MARSH

Ransomware: Remove Response Paralysis with a Comprehensive Incident Response Plan

Ransomware attacks are becoming more frequent, severe, and sophisticated. For affected organizations, it's not uncommon to be caught off guard and experience a "paralysis" that lessens response effectiveness. In the past year, approximately **51%** of organizations globally suffered a ransomware attack. The escalation in attacks —involving higher ransom payments and increased downtime—has significant financial and operational impacts.

Organizations should anticipate and prepare well in advance for the possibility of ransomware attacks. Below, we explore how organizations can avoid response paralysis and what they should consider before, during, and after an attack.

Pre-Incident

Know Your Options:

- Recognize that as a victim of ransomware you will have three basic approaches to recovery:

  1. Restore from backup.
  2. Attempt to break the encryption.
  3. Pay the ransom and follow the threat actor's instructions.

- Note that insurance proceeds may be available to cover the costs associated with ransom and recovery. In such cases, follow specific policy requirements to maximize total recovery.

- Be aware that these approaches are labor and time intensive, and do not guarantee that you will recover all of your lost data.

Develop Internal Policies and Guidance:

- Procedures for handling ransomware incidents should be incorporated into your incident response plan. Unfortunately, many such plans do not incorporate ransomware procedures. Organizations should consider developing a ransomware "playbook" of activities and actions specifically related to ransomware response. This should include advance discussion of ransomware response with executive leadership to understand their overall guidance related to a ransomware attack.

- Develop policy to guide decision making on the question of whether to pay a cryptocurrency ransom demand. The policy should specify the parameters to be considered, including the cost of the ransom vs. the estimated cost of restoration, the likelihood of successful restoration whether the ransom is paid or not, regulatory implications (see below), and the criticality of the data. Senior executives and the cyber incident breach response team should be aware of the policy details.

- While paying a ransom should be considered only under extreme circumstances, it is wise to develop a plan for how to pay a cryptocurrency ransom demand should it become necessary. It is a best practice to pay a ransom demand through your external cyber legal counsel or cyber forensic provider (see below).

Understand Regulatory Implications and Potential Sanctions:

- Obtain a documented position or perspective from external cyber counsel on the potential legal implications of paying a ransom demand to a cyber threat actor. For example, the following two legal frameworks related to international funds transfer may be relevant.

  – **Foreign Corrupt Practices Act (FCPA):** FCPA prohibits US citizens from bribing foreign government officials to benefit their business interests. In most cases, paying a ransom would not violate FCPA, but individual circumstances may warrant close examination of potential FCPA liability.

  – **Department of Treasury Office of Foreign Assets Control (OFAC):** On Oct. 1, 2020, OFAC published an **advisory** reiterating the prohibition against US businesses and persons conducting business or paying funds to any person on the "Specially Designated Nationals and Blocked Persons" (SDN) list. OFAC regulations are relevant in a ransomware event because the attacker demanding the ransom may be on the SDN list. US companies can be sanctioned for violation of OFAC's rule even if they do not personally execute a transaction or know that a payment is being made to a prohibited organization or person.

Secure Approval from the Board:

- Obtain approval from the board of directors on policy documents. Recognize that policies are likely to be discoverable if legal action is taken against the company due to its handling of a ransomware event.

Examine Impact on Insurance:

- Understand any cyber insurance coverage that you may have as it pertains to paying ransoms, as well as other resulting losses from a ransomware incident.

- Consider the following factors to enhance the likelihood of recovery under the policy:

  – It is critical to report the incident per the insurance policy's claims and loss reporting guidelines. This is in addition to any reporting you make to authorities. According to the terms of the insurance policy, not filing notice could jeopardize coverage.

  – Obtain from the insurer approval that allows third-party vendors to respond to the incident. This is particularly important if the third-party firm is not one of the insurer's pre-approved vendors. Insurable vendor expenses may include costs related to the following services: data breach coach/privacy counsel, IT forensic investigations, call center and credit monitoring/identity theft monitoring, crisis management and public relations, the cost to obtain cryptocurrency, the demand itself, and ransom demand negotiation.

  – Cooperation with the insurer throughout the incident response and any resulting claim is critical.

Seek Legal Counsel:

- If you are not already doing so, you should consider working with a law firm that specializes in cybersecurity and data protection to serve as your cyber incident response coach. Ensure the firm is experienced in handling ransomware events. If not, consider selecting a different firm. The law firm should:

  – Coordinate response activities with your insurance broker and insurer if you have cyber insurance.

  – Provide guidance on legal and regulatory considerations related to ransomware such as cryptocurrency, FCPA, and OFAC.

  – Help you identify a cyber forensics provider with documented expertise in ransomware incidents.

  – Support interactions with law enforcement and other external entities as necessary.

  – Secure functional specialists as needed, including crisis communications professionals and call center support.

  – Assist in managing other aspects of the incident that are not specific to ransomware, such as notifications and insurance claims.

  – Ensure that the entire response falls under attorney-client privilege.

Engage Outside Expertise:

- Survey the market for cyber forensic service providers and understand the range of capabilities they offer for dealing with ransomware incidents. Focus on companies that have strong credentials, experience, and a superior reputation for cyber forensics. Your insurer, cyber broker, and your cyber incident response coach can help to identify providers.

- Learn about tools that may be available to decrypt different strains of known ransomware. Document learnings as a possible incident response resource. For instance, the **No More Ransom Project** is a good source of free tools for decrypting certain ransomware varieties. Other resources are also available, and should be investigated as part of pre-incident preparedness. Engage your cyber forensic service provider for support.

