A cover of a computer security

Description automatically generated

This document provides the Tabletop Leader Exercise Leader with a post-exercise discussion guide for the Ransomware scenario, using Worksheets #1 and #2.

The leader should ensure that any materials documenting the results or workplans are labeled with the appropriate security classification for the company (e.g., confidential, highly confidential).

| **Worksheet #1** | |
| --- | --- |
| **Section/**  ***Suggested Time Limit*** | **Questions for participants to address during the exercise** |
| Section 1  *10 minutes* | 1. Do employees know who to contact and what to do when they receive this message? 2. Does our company have a Cybersecurity Response Team? If not, who should be the Cybersecurity Response Team? 3. What should the Cybersecurity Response Team be doing? 4. Who should control the investigation, and what tools should they use? |
| **Section 1**  **Discussion Points** | Participants should discuss the steps that the Cybersecurity Response Team should take to identify, contain, eradicate, and recover from the ransomware attack. There should also be a clear delineation of responsibilities between team members and an employee tasked with documenting, in detail, each step the company takes in response to the attack.  In taking these steps, the investigation should be controlled by a leader that can be objective and has the authority to delegate and direct other company employees as part of the response. For example, IT security employees may want to defend their actions leading up to the attack. This may hinder the investigation. Therefore, it is advisable to have a neutral employee lead the investigation.  The tools used, including threat scanning, removal, and decryptor software, should create an auditable trail and should not modify or change any information that will be necessary for the forensic investigation. |
| Section 2  *15 minutes* | 1. What additional investigation should be done? 2. What should our protocol be for activating our Cybersecurity Response Team? 3. How should the Cybersecurity Response Team communicate with each other? 4. What are the next steps for determining the extent of the intrusion? 5. What external experts should be contacted and when? |
| **Section 2**  **Discussion Points** | The Cybersecurity Response Team should investigate the extent to which the company’s system has been compromised and do a full system scan for additional malware. The Cybersecurity Response Team should not assume that the hackers’ infiltration is limited to the systems immediately identified.  The Cybersecurity Response Team members should use oral or secure communication channels to ensure that the hackers are not monitoring the company’s communications as it addresses the attack.  The Cybersecurity Response Team should have a predetermined list of third-party cybersecurity experts, attorneys, and public relations specialists to assist it with addressing the attack. It is best to include these experts early in the process to guide the company through the event. The company’s cyber incident insurance policy may name the external experts or “Cyber Buddies” who should be used. |
| Section 3  *5 minutes* | 1. Who should negotiate with the hackers? |
| **Section 3**  **Discussion Points** | Although the company will control the negotiations, it is important that an expert in ransomware negotiations take the lead in communicating with the hackers. A company should not undertake these negotiations on its own, including making any payment to the hackers. |
| Section 4  *15 minutes* | 1. When do we notify customers, employees and third parties, what would we say, how would we notify them, and who takes the lead? 2. When do we notify law enforcement about the intrusion, who takes the lead and what information do we provide? 3. Does our company know who in law enforcement to contact? 4. Which regulators, if any, do we contact about the intrusion, who takes the lead, and what information do we provide? |
| **Section 4**  **Discussion Points** | The communication strategy should be discussed early, and an employee should serve as the central point of contact. Communications, both internal and external, should be consistent. The company should consider the scope and content of the communications based on who is impacted by the attack.  It is usually best to notify law enforcement as soon as practicable because they may have additional resources to assist with responding to the attack.  The company should already know what regulators to contact, the deadline for providing notification and what information must be provided. Legal counsel can advise on these issues, but it may be advisable to appoint an employee to be the central point of contact and ensure that all communications are consistent and factually accurate. |
| Section 5  *10 minutes* | 1. What processes should we have in place? 2. How does our company continue to conduct business? 3. What is our protocol for shutting off remote access? |
| **Section 5**  **Discussion Points** | The company should have a disaster recovery and business continuity plan that addresses how it responds to an attack. This should include access to databases, email systems and remote access. |
| Section 6  *15 minutes* | 1. What decisions do we need to make about using the backup system? 2. What steps should we take before using the system backup copy? 3. What should be communicated to our customers? 4. When, how, and who should send this communication? |
| **Section 6**  **Discussion Points** | The company should consider if using the backup system will be sufficient for business continuity. Before deploying any backup systems, they should be scanned for malware, including ransomware. It is often advisable to disable executable files in backup repositories.  If there is any impact to customers when the company deploys a backup system, such as temporary system unavailability, this should be communicated.  The company should also consider if the central point of contact or others will be available to answer customer questions and address any technical issues that customers may experience. The timing, form and content of the communications should be customized to fit the situation. |
| Section 7  *10 minutes* | 1. What should we say to our customers? 2. Are there guidelines for the relationship manager to follow? 3. How do we deal with multiple customer calls? |
