Barclay Damon Live Presents: The Cyber Sip Podcast

Episode 18: "Don't Be the Weakest Link: How Insurers Promote Cybersecurity, With Yosha DeLong"

Speakers: Kevin Szczepanski, Barclay Damon and Yosha DeLong, Global Head of Cyber, Mosaic Insurance

[Kevin Szczepanski]: Hey, everyone, this is a Barclay Damon Live broadcast of Cyber Sip. Practical talk about cybersecurity. I'm your host, Kevin Szczepanski. Let's talk.

[Kevin]: Welcome back. And today, we are so pleased to have Yosha DeLong, senior vice president and global head of cyber for Mosaic Insurance, a NexGen global specialty lines insurer with more than 25 years' experience managing liability, professional, and cyber lines. Yosha develops and oversees Mosaic's cybersecurity product globally. Before joining Mosaic a little over a year ago, when everyone joined Mosaic (it launched in February 2021) Yosha was technical director of cyber and professional lines at Zurich North America, where she oversaw professional liability lines and coordinated cyber risk coverage across all lines of business. Yosha DeLong, welcome to Cyber Sip.

[Yosha DeLong]: Thank you so much, Kevin. I'm really excited to be here.

[Kevin]: We're excited to have you. And I want to start really broadly, go back to the beginning. It wasn't that long ago. When did cyber insurance first come about? Why did it come about? And what were the early policies written to cover?

[Yosha]: Yeah, I always love talking about this because a lot of the people that are in cyber now weren't even you know, I wouldn't say they weren't alive, but they weren't in the market at the time when we first started looking at these policies. And some of the first policies came out in the late '90s, but they really started developing in the early 2000s and it was a response to the regulation that was primarily coming out of California around privacy and what privacy meant. And the conversations we were having at that time with clients was around, okay, these new regulations are in place. But, you know, what do you do when something happens and you actually have a regulator calling you saying, okay, you know, you've had a privacy violation, you have to notify all of your customers. And your customers are across multiple states and different states have different requirements for how you notify. Some you have to email, some you have to have an actual letter. And so, you know, these kind of requirements, we were selling it almost as a service to respond to the privacy regulations rather than really a financial backstop at that point.

[Kevin]: Almost like a vendor...You were...

[Yosha]: Exactly. So we were selling the vendors. Yeah. So it was really about who your vendor was and who you were working with at the time. That was going to be the ones that helped them. And there weren't that many back then because this was such a new concept. But I think also thinking about the threats, you know, and I graduated from the University of Washington in Seattle, lived in Seattle in the late '90s. And, you know, we would mess around in the computer labs trying to hack things. And I was not a hacker at all. I was a math major, but I had to take some of these computer classes as part of my major. But there was this kind of idea, you know, Microsoft was the big company there at the time. And there was this idea that if you could try to hack Microsoft or identify vulnerabilities, then they would hire you. And so it was a thing we talked about in school a lot, and a lot of people would try to do it. So a lot of the what I would call "malicious actors" back then or the hackers, it wasn't necessarily that it was a financial gain. And when we kind of look at the history of hacking and we look at some of the first hacking events that happened, you know, you can go back to the '80s, Matthew Broderick with, you know, WarGames, kind of ...

[Kevin]: I remember that...

[Yosha]: It was a game, it was fun. And so it was really about figuring out where the vulnerabilities, you know, the holes were, how you could get things. And there were a couple like worms that were created at the time that kind of got out of control. And they weren't really people's intent. But, you know, I mean, you and I are of an age where we remember when we didn't have online banking and, you know, email was used sparingly for business purposes. And we all had servers in our offices that really hosted all of our data and held everything. It was just a different time as far as what was actually available on the internet, what was connected. And I think, you know, when we were looking at creating policies to respond to this, we weren't even aware of the financial implication that was going to come out of hacking in the next 10 to 15 years.

