Can healthcare providers afford not to have cyber insurance in 2018?

By Brooke Murphy, Content/Strategist Editor, *Becker's Hospital Review*

Cyberattacks targeted hospitals and health systems at an alarming pace in 2017 – nearly exceeding the rate of one breach per day. These attacks are more than an operational inconvenience; the legal services, public relation expenses and regulatory fines it takes to recover from data breaches and cyber extortion are extremely costly, especially for small and mid-sized provider groups. As cyber criminals and disgruntled employees attack healthcare organizations at increasing rates, many providers are purchasing cyber insurance policies to ensure they are prepared with the appropriate financial protections and expertise to weather these incidents and preserve their reputation.

"As cyber threats become the reality, and as [insurance] carriers have identified how significant and complex online exposure is, cyber liability policies have become more refined and more necessary," says James Fasone, senior vice president and national healthcare practice leader for Key Insurance & Benefits Services.

This article aims to help healthcare leaders assess the key coverage elements of cyber insurance for their organization by reviewing the scope of cyberattacks in 2017, examining various cyber risks and coverage opportunities, and discussing key trends affecting insurance needs in the next three to five years.

I. A growing and expensive problem

Healthcare organizations must weigh their preparedness for cyberattacks against the cost of cyber liability insurance and the potential costs of a breach, Mr. Fasone says. As cybercrime soars, these costs are becoming increasingly apparent. For the seventh consecutive year, healthcare ranked as the most expensive industry in which to suffer cyberattacks in 2017, according to Ponemon Institute. Patient data breaches cost organizations $380 per violated record – more than 2.5 times the global average of $144 per record across industries.

Direct costs required to deal with breaches include attorney fees, data forensics services to investigate, restore and delete malware, and material and labor expenses for patient notification and credit monitoring services. These costs are in addition to regulatory fines when patient data are compromised, which can reach $1.5 million per violation per year.

Indirect economic losses from a cyberattack, although more difficult to quantify, can be just as costly. Post-attack disruption to business and clinical services, lost productivity and harm to a company's reputation may cause long-felt harm to an organization's financial performance.

Reputation and patient trust hold utmost weight in healthcare, suggesting data breaches can directly affect patient volumes. Some surveys show up to 70 percent of consumers affected by a data breach will not return to a practice.

Despite providers' best efforts to protect themselves, the high likelihood of experiencing a breach is particularly troubling. Businesses face a 25 percent likelihood of experiencing a material breach involving at least 10,000 lost or stolen records, Ponemon found. High-profile data breaches in 2017 included the malware NotPetya, a "wiper" program infecting Merck Pharmaceuticals and Nuance Communications, and the breach at University of North Carolina Dermatology, which may have compromised 24,000 or more patient records.

Not all breaches are limited to data exposure. Monetizing cyberattacks through ransomware became a leading example of new and evolving digital risk since 2016.

Ransomware are malicious, self-propagating software infecting computers and restricting users' access to critical systems until a ransom is paid, typically in the cryptocurrency bitcoin. These malware are particularly difficult to eradicate and increasingly hackers' program of choice; ransomware sales

on the dark web grew more than 2,500 percent year-over-year. High-profile ransomware cases in 2017 included WannaCry, which canceled hundreds of operations across 47 NHS hospitals in May, and the attack on Erie County Medical Center in Buffalo, N.Y., which took the 550-bed facility offline for six weeks.

Unlike data breaches, ransomware threatens an organization's ability to function normally or perform critical services. How will physicians and care teams continue to care for patients if a virus takes an enterprise's computer systems offline? This is a question every health system and hospital leader must probe today. Patient injury or death arising from cyberattacks is becoming a realistic risk, as medical devices are increasingly connected to and dependent on the internet.

Despite the increased frequency of cyberattacks, many healthcare organizations lack the money, resources and expertise to manage data breaches caused by evolving cyber threats, preventable IT or employee mistakes, and other dangers. Although organizations increased investments in cybersecurity technology and expertise in the last year, the majority of healthcare providers reported little to no confidence in curtailing or minimizing data breach incidents in 2016, according to Ponemon. Recognizing this challenge, many health systems are purchasing cyber liability policies to help them weather the economic fallout from a cyberattack.

"

The cyber insurance industry in the last three to five years has rapidly evolved to meet the needs of healthcare businesses in a digital world. That means there are many more companies in the market offering a greater variety of coverage.

– James Fasone, Senior Vice President and National Healthcare Practice Leader for Key Insurance & Benefits Services.

II. Evolution of cyber liability insurance

Cyber liability insurance helps hospitals cover the costs of a data security breach for things like identity protection solutions, public relations, legal fees, liability and more due to loss, theft and unauthorized disclosure of data.

