AMERICAN BANKRUPTCY INSTITUTE
JOURNAL
The Essential Resource for Today's Busy Insolvency Professional

Cyber-U

By Nicolette Corso Vilmos and Wesley McCulloch

Health Care Companies Face Financial Strain from Data Breaches

Nicolette Corso Vilmos
Nelson Mullins Riley
& Scarborough, LLP
Orlando, Fla.

Wesley McCulloch
Nelson Mullins Riley
& Scarborough LLP
Nashville, Tenn.

Nicolette Corso Vilmos is a partner with Nelson Mullins Riley & Scarborough, LLP in Orlando, Fla. Wesley McCulloch is an associate in the firm's Nashville, Tenn., office.

The intersection of health and bankruptcy law could not be more pronounced in the event of a cataclysmic event. A cyberattack is such an event. Following the cyberattack on Colonial Pipeline, which led to a multiday shutdown of the pipeline and an East Coast fuel shortage, the Department of Justice (DOJ) heightened the priority of ransomware attacks.[1] Recognizing the devasting impact that cyberextortion can have on individuals, businesses and supply chains, the DOJ now has protocols in place to treat ransomware attacks the same way it treats terrorism.[2] The health care industry has increasingly become a victim of these devastating cyberattacks.[3] Notorious for lax and outdated cyberprotection, health care companies provide the perfect combination of being an easy target with an abundance of data, not to mention the tangible risk to patient well-being and the unique financial pressures associated with breaches of electronic protected health information (ePHI).[4]

The combined costs of internal incident response, notifications to consumers, defense costs, and fines and damages are staggering, with the average cost of a health care data breach approaching $10 million.[5] As a result, even a single cyberattack can strain the financial solvency of health care organizations and push them to the brink of bankruptcy. Therefore, health care organizations should view cyberattacks as a risk to the survivability of the business as a whole and implement techniques to mitigate the occurrence of cyberattacks and the financial fallout that results.

Increased Cyberattacks on the Health Care Sector

Data breaches in the health care sector have set an annual record high since 2016,[6] and these breaches often compromise astronomical amounts of patient information.[7] A study on health care data breaches from 2020 found that an average of 40,000 people were impacted by each breach.[8] During the first six months of 2019, 31.6 million health care records were breached.[9]

Hackers infiltrating health care companies' networks are typically targeting ePHI,[10] which can include medical records, health insurance information and patient-identifying information such as Social Security numbers and addresses.[11] By gaining access to sensitive health, demographic and financial data, hackers profit by selling the information on the dark web, leading to an increased risk of patient identity theft, home equity loan fraud and tax fraud.[12] The Verizon 2021 Data Breach

[1] Christopher Bing, "Exclusive: U.S. to Give Ransomware Hacks Similar Priority as Terrorism," Reuters (June 3, 2021), *available at* reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03 (unless otherwise specified, all links in this article were last visited on June 28, 2021).

[2] *Id.*

[3] Hannah Mitchell, "Healthcare Hackers Demand $4.6M in Ransom on Average," *Becker's Health IT* (May 5, 2021), *available at* beckershospitalreview.com/cybersecurity/healthcare-hackers-demand-4-6m-in-ransom-on-average-6-other-report-findings.html.

[4] Andrew Steger, "What Happens to Stolen Healthcare Data?," *HealthTech* (Oct. 30, 2019), *available at* healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

[5] "2020 Cost of a Data Breach Report," IBM, *available at* ibm.com/security/digital-assets/cost-data-breach-report.

[6] "Healthcare Data Breach Statistics," *HIPAA Journal*, *available at* hipaajournal.com/healthcare-data-breach-statistics. HIPAA stands for the "Health Insurance Portability and Accountability Act."