[Kevin]: Right. It didn't start that way. Now, there is this resistance to change that is inherent in life and particularly in business I think. So, did you find in the early stages or can you talk to us about how businesses would respond to the earlier product? I imagine a lot of organizations would say, well, we already have GL coverage, we already have property coverage. Do we really need to make us spend on something entirely new that we really don't even understand?

[Yosha]: Yeah, I mean, terrifyingly enough, I've heard that, you know, in the last five years, even. But going back then, even the products that we initially created, they were privacy products. But then it started to become almost techie E&O, ride on. And so it was there was a lot of focus on technology and technology companies, and we were seeing a lot of technology at that time coming out of Silicon Valley, out of Seattle. And I remember when I first started working on these policies, I just kept thinking they weren't really fit for purpose for the general public. So how are we supposed to sell them to the general public? You know, how was I supposed to go into a school district or, you know, heaven forbid, a manufacturing, which we never would have talked to them back in the day about what their exposure actually was. But somebody like a school that held a lot of personal information where that privacy was triggered, they would look at this and everything was like in "tech-speak" like the policies were written for tech companies. So it was really challenging to have those conversations. They weren't really they weren't really fit for purpose for clients at that time.

[Kevin]: So you mentioned in the earliest stages, the coverage was almost a vendor service. What were, as the world evolves then in the aught years of the 21st century, what were some of the early threats that the cyber policies began to be written to address?

[Yosha]: Yeah, I always think when you look at the evolution, it was kind of a silent time in the early 2000s and really where we started to see the pops, the claims, the things where people were like, okay, this is actually a real product and we need to actually have it as part of our portfolio was really after Target, you know, and there was this realization that there was a monetary gain to be had from hacking companies, especially companies that store credit cards. So pre-tokenization where now, you know, your credit card is typically not stored on somebody's network. They were accepting credit cards and then storing them on their network. And so if somebody was able to get in, that was really what they were going after, was credit cards. So, you know, it was very focused on that. And from an underwriting perspective, when we were first looking at these maybe in like ‘06, ‘07, ‘08.

[Kevin]: Right.

[Yosha]: That was what we were very focused on from underwriting standpoint, was does this company have in-store credit card information? And then the privacy part is part of it as well. But the policies back then, you know, they didn’t include things like the business interruption that we see now. They were still very that third party liability. You know, how do you notify, breach costs, what do you do when something happens? And then really that regulatory aspect. So we saw a huge switch in the market in so many different ways right around that time that Target happened in 2013, 2014, closely followed by Home Depot and Premera, where the other big, advertised ones. So that was you know, it was a real switch in that type of threat. And that’s pre-ransomware really after that data, and the data breach aspect.

[Kevin]: Right, ransomware was not a thing during the Target crisis. And of course, Target had third-party claims from banks and financial institutions that had to make good on the credit card losses. But I remember, thinking back to that time, that was really when it dawned on me that the so-called first-party coverage was more important, probably the more urgent need in the marketplace. Can you just talk to us about the difference between the first- and third-party components of cyber coverage and why that first-party coverage was so important to the typical business that began to experience these cyber incidents?

[Yosha]: Yeah. And really, you know, for people that aren’t familiar with these insurance terms, you know, third party is a loss suffered by a third party and not the insured themselves. And first party has loss suffered by the insured themselves. So, you know, a property policy is typically a first-party policy and a liability policy like your casualty policy, slip and fall is third party. So that happens to somebody else and they’re the ones that need to be indemnified. So cyber policies have both components in it. And you’re right, the first policies did not have a lot of that first party and that was really around the breach response, which was what the first party was built to respond to. And then it was really driven by that third party. So that liability, you know, what happened was they sued you for, you know, losing their information. What happens when somebody sues you for losing their credit card information and they actually can prove that there’s damages affiliated with that. And then, of course, the class action that comes out of that, you know, people joining together to sue you for the negligence that you have caused by losing their information. So that’s been a huge, I would say, transition in the market that we’ve seen. But the interesting thing about it is that third party, you know, people are very focused on the first party loss in the last couple of years.