Deciding the type of cyber insurance to buy is no trivial matter; the aforementioned statistics illustrate the need for thoughtful discussion when it comes to purchasing coverage. This responsibility rests primarily with the board of directors and CFO. Directors and executives have the highest-level view of cyber risk across the organization and are best positioned to align insurance coverage with business objectives, asset vulnerability, third-party risk exposure and other external factors.

Although coverage has been available for over 20 years, cyber liability insurance has grown significantly in recent years and various types of policies are now available to organizations concerned with privacy breaches, data loss and ransom scenarios. A broker can be particularly valuable in helping leaders assess their organizations' risk and find bundled or standalone policies written to match their unique needs.

"The cyber insurance industry in the last three to five years has rapidly evolved to meet the needs of healthcare businesses in a digital world," Mr. Fasone says. "That means there are many more companies in the market offering a greater variety of coverage."

Mr. Fasone described three key domains of coverage healthcare organizations may consider when assessing cyber vulnerabilities.

1. Cyber forensics. Immediately following an attack or breach, cyber forensics investigators begin analyzing system information to understand the scope of damage. Most cyber insurance policies give healthcare organizations access to teams of computer forensic experts that

help providers fulfill regulatory reporting requirements as well as understand what happened and whom to notify.

2. Data breach notification and credit monitoring services. One cornerstone of a robust cyber insurance policy is the notification and response strategy by which providers appropriately and quickly respond to security breaches. Health systems must satisfy an important legal requirement when data are compromised, including patient notification. Currently, 47 of 50 states maintain data breach notification requirements. Each law demands the organization in question notify affected individuals when a breach occurs, and finer regulations regarding verbal phrasing and timeliness vary by state. Cyber insurance policies typically include legal services to support data breach notification processes which can help healthcare organizations get the right information to the right people at the right time. Breach notification specialists help hospitals write appropriate notification letters, establish call centers and respond to patient inquiries, alleviating organizations of substantial stress and financial burden.

3. Business interruption and crisis management. A business interruption policy offers financial protection if an organization's IT system is inoperable for a prolonged period of time following a breach.

Closely related to financial losses from a business interruption is a loss of goodwill or standing in the community. Brand awareness and reputation are increasingly valuable to provider organizations amid growing healthcare consumerism and competition. This makes minimizing negative press all the more critical following a data breach.

"The impact on reputational risk can be lessened if the organization moves quickly and effectively to manage the public relations and patient notification process," Mr. Fasone says. "[A quick response] would provide some assurance to the public and patients that we are a professional organization prepared for these events and we are going to take care of this as quickly as possible. Cyber insurance policies can provide a team of publicists and public relations experts to guide you through this process."

III. Other considerations for healthcare organizations

Mr. Fasone noted two other factors driving CFOs and healthcare leaders to see value in cyber coverage investments.

Cost-benefit analysis

Some healthcare leaders may be tempted to spend money fortifying cyber defenses rather than paying cyber insurance premiums. However, Mr. Fasone says the reality is no IT system is infallible. Providers can boast highly sophisticated cyber defenses and still risk exposure to low-tech threats, such as a disgruntled employee taking a laptop containing sensitive health data when he or she leaves the company. In fact, more than half of data breaches are attributed to mistakes, misuse or malicious acts by employees.

"The question executives have to ask themselves is, 'Are we absolutely certain that, regardless of the amount of money we spend, we won't be breached?' I think if you ask any IT professional out there, no matter the amount you put into protection, the answer is going to be, 'No.'"

As healthcare leaders grapple with the unpredictable nature of evolving cyber threats, providers see financial and strategic value in purchasing liability coverage.

Future merger, acquisition and affiliation plans

Value-based payment reform, in part, is driving consolidation as healthcare organizations aim to strengthen their foothold in the market and prepare to manage care across the continuum. Because the success of many of these partnerships depends on exchanging and using patient data, providers are challenged to connect multiple disparate legacy systems during mergers and acquisitions.

"As physician groups, hospitals and other providers consolidate and form strategic affiliations to broaden their networks, how you combine and connect your IT systems becomes one of the most complex items to get your arms around," Mr. Fasone says. "The nature of integrating IT systems means there could be more susceptibility to hacking and exposure risks."

Purchasing cyber liability coverage prior to a merger or acquisition ensures both organizations are financially protected should a breach or accidental exposure occur.

Conclusion

Healthcare organizations of all sizes are experiencing cyberattacks at increasing rates and realizing the significant financial costs associated with recovery. Purchasing cyber insurance is an important step in ensuring an organization is prepared for a cyber-related event. As the cyber insurance industry matures, policies will become more standardized. For now, this type of coverage is an evolving product in a dynamic market – something healthcare executives and hospital boards should closely monitor. As such, Mr. Fasone says organizations should partner with the right broker to understand precisely what each policy covers in different incidents.

"Don't assume that all cyber liability policies are created equal," Mr. Fasone said. "A good broker/consultant will work with you to fully understand your coverage options and limitations, as well as what's required of your practice for your coverage to adequately protect the unique exposures of a healthcare organization."