KPMG

Ransomware attack risks

Ransomware attacks and the potential threat to your company

2021

kpmg.com

Organizations of all sizes and across industries continue to be challenged with managing the risk and impacts of ransomware attacks. Developing a methodical approach to strategize, plan, prevent, identify, research, resolve, recover, and report ransomware attacks is critical to effectively mitigate the inherent risks and impacts posed by ransomware. One of the greatest challenges ransomware attacks present is the wide range of possible attackers because the attacker can be anyone using any of the many different attack vectors.

Veeam's 2020 survey[3] found that 95 percent of organizations globally experience outages and the average outage lasts **117 minutes**

Ponemon Institute[4] has estimated that the average cost of an unplanned outage is nearly

$540,000 per hour

66%

of companies estimate it would take **five or more days** to fully recover from a ransomware attack if they didn't pay the ransom.[1]

Gartner finds that downtime can be as much as

$300,000 per hour on average[2]

[1] "The 2020 Ransomware Resiliency Report," Veritas Technology LLC, 2020

[2] "The Cost of Downtime", Gartner, 2014

[3] Veeam press release; "CXO Research: Legacy Technology and Lack of Skills Hindering Digital Transformation and IT Modernization", 2020

[4] Cost of Data Center Outages Report, Ponemon Institute, 2016

What is ransomware?

Ransom malware, or ransomware, is a type of malware that prevents users from accessing their system or personal files using encryption and demands ransom payment in order to regain access.

Once the files or data under attack are encrypted, a user is shown instructions on how to pay the ransom in order to receive the decryption key. However, one of the major risks that result from ransomware is that paying the ransom does not always guarantee the successful restoration of the data encrypted during the attack. Whether the key is received from the attackers or not, having your data impacted by an attacker ultimately draws into question the integrity of the data. An organization who has not considered the risks and impacts that result from ransomware attacks may not only be more vulnerable to an attack, but also may suffer a greater impact than an organization that prepared for ransomware attacks.

It is critical for the organization to proactively consider and plan for potential ransomware attacks because a lack of resilience to an attack could lead to significant business interruption that can have a direct impact to the organization's top and bottom lines.

How is ransomware delivered?

Some common ways ransomware is introduced to an environment are through social engineering attacks, drive-by downloads, remote desktop protocol, pirated software, and removable media. Commonly, ransomware is spread through social engineering attacks, which include phishing or whaling attacks that contain malicious links or attachments. When the attachments are opened by the user, the malware automatically downloads and installs, typically without the user even being aware. Ransomware can also be introduced into an organization's environment through drive-by downloads. A drive-by download occurs when a user visits a web page and unknowingly downloads and installs malicious code. Remote desktop protocol is a secure network communications protocol that allows IT admins to gain access to systems remotely. These methods typically take advantage of, or exploit, browsers (and their plug-ins), applications, or operating systems that are out of date or unpatched in order to infect users. The malware then propagates through the network to maximize the amount of data impacted.

