**Workshop / Tabletop**

**Objectives**

The goal of this scenario is to identify where the business is in terms of preparation and the teams understanding of processes and procedures in regards to a cyber incident and incident recovery and response. This workshop will help validate an existing incident response and recovery plan, or it will help a business identify that they need to update or create one. The scenario will be graded depending on the circumstance and responses of the organization to the facilitator and the output will identify how well prepared the team is to handle a cyber incident.

* Identify the response procedures of the business and what the company believes they are
* Validate communication between teams including escalation processes
* Understand roles & responsibilities
* Identify gaps in understanding and experience

**Facilitator**

The goal of the facilitator is to walk through enough issues to identify if they are holistically prepared for the 5 domains of cyber prevention, preparation, response, detection and mitigation.

* 1st have a lot of fun and create a great environment for the organization to feel comfortable.
* Present the scenario to the team
* Define the criteria of the scenario and scope
* Have the organization fill in the variables and objects for the tabletop
* Present control messages to continue advancing the scenario
* Keep time and ensure additional ideas are retained to be reviewed later
* The mistakes will not be pointed out during the workshop, they will be identified as gaps if comments are retained on the workshop board or in the notes.
* Mistakes the organization makes can be used to bring up a new direction of control messages and dig into their lack of preparation.

**Workshop Format**

* Is this what the person would actually do?
* Can it be mitigated?
* Is the response helpful to the business objectives?
  + retain relevance to scenario and control messaging

**Adversary**

* We will use a different adversary every quarter or two to remain updated,
* Use the adversary data that is in the ransomware module, one of the adversaries and their MO will be used as context for the scenario. This data will be filled out in the Miro board under "Adversary"

**Context**

**Questions**

**Detection**

* Who identified it?
* Type of indicator (Our scenarios will be ransomware, phishing, insider threat)
* What details do they record?
  + Who identified it first?
  + What is the time of date of contact?
  + What is the time and date of the incident occurring? start and end
  + What system is affected?
    - Name
    - IP address
    - Location
* Does your team receive alerts for this event?
  + What security software your organization uses would be capable of detecting and reporting this?

Analysis

**Technical**

* Which critical system (name / IP)
* How many systems get attacked (% of business 15-100%)
* How did they identify it? (ransomware note)
* Calculating the severity of the attack
* Tools and software that can help prevent or mitigate attacks (The company actually uses, not theory)

**Management**

* Escalation process?
* Meeting management?
* Line of sight?
* Calculating the business impact
* calculating severity

**Executives**

* What information will convince the execs it is time to reach out to legal counsel for advice?
* What type of scenario will be severe enough for the execs to make an insurance claim:?
* Calculating the downtime and business interruption, and the costs
* Will the executives reach out to the regulatory authority regarding data loss? (For businesses that have sensitive or personal identifiable data)

**Scenario #1**

**Friday Nov 28, 2022 @ 4pm**

A ransomware attack is identified on your network. Multiple users called in distress to explain they cannot open files. There is a text file inside of every folder and when opened it describes that a ransomware attack took place, all of the files have been encrypted. There is a crypto address and they request 40 bitcoin for a program that will decrypt all of the files.

We want to answer the questions, but we also want to guide the scenario with the control messages.

The following section includes the control messages separated with multiple questions included under each one.

**Control Message**

**[1 - Detection] Because of multiple reports from staff members you are quite certain your company is facing a ransomware attack and as you begin to grasp what is happening you continue to receive phone calls of infected computers. As you speak with each individual who is calling in**

Evidence needs to be collected

Staff using infected devices needs to stop using the devices

Devices need to be disconnected from the networks or the networks need to be shut down to stop further infection of other devices

Need to identify who is reporting the infected devices and when

Identify which devices have been infected

**[1] What do you instruct the staff to do?**

1. Take a picture of the ransomware note with their cellphone and send it to you
   1. How do you ask them to send you the picture? is it through corporate email, text or cloud storage?
2. Do not tamper with the device or use the device in any way
   1. Do not attempt to uninstall software
   2. Do not attempt to disable antivirus or connect external drives to obtain files from backups
3. Disconnect the device from a physical network?
4. Do you ask them to power off the device?