[Kevin]: Right.

[Yosha]: What happens when your business goes down, ransomware attack, and you cannot function. And that’s where we’ve seen the costs go way up in recent years. But that third party is still out there and it’s still happening and there’s still some of the biggest losses are caused by that. Going back to Target, one of the things I thought was really interesting at that time and you know, we were having discussions in the market was that the actual the biggest loss suffered in the Target breach was by the banks.

[Kevin]: Right.

[Yosha]: And it was that cost to reissue people’s cards. And I think the number at the time was like $4 billion. And I don’t remember the case law. I’d have to look this one up, but there was a case that happened out of this where I believe the banks sued Target and we’re trying to get some of the information back and their carrier denied the claim because reconstituting the cards was never meant to be—I can't remember if it was property damage or casualty claim. But you might actually know better than I do on that one.

[Kevin]: I remember reading it then. You're right, though. It's been a long time and that was the chief, that was the most significant suit that we saw, at least in the early years.

[Yosha]: Yeah. And so, you know, those of us writing and selling cyber back then, we were like, okay, well, if this doesn't really result in damages to people, are people going to care and want to buy this product? Right? Is this product actually fit for purpose and, you know, self-manifesting our own nightmare situation of ransomware? But whatever we were doing at the time, you know, I think we started looking at it was kind of the term even though these events happened, we had a blip of hard market that was kind of trying to soft market of expanding the policy coverages at that time.

[Kevin]: Right. So I want to ask you about how you got into the cyber business. But first, I want to pick up on what you just said. So I guess forgive me, it's such a general question, but now you've been at this for a long time. How have you learned over time to convince your customers, policy holders that they do need this product? It was very difficult in the early ages and still today, as you say, it's hard to sit down with a business today, sometimes even professional services firms, including law firms, and explain to them why they need a cyber component to their risk management.

[Yosha]: Yeah, you know, I really I found that the best thing to do is really listen to what people's concerns are and give them a realistic picture of what's going on in the world. And, you know, I think with selling any type of insurance, everyone always wants claims examples, you know, tell me about. Okay. Well, I'm not a large law firm. I'm not a law firm that handles tax or I'm not a law firm that handles, you know, estates and divorces. Nobody's going to come after me. I think the threat environment has changed that it's about weakest link. And it's not about what you have, you know, it's not about what information you hold. That's still prevalent in a lot of different aspects of the coverage and a lot of different aspects of how we would underwrite a risk. But at the same time, if you don't have the proper controls, they're going to find a way to get try to get money out of you. And so it's not about, you know, what kind of information you hold. But, you know, I've had so many of these conversations where I've sat down with boards, I've sat down with, you know, owners of companies. And it's almost just talking them through what the coverage does, what it doesn't do, what their actual threats to their particular company are, and really understanding what they're concerned about, and how that ties in. And I think that's a part that we don't always do in the industry very well, is really listen to what the customers want and, you know, listening to their concerns versus us telling them what the solution should be to maybe a problem that doesn't exist in their own mind.

[Kevin]: And that makes good sense. And it's easier said than done. I mean, you sound like you are a good listener. So with that as a segue, tell us how you got involved in the cyber insurance line.

[Yosha]: Yeah, so I really started focusing on it in 2003 and I was a wholesale broker at the time and was trying to really define what I wanted to be as a wholesale broker. You know, what kind of solutions that I want to bring to people that were maybe a little bit different than everybody else. And I was I was struggling a bit with that. And I met with a couple of underwriters and they were telling me what they were doing in this, in the cyber space. I remember kind of thinking at the time, you know, this isn't really like a product that everyone needs, but it's something different and not everyone's talking about it. So I was going out and talking to my retail brokers and they're like, oh, I already have a wholesale broker, I've got a really good relationship. And I'm like, well, have they ever talked to you about cyber and really focusing on the states that had the regulations in place at the time where I knew that their concentration of clients were in that space. And so, you know, not to use a scare tactic, but I was then going to the retailers and saying, you know, your E&O is on the line if you're not having these conversations and something happened.

