Intellectual Property & Technology Law Journal

Edited by the Technology and Proprietary Rights Group of Weil, Gotshal & Manges LLP

VOLUME 31 • NUMBER 7 • JULY 2019

Best Practices for Effectively Defending Against Ransomware Cyber Attacks

By David J. Oberly

Ransomware, a type of malware, has been by far the fastest growing type of cyber threat faced by businesses in recent years. And with good reason—most variants of ransomware encrypt files on an infected system or network, blocking access to the files completely until the victim pays a ransom in order to unlock the files, leading to quick, large paydays for cyber criminals.

Without question, ransomware has developed into one of the most significant and lethal threats to companies of all shapes and sizes today. In 2016 alone, ransomware activities increased by 82 percent, and the amount demanded in ransomware attacks more than tripled. This increase in attack volume and severity illustrates the growing risks of ransomware for large enterprises and small businesses alike.

Fortunately, there are very effective preventive measures available to businesses to significantly mitigate a company's risk of falling victim to a ransomware attack. As such, now is the time for organizations to review the threat of ransomware, and the steps that can be implemented to steer clear of being on the receiving end of a crippling ransomware attack.

David J. Oberly is an associate at Blank Rome LLP representing clients in a wide assortment of complex cybersecurity and data privacy matters. He may be contacted at *doberly@blankrome.com*.

Ransomware Explained

Ransomware is a form of malware that allows attackers to extort victims for financial gain by blocking access to files on an infected computer or network until the victim pays a fee, or a "ransom." This particular form of cyber attack is typically deployed into a network by duping an unsuspecting user to click on a malicious link or download a malicious file through seemingly normal email messages or web page links. Other, more aggressive variants of ransomware, such as NotPetya, exploit security vulnerabilities to infiltrate networks without the need to deceive an end user.

Once activated, ransomware typically self-proliferates and encrypts data inside the environment, and renders the data inaccessible and essentially useless. In order to regain access to their files, victims must pay the attacker a ransom, which can range from hundreds to millions of dollars. However, the overall impact of a ransomware attack extends far beyond mere monetary loss.

For starters, ransomware victims are at great risk of suffering temporary or permanent loss of their files and sensitive information.

In addition, most corporate ransomware victims also suffer extended disruptions in the company's ability to carry on operations and conduct business.

Moreover, even after a ransomware attack has been remediated, the impacted company may also have to

deal with a flurry of litigation and regulatory consequences that oftentimes follow a ransomware incident.

Finally, once knowledge of the attack becomes public, the reputational impact felt by the targeted organization can be extreme, causing severe declines in consumer confidence and associated reputational brand damage.

Fortunately, there are a number of proactive measures that companies can take to minimize the risk of falling victim to a ransomware attack.

Regular, Effective Systems Backups

The most critical way for companies to mount a stringent defense against ransomware attacks is through proper file backup practices.

Importantly, companies can eliminate the leverage that cyber criminals gain through a successful ransomware attack by regularly backing up their files so that an accessible copy of company information and data is available in the event a ransomware attack occurs, which can allow a company to restore encrypted data and files without having to pay a ransom. Backups should be completed at regular intervals, and backup files should be stored at a different location in a manner that is isolated from the company's primary network, so that any infection within the working network can be prevented from spreading to and infecting the company's backup files.

With that said, performing backups is only the first step in implementing effective backup protocols to guard against the threat of ransomware, as backups will do no good unless they work. As such, companies should also routinely test backups for data integrity and to ensure that they are operational.

Cybersecurity Policies

Second, companies should devise and implement robust written cybersecurity policies that set forth broad security requirements which are applicable across the entire organization. These policies should define expectations for employees or anyone with access to company devices or data regarding issues such as the use of personal email and devices, file-sharing programs, and the use of company systems from remote locations. In particular, there are several vital ransomware-focused policies that should be included in all written cybersecurity plans.

The first cybersecurity policy that is particularly effective in combating ransomware pertains the principle of least privilege. Importantly, granting unfettered access to networks and software applications can pave the way for an array of errors and other problems stemming from employees using programs or features they don't need access to.

As such, no users should be assigned administrative access unless it is absolutely necessary, and those with a need for administrator accounts should only use them when necessary. Companies can further restrict and limit exposure by granting employees only the minimal level of access or privilege that is necessary for the employee to carry out his or her job duties and responsibilities.

In addition, companies should also utilize internet restriction policies as well. In particular, companies should restrict access to common ransomware points, such as personal email accounts and social networking sites like Facebook and Instagram. Moreover, mobile device policies—which specify the company's security requirements for the safeguarding of sensitive company files and data that are accessed, transmitted, or stored on any type of mobile device—should also be included as part of any comprehensive cybersecurity policy as well.

With that said, drafting an appropriate security policy is only half the battle in ensuring that reasonable security measures are implemented and put into practice to guard against the threat of ransomware.

In addition, companies must ensure that the policy is also followed and adhered to in practice.

