Emerging Global Cyber Ransom Threats Require a Strategic Response From the C-Suite - Episode #143

Posted: Tue., July 31, 2018

Hosted by: John Czuba, Managing Editor, *Best's Recommended Insurance Attorneys*

Guest Attorneys:

Ed Lewis
Weightmans LLP

David Mackenzie
Blaney McMurtry LLP

David Shannon
Marshall Dennehey Warner Coleman & Goggin

John Czuba: Welcome to the *Insurance Law Podcast*, the broadcast about timely and important legal issues affecting the insurance industry. I am John Czuba, Managing Editor of *Best's Recommended Insurance Attorneys*.

We're pleased to have with us today three attorneys from Insurance Law Global, a network of law firms focused on helping clients respond to the challenges and opportunities presented by globalization and the increasingly diverse needs of the insurance industry.

Joining us today are Ed Lewis. Ed is a partner at the UK law firm, Weightmans LLP, and head of the firm's London market sector. A specialist in cyber insurance and related data protection and privacy liabilities, Ed's work crosses a multitude of jurisdictions and industries, including construction, technology, and professional services.

David Mackenzie is a partner with Blaney McMurtry LLP in Ontario Canada, where he focuses on cyber, information and privacy risk, and provides counsel on related coverage matters.

Also joining us today is David Shannon, a shareholder at Marshall Dennehey Warner Coleman & Goggin in Philadelphia, Pennsylvania, where he leads the privacy and data security practice group.

Gentlemen, welcome and thank you all for joining us today.

David Mackenzie: Thank you, John.

David Shannon: Yes, thanks for having us, John.

John: Today's topic of discussion is Emerging Global Cyber Ransom Threats Require a Strategic Response from the C-Suite. In this episode, attorneys from the UK, US, and Canada discuss the latest emerging cyber threats and the expansion of regulatory risk under the General Data Protection Regulation, or GDPR, and Canada's Personal Information Protection and Electronic Documents Act, or PIPEDA.

Ed Lewis, we're going to start the questioning today with you. Cyber ransom attacks continue to increase in magnitude and sophistication around the world. What are the newest threats you are seeing in Europe?

Ed Lewis: Thanks, John.

From my perspective, I'd say ransomware was probably the most prevalent attack vector in 2017 but this year it's rapidly being overtaken by what I like to call "data nap." That's the theft or ransom, often in cryptocurrency, of personal data, and it's proving far more lucrative in 2018 for hackers preying on businesses wary of substantial fines from regulators after the GDPR came into force in May.

Based on the work my team is handling at the moment, I'd say that professional service companies have been a particular target for this new threat vector. There have been persistent and carefully planned attacks springing up across Europe for several months now, and the signs are, they're spreading into Canada and also into the U.S.

The groups behind these attacks are sophisticated, they're well organized and they're utilizing dispersed infrastructure across multiple jurisdictions, which is making it extremely difficult for law enforcement to deliver an effective response.

Of course, it means the challenge for C-Suite has moved to a completely new level, too. It was hard enough weighing the business interruption and reputational consequences of ransomware, but with data nap come the additional complexities over the legality of paying a ransom against the uncertainty of whether cyber insurance, even if it has been purchased, will actually lawfully indemnify fines.

Right now, my team is learning about many organizations who are really struggling with the force of the new mandatory notification requirements that the GDPR has imposed. Faced with paying a ransom or drawing public attention to a breach, some are choosing to roll the dice and pay the ransom instead, whilst keeping news of the breach locked down in spite of the new regulatory regime.

It's a really high risk strategy, and it's one that could reap even greater recriminations, not to mention higher fines, if the hackers can't be bought off or word of the breach leaks out anyway.

There's also a further problem in that it could invalidate policy response, and signal possible claims on D&O cover.

For me, there's got to be an increased focus, too, on where the ransom money, if it is being paid, is actually going. In this respect, the potential funding of terrorism is a key issue that needs to be considered.

Whilst generally the payment of a ransom here in the UK is not illegal, if a hacker is suspected of having links to terrorism, then that suddenly becomes a whole different ball game, because the funding of the terrorism is illegal under the Terrorism Act.

John: It all sounds pretty complicated, Ed. Is the insurance industry able to prepare for these challenges?

Ed: Yes, I think it is. But it needs to proceed very carefully, and it's got to engage expert advisors early on. It's a completely new landscape that we're dealing with, John, with more regulatory and legal hoops than ever before, as well as increased commercial pressure due to the immediacy of news and views being shared over the Internet, and in turn, of course, consumer visibility.

Boardrooms and their insurers need to understand the threats and how to deal strategically with all the competing issues in any given incident, balanced finely against fiduciary obligations, and of course, shareholder interests.

More fundamentally, though, what it also means is that we need greater awareness around the importance of cyber resilience. Identifying risks and vulnerabilities, and taking steps to mitigate the impact of a breach before one happens, is still by far and away the best advice.

From my perspective, insurers have a big part to play in that message, not to mention it may help their loss ratios a little bit in the long run, too. Don't get me wrong, some are really passionate about it and doing excellent work to educate insurance buyers already. It's just that what we really need is a unanimous call to action.

John: Ed Lewis, thank you very much. We're going to switch our questions now to David Mackenzie. David, can you tell our audience, what is the Canadian perspective on cyber attacks?

David Mackenzie: Sure, John, thanks again for having me on this morning.

The Canadian perspective has a lot of parallels with the UK perspective. As Ed has said, the criminals are global in nature and are always looking for new revenue streams and posing new security hazards.