[Kevin]: And it's true, it's true.

[Yosha]: I'm kind of sitting down and walking through how the casualty policies in particular weren't really responding to this threat. And, you know, it was it was a lot of work, to be honest, but I learned a lot in the process. And then really what I took back was I went back to the underwriters that were writing this at the time and said, this is what my customers want. This is the need that they're seeing, and this is where we aren't feeling like the policies are fit for purpose. And there were a couple of markets at the time that I was working with that were really receptive to that kind of feedback and wanted to work with me to create better products. So just having that that relationship and that give-and-take was really how I started. And then I actually went from there and worked with one of the companies that I been working on to develop products. And yeah, so just been kind of doing it ever since.

[Kevin]: So flash forward less than 20 years, which is maybe not a nanosecond, but a very short period of time in the insurance industry. We now have a hardening market. We have, I believe, and I may not be current...over $2 billion a year in premiums. And just less than a decade ago, it was not even a billion dollars in cyber premiums. And I want to read to you something that you said recently as a jumping-off point to talk about underwriting. This is from the March 16, 2022 edition of Insurance Business Magazine. And these are your words. Quoting now, "Cyber is a peril, not just an insurance product. And cyber events affect all insurance lines of business. There's an opportunity for innovative cyber insurance solutions, as well as an obligation for cyber insurance carriers to influence and implement overall cybersecurity improvements and minimum expectations across the globe." Unquote. What did you mean by that? And why is it so important?

[Yosha]: That's a lot. So I think just kind of starting at the beginning, what cyber has turned into is the exposure presented by cyber, by the interconnectivity of our world has become our everyday reliance in almost every aspect. And as we advance in technology, you know, technology is not going away. We're not going back to having flip phones. You know, you might want to, but we're not going to as a society. We're just going to continue to see this this interconnectivity become more and more important in our lives. And as a result, the threat of destroying that interconnectivity, the vulnerabilities, the possible potential payout from, you know, a bad actor taking advantage of those vulnerabilities, and that our connectivity is going to continue to grow. You know, you start to think of we have autonomous vehicles, if we have flying vehicles. I mean, all those things are going to present new avenues of vulnerability and bad people are going to continue to take advantage of that.

[Kevin]: Yeah.

[Yosha]: So when we think of this, every single insurance policy that we're writing out there, from auto to casualty to property, they're going to have some element of this exposure in them. And if we don't address it and we just continue to be the insurance industry that's plodding along saying, well, this is how we've done it for 100 years, the industry is going to get caught in a really bad position. Not only are they not going to be meeting the needs of their clients, but they're going to potentially be covering things that they never intended to and didn't want to.

[Kevin]: Right.

[Yosha]: So we as an industry really need to reflect on that part. Definitely.

[Kevin]: But I was going to say just insurance. When I think of insurance, I don't mean to cast the entire industry, but it is it is traditionally a reactive industry. You get a claim, you submit a claim, the claim is covered, and you have a lawyer to defend and pay a judgment or settlement. But the cyber industry seems to work differently. We talk about a hardening market, but what's happening in the hardening market is insurance companies are placing an ever-expanding suite of controls on their policyholders as a condition to getting coverage. That may seem onerous, but what's really happening is the industry is, in effect, pushing its customers into an enhanced cyber hygiene, which is not only going to enable them to get insurance down the road, but it's going to protect them from some of the very risks you've been talking about. So I, I see this as a very...is a unique form of insurance that we really haven't seen. Not even you know, I wouldn't even say the D&O, E&O, as important as they are, have really taken this next step to change an entire industry, make it more cyber secure.

