

Actuaries Institute Podcast

Cyber Risk and the Role of Insurance

Date: 28 September 2022

Interviewer: Vanessa Beenders

Guest: Win-Li Toh

Duration: 17:57 minutes

Vanessa Beenders: Hello and welcome to this Actuaries Institute podcast. My name is Vanessa Beenders, and I am Executive General Manager of Public Policy and Professionalism at the Institute. Today the Institute has launched its latest Green Paper titled Cyber Risk and the Role of Insurance. The paper has been written by Actuaries Win-Li Toh and Ross Simmonds of Taylor Fry and Michael Neary of DXC Technology. Today I am thrilled to welcome Win-Li Toh on the podcast to discuss the paper. Welcome Win-Li.

Win-Li Toh: Thank you Vanessa.

Vanessa Beenders: So, let's first contextualise cyber risk and the insurance that's available. Can you paint us a picture please Win-Li, of the current market and the key issues?

Win-Li Toh: I think we need to start on technology. Australians are more dependent than ever on technology at work, at play, in the bus. It's woven into just about every aspect of our lives and more so since the pandemic with all of us working from home. So cyber risk and the potential for cyber criminals to really disrupt our social fabric, is greater than ever. Did you know that every eight minutes there's a cyber crime reported in Australia? By the time we've finished this podcast, Vanessa, there'll be two, three parties in Australia who would've reported being attacked. That's quite a shocking number. The total reported loss from cyber incidents, that's the total loss, not just insured losses, was \$33 billion in the last financial year and it's increasing year on year, it was up 13% on the year prior.

Win-Li Toh: Globally, ransomware attacks tripled in two years. So, you can imagine against this backdrop as cyber attacks grow, cyber insurers themselves have been having a pretty rough time with claims. So as a consequence, cyber premiums are going up, some cases doubling, to offset these losses. There's been reductions in policy limits, there's been more restrictive terms and conditions. So, I see the market has huge potential, but these tumultuous events in the last couple of years have made insurers more cautious in growing this class.

Vanessa Beenders: Against that backdrop then, what is the objective of this paper?

Win-Li Toh: The Government and businesses have been spending a lot to combat this problem, but if anything, cyber crime is getting easier. You can literally buy ransomware hacking tools off the internet. I think that in this environment, or at least the authors believe, that is, it is crucial there's a vibrant and resilient cyber risk management framework, and cyber insurance is a key part of that framework and therefore the focus of this Green Paper.

Vanessa Beenders: Thank you. Drilling down a bit further, cyber risk is a so-called wicked problem. And that does sound like an accurate descriptor because it's got a sinister connotation to it, but it's not just a colloquial expression there, there is actually an academic basis to this. Can you talk us through what that is and why cyber risk is actually a wicked problem?

Win-Li Toh: A wicked problem is one that's complex and unpredictable. It's dynamic, it's always changing, it's interwoven with other problems. So, it's kind of futile to carve off one aspect of it and try to solve that in isolation because when you do that, it'll often reveal some new dimension of the problem. I think of it like Whack-A-Mole. You whack one here and you whack one there and the next one will pop up. Cyber is a classic wicked problem. Let me give you an example. If let's say, the government spends, as they just have, several billion dollars to shore up its cyber defenses, that's fantastic for the security of our nation. But what this could be doing is it could be concentrating an already very sparse cybersecurity workforce in just one party's hands and leave other businesses exposed.

Win-Li Toh: That's certainly not what the government would intend. In the same way insurers and businesses will all have their own legitimate perspectives for raising rates or wanting rates to go down and so forth. The landscape's continually changing and cyber criminals are just getting more and more sophisticated. As we said, it's a really dynamic landscape, there's not one solution, like mathematicians like to do in finding the answer to a puzzle. Progress on wicked problems like this needs all parties to work together to be flexible, to be pragmatic about it.

Vanessa Beenders: I think you're going to talk us through three particular aspects of cyber risk, which add to its wickedness if you like. We might begin with the act of war exclusion, if you could talk us through what that one is.

Win-Li Toh: As you know, acts of war exclusions are typically found in traditional insurance covers like commercial property – because damages in a war can be catastrophic and potentially just too large to ensure. Insurers can be driven to bankruptcy covering all the damages in a war. For commercial property, for example, acts of war is excluded and there's a pool in Australia run by the ARPC to fill the gap. So, the reason for excluding acts of war is the same for cyber insurance, it's potentially too big an issue for insurers to take on. But in a cyber realm, these exclusions are very difficult to apply because there are greater nuances to where an

attack may be attributed. It can be a combination of state actors or financial motives and mere indications of fault are just not enough to attribute fault beyond reasonable doubt. And also, can you imagine Vanessa, the diplomatic consequences from a flawed attribution?

