17 Best Practices For Defending Against Ransomware Attacks

By **Richard Sheinis, Brett Lawrence and Charles Langhorne** (August 16, 2021)

Richard Sheinis

Brett Lawrence

Charles Langhorne

There has not been a shortage of headlines recently about large companies paying many millions of dollars to recover data encrypted by ransomware.

One of America's largest beef producers, JBS USA, reportedly paid $11 million to the ransomware group REvil.[1] CNA Financial Corp. allegedly paid hackers $40 million after being infected with Phoenix Locker ransomware.[2] Colonial Pipeline Co. paid hackers nearly $5 million to recover their data.[3] It is estimated that in 2020, victims paid approximately $370 million in ransom, which was a 336% increase over 2019.[4]

The latest spate of ransomware attacks, which are believed to have emanated from Russian cybercrime groups, led President Joe Biden to demand that Russian President Vladimir Putin shut down the ransomware groups attacking American companies.[5]

On June 2, Anne Neuberger, deputy assistant to the president and deputy national security adviser for cyber and emerging technology, issued a memorandum to corporate executives and business leaders titled, "What We Urge You to Do to Protect Against the Threat of Ransomware."[6]

This memorandum contains several recommended best practices for companies to protect themselves against ransomware. None of these best practices are new, and they have long been recognized as elementary aspects of a cybersecurity program.

An unintended consequence of highlighting ransomware attacks against exceptionally large corporations is that it can lead to the false belief that much smaller organizations or corporations are not targeted with false ransomware by cybercriminals. Some companies may get a false sense of security from the misguided belief that they are too small or inconsequential to be targeted by cybercriminals.

While ransomware can affect the day-to-day lives of millions of Americans when it affects a company like Colonial Pipeline, the fact is that every company is a ransomware target. Although no one will read about ransomware infecting a local construction company, the construction company can be devastated by the inability to conduct business because its computer system and all its data has been encrypted. As Neuberger's memorandum stated, "[n]o company is safe from being targeted by ransomware, regardless of size or location."

The problem for many companies is actually putting security processes into practice. Companies often know what to do to harden their computer security, but there is insufficient emphasis on follow-through and implementation. This can sometimes be due to the failure of leadership to recognize the attention required for effective cybersecurity.

Having an information technology department without a dedicated security specialist may no longer be sufficient. Computer security has advanced to the level beyond the expertise of

an IT generalist and requires the attention of a security specialist.

The specifics of how a company can improve its computer security to protect against ransomware are somewhat dependent on the company's industry, the type of data or information that needs to be protected, the size of the company, the flow of information within the company as well as information sent and received by the company, and numerous other factors that are specific to each company.

While the White House memorandum provides good, practical advice, it is not likely that the memorandum will reach the many companies that need to hear this advice. The memorandum does not take the place of comprehensive federal legislation to address computer security. To date, federal computer security and data privacy legislation, such as the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act, are fragmented in that they each apply only to specific industries.

Only a few states, such as Connecticut, have incentivized companies to institute computer security mechanisms by offering a certain level of immunity or safe harbor from lawsuits if they have implemented a certain level of computer security.

In the absence of legislative requirements, or other incentives, it is simply up to each company to take the initiative to implement safeguards to protect against ransomware. The emphasis is on not just planning the following measures, but on following through with implementation and testing. Many companies have been victimized by ransomware because they failed to confirm whether intended safeguards were effectively implemented and maintained.

Best practices for preparing for and protecting against ransomware attacks, derived from the White House memorandum, the National Institute of Standards and Technology,[7] the Cybersecurity and Infrastructure Security Agency[8] and other materials, include the following.

1. Back up data and systems.

Adequate backups from which data and systems can be restored are often the difference between paying or not having to pay the ransom. Companies should back up data frequently. While a backup from a week or a month earlier is useful, it can still leave gaps of data that cannot be recovered. Ideally, two sources of backups should be maintained, unconnected to the main computer network.

Ransomware is designed to search through computer networks, and if the backup is connected to the network, both the primary database and the backup database can be encrypted. Backups should be regularly tested. Finding out that a backup system was not working properly only after the primary database is encrypted is obviously too late. If a database can be completely restored from backups, ransomware can be limited to being a business interruption or inconvenience, rather than a major catastrophe.

2. Segment networks.

Ransomware is often programmed to search and encrypt particular types of documents or files. Often, ransomware will have other malware with it, which will allow the cybercriminal to exfiltrate or steal files.

When this happens, in addition to the unavailability of data, the company must be

concerned about the cybercriminal's use of the stolen data for other illegal activities, e.g., fraud, identity theft and reputational harm. Segmenting networks makes it more difficult for a cyberattacker who accesses a certain component of a company's system to access files on other parts of the system.

3. Patch systems promptly.

Operating systems and applications can have vulnerabilities that are not discovered until they are in widespread use. When this happens, patches are issued by the provider to remediate the vulnerability. There have been several cases in which cybercriminals have accessed systems because companies did not apply patches promptly after their release.

4. Replace end-of-life components.

Manufacturers may announce that they are no longer supporting certain computer components after a specific date. This is referred to as the end-of-life date, after which the manufacturer will no longer address vulnerabilities or issue patches. By keeping components, such as servers, as part of a network, vulnerabilities that are not remediated can be exploited by attackers.

5. Use antivirus and threat-detection software.

This software will block threats before they enter a computer system and will locate malware that may have bypassed initial defenses. Applications that are specifically designed to detect and block ransomware are available.

