Marsh

Ransomware

Remove Response Paralysis with a Comprehensive Incident Response Plan

May 2021

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

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

PRE-INCIDENT

Know Your Options

- Recognise that as a victim of ransomware you will have three basic approaches to recovery:
  - Restore from backup.
  - Attempt to break the encryption.
  - 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 maximise total recovery.
- Be aware that these approaches are labour 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. Organisations 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 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 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.

Australian Sanctions Regime under DFAT:
Australian Sanction Laws require organisations to be compliant with United Nations Security Council (UNSC) and Australian autonomous Sanction Regimes. This can be applicable during a ransomware event because the attacker demanding the ransom may be on the list of sanctioned countries/entities.

Global Trade and Economic Sanctions:
OFAC and other global regulations are relevant to Australian organisations during a ransomware event because the attacker demanding the ransom may be on a Sanction list. Insurance companies can be sanctioned for violation of global sanctions including the European Union, United Kingdom and United States when paying ransoms even if the insured does not operate in those countries.

Secure Approval from the Board

- Obtain approval from the board of directors on policy documents. Recognise 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 jeopardise 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 centre 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 specialises 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, Australian Sanctions Regime 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 centre support.
  - Assist in managing other aspects of the incident that are not specific to ransomware, such as notifications and insurance claims.
  - Assist you to ensure that the appropriate parts of your response fall under legal 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 cyber counsel will also ensure compliance with NBD Scheme or other regulatory guidance related to ransomware payments. Remember that cryptocurrency exchanges charge fees for cryptocurrency purchases.

DURING THE INCIDENT

Minimise Exposure and Maximise Backup

- Isolate the ransomware infection by turning off servers and computers throughout the enterprise and disabling 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.
- Recognise 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 organisation'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 insurer may offer (such as cryptocurrency payments support).
- If you decide to pay the ransom, confirm with your insurer before making the payment. Many insurers require that they pre-approve in advance of a client making a ransom payment.

Follow Your Internal and External Guidance

- Follow the organisation'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 legal 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 defence service provider to perform an "indicators of compromise" assessment of the entire network. Find and eliminate any remaining malware or associated files or artefacts. 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 organisation 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.

Contact

For more informationplease contact your Marsh representative.

KELLY BUTLER
Cyber Practice Leader – Pacific
Marsh
+61 (03) 9603 2194
kelly.butler@marsh.com

About Marsh

Marsh is the world's leading insurance broker and risk advisor. With around 40,000 colleagues operating in more than 130 countries, Marsh serves commercial and individual clients with data-driven risk solutions and advisory services. Marsh is a business of Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people. With annual revenue over $17 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses: Marsh, Guy Carpenter, Mercer and Oliver Wyman. For more information, visit mmc.com, follow us on LinkedIn and Twitter or subscribe to BRINK.