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 two session report: National market and regulatory structures in Singapore (part two)

Prepared by Caitríona Heinl, Research Fellow, Nanyang Business School, NTU Singapore

The second roundtable of this series was held on 28 September 2017 with an aim to more deeply examine several themes discussed in the first roundtable. Driving questions were furnished to the working group participants in advance of the meeting. They fall under four broad themes which are outlined below. Several questions expand upon the first session's discussion because they require deeper group analysis, and some questions were specifically raised by group members after the first meeting.

Theme one: Questions related to data
Are breach notifications a key driver for the insurance market? How important is the data really?
What is the role of mandatory breach notifications?
Which countries are implementing data breach mandatory report or notification requirements?
Who should own data that has been collected?
Who should analyse the outputs from various sources?
What is the role of information sharing to allow insurance companies establish the right pricing?

Theme two: Legislative Issues
Are legislative changes required?
Would guidelines be useful? If so, what kinds of guidelines?
What should these guidelines contain?

Theme three: Role of education
How important is education to support these developments?
In what way will it help? How important is improving the understanding and education of buyers to explain what they should do?
What types of initiatives could be considered that would have real impact? To whom should they be directed?
For example, how can education and understanding of buyers be improved to explain what they should do to protect themselves first before finally opting for the residual risk transference to the insurance company?

Theme four: Risk transfer
Is opting for insurance on its own the best (or worst) option?
What should be done before buyers opt to transfer risk to an insurance company? Should insurance be a last resort in case something happens after other protective steps have been taken?
What is the role of insurance companies providing premium discounts if such earlier steps are taken?

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 one session report. The discussion first focused on some of the background reading material provided to the working group in advance of the sessions. The article on the cyber insurance market in Sweden [Franke, 2017] was raised as an interesting case study in another jurisdiction where it seems that those claims which were actually made were to offset response costs rather than reduce risk. This means that there is a market where some insurers do not care about the cybersecurity posture of an organisation (the insured). Other insurers require a type of attestational form where they may even end up refusing insurance. It seems that the market has no standardisation and yet premiums are being offered. This means that there is no reduction of underlying cyber risk with insurance. In other cases, insurance could not be obtained without some basic practices but the overall effect of this is not clear. Nonetheless, this is a small market which may mature and so the question for experts in the Singapore working group is how to avoid these problems and to think ahead so that this becomes a more virtuous cycle in the near future? The next roundtable is due to explore in more depth good practices in other jurisidictions (as well as pitfalls) that could be applicable to Singapore.

The second point raised by a participant with experience as a buyer from a large corporation is that where third parties are supplying such a buyer, they are tested for their current practices. Where they sometimes present evidence of an insurance policy, this does not provide confidence for the buyer. From the buyer's perspective, whether a third party is insured or not, it is what the third party supplier is doing security-wise to ensure that data will not be lost which is important to a large company. Another member agreed that in examining the control and transfer aspects of risk that insurance can provide reimbursement after an incident but it does not bring back reputational damages. These members thus argue that it is preferable to have measures for control to avoid irreparable damage and a way to benchmark (ways to benchmark were discussed in the first roundtable).

In relation to SMEs, the provision of cyber insurance with providers of cybersecurity beyond traditional insurance could be a game changer. This is especially the case where SMEs may not always have the funds to invest in cybersecurity but they have a very important role in the broader ecosystem. They may, for instance, be part of the chain of sourcing and servicing for critical information infrastructures (CII) or other large companies. It was felt that combining insurance with baseline security products or solutions is where there is space to change the game. Moreover, the cyber insurance industry can obtain better insights into events so that it can then adjust premium accordingly.

A third point related to the role of government and what might be unique about Singapore where the Government may have a bigger role than in other jurisdictions. Reasons for this can include the size of the country, a traditional government role for stronger intervention as well as high levels of overall regulatory efficiency. Fourth, a member raised questions about propositions globally for data repository centres where information and data on cyber incidents might be shared to enable the insurance industry to better develop policies and premiums. This is based on industry arguments about insufficient amounts of data. It was observed that while this sounds like a good idea, how should such a repository be designed? If it is a public-private partnership (PPP), what are the incentives for companies to join? How should they be incentivised? If it is a government repository, what is the basis for this and how can the quality of data be ensured? It seems that two models are being discussed, namely a PPP with government and a government agency centre. However, how might other models develop that will allow industry to tap into available data?

