Cyber Exercise Table Top Exercise

Instructions: This workshop is to identify gaps in current policies and plans related to cyber incidents. It is understood that some portions of the scenario details may be general and responses different than your organization takes, the goal is NOT to fight the scenario, but to identify what may be missing from critical policies and plans. Remember to work through the stated issues as led by the facilitator and apply your organization's policies and plans as best as possible to list areas for improvement and create a Corrective Action Plan to improve your organization's cyber resilience. The back of the pages are intentionally left blank to allow space for you to write any notes or brain dumps.

Scenario:

It's a new year – 2020! Your organization is starting the year off right by ensuring your employees haven't forgotten risks associated with phish email tactics over the holiday season by pushing out an email phishing test with different scenarios across all of your employees on January 6 through January 10. Employees seem to still be on holiday time as there is a higher percentage of employees falling for the tests coming in at 9%. Typically, your organization holds an approximate 3% click rate. Those who have fallen for the test are presented with education addressing only phishing email tactics through your organization's tool of choice. During this time, some employees are reporting multiple suspected phish emails - some are the test emails your organization deployed; however, 2 versions of emails that have been reported are legitimate phishes and one includes an attachment titled "PAST DUE - invoice attached" and the other phish includes a link requesting network username/password masked as need for password resets.

Fill out the following table based on what's been presented up to this point:

What existing policy(ies) and plans does this situation apply to?	What actions are being taken at this point?	At what point would this situation escalate to an incident?	What teams are involved and at what level?	How are teams informed of the situation?	What teams should you consider to be contacted?

Are there policies and plans that are missing? Yes/No

Has it been over a year since any of the documented plans were reviewed, updated, and/or exercised? Yes/No

Are any teams identified in the table above missing from documented plans mentioned? Yes/No

Is contact information for individuals on response teams included in the plans? Yes/No

Facilitator Questions:

- How are users reporting suspected phishing attempts?
- Is user training a help or a hinderance?
- What teams are involved to identify which ones are real phishes?
- How is this being communicated to the teams that need to be involved?
- How are those teams extracting the real phish emails from email servers?
- How are those teams monitoring any activity that may have been initiated by the real phishes?
- Which teams are involved with this monitoring and blocking of traffic?
- How much time do these activities take from start to finish?
- Are phishes being shared with community organizations such as the Department of Homeland Security (https://www.us-cert.gov/report-phishing)?

Scenario Continued:

During this time, your organization's spam filters are also reporting that employees are receiving an 25 % increase above normal spam levels. Many of these emails are bypassing spam filters. The IP addresses Domain Names, IP addresses, and IP ranges are being blocked as these are identified.

On January 14 at 4pm, EMPLOYEE A from Accounting, contacts your organization's service desk to follow-up on calls previously made from "service desk personnel" about "fixing" unusual traffic from their computers. The service desk cannot find any record or tickets assigned to this employee or the situation reported by the employee. The employee attempts to explain that the "service desk person" remoted into the employee's computer to perform the "fix" and since that time, the computer has been running unusually slow. This "fix" occurred on January 6. The service desk technician taking the call remotes into the computer and sees Microsoft Word and Excel running using a slightly larger CPU percentage, but

nothing alarming. The service desk technician closes the instances Microsoft Word and Excel in Task Manager and reboots the users' systems expecting the slow performance issue to be resolved and closes the ticket.

On January 16 at 9am, EMPLOYEE B from HR, contacts the service desk and reports the same situation as reported by EMPLOYEE A. A different service desk person takes the call, creates a ticket, and closes the ticket after closing the Microsoft Office process as did the first service desk member.

Fill out the following table based on what's been presented up to this point:

What existing policy(ies) and plans does this situation apply to?	What actions are being taken at this point?	At what point would this situation escalate to an incident?	What teams are involved and at what level?	How are teams informed of the situation?	What teams should you consider to be contacted?