[7] *See* "Cases Currently Under Investigation," U.S. Dep't of Health and Human Servs. Office for Civil Rights, *available at* ocrportal.hhs.gov/ocr/breach/breach_report.jsf. Steve Alder, "First Half of 2019 Sees 31.6 Million Healthcare Records Breached," *HIPAA Journal* (Aug. 2, 2019), *available at* hipaajournal.com/first-half-of-2019-sees-31-million-health-care-records-breached.

[8] Mitchell, *supra* n.3.

[9] Alder, *supra* n.7.

[10] "Healthcare Data Breach Statistics," *supra* n.6.

[11] Steve Alder, "What Is Protected Health Information?," *HIPAA Journal* (Jan. 10, 2021), *available at* hipaajournal.com/what-is-protected-health-information.

[12] Brian Stack, "Here's How Much Your Personal Information Is Selling for on the Dark Web," Experian, (Dec. 6, 2017), *available at* experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web; Andrew Steger, "What Happens to Stolen Healthcare Data?," HealthTech (Oct. 30, 2019), *available at* healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

Investigation Report (DBIR) found that of the data incidents surveyed, 66 percent of the data breached was personal data and 55 percent was medical data.[13]

Cybersecurity attacks in this sector are *not only* aimed toward hospitals and doctor's offices, but also pharmacies, insurance companies and business associates of health care providers.[14] A 2020 survey of more than 1,000 data breaches found that one out of five incidents targeted the health care sector.[15] Data breaches in health care increasingly come from ransomware that often gains access to a company's network through phishing emails.[16] Ransomware is used to infiltrate electronic devices and encrypt valuable files, making them unusable.[17] Once ransomware actors have encrypted the files, they then demand monetary payment to decrypt the files and threaten to lock out the user permanently — or even sell the data on the black market.[18] Other sources of vulnerability for health care entities are their business associates and vendors.[19] Health care companies share credentials and grant remote access to their business associates and vendors, thus increasing their risk of a data breach.[20]

The financial fallout of these breaches and the marked increase in dollar amounts at stake can be calamitous for health care companies. In 2020, the average initial ransom demanded by hackers in attacks on the health care sector was roughly $4.5 million and the average paid out by health care companies was approximately $900,000.[21] In addition to potential ransom payouts and remediation costs, health care companies that experience a data breach for failure to comply with HIPAA security regulations can be subject to substantial fines and can face massive lawsuits brought by those impacted by the breach.[22]

The Department of Health and Human Services Office of Civil Rights (OCR), which investigates reported breaches of protected health information under HIPAA, is willing to impose fines and require costly audits and compliance-monitoring of entities that manage data-protected health information. The OCR settled more than $13 million in penalties alone in 2020.[23]

Data breaches can also trigger notice and credit-monitoring obligations under both HIPAA and state law, which can be extremely costly. As a result, covered entities in multiple states must also review each individual state law to determine compliance obligations. State attorneys general also enforce their own data-protection and trade-practice laws in the wake of large-scale breaches. Recognizing the ever-increasing risks of these attacks, the Healthcare and Public Health Sector Coordinating Council recently urged President Joe Biden to include cybersecurity for the health care industry in his infrastructure plan.[24]

Hospital Cyberattacks

Given the impact and increased frequency of these cyberattacks, hospital systems have continued to make disturbing headlines over the past year, particularly as these attacks have involved the use of sophisticated ransomware to paralyze providers and endanger patients. As a result, hospitals suffer unique ethical concerns in providing acute health services and protecting patient data, but also staying financially afloat.

