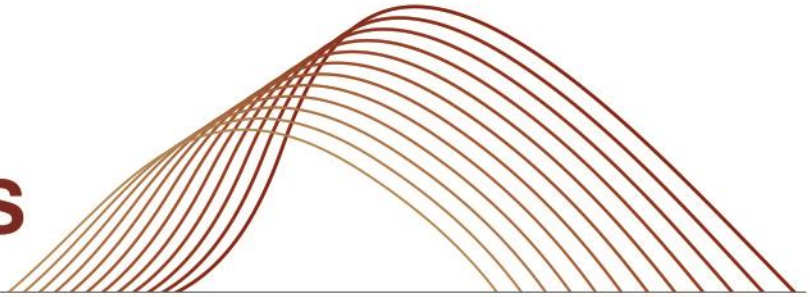
PAUL HASTINGS

PH PERSPECTIVES



September 2017

Follow **@Paul_Hastings**

In-House Counsel Guide to Ransomware Prevention, Preparedness, and Response

By Robert Silvers, Jacqueline Cooney & Reade Jacob

Ransomware Response Plan

Background

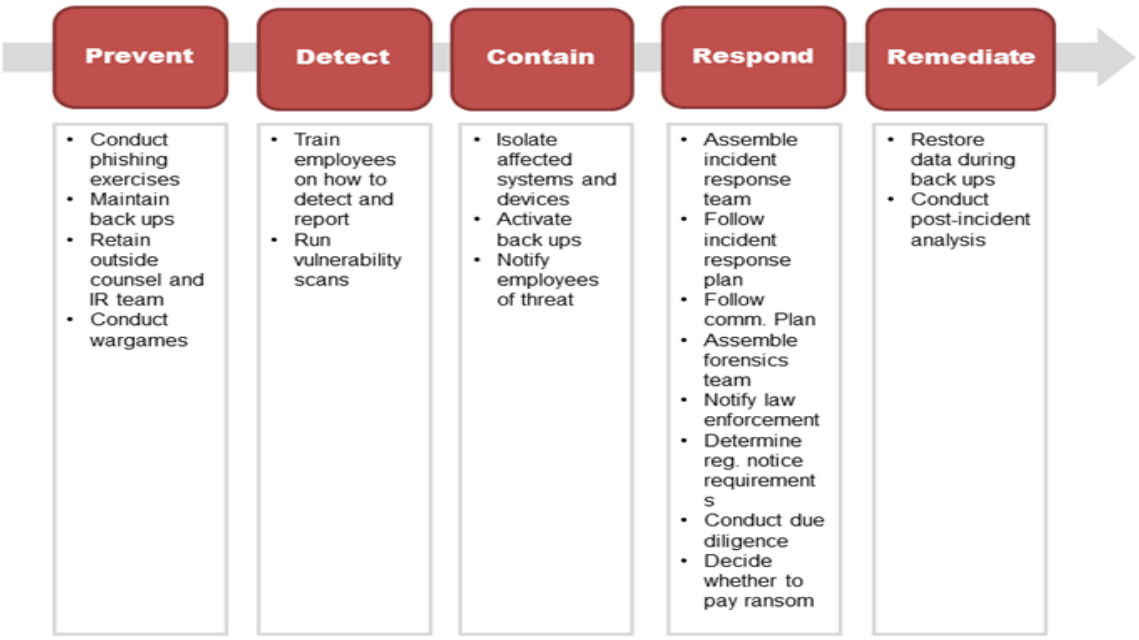
Ransomware is a variant of cyber-attack in which the perpetrators encrypt an organization's data and then demand a monetary payment for the decryption key, usually in the form of cryptocurrencies such as bitcoin. Ransomware is most frequently delivered through phishing emails that corporate employees click through, introducing the ransomware onto the corporate network. By rendering critical data and systems inaccessible, ransomware can have severe operational consequences and can bring the business of even multinational companies to a halt.

A ransomware strike raises urgent operational, IT security, and legal and compliance questions for a victim company. Companies must be able to rapidly work to restore operations and communicate with customer and commercial partners. They must simultaneously grapple with difficult questions like whether to pay ransom, how to coordinate with law enforcement, and how to contain potential liability for financial damage caused by any disruption of operations or from regulatory inquiries that the attack may trigger.

Because ransomware strikes with no warning, companies need to think ahead. They need to take all available preventative measures in advance. And they also need a response playbook ready in the event the preventative measures fail. This planning should be incorporated into, or developed complementary to, an organization's existing cyber preparedness and incident response planning.

Purpose

Effective corporate ransomware plans outline the company's strategy to prevent, detect, contain, and respond to a ransomware attack. The paramount objectives are to protect the company's assets, its continuity of operations, and the sensitive information in its possession.



Prevent

- Conduct regular counter-phishing training for employees, as phishing emails are the vector for the vast majority of ransomware attacks. Test employees through periodic fake phishing emails sent by the IT department, and hold employees to account should they repeatedly click through.
- Maintain robust data back-up procedures. If data is backed up regularly and readily accessible, the need to pay ransom may be obviated because the data can be restored by tapping into the backup.
- Retain outside cyber forensics firms and legal counsel ahead of time so that they can begin work immediately upon detection. As in any significant cyber incident, retain the cyber forensics firm through counsel to preserve the privilege over their investigation and findings.
- Conduct internal exercises (e.g., tabletop exercises or wargames) to test the effectiveness of incident response and ransomware response plans, escalation procedures, and response to data security incidents and privacy breaches.

Detect

- Employees should notify their IT department immediately when a potential ransomware attack has occurred, including when they have clicked on a potential phishing email or when they receive workstation display of a ransom demand. Employees should be trained never to pay ransom or attempt to negotiate or communicate with the attackers.
- Run regular scans on systems, databases, and endpoints to detect any ransomware that may have been deployed and/or is deployable.

Contain

- The IT security team should actively establish remediation measures to include the following categories of work: (1) isolate infected system by removing infected systems from the network as soon as possible; (2) isolate or power-off affected devices that have

not yet been corrupted; (3) secure backup data or systems by taking them offline, as applicable.

- Notify employees of the presence of ransomware and advise them of specific actions to take, such as refraining from using emails, contacting IT as soon as any suspicious activity is identified, and refraining from responding to any ransomware demands.

Respond

- Assemble Incident Response Team: Establish, in advance, an incident response team to act as the coordinating body for all post-detection decisions. The incident response team should include all relevant divisions, including IT security, legal, compliance, human resources, customer relations, and public relations, as well as the company's outside cybersecurity firm and outside counsel.

- Follow Incident Response Plan: Review and follow the company's incident response plan and playbook, which should contain a step-by-step guide that details each incident response team member's role in responding to a ransomware event.

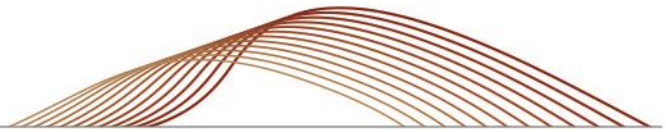
- Assemble Forensics Team: The outside cybersecurity forensics team should investigate the root cause and extent of the incident, in coordination with and under the direction of counsel. The forensics team should work closely with the company's IT security team to capture images of affected systems, collect and analyze evidence, and outline remediation steps. The forensics team should report findings back to the incident response team.

- Follow Incident Response Communications Plan: Depending on the severity of the ransomware incident and the impact on operations, news of the attack may spread quickly, triggering the need for a fast crisis communications response. Review and follow the company's incident communications plan to reach all affected audiences—employees, customers, investors, key commercial partners, regulators, law enforcement and the media. External communications should be coordinated with the incident response team to ensure all operational and business objectives and legal considerations are accounted for.

- Consider Notifying Law Enforcement: Determine whether to notify law enforcement, which can provide guidance and support in responding to ransom demands and technical remediation.

- Determine Regulatory Notice Obligations: Counsel should immediately begin to review applicable federal, state and international regulatory data breach notification obligations, which can vary depending on jurisdiction, which regulators have oversight, and whether individuals' personal information may have been compromised.

- Determine Contractual Notice Obligations: Commercial agreements now routinely require parties to notify others when a cyber-attack may endanger performance of obligations or put sensitive data at risk. These contracts also often require specific mitigation measures to be put in place. Counsel should advise the company on its obligations to its commercial partners so that the company is not in breach and can reduce potential liability.



- Pursue Investigation, Diligence, and Decisions Around Ransom Demands: The decision whether to pay ransom is highly sensitive. All deliberations and processes surrounding whether to pay ransom should be conducted at the direction of counsel so that they are protected under the attorney-client privilege. When making a decision whether to pay ransom, the company should:
  - Identify and immediately engage decision makers, which, at a minimum, should include the CEO or COO, the CIO or CISO, and the General Counsel. It may also be appropriate to brief the board of directors or a relevant committee thereof.
  - With the assistance of outside experts, the company should conduct whatever diligence it reasonably can to identify who may be the perpetrator. This can assist in evaluating sanctions compliance risk, the likelihood the perpetrator will indeed furnish the decryption key upon payment, and other relevant context.
  - Evaluate all options when deciding whether to pay ransom. Such considerations may include technical feasibility, timeliness, and costs of restarting systems from backup; ransom value; attacker reputation and whether the attacker could strike again or demand more; and legal and compliance considerations.
  - Review the company's insurance policies to determine coverage and required steps for pursuing coverage, including notification of the insurance company prior to paying ransom.
  - If a company decides it will pay ransom, it should consider whether first to notify law enforcement that it is planning to do so, a step that can mitigate compliance risk and also may be required to pursue insurance coverage.
  - Consider in advance avenues of purchasing bitcoin quickly or maintaining bitcoin assets in reserve as a contingency measure.

Remediate

- Restore Data During Backups: Recover from the ransomware attack by restoring data backed up prior to the attack and returning to "business as usual" operations.
- Conduct Post-Incident Analysis: Conduct post-incident analysis, at the direction of counsel to preserve the privilege, to determine whether the situation was appropriately handled and whether the company's incident response planning or related policies should be updated or improved.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Frankfurt

Bernd Meyer-Witting
49.69.90.74.85.116
berndmeyerwitting@paulhastings.com

San Francisco

Thomas P. Brown
1.415.856.7248
tombrown@paulhastings.com

Thomas A. Counts
1.415.856.7077
tomcounts@paulhastings.com

Seoul

Jong Han Kim
82.2.6321.3801
jonghankim@paulhastings.com

Shanghai

Haiyan Tang
86.21.6103.2722
haiyantang@paulhastings.com

Tokyo

Toshiyuki Arai
81.3.6229.6010
toshiyukiarai@paulhastings.com

Hiroyuki Hagiwara
81.3.6229.6015
hiroyukihagiwara@paulhastings.com

Washington, D.C.

Benham Dayanim
1.202.551.1737
bdayanim@paulhastings.com

Robert Silvers
1.202.551.1216
robertsilvers@paulhastings.com

Sherrese M. Smith
1.202.551.1965
sherresesmith@paulhastings.com

Washington, D.C.
PH Cyber/Privacy Professionals

Jacqueline Cooney
1.202.551.1236
jacquelinecooney@paulhastings.com

Katie Clare
1.202.551.1937
katieclare@paulhastings.com

Matthew Majkut
1.202.551.1700
matthewmajkut@paulhastings.com