Standards Lacking for Cybersecurity

Insurance and data privacy safeguards muddled

By George Berkheimer
Senior Writer

Adequate cybersecurity measures are difficult enough for any business to achieve. When it comes to the privacy and protection of customer data, the lack of a national standard means companies must adhere to different requirements for each state they do business in.

Cybersecurity insurance presents a logical choice for companies looking to protect themselves from the consequences of a data breach, but even so, exclusions and evolving threats leave policyholders vulnerable.

The Cybersecurity Association of Maryland (CAMI) shone some light on where these problems overlap at a Sept. 27 Breakfast Club event hosted by the University of Maryland University College at the College Park Marriott & Conference Center in Hyattsville.

Presenters Howard Feldman, a partner in the Whiteford, Taylor and Preston law firm's Baltimore office, and Cyber Risk Expert Mike Volke of PSA Insurance & Financial Services of Baltimore, led the discussion.

Throughout the United States, cybersecurity laws and regulations change nearly every day, said Feldman.

"Lawyers like well-settled principles of law," he said. "That's what having a stable legal and regulatory market promotes, but [in this environment] it's hard for businesses to plan, adjust and know what to do."

So far, Feldman said, Congress has only taken a sector-by-sector approach as different problems arise, while it has been the states themselves that have thought more globally. That disconnect has resulted in a labyrinth of consumer notification laws and regulations for large retailers like Target or Home Depot to follow when they experience a data breach.

"If you represent companies that do business nationwide or state to state … it's a real pain to try to comply with all 50 state laws," he said.

Default Standard

Members of the European Union (EU) began enforcing the data privacy and protection requirements of the organization's universal General Data Protection Regulation (GDPR) in May this year.

Mike Volke (left), PSA Insurance Cyber Risk Expert, and Howard Feldman, a partner with Whiteford, Taylor and Preston, illustrated the challenges posed to businesses by a lack of national data privacy standards at a CAMI event in September.

In the months that followed, the state of California enacted the California Consumer Privacy Act of 2018, something Feldman considers troubling because the hastily written law has already been amended and is expected to be amended several more times before taking effect in early 2020.

Companies doing business in the state and collecting data from California consumers — meaning virtually every company in the United States — will have to comply with the legislation.

"Unless Congress acts, that's going to become the default law for the country for data security," Feldman said.

Congressman Dutch Ruppersberger, representative for Maryland's 2nd Congressional District, acknowledged that California has a powerful economy, but said he believes local officials will fight for what is best for their own citizens and business community.

"I'm confident we can all work together toward robust data privacy standards," he said. "More effort at the federal level to make sure these issues are ironed out before the California law goes into effect would certainly be common sense."

Too Many Cooks

Many industries in the United States have lobbied Congress to establish national cybersecurity privacy and data protection standards for a number of years.

"[The GDPR] may be a very onerous standard, but at least you have one standard that applies across the entire European economic group," Feldman said.

Ruppersberger, however, cautioned against rushing legislation based off the European model, despite its positive privacy measures.

"I am glad more American businesses are proactively protecting online users – like the Cybersecurity Tech Accord and other [measures] — without a legislative intervention," he said. "Consumers over the last few years are learning so much more about how much of their personal data is held, traded, and sold by the private sector, such as Google and Facebook, and many are demanding to know more about how their data is used. That should push us to create better solutions for our constituents."

"The main issue has been committee jurisdiction," he said. "Issues like cybersecurity and technology policy are very hard to tackle in Congress because the fault lines lie across many different committees. This is why I've co-sponsored legislation to fix how issues such as cyber are delegated in the House."

Cyber Insurance

According to Volke, cybersecurity insurance requirements are beginning to appear in more business contracts as companies try to protect themselves against the high cost of data breaches.

"Some will exclude liquidated damages and contractually assumed liability, so it's important to understand what you have in your policy," he said. "It's not always possible to push that liability to a third party … through a contract."

Aside from covering liability, cybersecurity insurance policies can be useful tools that provide forensics experts, legal obligation reviews and other resources in response to a cyber attack, and can also cover costs associated with system damage, malware removal and lost revenue due to business interruption.

The product is still in its infancy, however, with industry experts still struggling to figure out how to underwrite risk without the means to do an intrusive network assessment or require customers to provide one.

While insurers can monitor what a company does to control risk, there's no way to monitor a completely dynamic threat environment.

"At some point there's going to be a way for the insurance carriers to get better data and information about the risk they're underwriting, but it's not a traditional model for insurance," Volke said.

On the national level, state legislatures and Insurance Commissioners are currently evaluating cybersecurity regulations, Ruppersberger said, and a few states have actually passed laws dealing with the insurance issue.

"I think Congress has been reluctant to preempt the states on this one, but the passage of state laws has certainly been good for the community as a whole," he said. "The more businesses and local entities that are having discussions around cybersecurity standards and models, the more secure we will all be in the long run."