Risks and impact of a ransomware attack

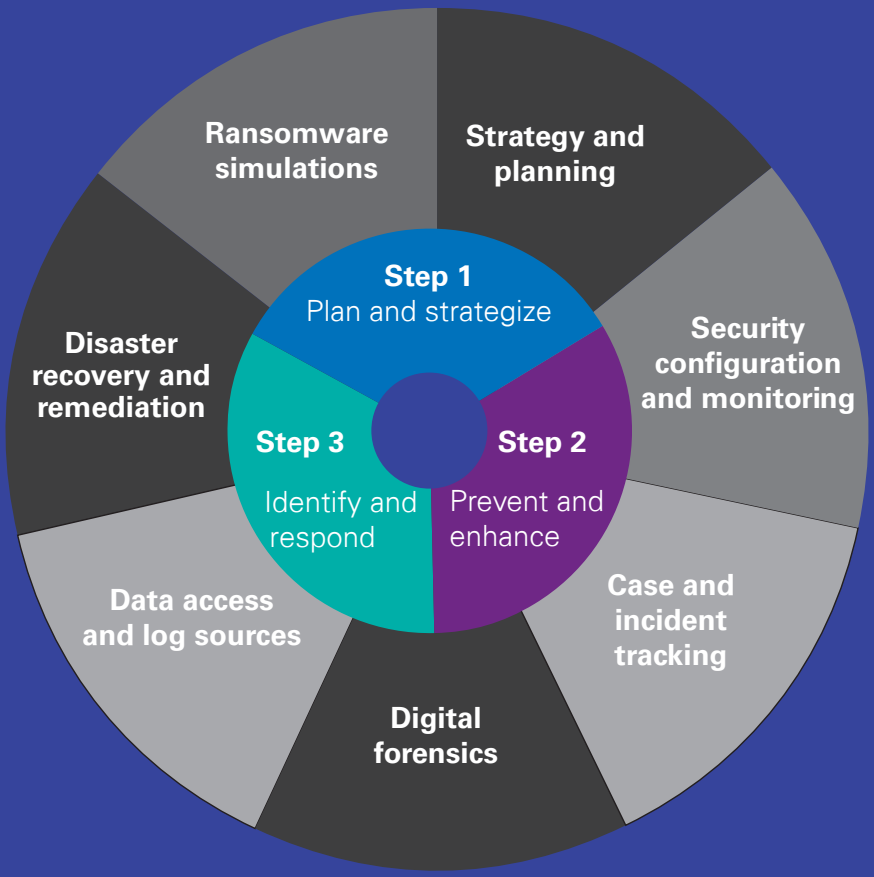
- Loss or reduction in productivity due to the inability to access data or systems
- Restoring data from an older recovery point can result in a significant amount of lost business transactions or other critical data
- Data encrypted during the attack may not be able to be recovered, resulting in a significant loss of data
- Paying the ransom can lead to being targeted more in the future
- Significant financial liability can result from inability to perform business functions
- Misunderstanding cyber security insurance policies can lead to a greater financial impact to the organization if claims are denied
- Any data touched by cybercriminals or malware will bring into question the integrity of the data
- Legal and other professional fees may be required in order to investigate and prosecute responsible parties
- Paying the ransom may not restore and/or decrypt the data files
- Reputational risk to the organization

Who is responsible for preparing for, and responding to, ransomware attacks?

In order to reduce the impact of a ransomware attack, it is critical for an organization's IT Operations, IT Risk and Compliance, Internal Audit, and legal counsel functions to be involved and work together in all aspects of ransomware preparation and response. Although IT Operations is responsible for implementing the technical controls and performing immediate response to an attack, IT Risk and Compliance needs to play a major role in challenging the organization's current state and ultimately the organization's preparedness for ransomware vulnerabilities. IT Risk and Compliance should identify emerging risks related to ransomware and work with IT Operations to ensure the risk is assessed and treated appropriately. IT Operations and IT Risk and Compliance should work with their organization's legal counsel in order to ensure they are appropriately covered by cyber security insurance and have the necessary controls or requirements in place to be eligible for coverage. The Internal Audit function should play an active role in reviewing the response playbook developed and should participate in any tabletop exercises or simulations performed in order to provide constructive feedback on the design, implementation, and operating effectiveness of controls. Additionally, Internal Audit should periodically test controls implemented around preventing, detecting, and responding to ransomware attacks. Lastly, all three functions should coordinate in planning and executing tabletop exercises to ensure the plan is feasible and that all parties know their responsibilities.

KPMG approach to manage ransomware risk

A three-phase approach can be used to effectively manage and address the risks that result from potential ransomware attacks:



1 Plan and strategize

Implement and routinely test and enhance robust resiliency plans specific to ransomware attacks to optimize the organization's response in the event of a threat or attack. Resiliency plans should be focused around an organization's critical data sets.

Develop a detailed recovery playbook for ransomware attacks to recover more efficiently with the following considerations:

- Identification and notification
- Initial steps
- Identification of most common ransomware scenarios applicable to the organization to proactively build responses
- Assessment of impact and magnitude of incident
- Steps to determine if the organization should pay the ransom
- Identification of a clean backup for restoration
- Steps on restoring data
- Contact information and details around how to work with legal counsel to engage with cyber security insurance providers and what information needs to be available
- Resolution steps
- Postmortem review process.

