COSMOS
Navigate the Compliance Universe

Compliance Today - June 2022
Ransomware and the healthcare industry

By Nathan Reilly, Kate Driscoll, and Melissa Crespo

Nathan Reilly (nreilly@mofo.com) and **Kate Driscoll** (kdriscoll@mofo.com) are Of Counsel in the New York City office, and **Melissa Crespo** (mcrespo@mofo.com) is Of Counsel in the Washington, DC, office of Morrison & Foerster LLP.

Nathan Reilly

Kate Driscoll

Melissa Crespo

As the threat of ransomware has grown across sectors and industries, the impact on healthcare organizations has been particularly stark. Ransomware attacks on healthcare providers threaten not only patients' privacy and the economic well-being of the providers, but they also can compromise healthcare outcomes and facilities' ability to care for those in need. Healthcare organizations have been and remain prime targets for these attacks as they maintain valuable electronic sensitive personal health records and provide critical, often lifesaving, services that require continued access to systems. Businesses suffered roughly 50% more cyberattacks each week in 2021 when compared to the prior year, with cyberattacks reaching an all-time high in the fourth quarter of the year.[1] Sector-specific attacks on healthcare entities increased by a stunning 71%. This trend, and the corresponding exponential growth in the economic cost of ransomware—predicted earlier to have reached $20 billion in 2021—show no sign of slowing.[2]

Ransomware operators have targeted healthcare systems of all types: from multinational companies to small, independently owned offices. Ransomware attacks typically arise from unauthorized access to healthcare networks through a variety of means, including exploiting weaknesses in Remote Desktop Protocol, compromising software vulnerabilities, and phishing emails that include weaponized malicious links or attachments.[3] In many cases, ransomware operators steal files in addition to encrypting the servers and workstations in an effort to increase leverage and force a ransom payment from the victim. The ransom letter typically instructs victims to contact the actors through an online portal to complete the transaction. If the ransom is not paid, the stolen data is sold or published on the dark web and the decryption key is deleted. In some instances, even when a ransom is paid, not all of the encrypted data is restored.

Ransomware attacks on healthcare systems have compromised millions of personal health records and undermined the timely delivery of health services, at times resulting in grave health outcomes.[4] A 2021 report issued by the Cybersecurity & Infrastructure Security Agency indicated a strong positive correlation between cyberattacks and increased mortality.[5] In a recent survey, 70% of health organizations queried reported that "healthcare ransomware attacks have resulted in longer lengths of stays in hospital and delays in procedures and tests that have resulted in poor outcomes including an increase in patient mortality."[6] Another report found that more than 50% of internet-connected devices in hospital settings are vulnerable to hacking. Ransomware attacks can also lead to substantial financial costs in regaining control of hospital systems and patient data as well as potential future litigation.The ransomware landscape is dynamic as cybercriminals continue to develop

tactics to increase extortion pressure and maximize their pay. Given the evolving nature of ransomware attacks, all healthcare organizations need to be armed with the tools and expertise to prevent and—in the event of an attack—swiftly respond to minimize business disruption and provide continuity of care.

The law enforcement response

Whether measured in terms of the economic costs of ransoms and recovering from digital extortion or in terms of public notoriety and threats to health and public safety, there is no question that the dangers of ransomware have been on the rise. Law enforcement authorities have taken notice.

In April 2021, the U.S. Department of Justice formed a Ransomware and Digital Extortion Task Force (RDETF) designed to investigate and prosecute those perpetrating attacks in a coordinated manner.[7] The RDETF was designed to coordinate the enforcement activities of the individual U.S. Attorney's Offices and the Federal Bureau of Investigation agents throughout the country with the subject matter experts in computer technology and national security issues located at the Department of Justice and Federal Bureau of Investigation headquarters. The federal response was not limited to the establishment of RDETF. In May 2021, the White House issued an executive order directing improved coordination between federal agencies and the private sector, and encouraging private-sector companies to prioritize improved cybersecurity as a critical part of their business.[8] In July 2021, the federal authorities created the website StopRansomware.gov, designed to serve as a "one-stop hub for ransomware resources" for individuals and organizations.[9] The announcement again heralded the increased coordination and sharing of information between numerous federal agencies.

