It Adds Up Quickly

By Kari Stearn

Over the past decade, rapid advancements in technology have enabled a vast and expansive digital economy. As a result, medical practices of all sizes are using a broad range of personal and company-issued devices to keep employees connected to each other and to their workplace. But as connectivity grows, so too does the number of cybersecurity risks and threats.

It has been shown time and again that a seemingly harmless act like a misplaced laptop or a casual click in an email can put a practice, its employees, and its patients at risk. While we're constantly innovating to keep pace with these risks, we believe that education and preparedness is equally important when it comes to mitigating and preventing a cyber breach.

The claim below provides a real-life example of the impact and costs of a cyber breach, and the protections provided by cyber insurance.

An employee of a medical research institute carried his laptop with him to and from work each day. One day, the employee left the laptop in his car and returned to find the laptop had been stolen. The employee informed the institute, and the institute immediately notified its cyber insurance carrier of the incident. The carrier engaged legal counsel and an IT/forensics vendor to investigate the nature and scope of the data stored on the laptop. The findings revealed that the laptop contained the electronic protected health information (ePHI) of approximately 296,000 patients and research participants, including names, dates of birth, addresses, social security numbers, diagnoses, and laboratory results.

Because of the sensitive nature of the information stored on the laptop and the fact that the laptop was only password-protected and not encrypted, the institute was required by law to notify all affected individuals. As required by federal law, the breach was also reported to the Department of Health and Human Services, Office for Civil Rights (OCR), who launched an investigation. In addition, a public relations firm was hired to handle media inquiries and communications.

The OCR investigation revealed a host of violations and inefficiencies on the part of the institute. The agency determined that the institute's security management process violated HIPAA law because it was limited in scope, incomplete, and insufficient to address potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the institute. Further, the OCR claimed that the institute had failed to implement

proper mechanisms to safeguard ePHI and lacked appropriate policies and procedures for authorizing access to ePHI. To make matters worse, the institute faced multiple lawsuits filed by individuals affected by the breach.

Costs associated with the breach escalated quickly. Privacy breach response costs amounted to $960,000, including IT/forensic expenses, public relations fees, legal expenses, notification costs and credit monitoring. Defense expenses incurred in the OCR proceedings and patient lawsuits reached $860,000, and settlements amounted to a combined $2.1 Million. While the institute's cyber incident costs totaled $3.92 Million, $2.82 Million was covered by the policy, and the institute was responsible for the remaining $1.1 Million.

As previously announced, SVMIC added Cybersecurity Insurance as a supplemental coverage to each physician's policy and each practice entity's policy a couple of years ago. Please note, however, that it is "basic" coverage in that the coverage limits in most cases is up to $50,000, which is enough for some cyber-related claims but certainly not for situations described above. SVMIC recommends that practices review their individual situation to assess whether their needs are covered by this basic coverage. For more information, please contact SVMIC at 800.342.2239.
