Published on *The National Law Review* https://natlawreview.com

As Cyberattacks Rise, U.S. Business Readiness Falls

Article By:

Kristin Ann Shepard

Two recent reports reflect that cyberattacks and resulting data breaches continue to threaten U.S. companies and public entities. The Hiscox Cyber Readiness Report (April 23, 2019), compiled from a survey of more than 1,000 U.S. cybersecurity professionals at private companies and public-sector entities with 50 to 1,000+ employees, found that 53% of firms reported at least one cyberattack – up from 38% in 2018. Interestingly, only 11% of U.S. firms qualified as experts based on their cybersecurity preparedness and responses – down from 26% in last year's survey; 16% of firms ranked as intermediate, and the remaining 73% ranked as novice. These statistics reflect a continuing need for public- and private-sector emphasis on cybersecurity preparedness and incident response.

The Verizon Data Breach Investigations Report (May 8, 2019) analyzed 41,686 cybersecurity incidents, of which 2,103 were confirmed breaches. Of the confirmed breaches, 16% were in the public sector, 15% in health care, and 10% in the financial services and insurance industry. Approximately 43% of the victims were small businesses. The report confirmed that the majority of breaches (69%) were perpetrated by outsiders, whereas a minority (34%) involved internal actors. Twenty-three percent of actors were nation-states or nation-state affiliated; this percentage was highest in the public sector, where cyber espionage accounted for 42% of breaches reported in 2018 (up from 25% in 2017).

Per the 2019 Verizon Report, email remains a popular point of entry for cyberattacks. Compromise of cloud-based email servers accounted for 60% of hacking-related breaches, and the median company received more than 90% of detected malware by email. Mobile devices remain the most vulnerable to hacking, partially due to their smaller, simplified display and the fact that they are often used when people are distracted or multitasking.

In a bit of good news, phishing click-through rates reported from testing exercises are now down to 3% (compared with nearly 25% in 2012). Click rates were highest in education (4.9%), where human error accounted for the largest number of breaches, and lowest in retail (1.3%). Retailers experienced a continued decline in point-of-sale and card-skimming breaches (in part due to the implementation of microchip payment cards, which are more secure than their swipe-and-use predecessors); now, card data is increasingly stolen through web-based e-commerce applications. The financial services and insurance industry was most threatened by web-based email attacks using phishing and social engineering designed to harvest personally identifiable information (as opposed to payment card data).

Awaiting Answers

Will the California Consumer Privacy Act (CCPA) – which provides a private right of action and statutory damages of up to $750 per violation for California consumers whose personal information is stolen in a data breach – prompt U.S. companies to strengthen their cyber readiness? Will President Trump's May 15, 2019 Executive Order on Securing the Information and Communications Technology and Services Supply Chain: Infrastructure & Technology – declaring a national emergency to combat nation-state-affiliated cyberattacks and cyber espionage – be effective in combatting the increasing threat of cyberattacks by nation states and their affiliates?

National Law Review, Volume IX, Number 140