6. Train staff to avoid opening suspicious files or links.

We are all familiar with phishing emails. A good resource is the Phish Scale, a method developed by the NIST that helps organizations better train their employees to avoid phishing emails.[9]

7. Avoid accessing personal applications in websites.

Companies should have a policy prohibiting employees from accessing social media and personal email accounts while using company devices. People tend to be less vigilant about suspicious messages and links when accessing these sites for personal reasons, even though they are on a company computer.

Social media channels are ripe for social engineering because people are looking for advertisements, news and new connections. Companies can also use security settings to block certain social media channels.

8. Configure operating systems, or use third-party software to allow only authorized applications to run on computers.

By prohibiting unauthorized applications from running, ransomware can be blocked. Software applications can have vulnerabilities, which can be exploited by threat actors to access a computer system. By only using software from trustworthy sources or developers, a company can reduce the likelihood that threat actors will find a vulnerability that allows them to proliferate their ransomware.

9. Limit administrative privileges whenever possible.

By limiting administrative privileges, there is less likelihood of a compromised account providing ransomware with widespread access to the system. When employees have administrative privileges, they have greater access to the system. If a threat actor compromises the credentials of an employee with administrative privileges, it is like getting the keys to the castle.

10. Implement multifactor authentication.

Multifactor authentication can block an attacker from using a compromised password or credential to access the system. When an employee attempts to log in to the system remotely, after entering his or her credentials, the multifactor platform sends a code to his or her mobile phone. The employee must then enter the code to complete his or her access. If a threat actor steals the employee's credentials, unless he or she also has possession of the employee's mobile phone, he or she will not get the code to complete the login process.

11. Test your incident response plan.

Companies should test their response plans to find gaps. Using a tabletop exercise to find gaps by running a mock attack can be an effective way to make sure companies are ready when a ransomware attack inevitably comes.

12. Conduct regular testing and vulnerability scanning.

One aspect of penetration testing is when the company, usually through a vendor, sends fake phishing emails to employees to see who will bite. This tells the company if its employees are being vigilant and if its training is working. Vulnerability scanning assesses a company's system for vulnerabilities a threat actor might use. Identified vulnerabilities can be remediated before they are exploited by an attacker.

13. Check remote desktop protocol and other remote desktop services.

Remote desktop protocol, or RDP, is a solution to connect remotely to a system or network. It has ports to allow remote connection to the system. Threat actors scan the RDP for open ports that are not secure. Out-of-date versions of RPD without security patches are especially vulnerable to attack. Once illegal access to RDP is established, the access can even be sold on the dark web.

14. Implement an intrusion detection system.

An intrusion detection system, or IDS, is a tool or software that flags when someone is trying to break into a company's system. It can monitor inbound and outbound network traffic to identify malicious activities. An IDS can alert companies to malicious network activity that occurs prior to ransomware deployment, allowing them to prevent the ransomware from being deployed.

15. Evaluate the cybersecurity practices of any third parties that have access to your system.

A company can have excellent computer security practices, but if a vendor has poor cybersecurity hygiene, a threat actor can use the vendor to access the vendor's clients. A well-known case highlighting this danger was when Target Corp. was compromised through an HVAC vendor.

16. Restrict usage of applications leveraged by threat actors.

Threat actors can use applications such as Power Shell, a component of Microsoft Windows commonly used for automating management of a system, to deploy ransomware and hide their malicious activities. Hackers use PowerShell to find security holes in enterprise IT systems. They then use PowerShell to deploy ransomware. If usage of PowerShell is restricted, it is more difficult for hackers to use it for malicious activities.

17. Obtain appropriate insurance.

Although insurance is not technically a computer security mechanism, it can save a company from losing thousands, or even millions, to investigate cyberincidents, conduct forensic investigations, restore systems and pay ransom, when necessary. Several years ago, the typical ransom demand was only a few thousand dollars. Now we know, of course, that ransom demands are often in the millions of dollars.

The appropriate insurance for a company is very dependent on the risk for that company based upon its size, industry, potential losses and numerous other factors. Insurance to cover forensic and legal expenses may not cover ransom payments. The best practice here is to make sure a company engages with an insurance broker educated in the cyberinsurance business so that it can purchase the insurance that addresses its individualized risk.

Unfortunately, there is no reason to think that ransomware will go away any time soon. Biden's diplomatic efforts with Putin notwithstanding, ransomware attacks will continue to be a lucrative business for state actors and other cybercriminals.

Richard N. Sheinis is a partner, and Brett L. Lawrence and Charles R. Langhorne IV are associates, at Hall Booth Smith PC.

[1] https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781.

[2] https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack.

[3] https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636.

[4] https://www.cnbc.com/2021/04/06/the-extortion-economy-inside-the-shadowy-world-of-ransomware-payouts.html.

[5] https://www.cnn.com/2021/07/09/politics/biden-putin-call-syria-ransomware/index.html.

[6] https://www.documentcloud.org/documents/20796934-memo-what-we-urge-you-to-do-to-protect-against-the-threat-of-ransomware.

[7] https://www.nist.gov/news-events/news/2021/05/nist-releases-tips-and-tactics-dealing-ransomware.

[8] https://us-cert.cisa.gov/ncas/current-activity/2021/06/30/cisas-cset-tool-sets-sights-ransomware-threat.

[9] https://www.nist.gov/news-events/news/2020/09/phish-scale-nist-developed-method-helps-it-staff-see-why-users-click.