YOSHA DELONG

mosaic moment

EPISODE_01

THE CYBER CONUNDRUM

VINCE VOCI

INTRO

0:01 **Got a moment? Fast changing risks affect people, businesses, and economies in today's turbulent world. Perils like cybersecurity, political violence, or threats to financial institutions. Listen in as Mosaic Insurance specialists quiz fellow experts on trending industry topics. Welcome to this Mosaic Moment.**

0:23 Ransomware, system breaches, catastrophic threats to critical infrastructure around the world and nation-state warfare. We're talking about the fast-changing sphere of cybersecurity. Hi, I'm Yosha DeLong, Global Head of Cyber for Mosaic Insurance. Today I'm speaking with friend and colleague, Vince Voci. Vince is the Vice President of Cyber Policy for the Cyber Intelligence and Supply Chain Security Division of the US Chamber of Commerce. Thank you for joining me. Vince. I had the honour of being invited by the Chamber to a debriefing in Washington DC back in 2018 on the cybersecurity threat to critical infrastructure. A lot has changed in the last four years since then: we've seen an increase in ransomware, and actual attacks on critical infrastructure like last May's Colonial Pipeline breach. How has the Chamber increased its work in Washington on behalf of your clients, and where do you feel that we, the insurance industry, could do more for them?

1:19 Absolutely, and Yosha it's great to see you, and it was great to see you in DC with Yigal Unna, former head of INCD for the Israeli National Cyber Directorate a couple of months ago. Yeah, I mean, so much has happened since that National Security briefing that we had three, four years ago now, and, you know, the attacks on critical infrastructure are significant: the Colonial Pipeline, Kaseya, that happened in 2021, and the exploit of the Microsoft on-premise exchange, and certainly the SolarWinds exploit notwithstanding, and we'll get into this in a few minutes, the events in Eastern Europe and the implications for critical infrastructure and for cyber companies.
The threat environment has expanded significantly. Threat actors who have gotten more sophisticated, have leveraged vulnerabilities and third parties, or weaknesses in passwords or even simple basics. So, you know, what does this all mean? I think this really underscores the importance of public-private partnerships, on critical infrastructure, working with your insurers, working with third-party incident-response firms, and bringing that information to government to enhance real-time visibility across the ecosystem to use some generalities.

2:47 Yeah, I know—for me, that was really eye-opening to hear from your guys' perspective as advocates on behalf of your clients and what you were really trying to achieve for them, but also to hear from your clients directly, and the challenges that they were facing. So, it made it very real for me as an insurance professional to understand their…

...perspective and what they were actually going through, in addition to the insights that we actually got from the government, Homeland Security, and what they were actually seeing in combat, and every day, so, you know, it kind of pulled it all together and I know that was very useful for me. I was able to take that back and try to create some better solutions for your customers, really realising what their cyber insurance needs and concerns were. So, that was great and I'm so appreciative to have been involved in that. You know, we're seeing a little bit of a shift recently towards gathering of information and reporting, and the SEC recently proposed new rules governing disclosure related to cybersecurity risk. In addition, Biden recently signed a reporting bill into law. You know, they're looking to include both the declaration of cybersecurity risk management plans and reports on actual incidents. Do you feel like this will benefit your clients? And also, on the other end, do you have concerns about the related burden of disclosure on your clients?

4:07 Yeah, great observations. You know, over the past 12 months, we have spent at the Chamber a considerable amount of time working with Congress, working with members of the Administration on this cyber-incident reporting bill. So, a couple of key things about it: one, this establishes for the first time a horizontal requirement for covered critical infrastructure to be determined in rulemaking by CISA, to report certain cybersecurity incidents, substantial cybersecurity incidents to the Department of Homeland Security, within 72 hours, that a covered entity reasonably believes that a covered incident has occurred. That and the protections that it affords companies is a really good starting block from which we can, acting through the Department of Homeland Security, take steps to align additional recording requirements. We have a regulatory coherence issue that I think that the Cyber Incident Reporting Bill can help us take steps to align some of the existing reporting requirements that are out there. For example, entities that fall under DoD DFARS, regular rulemaking and cybersecurity requirements have to report certain cyber incidents, to DC, and into their ISAC within 72 hours; that is substantially similar to the envisioned reporting requirement under the zero bill. So, what the bill does is it tasks the Department of Homeland Security, acting through the new Cyber Incident Reporting Council, to inventory, and then to make recommendations on how to align those proposals. I think we're still studying the SEC proposal, but it's not the only one that's promulgated this year.

