Ransomware Attacks: Prevention and Preparedness

By Joseph J. Lazzarotti, Jason C. Gavejian, Nicky Jatana, Marlo Johnson Roebuck and Damon W. Silver

May 14, 2017

Several years ago, cyber criminals developed a profitable form of malware, now known as ransomware. A "ransomware" attack occurs when a hacker takes control of the victim's information systems and encrypts its data, preventing the owner from accessing it unless the victim pays a sum of money, usually in the form of bitcoins.

The FBI reported that ransomware attacks jumped from 1,000 a day in 2015, to 4,000 a day in 2016. In the middle of May 2017, criminals using tools believed to have been used by the U.S. National Security Agency unleashed a global ransomware attack against governments and companies in nearly 100 countries around the globe.

Beyond the absurd number of attacks in 2016 and 2017 is the amount of money organizations and individuals have paid with the hope of decrypting and retrieving their data. Reports estimate close to one billion dollars in ransom payments in 2016.

Although it is tempting to simply pay the ransom, obtain the decryption keys, and move on, there are serious risks to this approach. And there is no guarantee that, upon receipt of the ransom payment, the hacker will provide all the applicable decryption keys allowing your organization to regain full access to its data.

The rapid growth in ransomware attacks and their potential damage on organizations is frightening. Organizations may not be able to prevent all attacks, but there are steps they could take to minimize the chance and impact of a successful attack, and to be prepared to respond.

Before an Attack

1. Build the right team

- Ensure you have an IT team in place, whether internal or through a third-party vendor, well-versed to handle ransomware and other forms of malware.

2. Secure the systems

- Conduct a risk assessment and penetration test to understand the potential for exposure to malware.
- Implement technical measures and policies that can prevent an attack, such as endpoint security, email authentication, regular updates to virus and malware definitions/protections, intrusion prevention software and web browser protection, and monitor user activity for unauthorized and high risk activities.

3. Make your employees aware of the risks and steps they must take in case of an attack

- Educate employees on how to recognize phishing attacks and dangerous sites — say it, show them, and do it regularly. This includes instructing them to use caution when clicking directly on links in emails, even if the sender appears to be known — verify web addresses independently. Be particularly wary of compressed or ZIP file attachments.
- Employees should avoid revealing personal or financial information about themselves or other employees and customers in email, and avoid responding to email solicitations for this information.
- Direct employees to pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (*e.g.,* .com vs. .net).
- Instruct employees on what to do immediately if they believe an attack has occurred (*e.g.,* notify IT, disconnect from network, and other measures).
- Instruct employees on what *not* to do (*e.g.,* deleting system files, attempting to restore the system to an earlier date, and the like).

4. Maintain backups

- Backup data early and often.
- Keep backup files disconnected from the network.

Meet the Authors

Joseph J. Lazzarotti

Principal
Berkeley Heights 908-795-5205
Email

Jason C. Gavejian

Principal
Berkeley Heights 908-795-5139
Email

Nicky Jatana

Office Managing Principal
Los Angeles 213-630-8233
Email

Marlo Johnson Roebuck

Office Managing Principal
Detroit 248-936-1928
Email

5. Develop and practice an "Incident Response Plan"

- Identify the internal team (*e.g.,* leadership, IT, general counsel, and HR).
- Identify the external team (*e.g.,* insurance carrier, outside legal counsel, forensic investigator, and public relations).
- Outline steps for organizational continuity — using backup files and new equipment, safeguarding systems, and updating employees.
- Plan to involve law enforcement (*e.g.,* FBI, IRS, Office of Civil Rights, and so on).
- Plan to identify, assess, and comply with legal and contractual obligations.
- Practice the response plan with the internal and external teams, reviewing and updating the plan to improve performance.

After an Attack

6. Secure your systems

- Review and follow your Incident Response Plan.
- Avoid compromising your investigation! This includes being careful to preserve firewalls, network and other access and activity logs and artifacts on the system that could have valuable information needed to confirm whether or not a breach occurred.
- Determine whether all malware has been removed and systems are protected from future attacks, including whether the attack is completed or ongoing, and, if ongoing, how to contain it.
- Evaluate feasibility of restoring the affected systems for normal use, mindful of the need to preserve information necessary for a forensic investigation, litigation defense, and enforcement agency inquiry.
- Monitor restored systems for a period of time.

7. Consult legal counsel and other key vendors

- Ransomware attacks can trigger obligations under federal and state privacy laws, such as HIPAA and data breach notification laws.
- Recovering encrypted data can be complex and uncomfortable for the organization, particularly if negotiating and making a ransom payment is necessary.
- Members of IT staff may not have sufficient experience with the latest cybersecurity tools and ransomware attack methodologies to provide competent direction.
- Consulting with your insurance broker or cyber-insurance carrier is important not only to confirm applicable coverage, but also because the insurance contact may provide valuable early guidance.

8. Investigate the incident

- Determine what happened, when, and the method the hackers used to carry out the attack.
- Identify which systems were affected and the nature of the data affected (*e.g.,* protected health information ("PHI")).
- Identify the total number of individuals (in each state of residence) whose data was affected.
- Confirm whether evidence shows that the affected data was accessed, acquired, and/or exfiltrated to the outside of your systems.
- Evaluate what mitigation measures were in place (e.g., were the affected files encrypted, extent of data backup, and so on).

9. Provide notifications, if needed

- Determine whether state or federal laws require notification to affected individuals.
- Federal and state agencies and credit monitoring bureaus may need to be notified based on a number of factors, including the states of residence of the persons affected and the number of persons affected.
- Contract and ethical obligations may exist requiring notification.
- Credit monitoring, call center, and other services also may be required or appropriate under the circumstances.

10. Lessons learned

- Prepare an Incident Response Report including the *Who? What? Where? When? Why? How?*
- Review the Incident Response Report with all internal and external team members to learn from and prevent future attacks.

Jackson Lewis has a 24/7 Data Incident Response Team to assist with a ransomware attack, data incident, or data breach.

Damon W. Silver

Principal
New York Metro
New York City 212-545-4063
Email

Practices

Privacy, Data and Cybersecurity

Industries

Chemicals
Energy and Utilities
Financial Services
Healthcare
Higher Education
Hospitality
Insurance
Life Sciences
Manufacturing
Media
Professional Services
Real Estate
Retail
Technology
Transportation

material. This material may be considered attorney advertising in some jurisdictions. Prior results do not guarantee a similar outcome.

Focused on labor and employment law since 1958, Jackson Lewis P.C.'s 950+ attorneys located in major cities nationwide consistently identify and respond to new ways workplace law intersects business. We help employers develop proactive strategies, strong policies and business-oriented solutions to cultivate high-functioning workforces that are engaged, stable and diverse, and share our clients' goals to emphasize inclusivity and respect for the contribution of every employee. For more information, visit https://www.jacksonlewis.com.

*The National Operations Center serves as the firm's central administration hub and houses the firm's Facilities, Finance, Human Resources and Technology departments.