Vanessa Beenders: **Precisely. And I think Lloyd's has recently announced changes, haven't they, about the acts of war exclusion?**

Win-Li Toh: It has, and I guess it's still to be tested in the market and it's still to be discussed I guess, with governments as to how they would react to it.

Vanessa Beenders: **That perfectly demonstrates there's no answer yet to the acts of war problem. Another aspect of wickedness then is accumulation risk. Can you talk us through what that problem is and perhaps even begin by explaining what is accumulation risk?**

Win-Li Toh: Acts of war itself is one type of accumulation risk. It's where there's a concentration of insured risks so that one event can trigger substantial losses across multiple insurance policies. One unique feature of cyber insurance is that there are no geographical boundaries to where a claim can arise. A computer virus can quickly spread around the world and infect many computers across different industries and make claims under different cyber policies. You might remember the NotPetya attack in 2017.

Vanessa Beenders: **Yes.**

Win-Li Toh: Well, that affected thousands of companies across 60 countries, and it caused losses around US 10 billion and that's just the one virus. So, accumulations can arise from several sources, things like software vulnerabilities and commonly used software attacks and IT providers with large user bases or attacks on critical infrastructure providers. So, one example of the last of these is the ransomware attack, the colonial gas pipeline, if you remember.

Vanessa Beenders: **Yes.**

Win-Li Toh: I think last year that caused major disruption in the US. But I think they recovered most of the ransomware funds and identified most of the perpetrators.

Vanessa Beenders: **And so, accumulation risk, the normal way that insurers would be able to manage that is by geographic diversification. So, you're just pointing out to listeners here that that usual management technique, it's not available for cyber because of the characteristics of cyber risk.**

Win-Li Toh: Absolutely right. I mean insurers have made some progress in understanding and modeling accumulation risk. For example, that attacks

tend to cluster by industry sector, but they tend to cluster by industry sectors it's not like they're all in one industry sector. But it's still a way to go yet. It's focusing a lot of resources and attention to it, but it remains the key impediment to establishing a really resilient and sustainable cyber insurance market.

Vanessa Beenders: **And then a third one that I'd love to talk through is about market capacity. You make some observations in the paper and there's what I would say the knockout chart in the paper, I think it's called Figure3, and it shows the size of cyber risk compared with other lines of business. Can you explain that to us please?**

Win-Li Toh: Okay. As I mentioned in the paper, I quite like Figure3 myself with all the floating balls. The total reported economic loss from cyber events in Australia was over \$30 billion in the past year. So that's a billion, not a million. Cyber insurance premiums in Australia were around about 200 million dollars. That's less than 1% of these losses. So even if only half of these 30 billion losses were insurable or insured, that would still swamp every other class of insurance in Australia. I mean, I'm thinking about Fire & ISR that's been around for nearly 200 years in our country and it only has around 6 billion dollars in GWP annually. The fact is the...

Vanessa Beenders: **Gross written premium? GWP?**

Win-Li Toh: Correct. GWP, gross written premium. The fact is, if cyber losses are unaddressed, it would be too big a problem for insurers to tackle alone and it would stretch the market beyond capacity and beyond their resources. The ARPC didn't recommend a cyber pool in its latest strategy, but it remains a watch point.

Vanessa Beenders: **Okay. So, we've got those three wicked aspects if you like, to cyber risk. What then is the role of insurance in helping manage cyber risk?**

Win-Li Toh: Okay. The first thing I'd like to mention is that good cyber hygiene and security, not insurance, will always be the first mitigant to cyber threats. So, these come from technology protections like firewalls and as well as people - so specialist staff, widespread training and education in cyber security. I see a vibrant cyber insurance market as having two key roles. The obvious one that people think of is in helping businesses recover after an event and getting compensation from a cyber event. But the second role for cyber insurance is by actively boosting the first mitigants, I mentioned cyber hygiene and security. And they do this by offering clear signals and incentives to business on best practice standards.

Win-Li Toh: So, for example, eligibility. Insurers will not provide cover where there exist the most egregious gaps in cyber security. So, they raise standards. They will price to reflect risk, so encourages companies to improve their cyber resilience. And more recently some of the insurers and some of the

larger brokers like Marsh, are offering cyber self-assessment tools and providing some great insights on where your security gaps are as part of the underwriting process. So historically this approach is in insurers' DNA. I mean if you think about it in traditional classes, insurers already have a track record in setting best practice standards. So, think plimsoll line in marine insurance or smoke detectors and sprinklers in commercial property. Insurers started it all.

