DATA PRIVACY

Cybersecurity team should include a breach lawyer

DARIUS DAVENPORT

Imagine coming to work and being greeted by a sign on the door instructing you not to turn on your computer because your company's network has been breached.

Once inside, you learn all work must be done manually, with pen and paper, until IT professionals can rebuild all servers and computers. You have pending deadlines, but you cannot access your calendar.

Your company-issued cell phone must be wiped and rebuilt, and you don't know what data has been lost, what confidential information has been exposed and how long it will take to fix the problem and at what cost.

On average, a data breach can cost your business about $141 per lost or stolen record. That figure includes the cost of breach remediation efforts like a data forensic investigation, breach victim notification, credit monitoring and legal fees.

Additionally, Virginia has enacted a data breach notification law, which imposes a civil penalty of up to $150,000 per breach if it resulted from the organization's negligence. A poorly handled data breach can also cause irreparable damage to a reputation and erode consumer trust.

As then FBI Director Robert Mueller famously quipped in 2012, "I am convinced that there are only two types of companies: those that have been hacked and those that will be." Reputable studies put the risk of a breach of your business over the next 24 months at nearly 30 percent.

To mitigate the breach ahead of time, you need to establish a comprehensive team to assess your network security, develop a cybersecurity incident response plan, formulate employee policies and insure your firm for potential losses. Your IT department can't do it all. Attorneys must be in the mix.

The first step is to adopt a security framework to improve your ability to prevent, detect and respond to a cyber attack. A useful framework is NIST Special Publication 800-171, designed with private businesses in mind. It is relatively easy to understand and provides a sound road map for a robust cybersecurity infrastructure. It is also the required framework for defense contractors.

The next step is to engage an attorney who specializes in cybersecurity to create an incident response plan that defines the different kinds of data security events and how to respond to each one.

The plan assigns key employee roles and establishes lines of internal and external communications. It also serves as the guide for your breach attorney, who will not only start the investigation but also can keep it confidential as "attorney-work product." The plan should mandate testing and be updated at least annually.

Your attorney should also suggest cybersecurity policies that give employees notice and govern how they access your company networks.

Finally, be sure to obtain cybersecurity insurance. According to IBM Security and the Ponemon Institute, unsuspecting employees cause roughly 28 percent of data incidents by inadvertently clicking on a malicious email or losing a portable device filled with sensitive information. This is where cyber insurance kicks in.

Ask your agent to include coverage for ransomware payment in cryptocurrencies, and check on retroactive date exclusions. If a hacker gets access to your network, the resulting data incident could be considered an event that occurred prior to the policy period and would therefore be excluded.

Also, be certain your policy covers losses and expenses incurred as a result of business interruption due to a breach at a third-party upon which your company depends. And, ensure all employees, volunteers, interns and contractors performing work within the scope of your firm's business are included in the policy.

A comprehensive cybersecurity plan requires significant internal and external collaboration to address IT security, incident response plans, employee policies and insurance coverage. The key is to start now by following the steps above and having the right players on your team.

Darius Davenport *leads the cybersecurity and data privacy practice group at Crenshaw, Ware & Martin in Norfolk. He can be reached at 757-623-3000 or* ***ddavenport@ cwmlaw.com***.