Published on *The National Law Review* https://natlawreview.com

Ransomware: A Guide to Practical, Regulatory, and Reputational Risk Management

Article By:

Alaap B. Shah

Stuart M. Gerson

Andrew (Andy) P. Rusczek

Marylana Saadeh Helou

Ransomware Particularly Inflicts Health Care and Life Sciences Organizations

Ransomware is a malicious cyber threat vector that employs encryption malware to prevent users from accessing their systems and data unless ransom is paid in exchange for decryption keys. What once was simple extortion has morphed into a triple threat. Criminal hackers now not only threaten to publish data unless a ransom is paid with crypto-currency in exchange for an unlocking key and assurances that any data taken are deleted, but also increasingly exfiltrate sensitive data and share it with others, often host governments adverse to U.S. interests. These hackers also use the data of a victim's customers or contacts to perpetrate additional exploits.

The recent ransomware attack against Colonial Pipeline shut down gasoline supplies for much of the East Coast and highlighted the vulnerability of our critical infrastructure of which the health care and life sciences sector is an important part. One easily can envisage the risk to hospitals, for example, being cut off from their electronic records needed to evaluate their patients, who then might not be able to get life-saving care. Likewise, pharmaceutical and medical device companies are at great risk if their coded clinical trial participant data, some of which contain trade secrets, are implicated in a ransomware attack. In sum, thieves crave health care data for a variety of reasons, including the weaknesses of their targets' cybersecurity, the potential utility of identifiable personal information, the value of clinical and device intellectual property, and because health information can be used as the basis for phony billings to federal and state payment authorities. And many, if not most, of these cybercriminals, are based in countries, China and Russia particularly, that protect them from the reach of U.S. law enforcement.

As a result, many institutions have met ransomware attacker demands and paid requested ransoms, seeing it as the most efficient manner of handling the situation. They have been supported by their insurers who have reckoned that the costs of system repair and data restoration often exceed the

cost of ransom payment. However, because the demands have escalated, hackers have been proving more ambitious and less reliable, and, most significantly, the U.S. government has come to recognize that ransomware attacks on elements of the critical infrastructure, including entities related to health care, are jeopardizing national security, the payment and compliance landscape has changed.

Recently, the Federal Bureau of Investigation ("FBI"), the U.S. Department of Health and Human Services ("HHS"), and the Cybersecurity & Infrastructure Security Agency ("CISA") released a report[1] calling attention to the rampant ransomware activity targeting the health care sector. Other parts of the Executive Branch, including the U.S. Department of Justice itself, have stated that ransomware is now a top priority for law enforcement and national security. Additionally, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") has cast a warning cloud over the payment of ransom to hackers who might be agents of countries hostile to the United States.

Given this evolution of enforcement policy, while as it indeed was in the case of Colonial Pipeline, which deemed it necessary to pay a ransom, it is manifestly more necessary than ever for an entity to have robust compliance and resilience measures in place to provide for security, regulatory oversight, and federal and state enforcement.

Thus, this Client Alert summarizes (a) the changing regulatory and enforcement landscape and risks for health care organizations, (b) proactive measures health care organizations should take to help prevent ransomware attacks, and (c) reactive measures that a health care organization should take in the wake of a ransomware attack.

Changing Regulatory and Enforcement Landscape

Federal Bureau of Investigation

For many years, entities have had little guidance on whether or not to pay ransom. Although, for example, the FBI has generally discouraged ransom payment, it also has recognized that payment might be the only viable option to resume operations, or even for an entity to survive, in some situations. While this remains true in some extremely grave situations, like that of Colonial Pipeline, where an approximately $5 million ransom was paid under the supervision of the FBI, there now is a presumption that payment should be avoided, even though the FBI will still view the extorted entity as the victim. This is less true of other agencies of government.

Office of Foreign Assets Control

On October 1, 2020, OFAC and the Financial Crimes Enforcement Network (known as "FinCEN") warned that companies risk violation of OFAC regulations, and the imposition of regulatory and financial penalties, when they make or facilitate ransomware payments to threat actors who are, or are agents of, sanctioned persons. In its Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments,[2] OFAC warns that, unless otherwise specifically licensed, relevant OFAC rules and regulations[3] dictate that U.S. individuals and entities are prohibited from directly or indirectly participating in or facilitating transactions with individuals and entities on OFAC's Specially Designated Nationals and Blocked Persons List ("SDN List"). The SDN List includes those persons that are covered by comprehensive country or region embargoes, such as Iran, North Korea, and Syria, as well as other blocked persons.