Are there policies and plans that are missing? Yes/No

Has it been over a year since any of the documented plans were reviewed, updated, and/or exercised? Yes/No

Are there teams documented in the table above that are missing in documented plans mentioned? Yes/No

Is contact information for individuals on response teams included plans? Yes/No

Facilitator Questions:

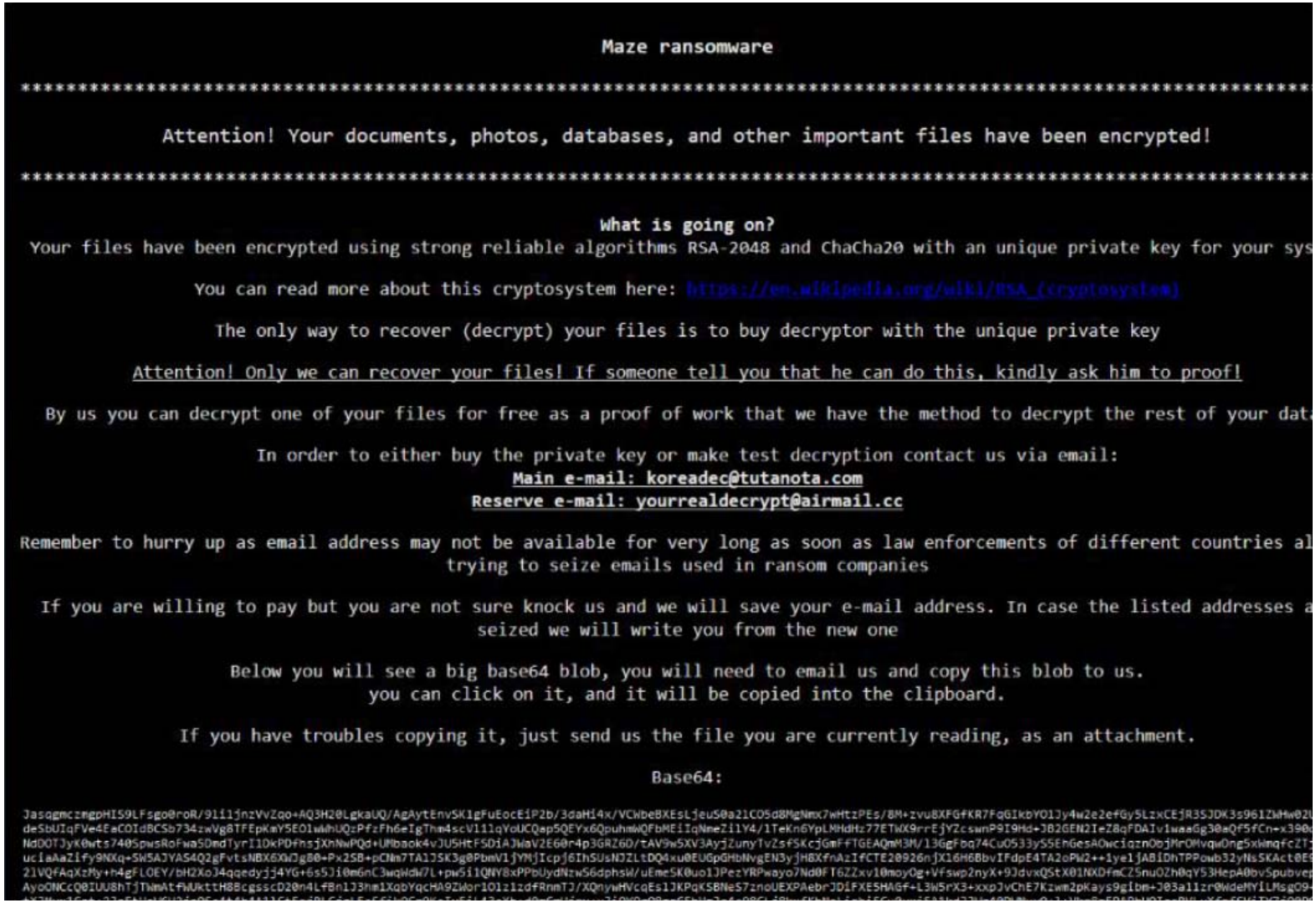
- How is this second ticket associated with the previous ticket?
- Is there a way to search for this issue being reported by multiple employees with the ability to tie the two together?
- Would the Service Desk communicate this activity to any other teams?
- If so, which teams and by what method does the communication occur?
- How do users report possible Social Engineering attempts? Are employees trained to recognize Social Engineering?

