ReedSmith

Driving progress
through partnership

Preparing for the Inevitable Ransomware Attack

By: Bart Huffman, Wendell Bartnick, and Kelley Chittenden

The frequency and sophistication of ransomware attacks have risen tremendously over the past couple of years. Ransom amounts demanded by attackers have also materially increased. Ransomware attacks are potentially more damaging to organizations than other types of cyberattacks because they affect business systems and data in a way that could severely (and even permanently) disrupt an organization’s ability to do business. Fortunately, organizations can take steps to significantly reduce the probability of being victimized by a ransomware attack and reduce the magnitude of the damage should an attack occur.

Ransomware is a form of malware that encrypts data where an organization stores it, and only the attacker has the key to decrypt it. With this attack, an organization still possesses the data; however, the organization is unlikely to be able to decrypt the data without the hacker’s key. So, in effect, the encrypted data is unusable to the organization without that key. The hacker contacts the organization asking for payment within a short deadline in exchange for the decryption key. If the organization refuses to pay by the deadline, the data remains encrypted and unusable. If the organization pays, the attacker may provide the decryption key so the organization can recover the data. If an organization is unable to decrypt the affected data, its operations could be severely hampered.[1]

To reduce the probability of an attack, organizations can incorporate the ransomware threat into their cyber security risk assessments and regularly review the applicable administrative, technical, and physical data security measures, including employee training. To reduce the damage from a ransomware attack, organizations can formalize, implement, and test their business continuity and disaster recovery plans, which should include system and data backup plans. Organizations can also specifically address ransomware attacks in their incident response plans to ensure they incorporate the special circumstances that ransomware attacks present.

1. Implement Security Measures that Incorporate Risks Unique to Ransomware

Various U.S. laws require that organizations implement reasonable security measures that protect the personal information they handle.[2] These laws have become more specific and prescribe certain data security measures. While most of these laws apply to the protection of personal information only, some government agencies have published regulations and guidance that require the protection of other types of sensitive information.[3]

a. *Federal Legal Requirements*

[1] We have also seen an increase in other types of extortion, including data breaches followed by threats to release the stolen information unless payment is made or certain actions are not taken, or threats to attack online services unless payment is made or certain actions are not taken.

[2] *See* Fed. Trade Comm’n, Protecting Consumer Privacy in an Era of Rapid Change 24 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [hereinafter FTC 2012 Privacy Report].

[3] For example, the Department of Defense requires defense contractors to protect controlled information related to their work for the agency. *See* NIST Manufacturing Extension Partnership, DFARS Cybersecurity Requirements (2017), https://www.nist.gov/mep/dfars-cybersecurity-requirements. The Federal Energy Regulatory Commission (FERC) has approved mandatory cybersecurity reliability standards for the organizations it regulates. *See* North Am. Electric Reliability Corp., CIP Standards, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

One key aspect to reasonable data security is to implement a comprehensive data security program. According to the FTC, such program should contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, and the programs should address and prevent well-known and easily addressable security vulnerabilities.[4] To properly scope a data security program, the FTC has recommended regularly performing a cybersecurity risk assessment that, at minimum, "should include consideration of risks in each area of relevant operation, including: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures."[5] After the completion of the risk assessment, the FTC recommends that organizations "design and implement[] . . . reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures."[6] Data security programs should address not only well-known threats but also business-specific vulnerabilities, and they should be tailored to an organization's specific business model and data.

b. ***State Legal Requirements***

Similarly, many states require organizations to implement reasonable security measures to protect personal information. Massachusetts has led the way at the state level by requiring a comprehensive written information security program that contains administrative, technical, and physical safeguards appropriate for the organization's size, scope, and type of business, the organization's resources, the volume of personal information, and the need for security measures. [7] Recently, the New York Department of Financial Services released a cybersecurity regulation that requires banks, insurance companies, and other financial services organizations to have a cybersecurity program to protect consumer data.[8] The New York law requires that a cybersecurity program include performing a risk assessment to identify reasonably foreseeable internal and external security risks[9] and cover employee training, employee compliance with policies and procedures, and methods for detecting and preventing security failures. The law also requires firewall protections, system security patches, and updated malware detection and protection software.

c. ***Risk Assessments Should Assess Ransomware as a Threat***

Federal and state laws require organizations to tailor their information security measures to their unique circumstances based on a cybersecurity risk assessment. A critical component of a cybersecurity risk assessment is a review of reasonably possible threats to an organization's data and systems. One relatively new threat for organizations to consider is ransomware.

Ransomware is a type of malware, and organizations may incorrectly believe that their information security programs already adequately reflect the risk from it. However, organizations' risk assessments

[4] *See* FTC 2012 Privacy Report, fn 108, *supra* note 2; Fed. Trade Comm'n, Start with Security: A Guide for Businesses (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf ("Take reasonable steps to keep [personal information] secure."); Fed. Trade Comm'n, Protecting Personal Information: A Guide for Businesses (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf [hereinafter Protecting Personal Information]. The Health Insurance Portability and Accountability Act (HIPAA) also requires regulated entities to implement reasonable and appropriate security measures that take into account the size, complexity, and capabilities of the regulated entity, the technical infrastructure, the costs of the security measures, and the potential risks to the regulated personal information. *See* HIPAA, 45 C.F.R. 164.306 (a), (b). The Gramm-Leach-Bliley Act (GLBA) also requires financial institutions to protect nonpublic personal information with a comprehensive information security program. *See* 15 U.S.C. § 6801 et seq.; 16 C.F.R. 314.3 (FTC Rule); 17 C.F.R. 248.30 (SEC Rule).