| **Section 7**  **Discussion Points** | It may be best to keep customer communications concise, easy to understand and proactively address questions or concerns that are likely to be raised. The content of the communications should be consistent and not contain superfluous facts or speculation.  The company may use a template communication form, but the communications should be customized to fit the situation. Relationship managers should be provided guidance on what the company can and should disclose.  The company will want to make sure that its customer-facing employees understand where to direct customer calls and ensure that it has sufficient resources to handle these calls. For example, if an influx of customer calls is expected, the company’s call center should be appropriately staffed and that call center operators have guidelines on how to address customer concerns. |
| Section 8  *10 minutes* | 1. What should we consider before talking to the press? 2. Why should we have a central point of contact? |
| **Section 8**  **Discussion Points** | There are risks and benefits to talking to the press and a company should keep in mind that failing to respond to press inquiries may prevent the company from controlling the narrative and may encourage speculation.  The company should consider if it should utilize a public relations expert to craft external communications, including providing press releases. The company should also consider the impact that media coverage will have on customer relationships and if company statements will cause unnecessary concerns.  Communicating facts is often appropriate, but the level of detail provided will depend on the situation. In most case, it is best to keep media communications simple and jargon-free.  Finally, the company should keep in mind that whatever is said to the press will likely be received by the hackers and could impact negotiations. |
| Section 9  *10 minutes* | 1. How do we decide if we are going to pay the ransom? 2. Who should be involved in this decision? 3. Who should pay the ransom? |
| **Section 9**  **Discussion Points** | The determination on whether to pay the ransom will depend on the attack’s impact on the company’s system and other factors, such as if the hackers possess sensitive information that they will release to the public.  Although law enforcement may have a view on whether the company should pay the ransom, this is generally the company’s decision. OFAC sanctions may be a consideration and legal counsel will be able to help address this concern. In addition, an insurance carrier may have a viewpoint on if the payment is covered.  Any payment should be handled by a third-party expert in making ransom payments and not by the company directly. Experts can help track the payment and protect it from interception by other bad actors. |
| Section 10  *10 minutes* | 1. What needs to be done before our IT team restores remote access? 2. Going forward, what should we do with our system backup program? |
| **Section 10**  **Discussion Points** | The company should re-test its systems and scan employee devices before remote access is restored. This goes beyond testing the original source of the infection and should include all systems and devices potentially infected by the ransomware or other malware that may have been installed by the hackers.  The company should consider what lessons it learned from the attack, including if the frequency and scope of the system backup was sufficient for business continuity. In addition, the company should consider if backups should be proactively scanned for malware and kept on a removable storage medium, such as DAT tape. |
| Section 11  *10 minutes* | 1. What do we say to customers? 2. What other remedial steps should we take, and how should they be documented? 3. What do we say to the press? 4. How should we document the ransomware attack? |
| **Section 11**  **Discussion Points** | At the conclusion of the incident, the company should inform impacted customers of any remedial measures affecting them and be prepared to respond to customer questions and concerns. Although a detailed explanation is likely not necessary, it may be advisable to assure customers that the company has identified the extent of the attack and addressed any customer impact.  In addition to re-testing and scanning systems, the company should consider how it can improve its response in the event that another attack occurs. For example, the company may want to update its plan for responding to a cyber incident, including its law enforcement and external contacts.  In determining whether to talk to the press about the resolution of the attack, the company should consider if it will further damage the company’s reputation or be used by competitors in marketing. Any communications with the press should be consistent with previous statements and demonstrate that company handled the attack proficiently (if true).  It is advisable to draft a root cause analysis that can be used to protect against evolving threats. Often a root cause analysis can be useful in communicating with regulators and law enforcement and avoid a full-blown investigation. Some customers may also demand to know the root cause of the attack; this is a customer relationship management issue that should be addressed.  It is important to separately document the ransomware attack and the company’s response in detail, including remedial measures to further secure the company’s systems. The company should ensure that this document remains confidential because it can identify vulnerabilities that could be exploited before they are addressed. Any documentation, including the root cause analysis, should not assign blame for the attack and should be reviewed by legal counsel. |

This worksheet is for participants to log any observations or capture other notes during the exercise that will be discussed following the completion of the exercise.

|  |  |
| --- | --- |
|  | **Worksheet #2** |
| **Section** | **Participant observations during the tabletop exercise** |
| **Discussion Points** | Incorporate any participant observations in the post-scenario evaluation. |

**Payments Innovation Alliance – Cybersecurity Response Project Team**

The Payments Innovation Alliance is a membership program that shapes the future of the payments industry and develops thought leadership relevant to financial service institutions.   
The Alliance established the Cybersecurity Response Project Team to help organizations understand evolving threats related to potential cyber attacks.

A green card with a lock and numbers

Description automatically generatedThese resources may be downloaded and shared with employees, colleagues, and clients as appropriate. If you’d like more information on the Payments Innovation Alliance, including the work we have done and how your organization can get involved, please visit nacha.org/payments-innovation-alliance.