Best’s Insurance Law Podcast

How Insurance Claims Professionals Are Responding to Evolving Cyber Threats - Episode #196

Posted: Wed., Oct. 26, 2022

Hosted by: John Czuba, Managing Editor

Guest Expert: Duc Nguyen, managing partner of digital forensics and cyber claims from United Litigation Discovery

Qualified Member in *Best’s Insurance Professional Resources* since: 2006

John Czuba: Welcome to “Best’s Insurance Law Podcast,” the broadcast about timely and important legal issues affecting the insurance industry. I'm John Czuba, Managing Editor of *Best's Insurance Professional Resources.* We're pleased to have with us today Duc Nguyen.

Duc is the Managing Partner of Digital Forensics and Cyber Claims at United Litigation Discovery. Duc has 20-plus years of professional experience, including software development, criminal investigations, insider threat investigations, cyber claims, and litigation support. Duc has also consulted on headline-making multinational cyber claims.

Duc, we're very pleased to have you with us today.

Duc Nguyen: Hi, John. Thank you for having me.

John: Thank you, Duc. Today's topic is streamlining cyber claims. Duc, for our first question, there have been so many changes in the past couple years since COVID hit, and everyone being remote for the better part of almost two years now. What changes have you seen as a result in cyber over the past few years?

Duc: These are really metric-driven. These changes are shocking and eye-opening at the same time. Go back to about 2015, and you have cyber claims that weren't scaling above a million in damages. From about 2015, there's about a 400-plus increase in percentage of incidents having at least a million in reported losses.

At the same time, there's been a shift in the attack vectors, changing from malware sites, to now, the dominant attack vector has made headlines all over the place, but has been predominantly phishing attacks. That's switched over, because if you think about it, one of the easiest ways to enter into an organization is emails.

Everybody has emails, and you just send out email blasts with phishing content in there, and someone's bound to click on it.

John: What do insurance carriers in particular need to focus on today related to risk management, Duc?

Duc: This is interesting. There's been a lot of effort in developing robust assessments for the application process. You go back several years, and the typical application process were just really checkboxes, but not too many questions. Now, you're seeing very specific questions about types of cybersecurity products and technologies, whether they're in-place at the interested party trying to get insurance.

There needs to be more of that, building out this robust assessment, maybe even bringing on board third-party vendors to help out with that assessment to get a full picture of what kind of risk the carrier is looking to take on.

John: Now, Duc, you talked about cyber has really changed and evolved since 2015. How has cyber coverage changed in that timeline as well?

Duc: That's interesting, too. There was a time when the coverages were light, like they were more geared towards providing just a few services. Now, you're seeing very specific services being offered, like investigations and additional support from outside vendors to help with companies getting an audit in-place for PCI compliance.

Then also, the recertification to come back into compliance with regulatory needs and whatnot for PCI compliance concerns. Those weren't traditionally in policies that I've seen a few years back, but now, you're starting to see coverages and language in there for very specific items.

There's even more defined language now about limiting what's being covered. Whereas there would be vague language about data recovery or data restoration coverage, now, I'm seeing language where it's very specific to only restoring data from backup tapes and backup media, whatever your old backup might have been.

They're limiting the data restoration to just that effort right there, and not...If you read it black and white, it doesn't even talk about recovering data that's been impacted by the cyber event. So encrypted data, lost data, or anything like that, it's very defined to backup tapes.

John: Now, when carriers are looking to protect themselves from cyber situations, what's important for them to focus on in the claims process now?

Duc: What I've seen that's been helpful has been starting open dialog with the insured brokers. To keep the claims process moving along in an amicable fashion, being able to attack only low-hanging fruit, the items that aren't contentious, and coming up with payment decisions early on, and at a frequent enough cadence that it keeps the process moving along.

Then tackle the more contentious issues along the way as well but leave that for a more robust conversation. There doesn't need to be a delay in the items that are clearly supported, clearly within claims coverage categories, appropriate and necessary, reasonable for that type of incident.

Those are the payments that should be made early and often enough that it keeps everything moving along through the claims process.

John: What do you see for the future of cyber claims, Duc?

Duc: Honestly, this is interesting. I'd like to see the movement towards what you see in the auto coverage right now, where there are various apps. Different carriers have the apps that monitor driving behavior, and it can help with discounts and premiums.

That might not work for cyber claims, but what might work is maybe a cadence to bring in some kind of assessment. Whether that's quarterly, half-year, maybe just the annual, so they can come back to renew.

Have that metric there that, one, it could help with the renewal process, but two, there might be services that the carrier has in their vendor pool, in their network, that a smaller company at the insured side might not be aware of because budgeting reasons and whatnot.

They might not have a full, robust IT department, but there might be services and resources available from the carrier side within their pool of resources there that they could offer. That assessment would shine a light on a lot of issues or deficiencies that somebody seeing that type of information would be able to say, "Hey, we could bring somebody on board, or here are a list of vendors that fit that need and could help you out."

Again, if it's coming from the carrier side, one, it's a preferred vendor. They've been vetted, and they may even come with preferential rates. I'd like to see something like that come into the future of cyber claims.

John: Duc, thank you so much for joining us today.

Duc: I appreciate it. Thank you for your time.

John: You've just listened to Duc Nguyen, the Managing Partner of Digital Forensics and Cyber Claims at United Litigation Discovery. Special thanks to today's producer, Frank Vowinkel.

Thank you all for joining us for “Best's Insurance Law Podcast.” To subscribe to this audio program, go to our webpage www.ambest.com/professionalresources. If you have any suggestions for a future topic regarding an insurance law case or issue, please email us at lawpodcast@ambest.com.

I'm John Czuba, and now this message.

Transcription by CastingWords

To find out more about becoming a Qualified Member in *Best’s Insurance Professional Resources*, contact professionalresources@ambest.com or visit our Learn More page to start the application process.