[Yosha]: Yeah. And I think that along with that, there's lots of different things. So one is that it's really important for those public and private partnerships. So the partnership that the insurance industry has with the FBI, with our forensics vendors, getting the feedback, finding out what's going on, what the latest threats are, what our insureds are up against, working with security professionals to understand the best ways to protect our insureds against these things, pushing that information out to the insureds, setting minimums of things that we're willing to accept and people that we insure it is going to make a huge difference. You know, I jokingly, when I try to tell people what I do at cocktail parties, you know, I'm like, well, we're basically saving the world from cyber threat.

[Kevin]: I think that's true, there's a strong element of truth in that.

[Yosha]: We like to think so. But, you know, raising that those minimum requirements and what we're asking out of people is going to make huge advancements in a company's own security. And that's what ultimately the end result is. And it's not so much about, you know, us not wanting to pay the claims because we have been paying the claims. And we pay a lot of claims, which is why the industry is in the situation it's in, but it's about making sure that we're there for the right types of claims. And this isn't something where you're getting three or four ransomware events a year, but when you do have something happen, how do you quickly recover from it? How is it not detrimental to your business because you have these controls in place and therefore it's a win-win for everybody involved in the claim. And that's ultimately what we'd like to get to. Unfortunately, you know, this is a game of whack-a-mole and every time that we kind of like close up a hole, something else happens. And another aspect of that is the world, the globe, is vastly under-insured in cyber. So while we are pushing out these minimum controls to the insured segment and I want to just focus on the US market, for example, you know, I think that the market penetration is still quite low. There's estimations that's anywhere from 20 to 30% of major corporations actually have cyber insurance, let alone the SMB space where, you know, they're quite vulnerable. They may not have a lot of information, but they're the ones that that shut down for a week, you know, three weeks and they go out of business. We saw this during COVID. It's really horrible that that happened. So it's really about, you know, not only how do we influence that for our insureds, but how do we also get that kind of information out to the larger public? And a large part of that is working with, you know, with the government on that those types of projects as well.

[Kevin]: So as far as we've come, it sounds like we still have a long way to go to expand cyber coverage to the...not only the large, but the SMB markets. I think that leads naturally to underwriting. So let's turn to that now here. So we're sitting in 2022, the market is hardening, meaning it's harder to get coverage. What coverage you get is going to be more expensive, perhaps narrower than you might like as an organization. So what do your cyber underwriters do? How do they do it, and how are they, you know, you're protecting the company, but you're also expanding the protection to the insurance market at the same time. Can you talk to us about that?

[Yosha]: Yeah, I think cyber insurance underwriting has really become quite an art and it is...it pulls in lots of different factors. So there's a lot of tools and vendors out there that we use to look at external scans.

You know, you look at a company's financials, you look at their investment in their infrastructure. But one of the things we keep talking about as well is really what their cybersecurity hygiene is, or their maturity, or their culture. And is it believed in at the top of the organization? Does the board buy into this and say that this is important? And I talk to a lot of clients where say, you know, we do look at where you are right now because that's obviously important. You know, we we're always talk about things like multifactor authentication and, you know, what your backups look like and, you know, what's actually on the cloud and how is your cloud exposure diversified? And, you know, what's your administrative controls around somebody getting into the secret sauce? And, you know, where are you actually holding your crown jewels of your company? So those are all things that we would ask of every company, but it comes from looking at how much they want to continuously improve. So somebody may not be perfect right now, but I always tell them, you know, get the opportunity to get in front of your underwriters and tell your story. Talk about where you were five years ago. Maybe that was a complete dumpster fire of cybersecurity and not at all where you should have been in an organization—like don't be embarrassed about that. Talk about the journey you're on and where you're at right now, but also where you're going. You know, any time a client would come in and say, well, we've got it figured it out and we are really, really good at this. And, you know, I think we can just sit back on our laurels for three years. I'm not going to write that risk because the threats that we see six months from now are going to be different than they were before. So it's a continuous journey. It's about buying into it from the top. It's about companies and senior people within the company saying this is important, this is important for our board. This is important for us to get D&O. This is important for my clients and my ability to retain clients. And I think, you know, speaking to law firms, that's something that is going to start coming up where clients are going to say, you know, do you have this? Are you invested in this?