In September 2020, Universal Health Services Inc., one of the nation's largest hospital chains, suffered a crippling ransomware attack.[25] In response, Universal shut down computer systems used for medical records, laboratory tests and pharmacy information across nearly 250 of its facilities, causing Universal to divert patients and cancel surgeries.[26] Although Universal later confirmed in February 2021 that the weeks-long disruption did not result in a data breach or require a ransom payment, the company did not emerge unscathed.[27] Due to the inability to take on patients as normal and expenses to restore its systems, Universal indicated that the cyberattack cost the company $67 million before taxes.[28] During a similar cyberattack in October 2020, Sky Lakes Medical Center in Oregon estimated $10 million in costs and lost revenue.[29] While a cyberhacker may have the option to wait for weeks on end for a ransom payment, a patient scheduled for an important surgery might not have that luxury. Further, cyberattacks impose substantial financial pressure on health care providers as they rebuild both their electronic infrastructure and public image, even absent the prospect of possible ransom payments or statutory fines from a data breach.

While present news headlines are reason enough for concern, health care providers should find recent litigation instructive as to the importance of maintaining robust cybersecurity infrastructure and the associated risks of falling short. In 2015, Anthem, one of the nation's largest health insurance companies, suffered a massive data breach, with nearly 79 million people impacted.[30] In this case, the hackers gained access to the private information of Anthem's members and employees, such as names, birthdays, Social Security numbers and home addresses.[31]

[13] Hannah Mitchell, "85% of Data Breaches Caused by Defrauding Humans, Not Exploiting Software," *Becker's Health IT* (May 20, 2021), *available at* beckershospitalreview.com/cybersecurity/85-of-data-breaches-caused-by-defrauding-humans-not-exploiting-software.html.

[14] "Cases Currently Under Investigation," *supra* n.7.

[15] Mitchell, *supra* n.3.

[16] *See* Steve Alder, "Healthcare Industry Cyberattacks Increase by 45%," *HIPAA Journal* (Jan. 6, 2021) *available at* hipaajournal.com/healthcare-industry-cyberattacks-increase-by-45; Michael Lichtenstein & Lori Khan, "Health Care Facilities Are Under Cyberattack; Cyber Insurance Provides a Valuable Defense - February 2021," *J.D. Supra* (February/March 2021), *available at* jdsupra.com/legalnews/health-care-facilities-are-under-4693994.

[17] "Ransomware Guidance and Resources," Cybersecurity & Infrastructure Sec. Agency, *available at* cisa.gov/ransomware.

[18] *Id.*

[19] Ellen Neveux, "Healthcare Data: The New Prize for Hackers," *SecureLink* (Feb. 5, 2020), *available at* securelink.com/blog/healthcare-data-new-prize-hackers.

[20] *Id.*

[21] Mitchell, *supra* n.3.

[22] Scott Ikeda, "Healthcare Cyber Attacks Rise by 55%, Over 26 Million in the U.S. Impacted," *CPO Magazine* (Feb. 26, 2021), *available at* cpomagazine.com/cyber-security/healthcare-cyber-attacks-rise-by-55-over-26-million-in-the-u-s-impacted; *see infra* n.36-43 and accompanying text.

[23] Steve Alder, "2020 HIPAA Violation Cases and Penalties," *HIPAA Journal* (Jan. 13, 2021), *available at* hipaajournal.com/2020-hipaa-violation-cases-and-penalties.

[24] "President Urged to Include Health Care Cybersecurity in Infrastructure Plans; DOJ Prioritizes Ransomware Attacks," Am. Hosp. Ass'n (June 11, 2021), *available at* aha.org/news/headline/2021-06-11-president-urged-include-health-care-cybersecurity-infrastructure-plans-doj.

[25] Robert McMillian & Melanie Evans, "Ransomware Attack Hits Universal Health Services," *Wall St. J.* (Sept. 28, 2020), *available at* wsj.com/articles/ransomware-attack-hits-universal-health-services-11601341873.

[26] *Id.*

[27] Melanie Evans & Robert McMillan, "Cyberattacks Cost Hospitals Millions During COVID-19," *Wall St. J.* (Feb. 26, 2021), *available at* wsj.com/articles/cyberattacks-cost-hospitals-millions-during-covid-19-11614346713.

