insurance policy like the guidelines for some sectors or by industry. The market could then compete for the price and quality of service. Such a policy could cover risk prevention and information sharing which means that it is relevant not only for insurers but for InfoSec companies.

From the supply side, a key point previously raised in CyRiM policy sessions included the concern that economies of scale are needed for policies because it is not economically viable to only have a small number of insurance contracts. A specific question then is what should be covered by such a standard insurance policy? It should be integrated with the prevention and liability side (the liability point is key especially in a complex network such as a supply chain framework). Similar to the concept of apportioning liability within the WEF working group, the CyRiM project had floated a comparable idea for law firms to provide legal analytical services to determine appropriate limits. These cannot be too high or low and should be formula driven when determining who is responsible and for how much. By doing so, it could reduce much friction.

Lastly, an insurance pool for insurance groups could be considered. For example, the SME sector is promising and perhaps there is a role that insurance companies should play as well as Infosec firms.

A number of points were then raised in the group discussion. First, there was a query as to whether there would be a market for aggregation to aggregate risk through part of the supply chain. It seems that this is not normally for price volume but for risk reduction and breadth.

Second, regarding the concept of a standardised policy, would this be feasible for SMEs since it is not clear that there should be standardisation for large firms. And if so, how could this be kick-started? One member felt that insurance companies would not like this concept since insurers may have developed their own cyber insurance policies. However, they often use standardised clauses. They would most likely prefer to keep separate the manner in which they design their insurance products. In addition, they would want to ensure that advice given to a customer to protect themselves and the level of service provided if something goes wrong remains individual to the company. These are examples of the factors that companies would use to compete and they would thus prefer to not see too standardised a policy (outside standardised clauses).

Professor Wang nonetheless feels that while several cyber insurance policies are similar, there is always some variation that is not well understood by consumers. He thinks that consumers may form insurance pools to ensure value. It would benefit insurance companies to show a new way of generating value - they are only facilitating protection and so an insurance company and information security company could add value by adopting a different model to the traditional insurance. While many insurers are not comfortable with this concept, academic thought leadership points in this direction. Except for workers compensation in the United States, there does not seem to be examples of standardised insurance policies in other areas. Nevertheless, others still feel that in terms of practical application, competitive advantage would mean it will always be difficult to not have some variation. It was therefore proposed that “simplification” could be a better way to describe this concept which seemed agreeable to the group - whereby there is simplification and certainty of some coverage. In other words, the actual services could be standardised with a certain policy and within this policy there would be some variation.

Third, there was an observation that breach data is still needed. The counter-argument is that this is not certainly the case since this is not always a data issue for insurance companies. Insurance companies can ask for lots of data but using lots of data does not mean obtaining a magic price. For example, some insurance underwriters for cyber insurance explain that that they do not need that much data, even where others may believe that they need a lot of data. It is a business decision and they need some key information rather than total visibility of the data. Another example provided is practice in Australia where some insurance companies are only focusing on SMEs without any data, calculating risk based on a questionnaire and some information. They are building the data set incrementally along with SMEs and therefore improving calculations.

In terms of economies of scale, while this is ideal, it would mean that only three insurance companies would do everything in Singapore. There are approximately 35 general insurance companies in Singapore, which is too many to achieve real economies of scale. However, it was suggested that to stitch this proposal together, in terms of insurance pools there could be a blend of two or three of the big companies providing basic support to those selling the product.