The FTC has another one that's out as well, there. You know, the purpose of these is really to enhance the government's visibility into certain cyber incidents and then it's for that purpose that we see that we're really evaluating the necessity of these reporting requirements for CISA, for broad, critical infrastructure, that is to better understand the risk landscape for covered critical infrastructure and the CISA community, we understand that, I think, we are working with the agency on some of the key definitions. But once we move away from that, we really have to take a critical eye on what, when, where, and how we can comply with these reporting requirements. And to what extent and what opportunities are for there to be alignment into that CISA-led reporting. So, that's a critical eye that we're working on with members; the SEC is deadline for comments, I think, is either May 6, or 10th. CISA, has at least the first 24 months to promulgate its first notice of proposed rulemaking, and then 15 months thereafter, US issue final rules. So, we've got a lot of work to do. We really do look forward to working with the agency and the Commission and as they craft these proposals, and of course, with our members and your members. They're very much affected by these.

7:32 Yeah, yeah. And I've heard from law enforcement, this could be very useful for them to help prevent future attacks and I think a lot of times people think of reporting, and they think of it's more of a look-back perspective, but, really, holistically, especially for people combating these bad actors, there's an opportunity to prevent further attacks, and then also improve the security of our critical infrastructure and really look at where the vulnerabilities do exist, and how we can help prevent those from becoming systemic and becoming a real problem later down the road. So, I do think there's a nice balance there and, you know, 24 months sounds like a long time, but I know with the work that you guys do, and how much back and forth there is, it goes very fast. It definitely does.

I do want to go back to, you know, one of your first comments and talk a little bit about the conflict in Ukraine; we're obviously very deeply concerned about the loss of human life and the displacement of so many people. It's really turned into a full refugee crisis at this time and there's so many things that we need to be concerned about and so many things that are shocking to watch unfold. But it's really also the first time we've seen the potential for a large-scale cyber war. And, you know, I think that this is a reality that we're starting, we've talked about for years, but we're actually starting to see play out a little bit. From your perspective, is this going to change the way that you're looking at, or looking to address, cyber and do you think this would lead to future cyber warfare and acts of hostility?

9:03 So, it's a great question, and one that we've been reflecting on considerably over the past couple of weeks. One, you know, just starting with what's happening in Ukraine. We've seen significant information operations and influence operations. We are seeing low-level disruption operations, whether it's website defacements, or website take-downs, and we're seeing destructive cyberattacks, but certainly not at the scale and the level that some had anticipated and some had predicted. And then lastly, I think the other significant point about the current conflict in Ukraine is how that has applied and how the attacks are really just striking the territorial integrity of Ukraine. Now, we've seen some non-state actors over the past couple of weeks get involved, whether that is Conti or LockBit Ransomware on the Russian-affiliated side stepped in and said they were going to hold at-risk entities affiliated with supporting youth, the government, Ukraine, and we've seen Anonymous and the Ukrainian government call for an IT army to go to war against Russian affiliated. So, there's definitely this escalation that we're looking at.

So, what does this all mean, for the Chamber and our members, both kind of thinking through the medium-term and long-term, because I think in some ways, CISA has urged companies, especially those in finance, DOD manufacturing, and those involved in the war fighting effort, and certainly in oil, natural gas, to go shields-up and to really be prepared for reprisal cyberattacks from rational minded entities, but really forecasting kind of what the next cyber incident might look like, and what the next cyberattack might look like. And I think it underscores the importance of the public-private partnership model and working with CISA, working with sector risk-management agencies, working with law enforcement—it really underscores the importance of instituting basic cyber basics. And for those that are mature and regulated industries, compliance with an information security programme, we've talked in the past about the importance of the cyber, the NIST cybersecurity framework that's going through an update, but that sort of those baseline cybersecurity requirements, that's really...

...critical for organisations to demonstrate some compliance with. And, you know, frankly, that's working with insurers on our compliance regime that makes sense for an organization's risk appetite and risk posture, and that's working increasingly with cyber incident-response firms to have muscle and capability to detect and report and respond to cyber incidents.

12:05 Yeah, I really, you know, the highlight on the things that we've talked about in the past and the importance of the NIST framework and the importance of cybersecurity, especially, you know, the detect and prevent and recover aspect of that, and how that's going to come into play in the next couple of months, and years, but it's really a long-term look at what a company's critical infrastructure and beyond should be doing anyway, and I think highlighting that while it's during a very devastating event, we're trying to find some silver lining in that.

12:38 Absolutely. We've got a long way to go on enhancing national cybersecurity resilience. But I think it is achievable. Not only for the most mature organisations, but everyone could be doing more in this space. And then that's everything from you know, the basics, deploying multi-factor authentication, deploying endpoint detection, any malware, anti-virus, software, those couple of things, and certainly use of encryption. Those are some basics that can be done as well.

13:08 Yeah, yeah. Well, thank you for your advocacy on behalf of those things that we are trying to get done in the insurance industry, as well as just advocacy and protecting the critical infrastructure for Chamber clients. Lovely speaking with you today, and I look forward to catching up with you again soon.

13:25 Absolutely. Great speaking with you, Yosha. Thank you.

OUTRO

13:28 Thanks for listening. Feel free to download follow and share on social and recommend us to colleagues and clients. See you here next time for another Mosaic Moment.