GALLAGHER BASSETT | SPECIALTY

EXISTING AND EMERGING CYBER RISK IN THE MEDICAL INDUSTRY

The healthcare industry is facing unprecedented challenges, not only as a result of the COVID pandemic, but also from its existing and emerging cyber risks. The industry has historically been targeted by cybercriminals due to the industry's vast collection of valuable medical data. However, the risks for the industry have grown even more acute recently as COVID has led more of its workforce to transition to a remote work environment, resulting in an expanded attack surface for cybercriminals to exploit. According to data reported by the U.S. Department of Health and Human Services in 2020, there was a 25% year-over-year increase in healthcare data breaches from the prior year. [1]Ransomware, hacking, and phishing attacks against organizations and their third-party vendors continued to rank among the top causes of data breaches for the industry. Not only are the costs of a data breach substantially higher for the healthcare industry as compared with other industries, but the industry is also facing significant enforcement activity and class action lawsuits. The healthcare industry's ability to manage these exposures through cyber insurance is also becoming more costly and difficult, as a hardening cyber insurance market is resulting in higher premium rates and greater scrutiny into organizations' cybersecurity controls during the underwriting process.

The Ransomware Threat

One of the main drivers for the increase in data breaches in the medical industry over the past year is the increasing threat of ransomware. The number of ransomware attacks impacting the industry increased sharply during the second half of 2020. As noted above, a key driver for this increase was the rapid transition to a remote work environment following COVID. Cybercriminals exploited new vulnerabilities created by this transition to launch e-mail phishing attacks, which are a top vector for ransomware attacks. [2]Ransomware attacks are enormously disruptive to organizations from an operational, legal, and patient care perspective. In 2020, around 560 healthcare provider facilities reportedly fell victim to ransomware attacks in 80 separate incidents. [3]One of the most significant of these attacks was the attack on Universal Health Services, which operates around 400 hospitals and other healthcare facilities. One report noted that "the impact of the attack was alarming: ambulances were rerouted, radiation treatments for cancer patients were delayed, medical records were rendered temporarily inaccessible and, in some cases, permanently lost, while hundreds of staff were furloughed as a result of the disruptions." Another attack on University of Vermont Health Network resulted in $1.5 million a day in increased expenses and lost revenue and resulted in the health system being forced to operate under Electronic Healthcare Record (EHR) downtime procedures for over a month. The attack could ultimately cost the health network over $63 million.

Cybercriminals are continuing to evolve their ransomware attacks to maximize payouts. Increasingly, attackers are putting tight deadlines on their ransom demands of around three to seven days, which if not met, will result in the attacker releasing the organization's data. Threat actors are also increasingly exfiltrating sensitive data off the healthcare organizations' networks in order to extort money from the organizations or to sell the data to third parties.

The consequences of a ransomware attack can be more harmful for the healthcare industry than for other industries due to the very real possibility of patient injuries and deaths. For example, in September 2020, an ambulance taking a 78-year-old woman, suffering from an aortic aneurysm, to her local university hospital in Dusseldorf, Germany was redirected to another hospital 32 kilometers away due to a ransomware attack on her local hospital, leading to a one-hour delay in the patient receiving treatment—and the patient's premature death. The growing prevalence of various connected medical devices in healthcare organizations, such as infusion pumps and CT scanners, also has increased the likelihood that a ransomware attack on a medical organization could have serious implications for patients if these devices are forced offline.

One of the first questions that must be addressed following a ransomware incident is whether or not the organization should pay the ransom. This requires thoughtful consideration of a number of factors. For example, does the organization have viable backups from which to restore its data if it does not pay the ransom? Even if it does have viable backups, it could still take weeks, or longer, to fully restore an organization's data. Under such circumstances, paying a ransom might be the most expedient solution. Another consideration is whether the criminal organization behind the incident has a history of living up to its promises. It is also critical to know whether the cybercriminals may have exfiltrated data off the victim's network, which is increasingly the case. If an organization does decide to make a ransom payment, before the payment is made, it must confirm that the threat actor is not a sanctioned group under the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), or risk potential sanctions.