Work with your organization's legal counsel to purchase and routinely review cyber security insurance for the organization

2 Prevent and enhance

A combination of preventive and detective controls should be employed in order to prevent an attack from occurring while also being able to detect or identify possible attacks quickly in order to resolve the incident and greatly reduce the overall impact to the organization. Typical controls for preventing and detecting ransomware include:

Implementation of data classification policy:

Classifying an organization's applications and associated data in a policy assists the organization in determining the level of security and controls needed for various IT assets.

Email protection:

Implementing email protection controls, including email filtering and sandbox, can help prevent employees from being exposed to phishing attempts to greatly reduce the risk of ransomware being introduced into the environment.

Patching:

Arguably the most important method of preventing ransomware is by having an established software patching process and applying software patches in a timely manner to protect your organization from known exploits.

2 Prevent and enhance (continued)

Endpoint protection:

Endpoint protection controls including antivirus and scripting can help prevent ransomware from being introduced into the environment while also helping to quickly detect an attack.

Data backups and testing:

Implementing automated data backups that are performed on a frequent basis (daily or weekly) can minimize the data lost during an attack with multiple recovery points being available. Periodically testing the availability of the backup ensures an organization is able to effectively use and recover from the backups.

Multifactor authentication:

Implementing multifactor authentication controls to help protect against the compromise of passwords for privileged accounts.

Data resiliency tools:

Data resiliency tools (i.e., Commvault, Cohesity, Rubrik, Veeam, etc.) can be deployed to help identify potential ransomware incidents and alert relevant parties in a more timely and efficient manner.

WORM and immutable file system controls:

Implement write once, read many (WORM) and immutable file system data storage technology in order to ensure that data backups cannot be rewritten or edited.

Network segmentation and file share management

Logically or physically segment your network in order to inhibit the spread of ransomware.

Tabletop exercises/simulations:

Routinely perform tabletop exercises or simulations in order to identify key gaps in the plan and to ensure preparedness of all participants who play a key role in the plan.

Training on cyber security threats for all employees:

Routine training on cyber security threats and industry leading practices for employees can significantly reduce the risk of ransomware being downloaded or ingested into the environment. The training should also be reviewed and updated on an ongoing basis as new cyber security threats arise.

Policies:

The organization's IT policies should outline the requirements for the above control considerations and should routinely be reviewed and updated.

3 Identify and respond

In case of an attack, the following steps are recommendations in order to help identify, research, resolve, recover, report, and review an attack, which can be detailed in the recovery plan and made available to personnel:

Step 1:

Upon identification, immediately escalate to senior management to initiate incident response plan.

Step 2:

Actively research the magnitude and breadth of the incident and take action to stop the spread of malware in the environment.

Step 3:

Work with legal counsel to determine whether insurance providers need to be contacted, what their requirements are, and whether they are required to be involved in ransomware negotiations.[5]

Step 4:

Resolve the incident according to the organization's plan while being in constant contact with legal counsel and insurance providers.

Step 5:

Determine appropriate notification to clients based on contractual requirements in collaboration with legal counsel.

Step 6:

Perform a detailed postmortem review in order to enhance and optimize control framework.

[5] While discussing ransomware negotiations with legal counsel, it is important to take into consideration the U.S. Government's Office of Foreign Assets Control (OFAC) listing of cyber actors that organizations are restricted to negotiate with.

Why KPMG

KPMG has highly trained Technology Risk Management and Cyber Security Services practices that support first-, second-, and third-line technology risk functions with vast experience in working with organizations to improve their ransomware resiliency plans, assessing and recommending preventive and detective controls to combat ransomware risks, and assisting in conducting tabletop exercises to help ensure preparedness for an attack.

Relevant services

— Risk and controls self-assessment

— Business continuity and disaster recovery assessments

— Internal audits

— Controls readiness assessments

For more information, visit read.kpmg.us/TRM.

Contact us

Beth McKenney
Principal, Technology Risk Management
T: 313-230-3406
E: bmckenney@kpmg.com

Richard Knight
Principal, Technology Risk Management
T: 703-286-8393
E: raknight@kpmg.com

Edward McCaffrey
Director, Technology Risk Management
T: 212-954-3747
E: etmccaffrey@kpmg.com

Edward Goings
Principal, Cyber Response Services
T: 312-665-2551
E: egoings@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia