Tabletop Exercise: Ransomware Attack Response

Critical Success Factors
Dealing with a Ransomware Attack

- **Reduction** – reduce risk through preparation
- **Response** – to the ransomware attack
- **Recover** – technology and business environments affected by the attack
- **Resumption** – restart business activities following the attack
- **Restoration** – business systems and files returned to normal
- **After-Action Report** – What worked, what didn't work, what can prevent another attack

Purpose of the Tabletop Exercise

- Walk through the ransomware response plan
- Verify the plan is adequate for a ransomware attack scenario
- Develop an after-action report on how well your plan worked and changes that can be made

Objectives and Scope

- Validate that ransomware response procedures will work.
- Confirm communication processes upon learning pf the attack.
- Verify that anti-malware software (including ransomware) works properly
- Verify that essential systems, applications, files, databases and other resources are protected.
- Team members understand their roles and tasks.
- Document plan gaps and shortfalls.
- Scope is <name of location(s)>

Exercise Format

- Present a "control message" about each situation to participants
- Exercise participants will discuss how to respond based on the ransomware plan
  - *Are the responses appropriate?*
  - *Is that what people will actually do?*
  - *Can the attack be mitigated?*
  - *Is the ransomware software sufficient to the task?*
- There are no wrong answers

Exercise Format

- Control messages are presented to continue the discussion
- If it is necessary to limit discussion to keep on time, open issues will go to a "parking lot"
- Open issues and challenges will be noted for the post-exercise debrief and after-action report.
- At the end, the closing debrief discussion should emphasize how well the attack was handled and the usefulness of the ransomware plan.

The Scenario

- Normal day at the office
- No unusual activities occurring in IT and the company’s network

First Signs of Trouble

- Employees call into the help desk reporting they are unable to access certain systems
- Alarms from firewalls and intrusion prevention system (IPS) begins sounding

  - **Who in your department would receive information on the situation, and from whom?**
  - **What actions do you take initially?**
  - **What actions does this trigger in your cybersecurity plan, if any?**

Second Wave of Problems

- Employees report they are unable to access files and databases, saying a code is needed to access them
  - **What is your response?**
  - **How do you communicate to your department staff? Senior management?**
  - **How many contact numbers or methods are you prepared to use?**
  - **Are they in the ransomware plan and are they accessible?**

Ransomware is Suspected

- IT staff alerts senior IT management of a suspected ransomware attack

  - **What do you tell employees?**
  - **Who communicates the message?**
  - **A disaster has not yet been declared**
  - **Would you choose to activate your ransomware plan? Your BC plan?**
  - **Who will decide to activate or not activate the ransomware response plan?**

IT Loses Access

- IT staff examines various systems and determines that access to them has been blocked, notifies senior IT leadership
  - **Is the time near where you must decide to activate your ransomware plan?**
  - **What is your RTO? How fast do you need to recover from the attack? What do you do?**
  - **Who has the authority to declare a disaster in such a situation?**

Issues Spread

- Employees and senior management are increasingly unable to access systems and files
  - **Who makes the above determination?**
  - **Who on the IT team receives that information and how?**
  - **What happens next?**

Culprit is Determined

- Senior leaders inquire of their teams and determine that the attack is causing operational problems; share this information with IT

  - **When does the cybersecurity team meet to make decisions regarding the situation? Where?**

  - **What happens next?**

Shutdown?

- Senior leaders meet to determine if the company needs to shut down until the ransomware issue is fixed

  - **How does this happen?**
  - **Will employees be working remotely?**
  - **Who should be contact outside the company on this decision?**

Remote Employees Affected

- Employees notify the help desk that they are unable to login remotely
  - **What is being done to address this?**
  - **Who is responsible?**

No Improvements

- Employees and senior management still report they are unable to access systems and files

  - **What happens next?**
  - **Who communicates with employees on status?**

Enact Recovery Plan

- Senior management instructs IT to recover damaged system, files and other assets from backup copies

  - **Where are employees working? Alternate site? Home?**
  - **Do you have access to the backed-up IT resources you need?**
  - **What other resources do you need?**
  - **What have you been communicating to your board, your customers and stakeholders regarding the event?**

Light at the End of the Tunnel

- Employees begin reporting they are able to access their systems and files

  - **How well are employees managing?**
  - **Are technology resources functioning properly?**
  - **Who determines that all key functions are resumed?**

Recovery successful!

- IT sends notification to all employees that systems have been successfully recovered

  - **Who updates senior management of the recovery?**
  - **What follow-ups do you make to internal and external contacts?**

After-Action Debrief

- What worked; what didn’t work?
- How well did the ransomware software work?
- Were critical business system, files and processes recovered?
- Did the ransomware plan perform as needed?
- Does the ransomware plan, as exercised, ensure continuity of the company’s systems?
- What needs to be done to update the company’s cybersecurity plans?

Questions and Comments?