Cyberattack Fines Can Cost Small Businesses Their Livelihood

In the past year, nearly 70% of small businesses fell victim to cyberattacks, while data breaches affected 58%. The number of cyberattacks on small businesses exceeded the 43% recorded between May 2015 and 2016, as reported by *Small Business Trends*, not only leaving customer data exposed, but also subjecting companies to hefty fines or costly lawsuits. Such implications are now facing the scrutiny of business law and technology management researchers, who argue that small businesses need guidance because many don't have the "big company" resources to handle the penalties.

Bloomsburg University of Pennsylvania researchers Loren F. Selznick, an associate professor of business law, and Carolyn LaMacchia, an associate professor of information and technology management, presented two main reasons why small companies should be protected from the same cybersecurity laws that govern larger companies: lack of security management resources and affordability. The researchers' considerations were published in the *Journal of Business & Technology Law* in addition to a question-and-answer article with *The Wall Street Journal (WSJ)* in November.

Selznick described current cybersecurity laws as "unfair" to small businesses because of the costs associated with proper data security implementation as well as the penalties if customer information is breached.

"Some state statutes charge fines as high as $2,500 per customer record exposed, sometimes without any showing of fault on the part of the business," Selznick told *WSJ*. "There are state notification laws [about letting customers know about data breaches, and sometimes problems arising from those breaches] that provide that if the consumer sues the company and wins, they get their attorney's fees reimbursed from the business owner. That could be a lot of money."

In some instances, she explained, businesses also have to provide customers with an identity-theft protection service, which can range from $25 to $60 per customer.

GoDaddy released an October survey on cybersecurity that states 67% of very small businesses—between one and five employees—spend between $1 and $500 every year to keep their websites secure. In addition to damaged reputations, the study of 1,000 small businesses noted that almost half of respondents experienced financial loss after a hack, one in eight losing more than $5,000.

"One in five small- to medium-sized businesses faced a ransomware threat in the last year, costing operators hundreds of millions of dollars," GoDaddy reported. "When entrepreneurs contact law enforcement, typically the advice is: Pay it."

Federal and state cybersecurity regulations are in place in the U.S. The National Conference of State Legislatures (NCSL) states legislation requires private entities or government agencies in all 50 states, Washington, DC, Puerto Rico and the U.S. Virgin Islands to notify individuals when their information has been exposed via security breaches. In 2016, an NCSL small business survey found 66% of respondents are concerned about protecting their customer records.

The NCSL announced last month that at least 35 states, Washington, DC, and Puerto Rico are introducing/considering more than 265 cybersecurity bills or resolutions, including funding for cybersecurity programs and initiatives, and promoting workforce training and economic development. The NCSL website states 52 bills have been enacted in at least 22 states so far this year.

A simple solution to assist small businesses is to put a cap on, lower, or eliminate fines against small businesses, Selznick told *WSJ*. Although changing the fine costs would be helpful, redirecting those fines to the card issuers or data-security systems providers may be an incentive for those parties to better train businesses.

“We’re suggesting that small businesses obtain cybersecurity services from their information-technology vendors so they get the advantage of the abilities of the vendor,” LaMacchia told *WSJ*. “A vendor could say, ‘If you use our application, we’ll give you cybersecurity protection.’ It would be a market-driven solution.”

—Andrew Michaels, editorial associate