BUFFALO
Law Journal

VOL. 86, NO. 40 www.lawjournalbuffalo.com ESTABLISHED 1929 • PUBLISHED TWICE WEEKLY MONDAY, OCTOBER 6, 2014 $1.25 SINGLE COPY

Cyber insurance a safeguard

"I am concerned that there are only two types of companies: those that have been hacked, and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again." Then-FBI Director Robert Mueller III might have startled some people when he said this back in 2012. But two years later, we know it is true. Cyber attacks are a certainty in today's world.

Your business could be under attack right now, but you just don't know it. That's because it often takes days, weeks or even months to discover an attack. By then it may be too late: A company's data or intellectual property may be lost, its reputation may be tarnished, and it may be facing lawsuits for which it has little, if any, insurance.

GUEST COLUMN

KEVIN SZCZEPANSKI

This liability could be ruinous to a small business. According to the annual report of the Ponemon Institute, in 2013 the average cost of a data breach to a U.S. business was $5.85 million. The average cost per compromised record was $201. So even if a business stores the data of only 5,000 customers, the potential risk of a data breach can easily reach $1 million. This does not include the cost of defending lawsuits — by clients, consumers or even the government — alleging negligence, violations of privacy or the failure to comply with state or federal consumer-protection laws.

High-profile attacks

No one knows the enormity of today's cyber threat better than the nation's largest retailers. In November 2013, Target discovered that hackers had installed malware on its payment system and stolen the credit- or debit-card data of 40 million customers. As of August, Target has paid $148 million in breach-related costs, only about a quarter of which is covered by insurance. According to the New York Times, some analysts expect Target's total breach costs to reach $1 billion.

Last month, Home Depot discovered an even bigger breach on its payment terminals, one affecting the card data of 56 million customers. According to the Wall Street Journal, the retailer has already spent $62 million to respond to the breach, less than half of which is covered by insurance.

In the months preceding these attacks, both Target and Home Depot had been implementing encryption programs designed to prevent the theft of customer data. But even two of the nation's largest retailers could not keep pace with the hackers.

Every business at risk

It's not only the nation's largest corporations that become victims. Aside from government agencies, some of the more common targets are professional-services, manufacturing, financial, insurance and real-estate firms. Smaller businesses are increasingly vulnerable: According to Symantec's 2014 "Internal Security Threat Report," attacks last year on businesses of 500 or fewer employees accounted for 41 percent of all attacks; businesses of more than 2,500 employees accounted for 39 percent. In other words, a small business is just as likely to suffer an attack but less likely to have the resources necessary to respond.

When an attack does happen, a business faces several potential risks. They may include the costs of responding to a data breach and defending certain types of cyber claims, including privacy, security, communications and regulatory claims. Cyber insurance is designed to safeguard a business against each of these risks.

Critical management tool

Cyber insurance has become critical today because most traditional forms of insurance — including general-, management- and other professional-liability policies — offer limited, if any, coverage for cyber risks. What coverage there is under these traditional forms may be curtailed by higher deductibles, lower policy limits or policy exclusions, e.g., precluding coverage for the failure to prevent unauthorized access to electronic data, or the failure to prevent the transmission of a computer virus. Cyber insurance "fills the gaps" in a company's existing coverage, providing protection from cyber threats.

A review of the potential claims companies face shows how this works. These examples show that the potential losses go beyond simply responding to a data breach.

• Data-breach response. A hacker installs malware on a company's computer network. Over several months, the malware extracts the personal data (names, addresses, Social Security numbers, payment information) of 5,000 customers. With the average cost of a data breach at about $200 per record, responding to the breach could cost this company over $1 million.

The company's liability policies will not help. Liability policies apply when a "third party" (a customer or consumer) sues the company for damages. But they do not apply to the company's own, "first-party" losses.

Here is where cyber insurance is invaluable. Nearly every cyber carrier offers "first-party" coverage for the costs a company incurs to notify customers of the breach, investigate and repair damage to the company's network, establish a call center to answer customer questions, and pay for credit monitoring to ensure that affected customers do not suffer theft or damage to their credit. Cyber coverage can even extend to crisis-management costs.

• Privacy claims. A data breach could also prompt affected customers to file lawsuits against a business for breach of their privacy rights. (Target faces many such suits today, and Home Depot surely will, as well.) Defending these suits can be expensive, even in states where the current law may ultimately enable the company to prevail. In other words, even winning costs money. And while general-liability policies provide some coverage for suits involving "personal injury," including the publication of material that violates a person's right of privacy, either the carrier or a court might not consider the breach to be a "publication," the suit could fail to meet other conditions for "personal injury" coverage or a policy exclusion could take coverage away.

Cyber insurance is broader than these traditional forms of insurance. A cyber policy will cover the costs of defending privacy suits and pay judgments or settlements covered by the policy.

• Security claims. An employee downloads a virus that spreads to several files on the company's network. Another employee accidentally sends an affected file to a client. There, one of the client's employees opens the file, causing the virus to infect the client's network. The client's network crashes, resulting in a shutdown and the loss of electronic data. The client sues, saying that the company was negligent because it failed to stop the spread of a virus.

Here again, the company's existing coverage could fall short. General-liability coverage, for example, applies to "property damage," meaning "physical injury to tangible property," or "loss of use of tangible property that is not physically injured." The carrier or a court may not consider the client's loss to be a "physical injury" or the client's electronic data to be "tangible property."

But cyber insurance generally covers liability for failing to prevent the transmission of a computer virus. A cyber policy will therefore protect the company by paying the costs of defending the client's suit and any judgment or settlement covered by the policy.

• Communications and media claims. A Web company advertises a vendor's services on its website. The vendor's competitor sues the company, saying the vendor's material on the website is defamatory or infringes on the competitor's copyright, trademark or slogan. Depending on how the competitor's complaint reads, the company could have some coverage under the "advertising injury" section of its general-liability policy. But that coverage might not extend to the entire suit. A cyber-insurance policy affords the company not only a defense to the suit but far better protection from liability for defamation or infringement of the competitor's intellectual-property rights.

• Regulatory claims. A hospitality company suffers a data breach involving customers in several states. In the view of one state's attorney general, the company does not respond timely or comply with the state's breach-notification laws. The attorney general starts an investigation, requiring the company to hire outside counsel to investigate and respond to a subpoena. Separately, the Federal Trade Commission launches its own investigation into whether the company's failure to safeguard customer data is an "unfair act or practice" under Section 5 of the FTC Act. This is, moreover, a publicly traded company, so the SEC issues its own information request, seeking information about the company's written cyber security policies, material cyber risks and relevant insurance coverage to determine whether the company has made adequate disclosures under securities laws.

Responding to a government investigation can be cost-prohibitive. Although traditional forms of insurance may not apply, many cyber policies cover the costs necessary to respond to an investigation, defend an enforcement action and, if allowed by law, pay the cost of fines or penalties.

Conclusion

There are many nuances in the analysis that go beyond the scope here. But the examples above are real and happening with greater frequency and severity than ever before.

Today's cyber threat is alarming but simple: If you have a computer system or you store personal data, your company is at risk. The risk comes from several directions and may go undetected for some time. Traditional forms of insurance may not cover this risk; many general- and professional-liability forms were not written with cyber liability in mind. Some include endorsements limiting or excluding coverage for this liability.

Cyber insurance is essential, then, to fill any gaps in a company's coverage and limit its financial exposure.

KEVIN SZCZEPANSKI is a partner at Hodgson Russ LLP.