Lastly, the 2017 Kaspersky Lab report on "New Technologies, New Cyber Threats" within the group's background reading material shows that, within the financial industry, the amount of losses are known from different types of incidents and they can be estimated. They might be large but they are not so dramatic and this is, in the opinion of a participant, a manageable risk for most typical incidents that can be expected.

Theme one: Questions related to data

In order to better frame the discussions and provide more context, the CyRiM project is broader than insurance in scope. The project framework has a more holistic approach to cybersecurity. Thus, in terms of meaningful discussions about data, there is a need to be clear about the purpose of such data, what data exactly should be discussed and how to work with it. One driving theme for the CyRiM research is quantification and measurement based on the premise that without measurement there is only rhetoric and no concrete achievements. In terms of the economics of information security when it comes to data, the following should be examined: 1) What are the threats, in other words threat intelligence data; 2) Incident reporting; 3) Data on vulnerability and what can be done to improve vulnerability; 4) Data for turning incidents to loss (direct and indirect such as third party and legal losses). In addition, it is not clear whether data is actually shared and how it is used. A group member felt that focus should rest on one aspect of data, suggesting intelligence data.

The information set is, however, limited. Another member felt there is a multitude of questions, including who owns the data and how it should be collected. This member suggested that the data that should be considered includes: 1) Incidents; 2) What breaches?; and 3) What recoveries or actions are being taken and what is the cost to carry out such recoveries? In other words, there are three layers of data types needed for insurance providers to know what kinds of products to design and how they should be priced. Another member added preventative measures taken prior to breach and the level of protection existing at that time.

While cybersecurity is on everyone's risk register and it is clear that the likelihood and impact of a cyber incident is high, one member highlighted that little is in fact done to counter this problem. In their experience, the term "cybersecurity" is too nebulous, it has little meaning and relevance to clients' business, and clients do not really understand it. Therefore, it is better to discuss clients' business processes and the most important parts of their business so that cybersecurity can be developed from there. In their opinion, this means that when thinking about the data and what can actually be affected, a taxonomy is highly important in deciding how to prepare for events in the security architecture as well as response and recovery. A taxonomy should be the first step in order to classify data. This will avoid situations where companies activate their insurance policy for a cyber incident but it is not a cybersecurity problem. An agreed-upon taxonomy means an organisation will know how to respond for a specific type of event which will have associated controls. If an insurance company wants to examine the kinds of risk being taken on, it can then see these controls.

Another member felt that a challenging question is requiring mandatory reporting where, without peer review, insurance companies never see the full landscape because disclosure may not need to be made to an insurance partner. Banks must do so because they are regulated, but it was felt that this information is important for wider industry in order to assess overall risk.

Mandatory reporting requirements in the United States has meant an increase in insurance purchase and demand since organisations do not want a breach to occur without cover. However, the data from this reporting has not necessarily led to insurers being able to develop good products since it is not very helpful data. Therefore, what is the point of collecting data? Reporting should not be done for the sake of driving insurance. Rather, it should be collected for something beneficial, including for government. It is not clear where data is being released in a manner that helps the insurance industry to develop products. It was felt that this should be considered going forward. What does this then mean for Singapore? It was suggested that structured data is needed instead since the problem to date has been the collection of unstructured data. For example, some banks might report a lot while others report little which means that it would now be preferable to have a far more structured way to receive data to achieve the requisite classification upfront.

This also relates to discussions within the first roundtable on the revision of privacy laws in Singapore. It is felt that thresholds of data can be helpful and it is most likely that the regulator will establish thresholds for required data, which is useful. Currently, however, it seems that when asked why the data is collected, the regulator only wants to know the current position and has not yet figured out what to do with it. This means that the work and recommendations of this working group is important where it can assist the regulator by showing how such information could be made available.

A difficulty with information sharing and data identification is the vast amount of data and how it can actually be used. Some questions include the following: 1) To whom should it be made available; 2) What should actually be done with it?; 3) Should it be given to the insurance industry, only the insurance industry? Or the banking industry?; and 4) Should they be asked to pay or is it better to distribute freely for everyone to examine, including the attackers? A key problem is how this data should be structured and ensuring that it has actionable value.

