UK US CA AU NZ Asia
Insurance BUSINESS AMERICA

Wrongful use of data: The next cyber storm brewing on the horizon

by Bethan Moorcraft 17 Aug 2020

It's one storm after another for the cyber insurance market. Five years ago, the biggest concern for cyber insurers was the protection and security of payment card industry (PCI) data. This is thanks partly to the infamous Target breach in 2013, through which the retail giant lost 40 million payment card credentials and 70 million customer records at the height of the holiday shopping season. The Target breach was followed closely by an even bigger breach at Home Depot in 2014, whereby hackers infiltrated the retailer's point of sale (POS) system and stole more than 50 million customer credit card numbers and 53 million email addresses.

Eventually, cyber risk controls caught up with the losses and the PCI data breach storm subsided … but it was blown over by the equally menacing storm of ransomware. Nick Economidis (pictured), vice president, eRisk at Crum & Forster, commented: "We're right in the middle of the ransomware storm, but it's not going to last forever. We're seeing some significant improvements in risk controls, and I'm optimistic we're going to see some effective responses from law enforcement to clamp down on the problem. This doesn't mean ransomware will go away completely, but it will become a lot more manageable."

With cyber insurers, risk managers and regulators starting to get to grips with ransomware, what's the next cyber storm brewing on the horizon? Economidis has his sights set on issues surrounding the wrongful use or wrongful collection of data.

"We're already starting to see this storm in the form of class action lawsuits arising from the collection of biometric information in the state of Illinois," he said. "Illinois has a fairly unique law that governs the use and collection of biometric information and the disclosures that need to be made to the consumer when that information is collected. We're seeing a fair amount of class action claims being made against entities in Illinois for their failure to meet the terms of those requirements."

While biometric data suits are limited so far to the state of Illinois, there are lots of other privacy laws and regulations that companies can easily trip up on. Two of the big ones at the moment include the European General Data Protection Regulation (GDPR), which has extra-territorial reach that applies strict regulation on any company offering goods or services to EU residents or monitoring the behavior of EU residents, as well as the California Consumer Privacy Act (CCPA), the strictest privacy law to be enforced in the US so far.

"As these laws go into effect, we'll start to see regulators looking to enforce them. They'll probably start with some soft enforcement, but then I think they'll start looking for people that they want to make examples out of," said Economidis. "Regulators often target the larger entities first, but then they'll go after smaller entities if they feel they aren't managing the law the way they want it managed. They want to set some examples and put some precedents in the world, and I think we'll soon start to see that more clearly with both GDPR and CCPA.

"Closely following that, I think we're going to see some attorneys, particularly plaintiff class action attorneys, looking at these privacy laws and trying to figure out how they can put these laws to use. I think they're going go after people in the market that they think are examples of the worst behavior, or at least examples of behavior that they don't want to see continued in the market. As they do that, I think we're going see more and more litigation around what is fair use and what is fair collection of information - and that litigation is going to be expensive, and someone's going to have to pay for it."

When asked whether he felt insureds really understand the connection between data collection, data security, and the cyber insurance policy, Economides said a lot of insureds overestimate the reach of a typical cyber policy.

"I think people expect their cyber policies to do a lot more than they actually do," he told Insurance Business. "It's like automobile insurance, where people expect their automobile policy to cover everything to do with their automobile. It's the same when it comes cyber; they expect their cyber policy to cover everything to do with their computer system, and so lots of people try to make claims for things that are far beyond the intention of the policies. Historically, when cyber policies first came out, they were limited to a failure of computer security, and very specifically a failure of the insured's computer security. They have broadened out significantly over time, partly because customers kept trying to make claims for things that were not covered. They just saw the word cyber and thought that gave them protection for all cyber-related risks."

Insurance carriers are somewhat tentative about providing coverage for wrongful use or wrongful collection of information because it's still very much an evolving risk. They don't have the loss data and they don't have a good understanding of what the aggregate cost will be, therefore it's a hard risk to price for. Forecasting such a gray area is "an area of difficulty and uncomfortableness for a lot of carriers," according to Economidis.

"There's also a bit of a maintenance problem," he added. "Cyber risks are constantly changing, and the policies need to be constantly updated, which is a lot of work for the insurers. They need to do the maintenance on their policy forms so they're covering the risks that are important to their policyholders today, but, at the same time, they're a little uncomfortable because these are new risks so they don't have a lot of data and they're not really sure what the ultimate costs are going to be. I think the dynamic between those two things makes this a little challenging for insurers."