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

Recent Studies Show Increasing Need For Employee Training in Data Security

Article By:

Mary Kathryn Curry

Two recent studies show an increasing need for companies to better train their employees in data security to prevent data and monetary loss. On September 7, 2016, Wells Fargo Insurance released a study on cyber security showing some interesting trends in companies with $100 million or more in annual revenue. The second-annual study questioned 100 decision makers on issues of data, hackers, network vulnerabilities, and other cyber security matters. The study showed that companies were nearly twice as concerned with losing private data as they were with being hacked or having some other security breach disrupt their system.

In particular, Wells Fargo noted the surprising trend that companies are not more concerned with employee misuse of technology (finding only 7% of companies believed that their employees' misuse of technology posed a potential threat). Yet this is a real issue. This was confirmed in another study released this month by the Ponemon Institute – 2016 Cost of Insider Threats – which showed that organizations are spending on average $4.3 million annually to mitigate and resolve insider threats. "Companies perceive insider threats as mostly driven by malicious employees, but the fact is that a significant portion of the risk is due to insider carelessness."

The Ponemon report polled 280 IT and security practitioners from medium and large organizations. It found a total of 874 insider incidents over the course of a year, 65% of which were caused by employee or contractor negligence, 22% by malicious employees or criminals, and about 10% by imposter fraud. The security incidents from negligence cost the respondents about $207,000 per incident and about $2.3 million annually.

But both studies point out that what companies are doing to combat what has been termed "the human factor," or an employee's misuse of technology, is not enough. As noted in the Ponemon report, the "training programs that companies have are just not very good. They are really focused on check-the-box compliance requirements to show everyone that [the] company [has] training on data protection." Wells Fargo noted, "[c]yber risk management is first and foremost about education," and this applies to companies both big and small. In the domain of imposter fraud alone, where a fraudster gains access to the email account of a company's senior executive and then requests a payment, the professional risk practice at Well Fargo handles five to ten of these incidents each week, from clients that are not well-known brands.

In addition, the time to contain these insider-related incidents correlates directly to the total cost to the company. The Ponemon study showed that it took more than 60 days to contain the incident or attack for 58% of their sample, with another 20% experiencing containment within 30 days.

So what should companies be doing? Companies are most frequently using data loss prevention tools and mandatory user training and awareness. However, as the Ponemon study shows, deployment of user behavior analytics would result in the largest total cost savings, at $1.1 million (based on the mean value of $4.3 million), and could drive the most impact in terms of cost on investment. The recommendation is to focus on visibility and transparency – not on stringent controls – and to build “a layered defense that delivers a comprehensive range of capabilities across visibility, detection, context and rapid response.”

National Law Review, Volume VI, Number 267