Actionable value is very important, especially when a breach occurs. One taxonomy includes: 1) The threat actor; 2) Action of the actor; 3) Which asset was compromised?; and 4) What attribute of the asset was compromised? This can provide a framework. However, use of that data is also important including who will have access to it. If government is collecting the data, not sharing it, and it has no plans on what to do with it, then why bother? At least with policing, there are good examples of using data to draw metrics and make sense of it to develop policies. It was suggested that this could work or a PPP where monetisation of data could help some industries, thus supporting the state's security posture. If the public will have access to the data, how might it then be used? The data could be released in a format of statistical and summary data to avoid concerns about criminal use. It is not that government should be discouraged from releasing data or that groups should not have access to it but there is a need to establish appropriate policies for sharing data. This should then allow a better feedback loop to the service provider which can enable the right link between technology choices and controls. The main difference between technology and other areas covered by insurance is that they are static (such as house insurance) whereas technology ages much faster. In terms of finding value, it is a lot harder than it seems to find value in data. While collection is easy, turning data into good value and information is difficult. It is not clear whether government would be willing to put that amount of energy into translating data to release it in a valuable state. In which case, it would probably be outsourced for a few years until it becomes too costly.

It was felt that there are two types of actionable information, namely real time to help prevent damages, and ex-post analysis. Information sharing should be timely and account for both types. Regarding information sharing, there are a number of recurring concerns that are discussed globally. Much of these concerns relate to incentives, as well as ensuring anonymity and privacy. A member wondered whether there is value in the argument for cybersecurity rating to support the need for incentives. Much like a bond, could companies be given such a rating? And could they receive a positive rating where they also participate in information sharing? Another member was not convinced based on their experience with other cybersecurity working groups for Singapore SMEs. It seems that these organisations are concerned that the use of the so-called ten principles of cybersecurity, or similar rating, is an invitation to attackers to target them. This could be particular to Singapore, reflective of cultural thinking that might be overly fearful around inviting such attacks, which members felt is rather pessimistic. In addition, it was felt that this type of certification would mean adding more cost for organisations.

In the United Kingdom, the Government released a voluntary cyber essentials scheme to raise security standards and some insurance companies are using this scheme as a form of certification. If a company uses the scheme, then the insurance company will reduce the premium. It was suggested that this might be a way to alleviate concerns among these Singapore organisations about inviting attacks through the use of certifications. This could be a useful mechanism, especially in Singapore. However, there is a deeper problem that must be addressed whereby cyber hygiene is still important – an attack will happen anyway and these organisations should have the courage to do something about it. Another group suggestion is to conduct this cyber hygiene in a low profile way so that preventative measures are put in place without being too obvious about it. Nevertheless, adding even further complication, many of these organisations will only take these actions if they see how it benefits them. Where, for example, they might be seeking a government contract that requires such cyber hygiene levels. Otherwise, they will not do it and even though everyone says cybersecurity is important, money is not being spent on it.

Another problem associated with a possible certification scheme is that businesses may see certain standards as an end goal and not then work beyond these standards. This means that there could be value in a scheme where insurers use such a scheme to assess the premium amount and insurability of an organisation, rather than as an assessment of the state of that business through a mark or branding on the entity. It seems that there could then be an expectation on insurers that they will make sure that basic standards are met and insurance can kick in where unknowns arise and best practice has been followed.

Theme two: Legislative issues

The draft Singapore Cyber Security Bill mentions future CII guidelines, which is an area that this group could inform ahead of time. First though, it was felt that there is a need to understand what types of data are needed and to then consider corresponding guidelines applicable to these types of data. There are so many types of data in systems as well as with incidents (for example, data on the system, customer and transaction data, metadata for transactions, and system logs on the nature of attacks). Yet, current cybersecurity legislation is mostly considering the system log data for investigations. Based on the literature, a related and somewhat confusing question then arises– if the focus is only on the system log for investigations, then how can this help insurers establish the right pricing? It was suggested that there is a real need to be clear that there are different types of data in cyber incidents, and so, when discussing data collection (mandatory or not), what type of data is needed? For example, CSA is mainly looking at the system log to investigate an incident whereas a government agency like MAS may be more concerned about items related to transactions for impact analysis of incidents on an institution's integrity.

This means that even where it is apparently actionable intelligence, this will actually depend upon an actor's perspective. Different agencies have different needs and actions to take, and they thus require different data. This should inform the need for different guidelines to enforce and empower collection. In short, we should go one step back and consider why people want data. Especially since the current situation is such that agencies and regulators may only collect it first, before even knowing what they need on the premise that they may need to do a follow-up post mortem. From the angle of establishing the right pricing for insurance companies, insurance experts should identify what types of information are useful. Then the right guidelines can be explored as well as the right agency to issue such a guideline.