The U.S. Department of Health & Human Services (HHS) has taken steps to specifically address cybersecurity and ransomware in the healthcare environment. The Health Sector Cybersecurity Coordination Center seeks to strengthen industry practices by providing threat briefings and sector alerts to healthcare entities.[10] HHS works with industry through the 405(d) Task Group, a standing public–private collaboration that includes more than 150 medical and information technology professionals that was formed pursuant to Section 405 of the Cybersecurity Act of 2015.[11] The 405(d) Task Group develops guidelines and best practices to improve cybersecurity efforts across the industry.

Finally, while federal actors are leading the way in combatting ransomware, law enforcement has aimed to increase cooperation at the state and local level as well. In June 2021, a bipartisan group of state attorneys general met with White House officials to better understand federal efforts and how state enforcement could complement federal enforcement.[12] Similarly, U.S. Department of Homeland Security officials highlighted the importance of state and local partnerships in combatting digital extortion.[13] Given that ransomware attacks can affect healthcare entities from the largest hospital networks to solo practitioners, the need for law enforcement to be engaged at every level is clear.

Navigating a complex web of obligations

The dynamic nature of data breach notification laws further complicates the challenging landscape that ransomware victims must navigate. While regulators are increasing their efforts to combat ransomware and provide resources for its victims, companies must fulfill their obligations under federal and state breach notification laws.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), which applies to "covered entities" (i.e., health plans, healthcare providers that engage in certain covered transactions, and healthcare clearinghouse)[14] and "business associates" (i.e., vendors or service providers to a covered entity that create,

receive, maintain, or transmit protected health information from, or on behalf of, the covered entity), requires notification to individuals,[15] HHS,[16] and, in some cases, media outlets,[17] for the acquisition, access, use, or disclosure of protected health information in a manner not permitted under HIPAA that compromises the security or privacy of the protected health information.[18] While the determination of whether a ransomware attack constitutes a breach under HIPAA is fact specific, a ransomware attack is presumed to be a breach unless the covered entity can show that there was a "low probability" that protected health information was compromised.[19] HHS has issued guidance on HIPAA compliance and ransomware that specifically addresses notification in connection with a ransomware attack, and specifically notes that high risk of unavailability of the data, or high risk to the integrity of the data, may indicate compromise and require breach notification.

Additionally, all 50 US states and the District of Columbia have enacted breach notification laws.[20] These laws generally require notification to individuals (and in some instances, regulators and/or credit reporting agencies) if there has been an unauthorized access and/or acquisition of personal information. Additionally, ransomware-related data breaches may also trigger disclosure obligations for healthcare organizations with the Securities and Exchange Commission and the Federal Trade Commission. The definition of personal information varies across the state breach notification laws, and, at the time of writing, 21 state breach notification laws include health or medical information in the definition of personal information. For instance, in August 2021, California Attorney General Rob Bonta issued a bulletin highlighting healthcare entities' obligations to put in place sufficient policies and procedures to protect patient information and health-related data.[21] It further reminded healthcare organizations that regulators have the authority to bring civil enforcement actions against organizations that fail to meet their obligations under HIPAA and under relevant state laws, such as California's data breach reporting statute.

As such, as healthcare organizations navigate the potential operational, reputational, and economic harms that result from ransomware attacks, they must also be certain that their response is compliant with the fast-moving and constantly changing regulatory requirements in this area.

Best practices in managing a crisis response

In the face of this growing threat, healthcare entities of all sizes must have policies and procedures in place designed to prevent cyberattacks and, where such attacks are "successful," to guide and manage the entity's response. Advanced planning is key to ensuring that a company's response is consistent with existing laws and regulations and is the product of thoughtful consideration and not panicked overreaction.

As an initial matter, a corporate target should establish a ransomware and extortion policy that outlines the company's response to a ransomware or other extortion incident, including the company's policy on responding to such incidents and the circumstances, if any, in which the company would consider paying a ransom. The policy should ensure that staff who identify the issue are trained to communicate with an in-house incident response team that, in turn, knows when to escalate incidents to executive leadership and necessary outside professionals. The policy should further identify who within the entity has the authority to authorize the payment of any ransom and identify the specific factors that the company will use when considering any such payment. Such considerations may include:

- The nature and scope of the compromised systems and their impact on the entity's operations,
- The threat that failing to remediate the attack may have on patient health and well-being,
- The ability to recover the compromised information through other means, and

- The likelihood of payment resulting in recovering the information or that of not paying resulting in further harm to the entity.