[28] *Id.*

[29] *Id.*

[30] *See* Rachel Z. Arndt & Shelby Livingston, "Anthem's $16M Breach Settlement Reminds Others to Assess Their Cyber Risks," *Modern Healthcare* (Oct. 16, 2018), *available at* modernhealthcare.com/article/20181016/NEWS/181019913/anthem-s-16m-breach-settlement-reminds-others-to-assess-their-cyber-risks (indicating that user at one of Anthem's subsidiaries opened phishing email and provided remote access to its systems).

[31] *Id.*

Anthem faced record-breaking monetary consequences from all angles. The OCR found that Anthem should have implemented measures to prevent hackers from gaining access to private information once they had entered its system.[32] The OCR fined Anthem $16 million, the largest fine to date, noting that a "'breach of trust' calls for a large penalty."[33] Consumers also brought a class action against Anthem for compromising their personal data. After nearly three years of litigation in 2018, a California federal judge approved a settlement for $115 million to cover credit-monitoring and out-of-pocket expenses for the class members,[34] not including the $31 million awarded in attorneys' fees.[35]

Although Anthem has not been pushed into bankruptcy by these staggering figures and has continued to grow as a business,[36] its negligence in maintaining its electronic infrastructure should serve as a warning to other health care businesses. Even though Anthem's data breach did not impact critical patient care, as has occurred with other hospitals, all health care providers should be aware that cyberattacks and corresponding data breaches can pose more than hefty litigation expenses and statutory penalties.

Another costly example is the data breach at American Medical Collection Agency (AMCA), which provided medical debt-collection services to laboratories and medical testing facilities such as Quest Diagnostics and LabCorp.[37] From August 2018 to March 2019, an unauthorized user breached AMCA's systems and compromised at least 24 million patient records.[38] Despite receiving multiple notices from the banks that processed its payments about potential security breaches, AMCA did not discover the intrusion until March 2019.[39] AMCA began notifying its clients in June 2019, and filed for bankruptcy within a few weeks.[40]

The direct costs of the breach were substantial. By June 2019, AMCA had incurred more than $400,000 in professional service fees alone to investigate and remediate the breach.[41] In addition, AMCA spent approximately $4 million to mail notices to 7 million affected individuals, representing only a fraction of the individuals ultimately affected.[42]

AMCA was also subject to claims from the attorneys general of 41 states where the affected individuals resided. In December 2020, AMCA obtained permission to settle the claims with the state creditors and filed to dismiss the bankruptcy.[43] As part of the settlement agreement, which was reached in March 2021, AMCA must develop and implement a new written information security program and incident-response plan, hire a third-party auditor to assess its new program, and provide ongoing cooperation with the attorneys general in investigating the breach.[44] AMCA will owe the states $21 million if it fails to comply with the settlement.

Mitigating a Breach's Financial Impact

Studies have shown that implementing cybersecurity measures to prevent an attack can, depending on the incident, represent an economic value of $400,000 to $1.4 million in savings versus containment, remediation and recovery costs.[45] Strong cybersecurity measures can also limit the scope of the breach, such as when the nation's largest propane provider was recently able to limit a security breach to only an 8-second intrusion that affected only 123 individuals.[46]

Maintaining cybersecurity controls can also impact fines. The OCR might consider several factors in assessing fines or requiring audits, including the nature and extent of the violation, nature and extent of the harm to the individuals affected, and whether a substantial fine would jeopardize the entity's ability to provide health care. Beginning in March 2021, the OCR must also consider whether the entity had "recognized security practices" for at least 12 months prior to the violation.