A second recommendation included guidelines that could delve more deeply into the supply chain for product manufacturers, apart from buyers and sellers, including possible import and export legislation on products. There is a need for action in the entire supply chain and some organisations are just not ready, especially where there are no guidelines. While this might be the case, it is also felt that innovation is very important. There is a risk that overly prescriptive requirements could mean that a country like Singapore could become a backwater market using outdated tools while innovation continues elsewhere. Moreover, 18 months is a long time in the IT industry for new disruptive technologies which will continue to challenge legislative requirements.

Rather than guidelines or overly prescriptive legislation, is there then value in exploring international standards where different countries are complying with the same standards and guidelines? While this suggestion was met with a positive response, it seems that there are not many such international standards. The NIST framework was raised, but this is a framework and not a standard and some felt that it is not easy for small businesses to test against this type of framework. One recommendation included thinking about resilience rather than security for guidelines. Insurance is a form of building resilience if sold on the premise that the insurers examine what the customer has done around security (although this might depend on the size of a policy where SMEs may only have a flat-based product and only larger complex risk will have that type of guidance).

It was reiterated that guidelines can be positively driven by market mechanisms rather than compliance. Where, for example, demands can be made when purchasing an IT product that security guidelines are followed by the vendor. Compliance may not always work and could be counterproductive. Some type of certification where the market forces itself and prompts industry to use guidelines in order to move up the value chain might be beneficial. It was counter-argued though that based on past experiences, government must eventually step in to tackle adverse issues that are inevitable.

A third point is a preference for standardising legislation and guidance across jurisdictions where global companies must work with different legislative frameworks globally. From a global insurance industry perspective, this consistency would make it easier for such companies to assess risk. Achieving this type of consistency can work dynamically too. Singapore is often a good country to adopt other good practices. Nonetheless, rather than seeking complete harmonisation, some countries are still rather competitive (at least in the Asia region) when it comes to variations in their cyber regulations.

For notifications, it is difficult for organisations when notifications are required across different countries following an incident. For example, where a Singapore company has a data centre in China with European and Australian client data and a breach happens in China, each country must be informed in a timely manner. The sequencing of this for crisis teams in different locations is highly challenging. This means that it often ends up moving to the highest common denominator – for example, 30 days in Australia vis-à-vis 72 hours elsewhere.

For insurance, it was felt that there is a need for a baseline security level across the board but where line should be drawn needs further analysis. Moreover, what is the ideal design for liability insurance so that someone is held accountable to others (if it is even desirable)? Could this be used not just for protections but to provide assurance or certification that a firm has done due diligence and could now be a suitable contractor to a large company like a bank? Is there a place for cyber liability or a policy for mandatory cyber liability coverage akin to motor or Director and Officer liability insurance?

In response to these questions, it was not clear for whom this would be made compulsory. There is no third party responsibility in a sense so it is harder to make companies buy mandatory liability coverage. This would be almost like third party cover for damage done to customers, especially where supply chain liability is one of the biggest concerns for companies to deal with the exposure left after one's own security is taken care of. Organisations try to make third party assessments but they can only see so far down the chain. However, in the car industry analogy, damage caused can be rather limited but this may not be the case with third party software. As evidenced in the recent case of the petya software from a small company that supplied MNCs globally. This begs the question as to the extent to which such a company should be insured and what premiums should be required when there is no idea about the extent of possible damage. How can insurers cover the liability where small suppliers are sometimes only a stepping stone? It is very hard to understand potential exposure and to aggregate at the moment. In order to understand these types of situations, CyRiM will be working with affiliates of the Cambridge Risk Research Centre. One member queried whether there is precedent for such cases of third party liability? It seems that in the United States several cases were settled.

In the financial industry, there are guidelines for management of third party vendors and aspects of due diligence has developed in a very structured way in Singapore so that service providers can show that requirements have been met. This is proof that guidelines do work and change the game. Moreover, risk can be transferred contractually whereby a bank owns risk but can outsource a service and they work out contractually what the vendors will do – this brings clarity on how risk can be measured, and what risk can be transferred (such as financial risk) or not (such as reputation risk).