Cybersecurity vendors who specialize in negotiating and responding to ransomware incidents can

provide critical assistance to organizations in dealing with a ransomware incident. One of the many benefits of cyber insurance is having immediate access to the carrier's panel of experienced and vetted cybersecurity vendors, including breach counsel, forensics, and ransom negotiators, who can help organizations assess and effectively respond to a ransomware incident. Victims should also consider notifying law enforcement, such as the FBI's Internet Crime Complaint Center, since reporting such incidents provides law enforcement with a greater understanding of the threat.

Other Cyber Risks Affecting Healthcare Organizations

Aside from ransomware incidents, there are numerous other types of cyber threats that healthcare organizations also need to manage and avoid. While this article will not detail all of the cyber threats impacting the medical industry, we focus on several of the most significant risks below.

Third-Party Vendors: Data reported to HHS in 2020 revealed that 30% of all breaches impacting the healthcare industry involved a business associate. [4]Two major incidents in 2020 highlighted the risks to the healthcare industry in relation to third-party vendors. First, Blackbaud, a company that sells software to not-for-profits to support fundraising, marketing, and operations, reported a ransomware attack affecting at least 100 healthcare clients and patient data of at least 10 million people. Blackbaud is now facing regulatory investigations as well as more than 20 lawsuits for breach of contract and invasion of privacy. Some healthcare organizations are also now being named in class action lawsuits arising out of the Blackbaud incident. [5]Second, SolarWinds, a company that sells the Orion software, which allows organizations to view the inside of their computer networks, reported that Russian hackers had inserted malicious code into an Orion update. Around 18,000 SolarWinds customers installed the tainted update onto their systems, giving the hackers substantial access to their computer systems. One of the affected customers was the California Department of State Hospitals. [6]

Hacking Incidents: Hacking is the largest root cause of data breaches for the healthcare industry. In 2020, hacking was responsible for about 67% of all reported breaches and 92% of all breached records. [7]Hacking incidents can often be traced to leaked credentials. One reason why the costs of a data breach are higher for the healthcare industry than other industries is that the average time to identify and contain a data breach is longer than other industries. [8]In general, the length of the hacking incident is correlated to the cost of the incident. In 2020, Dental Care Alliance (DCA), a dental support organization with over 320 affiliated dental practices in 20 states, reported one of the largest hacking incidents of the year. In that incident, over one million individuals' dental records were potentially stolen.

Phishing: Hackers are also continuing to rely on e-mail phishing as a key strategy to target victims in healthcare organizations. Phishing e-mails are frequently used to spoof a trusted sender and trick unsuspecting victims into inserting their credentials onto a fake login page. In addition, phishing campaigns frequently deliver malware, including ransomware. Other malware variants can allow hackers to steal data, capture keystrokes, take screenshots, and launch malicious code. The largest phishing attack for the healthcare industry in 2020 involved MEDNAX Services, Inc., a provider of revenue cycle management and other administrative services to affiliated physician practice groups. In that attack, hackers were able to gain access to MEDNAX's Office 365 environment and potentially accessed electronic health information (e-PHI) of 1,670 individuals.[9]

Insider Threats: While high-profile data breaches by cybercriminals generally capture news headlines, a significant percentage of breaches are the result of basic employee negligence, including unauthorized access or disclosure incidents. This includes employees bringing Protected Health Information (PHI) home or sending PHI to a personal account or device, viewing data without the proper authorization, and e-mail errors, such as sending PHI to incorrect recipients. Such incidents accounted for about 21% of all data breaches reported to HHS in 2020. [10]Healthcare organizations have made significant strides in tightening their administrative, physical, and technical controls, leading to a decrease in these types of incidents.