[5] *Microsoft Corp.*, Decision and Order, Docket No. C-4069 (Dec. 20, 2002), https://www.ftc.gov/sites/default/files/documents/cases/2002/12/microsoftdecision.pdf.

[6] *Id.*

[7] *See* Office of Consumer Affairs and Business Regulation, *Standards for the Protection of Personal Information of Residents of the Commonwealth,* 201 CMR 17.00, https://www.mass.gov/files/documents/2017/10/02/201cmr17.pdf.

[8] *See* New York State Department of Financial Services, Cybersecurity Requirements for Financial Services Companies, § 500.02, http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf.

[9] *See id.* § 500.09.

may have reviewed malware solely from the perspective of an attack on personal information. For example, organizations that have a small amount of non-sensitive personal information may not have considered malware to be a significant threat and may not have implemented thorough security measures to prevent malware infections. However, ransomware, unlike many other types of malware, is typically targeted at business-critical data, which may not be personal information. Given that the threat from ransomware is different from other types of malware, organizations may consider reassessing the threat level of malware attacks and incorporating measures into their information security program to mitigate an increased threat level.

d. ***Data Backup and Recovery Is Crucial for Reducing Ransomware Threats***

Organizations may also reconsider the relationship between their data security measures and their business continuity and disaster recovery plans. Unlike other types of cyberattacks, which may permit a victimized organization to continue business-as-usual, a ransomware attack can create an existential crisis. If a ransomware attack permanently renders business-critical data inaccessible, an organization's operations can be significantly crippled. For this reason, an organization's data backup and other business continuity and disaster recovery plans become crucial. For example, an organization should consider the frequency of backups. The greater the frequency, the less data can be permanently lost. Backup processes should be tested to ensure they work properly and back up the correct data. An organization should regularly restore the data from backup files to ensure the organization is experienced at the process and the process proceeds smoothly. An organization should also consider how it secures backup files because ransomware attackers look for backup files to encrypt as well the live data. There have been instances where attackers have been able to encrypt data backup files stored electronically with a third party service provider.

2. Implement Cyber Incident Response Plans that Incorporate Risks Unique to Ransomware

Say a ransomware screen displays on your server, and you have 48 hours to pay the ransom. Do you know what systems and data are affected? Is this a reversible attack? Do you know if you have adequate backups? Do you know if you can restore the backups in 48 hours? Can you set up a cryptocurrency wallet to make a payment in 48 hours? Can you preserve evidence of the attack? These are the some of the questions that organizations consider when faced with a ransomware attack.

a. ***Effective Incident Response Plans Are Tailored and Tested***

Federal and state regulations and guidance indicate the importance of incident response plans.[10] Incident response plans help organizations by defining clear roles and responsibilities, identifying key outside experts, and standardizing a response framework. However, a generic incident response plan will not be successful with all types of attacks. Ransomware's time element, payment process, and possibly crippling effect on basic system functionality (e.g., the email system or entire computer network may be unusable while responding to the attack) are attack characteristics that require additional planning and coordination.

Organizations also benefit from real testing of their incident response plan. Testing the plan through tabletop exercises and other methods can greatly increase an organization's efficiency and response speed. When going through testing, participants should not just say they will restore the backups to counteract a ransomware attack. The organization should actually restore the backups to test the process given the constraints typical ransomware attacks create.

[10] For example, financial institutions may be required to have an incident response plan under the Gramm-Leach-Bliley Act. *See* INTERAGENCY GUIDANCE ON RESPONSE PROGRAMS FOR UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION AND CUSTOMER NOTICE, 12 C.F.R. 30, 208, 225, 364, 568, 570. See PROTECTING PERSONAL INFORMATION, *supra* note 4 for a breach response plan recommended by the FTC and FED. TRADE COMM'N, DATA BREACH RESPONSE: A GUIDE FOR BUSINESS (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf for FTC guidance regarding what a breach response plan should entail.

b. *Incident Response Plan Increases Organizational Ability to Successfully Respond to Ransomware Attacks*

Ransomware is typically time-loaded to require a ransom payment within a short period of time, or the attacker will not provide the decryption key. Therefore, time is of the essence. Unprepared organizations are less likely to successfully respond to and recover from a significant ransomware attack. Organizations can significantly benefit by having an incident response plan because such plans greatly improve an organization's response speed. For example, an organization is unlikely to have a cryptocurrency wallet, which is typically required to pay attackers. Obtaining a cryptocurrency wallet is challenging and can take several days, which may not be fast enough to make a payment before a deadline. An organization that has considered ransomware in its incident response plan has likely identified third-party consultants that specialize in negotiating with attackers and can handle the technical aspects to making payments to make sure that the payment process itself does not prevent an organization from making a payment by the deadline.

Ransomware raises unique challenges for cybersecurity and breach response. Organizations may have legal obligations to reasonably protect the data they have, some of which may require that they specifically consider the ransomware threat when implementing data security measures and developing incident response plans. Aside from meeting their legal obligations, organizations will benefit from considering the unique aspects to ransomware attacks and addressing how they can prevent and respond to ransomware attacks.