Rather than impose cyber insurance, it was felt that government could perhaps take a leading role here to drive regulation, especially for SMEs. There could be a role like that laid out in the EU GDPR. Moreover, when discussing insurance for cyber, there needs to be stronger understanding of the broader ecosystem. For instance, there should be no need to impose insurance standards on a financial industry that is already mature, whereas focus is best placed on CII that lack understanding of the cyber domain. Insurance should not be framed separately as something that needs to be imposed but as part of an ecosystem instead. Ultimately, it was felt that the model and guidelines should shift from focus on the small operator to the product.

Outside traditional and simple cyber insurance, one member suggested that there might be a business need for assurance. Other members countered that it is easy to say assurance is needed but the level then provided is very limited given the extent of what is actually required. This means there is a danger that an organisation might think it is covered. There is a very developed practice on the concept of assurance and audit in the IT sector - it is a very developed business with standards and independent bodies that provide training and frameworks but 100 per cent guarantees will never be provided. If CII operators in Singapore are asking for this, they are only seeking to transfer their own risk, not through insurance, but by buying a service and trying to hold the other party liable for the CII systems. The industry does not work this way.

The next question was whether differentiation of assurance is possible depending upon the threat actor, in other words it may not be the fault of the organisation? The group seemed to unanimously disagree arguing that it would be too difficult to prove and what about collateral damage? It is too hard to tell because of the problems associated with attribution. Nonetheless, even where this cannot be done, the nature of damage can be assessed. Particularly where tools are sold on the black market, one can, to some extent, predict possible damages and then assess what is the affordable damage that should be insured.

Lastly, under this section, it was felt that much of the CII requirements under the draft Cyber Security Bill are not overly burdensome but requirements that should be done anyway such as annual audits, risk assessments, and exercises (although aspects of the reporting are considered challenging).

Theme three: Role of education

Some cautioned that one risk associated with making cyber insurance mandatory is that organisations might lose understanding of the purpose of insurance. Furthermore, there is a need to explain the purpose of insurance generally, irrespective of cyber-related matters. In other words, insurance should place you in a better position after an attack or loss. This means that when purchasing insurance, a client should consider the consequences of attack such as reputation loss and how to deal with this so that the client is in a better position after a loss. This is especially applicable to the SME sector where there can often be a lack of education and awareness on these issues. It is recommended that there is a need to find ways to further assist companies' understanding of why cybersecurity is important, the nature of cyber incidents, the importance of cyber hygiene, and why insurance should not be a replacement. There is a danger when talking about mandatory limits and the kinds of limits that need to be imposed, that companies will only buy up to those limits without first understanding whether the limits are enough for the industry or business. It was felt that perhaps there is a role for government to focus on this difficulty.

A member emphasised that for education and awareness purposes, the term cybersecurity is not specific enough and means little to people. If, however, you describe liability or responsibility for customer data, it is specific and has relevance. This means it is then easier to incorporate guidelines and approach liability. In the insurance industry, there are cases where insurance policies are not being sold because customers abhor cyber policies since they seem too esoteric. The industry is finding that it is much better to use specific language to describe damage liability for a cyber-related issue rather than the more esoteric term cybersecurity - clients then have a far better understanding. This means that for education and awareness purposes, the insurance industry can help clients understand those risks to be dealt with by the client and those risks where it is important for insurance to step in. Further, there is a role for residual risk for those risks which cannot be controlled anymore which can be given to the insurance company where the client has acted in a reasonable manner (again begging the question, what is reasonable or responsible management and how does one benchmark?).

It is still not clear though what exact types of initiatives should be recommended to raise education and awareness for such gaps identified by the group. A prior example based on the motor industry analogy shows that one brand might push car safety as a selling point. Through one brand doing so, this then becomes a criterion for customers when choosing a car (even some of the most innovative cars by Tesla touted safety). So how does one reach this type of maturity and assessment in cyber? It seems to return to the need for some form of benchmarking and it is most likely that government must establish this rating in the end, even where the science community will criticise it as flawed. It is, however, enough to get things going and push best practice.

The group also felt there is value in emphasising that from a market perspective, some industries are more advanced in their thinking on cyber than others and there is a risk of overcomplicating these challenges. For example, the financial industry clearly understands the nature of their cyber risks and has a highly advanced understanding of cybersecurity. Especially in Singapore where the industry works very closely with government, sharing information and working on joint initiatives. This means that the industry itself could perhaps come up with its own list of what it would like to insure to help the insurance industry have a clearer understanding and enable better risk quantification, thus better products. While each industry has its own particular characteristics, there are ways for each, especially the banking industry, to formulate its own needs.