Cyberinsurance might also provide monetary relief, although in the case of ransomware payments, particular issues arise. If the cost of payouts begins to exceed the costs of replacing and restoring equipment and data, insurers will be less likely to continue underwriting such policies. In addition, the act itself of making ransom payments presents risks. First, there is no guarantee that the attacker will release ransomed assets once the payment has been made. As a result, the Federal Bureau of Investigation (FBI) does not recommend making these payments.[47] Second, making ransom payments raises questions of whether the payment constitutes funding terrorist groups and rogue states. The Department of the Treasury's Office of Foreign Asset Control has warned that entities making ransom payments to designated malicious cyberactors risk government sanctions.[48]

Conclusion

Robust cybersecurity practices are a must for any health care organization. When a cyberattack occurs, health care providers face the immediate concern of patient well-being, but also struggle to protect health information and reduce the financial impact to continue providing care. A quality information-security program helps reduce the likelihood, scope and impact of any secu-

[32] *See id.*

[33] *Id.* "Before Anthem, OCR's highest fine was $5.5 million — levied against Hollywood, Fla.-based Memorial Health System in 2017 for a breach that affected more than 115,000 people." *Id.*

[34] Kevin Stawicki, "$115M Anthem Data Breach Deal Gets Final Nod," *Law360* (Aug. 16, 2018), *available at* law360.com/articles/1073957 (subscription required to view).

[35] "Attorneys in Anthem Data Breach Settlement Get Fees Slashed," *Bloomberg Law* (Aug. 17, 2018), *available at* news.bloomberglaw.com/privacy-and-data-security/attorneys-in-anthem-data-breach-settlement-get-fees-slashed.

[36] *See* Arndt & Livingston, *supra* n.30.

[37] Matthew Jeweler, Meighan O'Reardon & Curtis Simpson, "From Data Breach to Bankruptcy — A Cautionary Tale for Those Without Cyber Insurance," *J.D. Supra* (July 16, 2019), *available at* jdsupra.com/legalnews/from-data-breach-to-bankruptcy-a-17755.

[38] "24.4M Patients, 21 Companies Now Say They Were Affected by AMCA Data Breach," Advisory Bd., *available at* advisory.com/en/daily-briefing/2019/08/13/data-breach.

[39] "AG Racine Announces Settlement with American Medical Collection Agency over 2019 Data Breach Affecting 12,530 District Residents," Office of the Attorney Gen. for the District of Columbia (March 11, 2021), *available at* oag.dc.gov/release/ag-racine-announces-settlement-american-medical.

[40] Jeweler, O'Reardon & Simpson, *supra* n.37.

[41] *Id.*

[42] *Id.*

[43] *See* "AG Racine Announces Settlement," *supra* n.39.

[44] *Id.*

[45] "Study: Preventing Cyberattack Penetration Can Save Enterprises Up to $1.4 Million Per Incident," *Bus. Wire* (April 7, 2020), *available at* businesswire.com/news/home/20200407005031/en/Study-Preventing-Cyberattack-Penetration-Save-Enterprises-1.4.

[46] Ax Sharma, "Largest U.S. Propane Distributor Discloses '8-Second' Data Breach," *Bleeping Computer* (June 15, 2021), *available at* bleepingcomputer.com/news/security/largest-us-propane-distributor-discloses-8-second-data-breach.

[47] "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations," Fed. Bureau of Investigation Internet Crime Complaint Cent. IC3 (Oct. 2, 2019).

[48] "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," U.S. Dep't of the Treasury (Oct. 1, 2020), *available at* home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

rity incident, which not only drives down direct mitigation costs, but may also lessen fines and the remedial measures that could result.

Falling prey to cyberattacks will force many health care entities to seek bankruptcy relief. However, the most effective way to address future cybersecurity incidents is to plan today. By taking steps now, health care entities and business associates can reduce the financial impact when a cybersecurity incident does occur. Doing so might help hedge against catastrophic financial strain on the company as a result of the attack, in turn preventing the need for bankruptcy. abi

Reprinted with permission from the ABI Journal, Vol. XL, No. 8, August 2021.

The American Bankruptcy Institute is a multi-disciplinary, nonpartisan organization devoted to bankruptcy issues. ABI has more than 12,000 members, representing all facets of the insolvency field. For more information, visit abi.org.