The policy must also consider the metrics for assessing the economic harm associated with a ransomware attack and ensure consultation with the entity's legal staff or, as appropriate, outside counsel to consider the legal and regulatory risks from any payments.[22] It should also set forth policies for contacting law enforcement entities as well as outside cybersecurity professionals. The policy should be periodically tested through tabletop exercises to ensure that the organization is prepared and to identify any opportunities for enhancement. Having a robust response plan in place that has been tested in cyberattack simulation exercises will place healthcare organizations in a far better position to protect their patients, staff, and critical infrastructure in the face of ever-increasing ransomware attacks.

Takeaways

- Ransomware attacks continue to grow exponentially; last year, they cost companies a projected $20 billion, nearly double the cost from 2019.
- Healthcare organizations suffered 71% more ransomware attacks in 2021 as compared to 2020.
- Law enforcement agencies at every level of government have recognized the enormous growth in ransomware attacks and are increasing their coordination to combat them.
- In responding to ransomware attacks, healthcare organizations must be sure that, if a data breach has occurred, they are complying with federal, state, and local notification requirements.
- Healthcare entities should develop an incident response plan that is battle-tested through tabletop exercises in order to swiftly respond to an attack, minimizing business disruption, protecting patients' private medical data, and ensuring continuity of care.

1 Chuck Brooks, "Cybersecurity in 2022 – A Fresh Look at Some Very Alarming Stats," *Forbes*, January 21, 2022, https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=714b39146b61.
2 Steve Morgan, "2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics," *Cybercrime Magazine*, January 19, 2022, https://cybersecurityventures.com/cybersecurity-almanac-2022/.
3 Coveware, "Law enforcement pressure forces ransomware groups to refine tactics in Q4 2021," Quarterly Report, February 3, 2022, https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021#vectors.
4 Steve Alder, "Lawsuit Alleges Ransomware Attack Resulted in Hospital Baby Death," HIPAA Journal, October 4, 2021, https://www.hipaajournal.com/lawsuit-alleges-ransomware-attack-resulted-in-hospital-baby-death/.
5 Cybersecurity & Infrastructure Security Agency, "Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm," *CISA Insights*, 13, September 2021, https://bit.ly/3jcvqCq.
6 Chuck Brooks, "Cybersecurity in 2022."
7 John P. Carlin, "Ransomware and Digital Extortion Task Force," memorandum, April 20, 2021, https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/dojransomwarememo.pdf.
8 The White House, "President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks," fact sheet, May 12, 2021, https://bit.ly/3JWFTwJ.
9 U.S. Department of Justice, "U.S. Government Launches First One-Stop Ransomware Resource at

StopRansomware.gov," news release, July 15, 2021, https://www.justice.gov/opa/pr/us-government-launches-first-one-stop-ransomware-resource-stopransomwaregov.
10 U.S. Department of Health & Human Services, "Heath Sector Cybersecurity Coordination Center (HC3)," last reviewed March 31, 2022, https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html
11 "About Us," HHS 405(d) Aligning Health Care Industry Security Approaches, U.S. Department of Health & Human Services, accessed April 7, 2022, https://405d.hhs.gov/public/navigation/aboutUs.
12 The White House, "Readout of Deputy National Security Advisor for Cyber Anne Neuberger Meeting with the Bipartisan National Association of Attorneys General," June 11, 2021, https://bit.ly/3xBS603.
13 Robert Silvers, Brandon Wales, and Jeremy Sheridan, Testimony Before the United States House of Representatives, Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, & Innovation and Subcommittee on Intelligence & Counterterrorism, November 17, 2021, https://homeland.house.gov/imo/media/doc/silvers_wales_sheridan_testimony_ic_cipi_111721.pdf.
14 45 C.F.R. § 160.103.
15 45 C.F.R. § 164.404.
16 45 C.F.R. § 164.408.
17 45 C.F.R. § 164.406.
18 45 C.F.R. § 164.402.
19 U.S. Department of Health & Human Services, Office for Civil Rights, "Ransomware and HIPAA," fact sheet, July 11, 2016, https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.
20 "2021 Security Breach Legislation," National Conference of State Legislatures, January 12, 2022, https://bit.ly/3K1VpqV.
21 Rob Bonta, "Obligation to Proactively Reduce Vulnerabilities to Ransomware Attacks and Requirements Regarding Health Data Breach Reporting," bulletin, August 24, 2021, https://oag.ca.gov/system/files/attachments/press-docs/2021AUG24%20Ransomware%20Bulletin.pdf.
22 Department of the Treasury, "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," October 1, 2020, https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.