Here in Canada, though, this is only part of the emerging risk facing business. The rise in attacks on sensitive data has led to increased focus on regulatory risk, which creates its own significant costs and expenses.

For example, Canada's Mandatory Privacy Breach Reporting Requirements go into effect on November 1st. Under these expanded rules, organizations will be required to provide notice to the Privacy Commissioner and those individuals potentially impacted by any privacy breach that may create a real risk of significant harm to an individual.

Now, that's a pretty low threshold, and one that if data was potentially lost in conjunction with a ransomware attack, may very well increase the cost of the breach many multiples over the cost of any ransom that's actually paid. The Canadian laws reflect those coming into force in other jurisdictions as well, like the GDPR.

The fact that the dataset involved may be collected from and stored in multiple jurisdictions makes these problems even more complicated. When you're dealing with businesses who work in multiple jurisdictions, the client wants to know which country's laws apply to their cyber event. The answer may very well be all of them.

John: David, then, in your opinion, how are insurance companies dealing with the uncertainties of emerging cyber risk?

David Mackenzie: It's a very difficult environment for insurers right now, and particularly claims people. They can't simply rely upon a "general sense" of what their policies cover, and what they don't.

There's really no such thing as a standard scope of coverage in this area. Each insurer writes these risks differently, and many are issuing broker-drafted policies along with their own.

What may be true for one policy is not likely to be true for another. For example, some policies may require the insurer to immediately appoint experts to protect their insureds' interest, while other policies may simply reimburse insureds for the cost the insureds themselves incurred in responding to the cyber event.

Claims people need to understand specifically what their policies cover and what they don't. They need to have that understanding as the breach is occurring. One often has little more than a day or two to pay a ransom or data will be compromised. Making sure they get it right will often warrant expert assistance in the application of their policy language when a cyber event occurs.

Just like their insureds, they don't want to be caught unprepared when they're facing a hacker threatening to steal their insureds' data. They want to provide the coverage that their policies give fairly and accurately, and retaining experienced cyber coverage counsel early on will help them do that.

John: David Mackenzie, thank you very much.

Switching now to David Shannon, David, what are you seeing with regard to this in the United States?

David Shannon: John, ransomware attacks continue to plague U.S. businesses as well. As everyone has said, it's a global issue. In many instances, smaller size businesses have come under attack, so this threat is not just for large corporations, but affects both small and large companies.

We've seen a wide variety of the types of businesses that have suffered an attack, from dental offices to accounting and law firms, country clubs, auto dealerships, and mortgage brokers, for examples.

Some attacks are sophisticated and some are not. A forensic computer security firm is usually retained immediately once an attack has been reported to an insurance carrier. The forensic firm is then able to quickly advise how sophisticated the attack is so the business can begin to make decisions on how to respond.

A significant issue is whether the company has appropriate backups for its systems so that a ransom does not have to be paid. Our firm has handled matters where the ransom has been paid and others where the professional services company has made a business decision on paying the ransom, if, say, the backup systems have failed or they just were not adequate.

Additionally, in the United States, many cyber insurance policies will cover ransom payments, so a company needs to understand what type of cyber insurance policy that it has purchased, and what is, and is not, covered if an attack occurs.

All this takes time, too, and each day that a company does not have access to its computer system can be extremely harmful, both monetarily, and obviously, to a company's reputation.

John: David, how are companies in the U.S. actually paying the ransom if they decide to make a payment?

David Shannon: Yes, John, a payment of the ransom can be pretty complicated. Most attackers are requesting that the ransom be paid in some type of cryptocurrency. Obviously, most companies do not have this type of currency or the ability to quickly obtain it, particularly if it's a small or mid-sized business.

Ideally, a company has a cyber policy that covers a ransom payment. The coverage will then assist with the payment, and it also adds individuals who can review it, approve it, and then get the payment out.

But what you should remember is, once again, when time is of the essence in restoring a company's computer system, having more people involved is going to lead to more delays and more of a burden.

In many cases, a third-party forensics firm that I mentioned earlier is responding to the ransomware attack and they will take over the ransom negotiations. They obtain the currency if the ransom is going to be paid. The forensic companies have access to cryptocurrency brokers and now openly market themselves as firms that can handle these issues when an attack occurs.

Typically, the payment amount is wired from the client or its insurance company to the forensic company's financial account. The forensic firm then purchases the cryptocurrency and will make the transfer to the hacker.

We have, however, seen instances where the ransom was paid and then the attacker requests another payment. The company then has to make another decision on whether to pay a second time or decide that they're just not going to get that key to unlock the system and move on to other ways to resolve their problems.

Furthermore, companies' insurance policies may not cover another payment, so then money's coming out of the company's bottom line. All types of separate issues arise with each instance when you have a ransomware attack.

John: David Shannon, thanks very much for that feedback, and gentlemen, thank you all for joining us today.

David Shannon: Thank you, John.

David Mackenzie: Thank you, John.

Ed: Thanks, John.

John: That was Ed Lewis, a partner at the UK law firm Weightmans LLP, David Mackenzie, a partner with Blaney McMurtry LLP in Ontario, Canada, and David Shannon, a shareholder at the Marshall Dennehey Warner Coleman & Goggin law firm in Philadelphia, Pennsylvania.

More information on this topic can be found at www.insurancelawglobal.com. Special thanks to today's producer, Frank Vowinkel. And thank you all for joining us for the *Insurance Law Podcast*.

To subscribe to this audio program, go to our web page, www.ambest.com/claimsresource. 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