Criminals and regulators validate CEO concerns: Cybersecurity and data privacy prevention is a must

COLIN BATTERSBY, CIPP/US | DATA PRIVACY SOLUTIONS | APR 02, 2019

Cybersecurity is the top external concern for U.S. CEOs in 2019, according to a recent survey by The Conference Board. At the same time, studies continue to highlight that the percentage of companies that are prepared to ward off or respond to cyber attacks is still relatively low. Only 26% of respondents to the McDonald Hopkins 2019 Business Outlook Survey reported being very prepared for internal and external data privacy and cybersecurity threats, with 60% reporting to be only somewhat prepared. The nuances that explain this incongruity are no doubt unique to each company. Regardless, the current landscape demonstrates both that company leaders are rightly concerned and that they need to be doing more to secure their businesses against a known, but ever-evolving, threat.

REASONS FOR CONCERN

Many of the reasons for concern are becoming better-known. Various sources place the cost of a single data breach between $1.1 million and $7.9 million. Ransomware continues to evolve with attackers taking a more targeted approach to selecting victims and deploying encryption to lock up the target's most mission-critical systems and information. This has resulted in significantly higher ransom demands and longer business interruption, with all of its negative impacts on customer and employee relationships. Wire fraud continues to grow while thieves insert themselves in the middle of a transaction and change wire instructions to divert funds to their accounts. And theft of customer and employee data continues largely unabated.

Compliance is another evolving area of concern. State regulators are taking closer looks at entities' compliance with laws and best practices for data privacy in the wake of even the smallest breaches. For example, Massachusetts, one of the early leaders in imposing affirmative data security obligations on businesses, is requiring entities reporting breaches to indicate whether they have the statutorily required written information security program at the time of the report, whether the breach involves the information of one Massachusetts resident or one thousand. Other states are stepping up their requests for information regarding pre-breach employee training, technical security measures, and policies and procedures regarding privacy and security. Businesses that are able to answer with substantive affirmative responses to these requests out of the gate are well-positioned to avoid a regulatory enforcement action, at least for a first event. It is only a matter of time, however, before a business that cannot provide substantive responses is faced with a substantial fine.

TURN YOUR CONCERN INTO ACTION

The good news is that the best defenses to criminal intrusion and regulatory fines continue to overlap. Employee training, up to date technology, and policies and procedures that require companies to identify what they have, where they have it, and how they protect it, have been proven to reduce the likelihood of, and damage done by, a successful attack. And now, those same measures provide cover in the event of a regulatory inquiry. Fear has been cited as the great motivator. There has never been a better time for businesses to turn their concern about cybersecurity into action.

For questions about your cybersecurity policies and procedures or for assistance with data privacy training, please contact the attorney listed below or another member of the McDonald Hopkins Data Privacy and Cybersecurity team.

COLIN BATTERSBY, CIPP/US

Read More