Duty to Notify Patients, Regulators, Business Partners

Following a data breach, organizations may have a legal duty to report the incident, depending on the type of data that was potentially compromised. Such duty may be based on contractual requirements, state law, or federal law. Healthcare organizations who are considered a "covered entity" under Health Insurance Portability and Accountability Act (HIPAA), as well as their "business associates," will be required to report certain breaches to the Office of Civil Rights (OCR) pursuant to HIPAA. Organizations may also have a duty under state law to notify affected individuals and/or regulatory authorities of a breach of Personally Identifiable Information (PII). Organizations must comply with the notification laws of the states in which the affected individuals reside, which may have different definitions of what constitutes PII, as well as different notification requirements. Organizations may also have contractual obligations to notify certain business partners in the event of a data breach. The decision of whether to notify, who to notify, and how to notify often requires a complex legal analysis. Therefore, it is strongly recommended that organizations consult with legal counsel prior to sending out any notifications. Notifying improperly could have negative consequences for an organization, including an increased likelihood of class actions or regulatory actions. Furthermore, consulting with legal counsel who are experienced in handling data breach matters can help organizations better respond to the numerous inquiries they are likely to receive following the breach notification.

Post-Breach Regulatory Investigations and Class Action Litigation

The completion of an investigation and notification of a breach unfortunately does not necessarily signify the end of a cyber incident. In many cases, it merely marks the beginning of class action lawsuits and regulatory proceedings against the organization, both of which can result in multi-million dollar settlements.

The U.S. Department of Health and Human Services' OCR has the responsibility to enforce the Privacy and Security Rules of the HIPAA, standards for the protection of certain e-PHI, through voluntary compliance activities and the imposition of civil monetary penalties. In 2020, the OCR engaged in significant enforcement activity against healthcare organizations. One major development was OCR's recent settlement with Anthem, Inc. Anthem agreed to a $16 million settlement and substantial corrective action to settle potential violations of the HIPAA privacy and security rules related to a 2014 data breach that exposed nearly 79 million individuals' health data. OCR also entered into a $6.85 million settlement with Premera Blue Cross over HIPAA privacy and security rules violations stemming from a 2014 data breach that impacted over 10.4 million individuals' e-PHI. While the likelihood of an OCR enforcement action is fairly low, as the above incidents demonstrate, sizeable monetary penalties can be imposed if OCR finds that the healthcare organization's actions were particularly egregious.

Healthcare organizations also face significant potential exposure from class action lawsuits following a data breach. Such lawsuits will typically assert common law causes of action, including negligence, fraud, etc., as well as statutory claims. The California Consumer Privacy Act (CCPA) is one statute that has become a new focus for plaintiffs' counsel in data breach litigation since it has been in effect.

Healthcare organizations also reported a number of significant class action settlements in 2020 resulting from data breach incidents. Anthem settled its class action lawsuit relating to its 2014 data breach for $115 million. [11]In addition, Premera Blue Cross agreed to a $74 million settlement arising from a 2014 cyber-attack impacting 10.4 million records, comprised of $32 million in damages and $42 million to improve its data security.

Given the sharp increase in security incidents impacting healthcare organizations in 2020, a proportionate increase in data breach litigation is expected in 2021.

Cyber Insurance Coverage for Healthcare Organizations

Cyber liability insurance policies provide first- and third-party protection to businesses in the event that sensitive information is compromised. They cover the first-party costs (expenses that an organization incurs directly due to a cyber incident), such as the cost to investigate and respond to a breach. They also provide first-party coverage for other types of loss resulting from a cyber incident, such as business interruption loss, data recovery costs, and extortion demands. As previously discussed, a cyber policy also provides access to the carrier's panel of experienced and vetted cybersecurity providers who can quickly assist policyholders with investigating and responding to a data security incident.

Cyber insurance policies further provide liability coverage to policyholders for third-party lawsuits or regulatory proceedings against them arising out of a data or network breach. Third-party liability coverage helps pay for both damages (settlements and judgments) the policyholder is legally obligated to pay and claim expenses (attorney's fees and court costs) to defend the policyholder against the claims.