**[2] What do you do?**

1. Identify which devices have been infected so far
2. Identify what type of ransomware has infected these devices
3. Record evidence
   1. Date / time of each communication, who you spoke with and the device they identified as compromised
   2. Date / time of the initial incident
   3. Details about the system (name, IP address)

1. Identify if it is spreading across a network to multiple devices?
2. Do you decide to shut down the network (switches, internet access, firewall)
   1. Computers cannot communicate with one another
   2. Computers cannot communicate with the servers
   3. Computer cannot communicate with the internet
3. Do you disconnect servers from the network to protect them or isolate them?

**Result**

* What is infected
* What is it infected with
* Evidence
* Stop staff from using infected devices and accidentally tampering with evidence
* Stop further spread if possible

------------

**[2 - Assessment] Your organization is in the middle of a ransomware attack, there have been multiple reports of infected devices and the symptoms are the same. You need to make a quick assessment to determine the severity and scope of impact.**

Who is responsible for analyzing the initial attack?

What type of ransomware is it?

How are they contacted? Do the teams know who to contact?

Severity needs to be determined before response teams can be activated

An initial scope of the impact should be determined to communicate to the senior management

**[1] What do you do next?**

1. [Scope of Impact] How do you identify what type of ransomware is being used? The adversary MO can be identified, including the TTPS they use.
   1. Ransomware changes filenames postfix and leaves a note
2. [Scope of Impact] How do you identify what types of data exist on the infected devices, file shares, and other systems they are connected to?
   1. Do you look up in the asset inventory to identify the data types and data sensitivity?
   2. Do you look up architecture diagrams to identify other devices on the network that these devices had access to?
3. [Priority of Infected Systems] Do you create a priority list of critical to low systems that are infected and could be infected based on the types of data and asset value?
4. [Classification of Incident Severity] How do you determine the initial severity of the incident
   1. This classification will define which teams internally need to be contacted.

Result

* Identify more information on the ransomware and the adversary gang
* Identify the scope of impact, what assets have been compromised, which assets are potentially at risk
* Priority of critical to low based on the known infected systems and potentially infected systems
* Classify the severity of the incident. Sev-1 Sev-2 Sev-3 Sev-4?

------------

## [3 - Management] The quick assessment has been completed, and the initial assessment personnel has an estimated impact and severity, it is time to include the senior management into the conversation. While speaking with the senior leadership the corporate email server stops working, you have no more access to corporate emails.

Incident response or incident recovery plan

* Does your organization have an incident response or incident recovery plan (disaster recovery could work)
* Who is responsible for managing these plans

----- [rewrite these questions]-----

What level of leadership/management would be notified at this point in the scenario? Is there a plan in place detailing the thresholds at which different notifications are made and what information is provided?

What is your department or agency’s primary concern? Mitigation of the incident (resolving the issue) or investigation (preserving the evidence to build a criminal case)? Who would make this decision? Are these mutually exclusive?

What response actions would your organization have taken at this point? Are these actions driven by a plan?

----- [rewrite these questions]-----

Resources

* What capability and resources are required for dealing with this cyber incident
  + Internal resources
  + External resources
* Which team or individual is responsible for handling cyber incidents at your company?
* What are the roles and responsibilities for cyber incident response?
* When are the incident response teams activated?
  + At what point do you activate the internal teams?
  + At what point do you activate the external teams?
    - What thresholds are necessary to be breached before making these decisions?
* Do you have a third-party IT or Cyber security firm to support your emergencies?
  + Are they on retainer to guarantee availability or are the requests ad-hoc?

Potential impact estimations

* How will you estimate the financial costs of the cyber incident?
  + What are examples of things the organization would pay for?
    - Fines / Penalties
    - Business Interruption
    - Wages
    - Rent
    - Bills
* Business interruption
  + How would this affect the company
    - For 1 week of recovery
    - For 3 weeks of recovery
* Projects, manufacturing, services that could go down?
  + SLA's, contracts, client issues

Who do you contact internally

* Contact internal stakeholders and all teams who could be impacted, in addition to teams who would support the IR efforts.
* When do you escalate this to the senior executive team?
* Is there a procedure for communicating with the team in case of cyber incidents?