Determine How to Manage a Ransom Payment:

- Understand the basics of **cryptocurrency**. Determine whether your legal counsel or cyber forensics provider will be responsible for managing any potential cryptocurrency transactions on your behalf. In addition to supporting a smooth, quick transaction, the external legal counsel will also ensure compliance with **OFAC** or other regulatory guidance related to ransomware payments. Remember that cryptocurrency exchanges charge fees for cryptocurrency purchases.

During the Incident

Minimize Exposure and Maximize Backup:

- Isolate the ransomware infection by turning off servers and computers throughout the enterprise and disabling their LAN and WiFi connections or blocking network traffic to them. Ransomware moves quickly and can substantially disable an entire enterprise in minutes. Speed of response is critical as infection spreads quickly.

- Eradicate the malware executable code from networks and systems. Be aware that there are likely to be many copies of the malware throughout your IT environment. Additionally, be mindful that hackers sometimes hide malware in unexpected places (such as connected network devices like printers) that can reactivate and execute the original attack.

- Do not delete related files such as key files, text files, or ransomware notes as they may be helpful for understanding the threat actor's tactics or needed for recovery. Secure the most recent good backup in offline storage.

- Recognize that regardless of the data restoration approach, full restoration of the affected data will require considerable hands-on work and can take many days.

Tap into Insurance Expertise:

- If you have cyber insurance, engage your organization's risk manager and your cyber insurance broker to review relevant requirements of the insurance program, the expectations of the insurer, and any ransomware-specific services that the carrier may offer (such as cryptocurrency payments support).

- If you decide to pay the ransom, confirm with your carrier before making the payment. Many carriers require that they pre-approve in advance of a client making a ransom payment.

Follow Your Internal and External Guidance:

- Follow the organization's incident response plan, including pre-established procedures related to ransomware, such as those outlined above.

- If your company has a pre-existing contract with a cyber forensics provider, consider separate contract arrangements if that provider is to support the ransomware incident. Consult with your counsel. Payment to the providers through a distinct budget and management structure may preserve attorney-client privilege.

Execute on the Ransom Payment – Or Don't!

- The final decision on whether to pay should be made through careful internal deliberation after sufficient legal advice and cyber forensic technical analysis.

- If the decision is made to pay the ransom, engage your external counsel or cyber forensics provider to handle the transaction, consistent with the guidance of the cyber forensic team. And be aware that payment of the ransom does not guarantee your files/data will be returned or access fully restored.

- If the decision is to not pay the ransom, then:

  - Identify impacted systems. Wipe and rebuild them in accordance with pre-defined IT procedures and priorities to ensure they have no remaining ransomware/malware. Do a complete wipe and reformat of all storage devices, and restore the data from known sound sources.

  - Once all systems are cleaned—and operating systems, applications, and data are restored—then the network can be re-established and declared operational.

Post-Incident

Update Internal Guidance:

- Document what you learned: how the infection occurred and what measures to put in place to prevent it from happening again.
- Review and revise the ransomware policy as needed.
- Update IT disaster recovery plans.

Bring In External Expertise:

- Engage a cyber defense service provider to perform an "indicators of compromise" assessment of the entire network. Find and eliminate any remaining malware or associated files or artifacts. Consider using a provider other than the forensics company that supported the response. While discovery and eradication of indicators of compromise is part of the response effort, an independent and comprehensive post-incident assessment will provide additional confidence that ransomware has been eliminated.

Identify Weaknesses:

- Address network and system vulnerabilities or gaps identified during the forensic analysis to prevent a repeat attack.
- Conduct an after action review and lessons learned (AAR-LL) session with all who were involved in the incident. Capture information on what went well and what did not go well, and identify corrective actions to improve the response process for future ransomware events.
  - For each gap or weakness, identify a senior manager or executive to be accountable for the completion of corrective actions.

Review Backup Strategy:

- Review and refresh the data backup strategy, incorporating accepted best practices and lessons learned in the ransomware event. This may require re-architecting the data backup system if it falls short of data security needs. The data backup strategy should articulate:
  - What data is to be backed up.
  - Where the data is hosted: on premises, remote, cloud, or offline.
  - How frequently different types of backup occur.
  - Who is responsible for performing backups.
  - Who is accountable for ensuring backups are successfully performed.
- Exercise and test data backup systems and processes regularly.

Remember:

The effects of a ransomware attack can be anticipated. With solid planning, your organization will be well positioned to handle a potential attack.

For more information and other solutions from Marsh, visit marsh.com, or contact your local Marsh representative.

JIM HOLTZCLAW
Senior Vice President, Cyber Risk Consulting, Marsh Advisory
+1 202 297 9351
james.holtzclaw@marsh.com

REID SAWYER
Practice Leader, US Cyber Risk Consulting, Marsh Advisory
+1 630 442 3506
reid.sawyer@marsh.com

Marsh is one of the Marsh & McLennan Companies, together with Guy Carpenter, Mercer, and Oliver Wyman.

This document and any recommendations, analysis, or advice provided by Marsh (collectively, the "Marsh Analysis") are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, tax, accounting, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. Marsh makes no representation or warranty concerning the application of policy wording or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage. Although Marsh may provide advice and recommendations, all decisions regarding the amount, type or terms of coverage are the ultimate responsibility of the insurance purchaser, who must decide on the specific coverage that is appropriate to its particular circumstances and financial position.