Finally, many cyber insurance policies now also include some limited eCrime coverage. This may include certain coverages typically found under a crime policy, such as social engineering, funds transfer fraud, or invoice manipulation coverage. It is evident that the costs of a cyber incident can be devastating to a business. Research has shown that healthcare has the most expensive data breach costs on average, at $7.13 million per incident, which is an increase of 10% from 2019.[12]

Cyber insurance is the most effective mechanism available for businesses to cover financial losses due to a cyber incident. There is ample evidence that the cyber insurance market is presently hardening due to increased frequency and severity of claims, reduced reinsurance capacity, and low interest rates. [13]Cyber insurance carriers have started making significant changes in their underwriting practices to manage their increased exposure. Such changes include pursuing rate increases of up to 15% to 50% per year, doubling and tripling deductibles and retentions, reducing policy limits, using sub-limits or co-insurance to manage ransomware exposure, and narrowing and tightening coverage wordings. Carriers are also becoming increasingly disciplined in the risk selection process, requiring a greater amount of data from applicants and scrutinizing applicants' data protection controls and compliance with regulatory requirements. Supplemental applications addressing ransomware risks specifically are also becoming more common. Carriers are also increasingly relying on security scans to gain a better understanding of the organization's cybersecurity vulnerabilities. In the wake of the SolarWinds ransomware incident, many carriers now ask applicants about whether the organization knows of any exposure as a result of that incident and may include a SolarWinds Exclusion in the policy. Some carriers also have non-renewed policies, where the organization cannot show that Multi-Factor Authentication (MFA) has been implemented across the organization.

Summary

Healthcare organizations face growing and evolving cyber risks that threaten not only their bottom line and reputation, but also patients' health and safety. There is no indication that these risks will abate any time in the foreseeable future. Just as the best defense is a good offense, the medical industry should invest in security, such as endpoint monitoring and pen testing, to reduce the average time to identify and respond to a breach as well as to reduce the potential cost of a breach. Employee training, particularly in relation to avoiding phishing e-mails, can be very effective in reducing the risk of a ransomware attack. Finally, cyber insurance, though it may be more costly and difficult to acquire than in previous years, is still an effective mechanism to manage an organization's cyber risk exposure and help an organization respond more quickly and effectively to a data breach.

Author

Lisa Jaffee

Sources

[1]"2020 Healthcare Data Breach Report: 25% Increase in Breaches in 2020," HIPAA Journal, https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/, Jan. 19, 2021.

[2]Coveware statistic.

[3]"The State of Ransomware in the US: Report and Statistics 2020," Emisoft, Jan. 18, 2021.

[4]"2020 Healthcare Data Breach Report: 25% Increase in Breaches in 2020," HIPAA Journal, https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/, Jan. 19, 2021.

[5]"Rady Children's sued over Blackbaud data breach: 8 details, Becker's Health IT," Jackie Dress, https://www.beckershospitalreview.com/cybersecurity/rady-children-s-sued-over-blackbaud-data-breach-8-details.html, Jan. 26, 2021.

[6]"SolarWinds Hack Victims: From Tech Companies to a Hospital and University," Kevin Poulson, Robert McMillan and Dustin Volz, https://www.wsj.com/articles/solarwinds-hack-victims-from-tech-companies-to-a-hospital-and-university-11608548402, Wall Street Journal, Dec. 21, 2020.

[7]"2020 Healthcare Data Breach Report: 25% Increase in Breaches in 2020," HIPAA Journal, https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/, Jan. 19, 2021.

[8]Cost of a Data Breach Report 2020, IBM Security, at p. 54.

[9]"2020 Healthcare Data Breach Report: 25% Increase in Breaches in 2020," HIPAA Journal, https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/, Jan. 19, 2021.

[10]Id.

[11]At the time of this whitepaper, the settlement is still awaiting court approval.

[12]Cost of a Data Breach Report 2020, IBM Security, at p. 25–26.

[13]"US Cyber Insurance Market at Exciting Crossroad," Bethan Moorcraft, https://www.insurancebusinessmag.com/us/news/cyber/us-cyber-insurance-market-at-exciting-crossroad-236496.aspx, Insurance Business America, Oct. 16, 2020.

GALLAGHER BASSETT

insurers.gallagherbassett.com