What do you say to your employees?

* Who communicates the message and how?
* How do you contact your employees, the email server is down. Do you have a contact list stored somewhere safe?

Setting up touch point meetings with the teams

* Ensure the teams at the ground level are in constant communication with the senior management and executives during the rough part of the incident.
* How often do you hold touch point meetings?

Secure Communications Procedure

* How are lines of communication opened between the teams?
* Using encrypted chats
* Stay off potentially compromised chats like emails or teams/slack if it could be compromised due to the severity.
  + Sev-1 Cyber Incident it would be assumed all corporate chats are unsafe to use

### Result

* Obtain the existing IR plan and who is the owner of maintaining it
* Manage resources, meetings
* Estimate the impact to the operations, finances
* Identify who needs to be contacted internally IE existing stakeholders
* Secure communication procedure

------------

## [4 - Analysis] The executive team has requested additional information on the cyber incident. There are concerns that the adversary continues to be operational inside the corporate network and additional devices could be compromised that remain unknown.

Will investigation and digital forensics be conducted on the device or service?

Which team / individual preforms the incident analysis?

* Do you contact them directly or do you inform your supervisor or management and they deal with it?

What resources are required for incident investigation and attribution?

* Who will conduct the digital forensics? internal, external?
* Is an external cyber security firm on retainer?

What capabilities do internal resources have for digital forensics?

Is there a process for preserving evidence during the investigation?

* What resources are used for evidence preservation?

### [4.1 Internal Analysis] While you wait for the cyber security team to be contacted your IT department starts a bit of an initial investigation.

Can your team determine if the incident is in still in progress?

* How?

Can this incident be contained?

* It continues to spread, losing access to more systems and services.

Does the response need to be escalated?

* Do the Incident response teams need to be activated?

Results

* Understand internal capabilities
* Identify available trained resources
* Processes they have for digital forensic analysis
* Identify if the incident is in progress
* Can it be contained
* Escalation procedures

---------------

## [5 - Management] The IT team has lost access to critical servers, some of their machines are infected, encrypted and unusable. Management and other teams are increasingly unable to access systems and files.

What happens next?

Is this incident serious enough to shut down the company until this is fixed?

* What criteria would have to be met for leadership to shut down the business and focus all efforts on recovery containment, eradication and recovery?
* Who makes this decision?

### [Corporate Concerns]

#### Brand and reputation

* If data is exfiltrated and leaked how would that affect your business
* If there is. you are sued?
* If you are fined for lack of compliance with a regulatory authority

#### Public Notifications

* Who is responsible for communicating with the impacted clients? (Partners, investors, board members)

#### How do you handle media?

* Do you have pre-written statements?
* Is a staff member trained in public relations?
  + Do you have or would you use a brand and reputation firm to assist in relaying the correct messaging to the public?

#### Personal Identifiable Data is stolen

* Does this change the public communications?
* Would this trigger legal or regulatory notifications?

-----------------

## [6 - Recovery] The incident looks serious and all efforts to contain the infection have faltered. The realization that business operations will be interrupted, corporate leadership wants to recover the business as quick as possible

Do you have backups, and are they usable?

* Who is responsible for backups and recovery?
* Do you verify backups function periodically by testing recovery?
* How often?

Is the data worth recovering?

Is it worth paying the ransom?

Are there additional devices available that would not have been infected that could be used to begin clean up and recovery?

-----------------

## [7 - Cyber Security Prevention]

This is what we know so far….. This is where we are, this is what management has decided.

Can you detect normal / abnormal network traffic or device usage?

* What capabilities does your organization have? (EDR, Logging?)
* What could have alerted this?

1. Discuss the difference between network and host forensics. How are you equipped and staffed to address this?
2. Do you have a network operations center? Security operations center? What are their roles during a response?

1. What type of hardware and/or software does your organization use to detect/prevent malicious activity of unknown origin on your systems/network?

What could have been used to help prevent this?

Tools / Software the company uses that could mitigate the attacks

* What controls should have stopped the attack?
* How do you figure out why they didn’t?
* How can you review the encrypted devices for forensic evidence?