The OFAC advisory states that this "applies to companies that engage with victims of ransomware attacks, such as those involved in providing cyber insurance . . . and financial services that may involve processing ransom payments . . . ."[4] If a U.S. individual or entity participates in such a transaction, OFAC reserves the right to take enforcement action, including the issuance of civil monetary penalties, criminal referral to law enforcement agencies, and other administrative actions.[5] The broad scope of the OFAC advisory also impacts cyber insurance carriers such that entities may be precluded from seeking insurance coverage if they violate the OFAC rules. In light of this new advisory, entities should proceed with caution when considering a ransom payment and should shift their focus to taking proactive compliance steps to reduce risk to prevent a ransomware attack.

Office for Civil Rights and HIPAA

The Office for Civil Rights ("OCR"), the HHS agency charged with the regulation of health care organizations that are "covered entities" and their "business associates" subject to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and the Health Information Technology for Economic and Clinical Health ("HITECH") Act, similarly exhibits an enforcement bias. Thus, OCR views a ransomware attack as a breach and its first responsibility to ensure, more with a stick than a carrot, compliance with the requirements of HIPAA's breach notification rule, 45 C.F.R. Part 164, Subpart D. Accordingly, OCR has issued guidance indicating that ransomware infection involving previously unencrypted protected health information ("PHI") will typically be deemed to be an acquisition and unauthorized disclosure constituting a compromise to the privacy and security of PHI. This would in turn require reporting and notification to regulators and individuals unless the entity conducts a risk assessment to establish a low risk of compromise. As such, it is imperative that covered health care entities and business associates maximize their compliance programs and, if subject to a ransomware attack, employ computer forensics to understand the root cause and nature of the attack in order to support a risk assessment and breach determination.

State Law Considerations

Echoing federal regulatory concerns, certain state regulators have also issued guidance related to ransomware and have taken strong enforcement stances. For example, in February 2021, the New York State Department of Financial Services ("NYDFS") issued Insurance Circular Letter No. 2,[6] which discussed cyber insurance carrier risk related to making ransomware payments. NYDFS takes the position that making ransom payments "fuel[s] the vicious cycle of ransomware." Further, NYDFS discourages making ransom payments for three main reasons: (a) the potential that ransom payments could violate OFAC rules, (b) the lack of guarantees from a threat actor that data access restoration (or return of exfiltrated data without public disclosure) would occur, and (c) the likelihood that ransom payments would fund future ransomware attacks against the same or other organizations. All of these things are true, but are not of much consequence to an organization that is faced with extinction if its files are impenetrably encrypted by a hostile actor.

Similar to federal regulators, NYDFS does provide guidance as to proactive and preventive activities to reduce risk. Focusing upon the important presence of insurers, NYDFS recommends that insurers and insureds should (a) assess the cybersecurity of the insured, (b) consider industry-wide risk as well as company-specific risk when assessing risk, (c) commit to cybersecurity education, (d) employ cybersecurity risk experts to advise about managing risk, and (e) require notice to law enforcement about cybersecurity incidents. In sum, it is clear that states are driving the industry to be more sophisticated in preparing for and responding to ransomware issues in order to reduce the financial impact of such events.

Recommended Proactive Measures

The first step for any organization to avoid the harms of ransomware is to proactively implement a compliance program and procedures to prevent ransomware before it occurs. Entities should implement a risk-based compliance program to mitigate exposure to cyber risks. OFAC has also stated that such a program is a factor it may consider when determining the extent of its enforcement activities. The core elements an entity should consider include (a) management commitment, (b) risk assessment, (c) internal controls, (d) testing and auditing, and (e) training.

1. **Management Commitment**: Given the gravity of ransomware, indeed of any hostile systems penetration by an adversary, any attack will substantively involve senior management, and hence, any viable compliance program must involve its origination, oversight, and operational support. An organization's compliance officer, whether particularly charged with ransomware issues or general cyber compliance, should have direct reporting access to an entity's most senior managers and board of directors. This is more than just displaying "tone at the top." It is viewed by enforcers as a sine qua non of an entity's demonstrable commitment to compliance.

2. **Risk Assessment**: No compliance program can be justified to regulators and enforcers if it is not premised on a data-driven risk assessment that encompasses potential cybersecurity vulnerabilities in technical systems, in elements of backup and resilience, and in human resources. Such assessments must be ongoing, subject to periodic training, testing, and documented outcome evaluations.

3. **Internal Controls**: An organization should have internal controls sufficient to identify, interdict, escalate, report (as appropriate), and maintain records pertaining to activity that may be suspected of involving ransomware. These controls include having implemented written policies and procedures outlining the compliance program, general internal controls, enforcement of policies and procedures, recordkeeping policies and procedures, and communication of the compliance program's policies and procedures to all relevant staff, particularly those operating in high-risk areas, and to relevant external parties performing compliance program responsibilities.