Vanessa Beenders: **Exactly. And I love those examples that you include of the paper that this is just the next wave of insurance, the next wave of the risk signals and how to strengthen the economic environment if you like. And another part then, so that's the value that cyber risk in insurance can play, but there's also a myth that you flag very clearly in the paper and that's widely held then by boards of directors. And can you tell us about that myth please?**

Win-Li Toh: For sure. This is very interesting to me. I've heard it myself in multiple forums where this myth has been discussed. It basically centers on boards worrying about relinquishing control and the insurer becoming a shadow director in a cyber event. From our discussions and research for this paper, we believe this to be a myth. I've spoken to various parties working in the front line of this. I'll quote Clyde and Co. They carry out instant responses to cyber events. They're a reasonably large company of lawyers and they say, forgive me for paraphrasing, something like, "While insurers may provide access to additional vendors in the event of a claim. They do not have the power to take over the management of the claim against the wishes for the insured."

Win-Li Toh: "So for instance, the board are involved in key decisions around payment of the ransom, communications to stakeholders, disclosure of the incident to ASX and where additional vendors are recommended by the insurer. And the relationship is a direct one between the vendor and the insured. The insurer may just simply end up paying the bill." We also spoke to Marsh, who's a major cyber broker in Australia, they shared the sentiment. They say "Cyber insurance provides access to the additional layer of specialist services. They bring extra hands on deck for swift recovery. They're not there to take over the role of the board." So myth is busted!

Vanessa Beenders: **Well done Win-Li. Now there's just so much more in the paper here, but we are running out of time. So, I'm going to attempt to highlight some of the other key areas for our listeners, Win-Li. So, there's a fair bit that you say about the substantial skills shortage and I think you would consider that even more chronic than for some other sectors of the economy. You make some comments about the very extensive changes that are happening by governments, by regulators, by industry. And then there's another area that you would like to highlight and that's about penalties if you like. And for example, that the level of penalties in Australia seem**

higher in particular than in the UK for example. So perhaps that's worth something being more closely looked at. Is there anything that I've missed in there, Win-Li?

Win-Li Toh: I think it's important to mention SMEs. Attacks are increasingly shifting towards smaller companies because they're being exposed as easier targets. Cyber criminals don't discriminate. They have this scattergun approach to finding the greatest vulnerability and exploiting it. And SMEs I guess, have got lower levels of security as a whole than larger companies, but yet only 20% of SMEs have cyber insurance compared to 35 to 70% for larger companies. So, I think there's a gap to address in ensuring SMEs receive better education on cyber risk and insurance and are better protected. I also want to mention one other part in the paper, which I think actuaries would like, on how our scenario analysis skills can provide organisations with insights to make better evidence-based decisions about their cyber protections.

Vanessa Beenders: And before we go on Win-Li, yes, because I would say that would also be a part that should be of interest to boards of directors just to understand the potential losses which could be mitigated by having a cyber insurance policy.

Win-Li Toh: Absolutely. We project not just financial compensation and what it costs, we also look at the costs of reputational damage and brand. So, I would say to all the boards out there, speak to your local actuary, they can help you.

Vanessa Beenders: Any final remarks Win-Li?

Win-Li Toh: Yes. I think it's worth reiterating that technology is insinuating every aspect of our lives. Cyber criminals are using this accessibility that digital tech affords us in nefarious ways. Small businesses are held to ransom, honest businesses are brought to a standstill, individuals are losing their livelihoods. So, this is a real problem. It's not just one for government or business or individuals, insurers to tackle on their own. If we really want to uplift the cyber security of our nation, of which a vibrant cyber insurance market is but one part, I think it will take all of our collective mindsets and skills to tackle. We need to talk, we all need to listen, we need to collaborate and really understand each other's perspectives to make real progress on this wicked problem.

Vanessa Beenders: Thank you Win-Li for joining me today to discuss this important research. It's an excellent demonstration of how actuaries use data for good. And again, it's Figure3 that comes to my mind as the knockout chart about capacity limits in the market. Thank you, Win-Li and your team.

Win-Li Toh: Thank you. You're very welcome.

Vanessa Beenders: So, listeners, we hope you enjoyed this discussion. You can listen to more Actuaries Institute podcasts by visiting the podcast section of Actuaries Digital, or via all mainstream podcast apps. If you'd like to continue the conversation with us on social media, please join us on Facebook and LinkedIn via at @ActuariesInstitute or our Instagram and Twitter via at @ActuariesInst. Please write in with your questions and comments on the show, we'd love to hear from you. I'm Vanessa Beenders, bye for now.

© 2022 Actuaries Institute

Find out more about actuaries and the Actuaries Institute:

- <https://www.actuaries.asn.au>
- <https://actuaries.digital>

Follow the Actuaries Institute on our social media channels:

- **LinkedIn:** <https://www.linkedin.com/company/792645/>
- **Facebook:** <https://www.facebook.com/pages/Actuaries-Institute/183337668450632>
- **Instagram:** <https://www.instagram.com/ActuariesInst>
- **Twitter:** <https://www.twitter.com/ActuariesInst>