In this regard, companies should complete regular internal or third-party audits of the organization's compliance with its security policy, and take appropriate corrective action to remedy any failures to follow protocol.

In addition, companies should also periodically re-examine and revise their policy as security standards evolve over time.

Patching and Updating

Third, because many file-encrypting ransomware takes advantage of vulnerabilities to penetrate a company's system, businesses must ensure that they keep all systems patched and up to date, as outdated systems and applications that do not have the most recent security patches are vulnerable to ransomware and other malware. Patching

and keeping the company's operating systems and programs updated is vital to defend against attacks that operate by exploiting security flaws, such as the massive WannaCry ransomware attacks of 2017, which exploited a key vulnerability in unpatched systems to spread at breakneck speeds across networks around the globe.

If a program or device is too old to update, retire it, as the limited range of tasks that it can perform is vastly outweighed by the risk that the outdated technology presents to the company's computer networks and systems, which can provide attackers with vulnerable entry points to launch a ransomware attack.

Software updates ordinarily provide patches for security vulnerabilities, and as such should be installed as soon as they become available. Companies should enable automatic updates whenever possible to streamline the process. In addition, companies should also consider using a centralized patch management system to manually update all software and systems according to a regular maintenance plan.

If a program or device is too old to update, retire it, as the limited range of tasks that it can perform is vastly outweighed by the risk that the outdated technology presents to the company's computer networks and systems, which can provide attackers with vulnerable entry points to launch a ransomware attack.

Whitelisting Software

Fourth, companies should further protect their systems and networks with whitelisting software, which only allows systems to execute programs known and permitted by the company's security policy, and prevents unauthorized applications from executing in the first place.

A whitelist is a list of programs and applications that are allowed to be run by the system administrator, and is the opposite of blacklisting, which entails a list of entities that are barred from being used on the company's system. Whitelisting-based application control is critical to protect the endpoint, as this measure prevents unknown or malicious programs, such as ransomware, from executing within the system.

Education and Training

Fifth, companies must also ensure that they provide their workforce with the necessary training that is required to give their employees the knowledge and tools to successfully avoid attempted ransomware attacks. Outside of regular backups, workforce training can have the most dramatic impact in deterring the threat of ransomware.

As such, companies should ensure that they conduct training and regularly educate all company employees on the threat of ransomware, the policies the organization has in place to help prevent ransomware attacks, and the proper practices that employees should follow to minimize the risk of falling victim to an attempted ransomware attack.

In particular, companies should include ransomware-focused training as an integral part of the onboarding process.

In doing so, companies should educate new employees on the company's security policies, procedures, and practices that are geared toward minimizing the risk of ransomware attacks, and the consequences of failing to adhere to these standards. Furthermore, on a regular basis, a refresher course in proper cybersecurity practices should also be given to all employees across the organization. This ensures that employees stay up-to-date on new and emerging threats, and keeps secure computer habits fresh in workers' memories. Moreover, testing employees in real-life, non-classroom settings can be an extremely effective training and educational tool.

In addition, companies should also thoroughly document the organization's compliance with its training programs, which can subsequently be utilized as a defense of the company's efforts to provide reasonable security measures in the event of any future litigation.

Cybersecurity-Oriented Work Culture

Finally, it is essential that companies foster and cultivate a security-oriented culture and work environment to maximize the strength of employees as a defense to ransomware attacks, as cybersecurity training is only beneficial to a company if its workforce genuinely believes in, and adheres to, the practices and strategies that are provided to them.

Here, companies should focus on regularly communicating information and tips regarding critical data security issues throughout the organization,

such as ensuring the security of mobile devices, never opening suspicious email messages or clicking on suspicious web page links, and remaining cognizant of the significant ongoing threat of ransomware scams.

Moreover, companies should ensure that all employees are held accountable for strict cybersecurity compliance and upholding their data security obligations, which can be accomplished by incorporating criteria relating to cybersecurity and data protection as part of employees' periodic performance evaluations and reviews. With the proper focus, companies can effectively instill a culture of cybersecurity and data security throughout their organizations, which can play an important role in avoiding ransomware attacks altogether.

The Final Word

Ransomware is one of the most widespread and damaging cyber threats that businesses face today. According to a recent reports, ransomware costs businesses more than $75 million per year, with the average cost of a ransomware attack totaling a staggering $133,000 per incident. To make matters worse, cyber criminals are becoming more and more adept in adapting their techniques and methods to maximize profits. As ransomware further evolves, so too should the safeguards deployed by businesses to protect their most sensitive, important information and data.

As the brazenness, frequency, and severity of ransomware attacks continues to increase with no end in sight, now more than ever companies must be proactive in implementing effective policies, procedures, and practices to mitigate the cybersecurity risk posed by ransomware attacks.

Through implementation of the several key ransomware-focused cybersecurity measures and safeguards discussed above, businesses can effectively minimize the risk of falling victim to a catastrophic ransomware attack.