   Ransomware prevention is one key aspect of a robust cybersecurity program that includes (a) imposing on-site and remote access limitations on an organization's network (including VPN connections, multi-factor authentication wherever possible, and increased restrictions on privileged accounts), (b) conducting security awareness training with specific treatment of ransomware prevention and response, (c) implementing firewalls and next-gen anti-virus solutions, (d) implementing email spam filters, (e) ensuring encryption of data in transit and at rest, (f) applying software patches on a regular basis, and (g) backing up data and systems routinely (and periodically testing such backups).

   To properly ensure business continuity when a ransomware attack occurs and operations are interrupted, an organization's policies and procedures should include a robust data backup and business continuity plan particularly targeted to reaction and resilience in the event of a ransomware attack.

4. **Testing and Auditing**: The compliance program should contain a comprehensive and objective real-time testing or audit function to ensure that the organization identifies program weaknesses and deficiencies and a methodology to enhance its program to remediate any

identified compliance gaps. This should include internal testing, such as simulating phishing and other email-based penetrations and “table top” war games to assess technical and human awareness and response. This might also include auditing and testing by third parties.

5. **Training**: While ransomware criminals are increasingly technically adept, most attacks still begin with social engineering, such as phishing or spear-phishing entreaties and the exploitation of human vulnerabilities. Thus, ransomware- and cybersecurity-related training should be provided to all potentially vulnerable personnel on a periodic basis and should include comprehensive job-specific knowledge and responsibilities, stressing accountability, reporting requirements, and the measurement of compliance with security parameters.

Recommended Reactive Measures

Even the most sophisticated organizations that have robust controls are still at risk of ransomware attacks. While not involving ransomware, the recent Solar Winds exploit that began with a foreign actor’s creation and dissemination of a phony program update, and resulted in the penetration of several high-tech companies and critical governmental agencies, including CISA, demonstrates that even the best prepared organization can still suffer a successful attack. Thus, any organization must implement a reaction plan that assigns responsibility to designated individuals to perform specific remedial actions. Among the critical elements of an effective response are the following:

1. **Contact Law Enforcement:** It is highly recommended that an organization facing a ransomware attack contact the FBI or other federal authorities and fully comply with requests for information from these authorities in consultation with legal counsel. We recognize that such contact can impose regulatory risk and reporting requirements that could tend to discourage such contact, and this contributes to the need for counsel’s guidance.

2. **Perform a Risk Assessment:** This is not the vulnerability assessment upon which the compliance program is predicated. Now, with an actual attack underway or, more likely, completed, an organization should assess the risks it faces, including whether personally identifiable information, PHI, or other critical information has been exposed; whether customer or patient care is affected; and whether any other aspect of operation or security has been compromised.

3. **Mitigate the Spread:** Immediately after activating the response plan described in the compliance program, an organization should take all available steps to mitigate the internal spread of the malware within its system. These steps may include (a) disconnecting impacted computers from the network (and Internet), (b) disconnecting shared drives, (c) blocking traffic to ransomware command and control sites, and (d) capturing “indicators of compromise” (“IoCs”) to be evaluated as part of investigation.

4. **Identify the Ransomware Attacker:** It is not always possible to identify the party that is committing the ransomware attack. However, if possible, an organization should identify the ransomware attacker, including to assess whether a potential ransom payment could trigger OFAC enforcement for payment to certain third-party actors.

5. **Assess Payment and Non-Payment Options**: An organization should determine whether it can effectively continue operations without payment of the ransom. A chief concern among U.S.-based organizations will be whether customer or patients can continue to be serviced or

properly treated, particularly in emergency and life-threatening situations, without payment being made or demands being met. A U.S.-based company should also assess whether it can actually operate and provide essential functions. These determinations should be clearly and robustly documented.

Upon this determination, the organization, likely with the assistance of a federal agency, may determine that payment is necessary. This could be for a variety of reasons, including that the ransomware cannot be removed from the system or that human lives or safety is at risk. In this case, it is advisable that this decision is robustly documented, and ideally with the written advice of federal authorities, such as the FBI.

Conclusion

Don't be caught off guard. We have discussed the basics. There are, of course, additional technical and human compliance tactics that can bolster an organization's ability to prevent and respond to ransomware attacks.

[1] *See* https://www.us-cert.gov/ncas/alerts/aa20-302a.

[2] The OFAC advisory is available at https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

[3] *See, e.g.,* 50 U.S.C. §§ 1701-06, 4301-41.

[4] Dept. of Treasury, Office of Foreign Assets Control, Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (October 1, 2020).

[5] 31 C.F.R. Pt. 501, App. A.

[6] *See* https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02.

National Law Review, Volume XI, Number 153