Scenario Continued. Two variations –

For 24/7 industries: On January 20, 24-hour employees' screens flash to a ransomware message at 12:01am and countdown timer that shows 72 hours remain before all data will be erased unless 100 bitcoin is received.

For Mon thru Fri industries: When employees report to work on January 21 after the MLK holiday and turn on/login to their computers, they are presented with a ransomware message and countdown timer that show 40 hours remain before all data will be erased unless 100 bitcoin is received.

The following ransomware message is seen:



*Note: Ransomware examples and screenshots taken from NCFTA Maze Ransomware Whitepaper, 2019

Fill out the following table based on what's been presented up to this point:

What existing policy(ies) and plans does this situation apply to?	What actions are being taken at this point?	At what point would this situation escalate to an incident?	What teams are involved and at what level?	How are teams informed of the situation?	What teams should you consider to be contacted?

Are there policies and plans that are missing? Yes/No

Has it been over a year since any of the documented plans were reviewed, updated, and/or exercised? Yes/No

Are there teams documented in the table above that are missing in documented plans mentioned? Yes/No

Is contact information for individuals on response teams included plans? Yes/No

Facilitator Questions:

- Based on your organization's functions, what partners, customers, and other stakeholders are impacted?
- What processes are impacted? What recovery plans do you have?
- What teams support those recovery processes?
- What is the process for activation?
- What plan includes this information?
- What are your data recovery priorities?

- What is the Recovery Time Objective (RTO) for the most critical processes?
- What data is lost based on the Recovery Point Objective (RPO)?
- What communications are developed, who is it distributed to, and how is it distributed?
- What communications team members are included in your incident response plan?
- What legal team members are included in your incident response plan? What other contacts would you make in your industry about this situation?

Definitions:

RTO – The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business processes. (https://csrc.nist.gov/glossary/term/Recovery-Time-Objective)

RPO - The point in time to which data must be recovered after an outage. (https://csrc.nist.gov/glossary/term/Recovery-Point-Objective); additionally, RPO points directly to how organizations backup there data over time (risk and policy – i.e. how often are backups completed, are they full/incremental/differential, are backups store offsite, has restoral been tested?).

Corrective Actions Plan

Instructions: Review the questions that you answered yes to after each section. This indicates there may be gaps in the ability to identify cyber incidents and quickly respond once an incident occurs. For those questions that were answered yes, fill out the following table, which will list the items that need to be corrected to improve your organization's cyber preparedness. Any gaps in this table should be discussed within your organization after the workshop to ensure it is completely filled out and responsible parties are assigned to those activities that you list.

List policy(ies)/plans your org need to create or update	List teams and individuals that need to be documented in those plans	Team(s) primarily responsible for coordinating effort	Team Point of Contact	Expected start date	Expected end date

***IMPORTANT NOTE:** The ransomware and events used in this workshop are realistic and each day we hear about new attacks on organizations and government entities. This workshop was designed to perform a quick scenario-based exercise to think through and document activities that you expect would occur within your organization during a real incident. It is imperative that what was discovered during this activity is shared within your organization AND the corrective actions documented are performed to improve your organization's cyber preparedness.

Thank you for participating in the exercise!

Resources

Business Email Compromise (BEC) - https://www.cisecurity.org/?s=business+email+compromise

Center for Internet Security – https://www.cisecurity.org/isac/

Delaware DigiKnow Website – https://digiknow.dti.delaware.gov/

Emotet Ransomware - https://www.cisecurity.org/white-papers/ms-isac-security-primer-emotet/

NIST Computer Security Resource Center - https://csrc.nist.gov/publications

Out of Date Software List - https://www.cisecurity.org/blog/end-of-support-software-report-list-2/

Report Scams –

- FBI complaint form - https://bec.ic3.gov/
- IRS resources: https://www.irs.gov/privacy-disclosure/report-phishing
- MS-ISAC email (for government agencies only): soc@msisac.org

Top Malware Types - https://www.cisecurity.org/?s=top+malware

Training Topics and Resources - https://www.cisecurity.org/?s=training