Theme four: Risk transfer

Rather than framing insurance through the lens of the best or worst option, it is best described as a good option. There are many so-called unknowns, in other words unpredictable events, in cyber risk so that even where protective and preventative controls are put in place, successful attacks will still happen. While insurance is good to have, it is important to balance it with controls and only transfer the residual part (the unknown unknowns and unpredictability associated with the dynamic nature of cyber) since it is impossible to know everything. Framing insurance as a last resort is not perceived as helpful given that preventative measures must be taken and insurance is useful for what is not foreseeable. This means it is the only resort – in other words, a combination between cyber hygiene and purchasing insurance as part of proper hygiene. This is especially the case for SMEs which may sometimes be ignorant about the risks - insurance should not be promoted as a last resort. Rather, it should be promoted as the proper way to ensure protection by first doing the IT hardening and then having insurance. Education and awareness can play an important role here too since every organisation must understand where they are in terms of cyber risk. Then they can decide how to manage it and insurance is one of the methods to choose, but it is not the only, or last, one.

From an insurance perspective, in order to properly assess risk it is essential to understand the steps first taken by the client. This means having some kind of framework or similar mechanism for insurers to use to work through that assessment to see that all steps have been taken mitigation-wise. Then insurance can step in to do the rest. Consistency is possible if there are some kinds of standards to help insurers assess different clients and make decisions. This would make the insurance process faster. This then led to a discussion as to whether the insurance industry experts selling insurance products for cyber actually understand cyber and whether there is a need for them to understand it better. Concern was voiced in the first roundtable that there could be a rush to revenue by insurance companies seeking a new area and fair growth, with less concern about standards.

There was unease that some insurance companies have no requirements for meeting certain types of risks, which begs the question as to how an underwriter is then assessing underwriting the risk. Nonetheless, insurance industry experts felt that SMEs do have such requirements but the questionnaire is normally more detailed for larger clients. While different approaches are taken in the market by different underwriters, there is usually a proposal form to address those questions (although a checklist may not be good enough). One approach is such that a client might obtain a score from a checklist whereas another approach, particularly for larger companies, means a risk manager will meet the CISO and discuss proactive measures that might need to be taken. The pricing and premium is then decided based on the nature of procedures and processes in place, which is a more bespoke product than for SMEs. Differences in the market naturally arise where there are differences in the level of awareness between larger corporations and smaller enterprises. In terms of SMEs, one member felt that such scoring is a good approach for cyber hygiene, especially where some insurance companies seem to have pre-determined fixed fees depending upon the amount of coverage sought and little interest in protective measures. It thus seems to depend on the sophistication of the insurer and the client. Nonetheless, one member is more concerned about SMEs given that they comprise 90 per cent of Singapore's economy and they require education and protection.

In the United Kingdom, the regulator has sought to prompt more responsible cyber insurance practices by creating guidelines for insurance companies to be very clear about their cyber exposure. This seems to be the only example of this type of exercise, although it is not yet clear how insurance companies have reacted. Regulators elsewhere are looking at these developments closely.

Some members were unclear as to how insurance companies can deal with the dynamic nature of cyber when a risk assessment conducted at the beginning of the year may be completely different later. Another felt that these challenges are still different for SMEs vis-à-vis larger corporations, which means the questions raised by insurers in such a risk assessment would also be different.

In terms of third party insurance, a member raised an important public protection argument vis-à-vis the recent Equifax incident where very large numbers of individuals were affected. In this scenario, the losses are piling up so that company resources and insurance may be insufficient. The loss due to be compensated may exceed the insurance limits. The question is how should insurance proceeds be divided between parties and will there be a priority between groups? It is particularly concerning that there may not be public protection in place. Does this mean a pool should be created, although it does not seem likely that the insurance industry will do this? If there is talk of mandatory insurance, what is the possibility of providing for public protection rather than see resources dissipate or divided on a first-come-first-serve basis (even where the company might lose future customers). This is a point of major worry given the volume of parties that can be affected as well as extraterritorial matters. Another member lastly recommended it could be better to consider guidelines for first and third party separately.