[Kevin]: Right.

[Yosha]: And those are going to be the things that we really look at. And the other thing is, we don't expect anyone to be perfect and nobody's going to be able to prevent something from happening. So it's really focusing on how you're going to recover from an event. So, you know, we want to prevent that event from happening in the first place. But in the case that it doesn't happen, maybe the vulnerability is presented by a third party, maybe the vulnerability is found in your own security software, you know, how are you going to recover from this event and recover quickly and make sure that it's not overly impactful to your own company, that you have to shut down?

[Kevin]: So I know we are running close on our time, but I wanted to ask you one more question. So let's say I am a small, medium sized business and I don't have cyber insurance. I come to you or even before I come to you...I am just curious how I measure up; whether I'm going to qualify for cyber insurance. What tools are there out there, what sources, what individuals can I go to to have that candid conversation before I come to an insurance company, before I take the SAT? What prep can I undertake to see where I am and to shore up my safeguards to maximize my chances for getting insurance?

[Yosha]: Yeah. I mean, usually I point them first to their broker. Brokers are the ones that are dealing with this day in and day out directly with their clients and really have some good advice and advisors on their teams to point them in the right direction and kind of benchmark them compared to their peers. So that's always the first place I point them. But a lot of times they also can have a partnership with a security professional or a security firm if they don't already. And those are another really great resource for telling them, you know, this is what you need to do, or this is where you need to go, and how you get there. And I think that's a huge part of it. You know, I've had clients with the like, I kind of know what I need to do. I just don't know how to do it. And we've between a combination of the underwriter, the broker and, you know, a security vendor, we've always been able to get them on that path.

[Kevin]: If you—let's say you're one of those organizations who isn't where it needs to be and may not be a worthy risk right now—how long does it take for me to go from unworthy risk to meeting with my broker, retaining a security vendor, fixing the gaps, covering the gaps that I have to a point where I can then come to a carrier or a suite of carriers and actually get cyber insurance in the marketplace.

[Yosha]: It really depends. I've seen healthcare entities that are unfortunately on the beginning of these stages or where they need to get, and that for them it's a three-year journey. I've seen smaller businesses that maybe don't have a lot of information or a huge dependency on online sales, and for them it can be a three-month journey. So it's really about, you know, how your organization operates, how complex your network is, what needs to be done, what the most important things are, what you're looking to protect, then make that determination. So it varies quite a bit. But I think just by having that realization, they're taking the first steps in the right direction.

[Kevin]: Right. Best to start now. So where you start, the more, the more...

[Yosha]: Yesterday.

[Kevin]: Right. Well, I have so many more questions to ask you. I wanted to talk about where you see the market going today, some of the expansions and contractions in coverage. Well, I know we're out of time, but will you come back and talk to us about those things on a second episode?

[Yosha]: Definitely, I'd love to.

[Kevin]: Thank you. And thank you for joining us on this episode of Cyber Sip. And thanks to all of you. We're back soon with another episode.

[Kevin]: The Cyber Sip podcast is available on barclaydamon.com, YouTube, LinkedIn, Apple Podcasts, Spotify, and Google Podcasts. Like, follow, share, and continue to listen.

Disclaimers:

This material is for informational purposes only and does not constitute legal advice or legal opinion. No attorney-client relationship has been established or implied. Thanks for listening.

Barclay Damon Live podcast transcripts and captions are automatically generated through artificial intelligence, and the texts may not have been thoroughly reviewed. The authoritative record of Barclay Damon Live programming is the audio file.