A cover of a computer workbook

Description automatically generated

This workbook is for participants to use during the ransomware tabletop exercise and can be customized by your organization.

* The exercise leader will reveal the scenario facts for each section.
* Participants will write their responses to each question using Worksheet #1.
* Participants should stay within their role during the tabletop exercise.
* Participants may have observations during the exercise that should be logged using Worksheet #2.
* Discussions about the exercise will be conducted after the scenario has been completed.

**Participant Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_**

**Participant Role: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

The ransomware scenario should take 2-3 hours to complete. Refer to the suggested time limit for each section.

| **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 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. Which external experts should be contacted and when? |
| Section 3  *5 minutes* | 1. Who should negotiate with 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 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 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 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 8  *10 minutes* | 1. What should we consider before talking to the press? 2. Why should we have a central point of contact? |
| 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 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 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? |

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** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**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 cyberattacks.

These 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.

A close-up of a blue background

Description automatically generated