Tabletop Exercise (TTX) – County Ransomware Incident

Situation Manual

November 2022

This Situation Manual (SitMan) provides exercise participants with all the necessary tools for their roles in the exercise. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Tabletop Exercise (TTX) - Cyber |
| **Exercise Dates** | DATE Month/Day/Year |
| **Scope** | This exercise is a tabletop exercise. |
| **Mission Area(s)** | Prevention, Protection, Mitigation, Response & Recovery |
| **Core Capabilities** | Planning, Public Information and Warning, Operational Coordination |
| **Objectives** | This TTX was written with six (6) SMART objectives listed. Choosing which objectives, you as the sponsoring agency have the responsibility of picking which objectives better fit your agency’s needs. As a discussion-based exercise, participating agencies discuss practicing group problem solving, familiarizing senior officials with a situation, conducting a specific case study, examining personnel contingencies, testing group message interpretation, participating in information sharing and assessing interagency coordination. |
| **Threat or Hazard** | Cyber |
| **Scenario** | A cybercriminal has infiltrated your organization; it began with phishing and escalated to ransomware. |
| **Sponsor** | FEMA – EMI/PEMA/Your Agency |
| **Participating Organizations** | Federal, state, tribal or local levels of government agencies while utilizing the whole community approach of including applicable representative organizations (such as private sector partners, voluntary agencies, school districts, etc.) within each jurisdiction. |
| **Point of Contact** | Your InformationGeneral Inquires: Kamie Hughes: PEMA: kamhughes@pa.gov |

# General Information

## Exercise Objectives and Core Capabilities

The following exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to core capabilities, which are distinct critical elements necessary to achieve the specific mission area(s). The objectives and aligned core capabilities are guided by elected and appointed officials and selected by the Exercise Planning Team.

| Exercise Objective | Core Capability |
| --- | --- |
| Increase senior county official’s awareness of cybersecurity risk management, cyber incident response planning, and other issues related to cyber incident prevention, protection, response, and recovery of critical systems. | Planning, Public Information and Warning, Operational Coordination  |
| Examine cybersecurity information sharing, escalation criteria, and related courses of action. | Planning, Public Information and Warning, Operational Coordination  |
| Examine cybersecurity incident management structures and processes. | Planning, Public Information and Warning, Operational Coordination |
| Review cyber resource requests and management processes. | Planning, Public Information and Warning, Operational Coordination |
| Increase awareness of cybersecurity efforts and capabilities. | Planning, Public Information and Warning, Operational Coordination |
| Identify cascading impacts of cyber incidents | Planning, Public Information and Warning, Operational Coordination |

Table 1. Exercise Objectives and Associated Core Capabilities

## Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

* **Players.** Players are personnel who have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
* **Observers.** Observers do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
* **Facilitators.** Facilitators provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members also may assist with facilitation as subject matter experts (SMEs) during the exercise.
* **Evaluators.** Evaluators are assigned to observe and document certain objectives during the exercise. Their primary role is to document player discussions, including how and if those discussions conform to plans, polices, and procedures.

**Exercise Preparation:** *What is needed to get the most value out of this exercise?*

Review provided exercise objectives and add additional objectives that the county wishes to demonstrate.

Develop any additional discussion questions that are relevant to the objectives of the exercise. While there are discussion questions included after each inject, you may develop additional questions to meet your identified objectives.

Cut and paste the exercise injects and discussion questions into a PowerPoint presentation for display to participants during the tabletop exercise.

Invited participants can include but are not limited to personnel from the county emergency management agency, 9-1-1 dispatch center, county Information Technology (IT) department, emergency medical services, local law enforcement agencies, and other public and private sector emergency management and cybersecurity stakeholders.

Participation by a member(s) of the county information technology (IT) team is strongly encouraged to get the most value out of this exercise. The exercise is designed to consistently engage all recommended participants throughout the exercise.

Identify an individual to present injects and solicit participant responses to the discussion questions.

Assign one or two recorders to document participant-identified best practices, and organizational strengthens and weaknesses to facilitate completion of an after-action report and corrective action plan.

Register participants and make up tent card displaying the participant’s name, title and organization.

During the exercise, tent cards should be placed in front of participants facing the exercise facilitator to allow for identification of participants and job responsibilities. The facilitator does not need an IT background to help conduct this exercise.

## Exercise Guidelines

* This exercise will be held in an open, low-stress, no-fault environment. Varying viewpoints, even disagreements, are expected.
* Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
* Decisions are not precedent setting and may not reflect your organization’s final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.

Issue identification is not as valuable as suggestions and recommended actions that could improve prevention/protection/mitigation/response/recovery efforts. Problem-solving efforts should be the focus.

## Exercise Assumptions and Artificialities

In any exercise, assumptions and artificialities may be necessary to complete play in the time allotted and/or account for logistical limitations. Exercise participants should accept that assumptions and artificialities are inherent in any exercise and should not allow these considerations to negatively impact their participation. During this exercise, the following apply:

* The exercise is conducted in a no-fault learning environment wherein capabilities, plans, systems, and processes will be evaluated.]
* The exercise scenario is plausible, and events occur as they are presented.
* All players receive information at the same time.

## Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned capabilities, capability targets, and critical tasks, which are documented in Exercise Evaluation Guides (EEGs). Evaluators have EEGs for each of their assigned areas. Additionally, players will be asked to complete participant feedback forms. These documents, coupled with facilitator observations and notes, will be used to evaluate the exercise, and compile the After-Action Report (AAR).

# BACKGROUND

**Phishing**

What is Phishing?

Phishing attacks attempt to steal sensitive information through emails, websites, text messages, or other forms of electronic communication that often look to be official communications from legitimate companies or individuals.

These emails often impersonate mail from a trusted or easily recognizable source and requests the recipient to verify some data point by clicking a link or opening an attachment. Some phishing attacks also have boxes where the recipient needs to enter their username and password to access the link or file.

Once the link or attachment is opened, malware is loaded on the device, and the system is compromised. Compromised credentials are used to gain system access.

**Ransomware**

What is Ransomware?

Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by visiting an infected website.

Ransomware typically encrypts files and folders or in some cases, the entire hard drive, preventing access to important files. Ransomware attempts to extort money from victims, often in the form of cryptocurrencies, in exchange for the decryption key.

Ransomware is one of the most lucrative revenue channels for cybercriminals, so malware authors continually improve their malware code to better target enterprise environments.

**Module 1: Phishing**

**Inject 1 - Tuesday, November xx, - 9:15 a.m.**

An ABC County employee, Jane, who works in the County Treasurer’s Office is responsible for processing all license requests and transactions (marriage, hunting, dog, fishing, etc.) as well as reporting and inputting licensing transactions to the finance department.

She begins her workday by catching up on her daily emails and opens an email from Human Resources (HR) directing her to review and update her beneficiary information. The email states that her medical beneficiary information needs immediately reviewed for accuracy “To ensure employee’s spouse/partner and dependent information is correct to ensure timely payment of medical expenses.”

A link to beneficiary information is provided with a caption stating, “Please review and update your medical insurance beneficiary information.”

Jane does not want anything impacting payment of her family’s medical expenses, so she clicks the link. A message appears saying she needs to authenticate her identity by entering her username and password in the below boxes. She enters both and sees a spinning blue circle for several seconds, followed by this message: SERVER ERROR: The server encountered an error and could not complete your request at this time. If the problem persists, please try again.

Jane shrugs and mutters “I guess I’ll try later when they fix it” and returns to the rest of her e-mails.

**Discussion**

*Do county employees recognize suspicious cyber activity?*

* Do employees know what constitutes suspicious cybersecurity activities or incidents?
	+ Do they know what actions to take when one arises?
	+ What established processes exist for employees to report cybersecurity incidents?
	+ Does the county have a Cyber Incident Response Plan and are employees trained on it?
* Does the county have a procedure for reporting suspicious emails?
* Does the county conduct regular phishing awareness training?

**Inject 2 - Wednesday, November xx, 2022 - 11:15 a.m.**

After getting caught up with some of her work, Jane begins to think about the earlier e-mail from HR. She tries again to access her medical beneficiary information, but she gets the same SERVER ERROR message.

She calls HR to see if they can help her confirm her beneficiary information. HR said, “that’s weird…we’ve received a couple of these calls yesterday and today asking about these emails.” They tell her that they did not know why employees are being asked to verify their beneficiary information but would be happy to help her.

HR is starting to get frustrated with these unexpected calls, but it is not taking that long to help these employees. In fact, they have found a couple of instances where employee’s beneficiary information needed updated.

**Wednesday, November xx, 2022 – 1:00 p.m.**

Jane returns from lunch and begins inputting the licensing financial data to the finance department in preparation for the upcoming county budget meeting. She is having trouble accessing some of her usual financial databases and continues to get errors when she tries to process the financial data.

She figures it was just her computer acting up, so she logs in with her credentials on another employee’s computer and completes her work. When she finishes, she goes back to her computer to work on license requests.

Jane has both administrative and elevated access privileges, which IT had to give her to access all the various systems and data she needs to complete her financial reporting.

**Discussion**

*How does the county handle providing elevated privileges to users?*

* Do employees only have the level of access on the network required to do their assigned job(s)?
* Are user account privileges monitored regularly and adjusted if an employee changes jobs or departments and no longer requires elevated privileges?
* Do users have local admin privileges?
* Is there a security policy in place for those employees who need elevated privileges that outlines qualifying roles and responsibilities?

**Inject 3 - Thursday, November xx, 2022 – 7:45 a.m.**

John, a newly hired county IT department employee, is casually scrolling through Intrusion Detection System (IDS) logs. He is supposed to ‘roll the logs’ every morning, but in reality, only gets done about twice a week. The last time anyone looked at alarms and events were over a week ago.

John finds two solid pages of email traffic, starting Tuesday at 5:01 am. “Where are all these emails coming from so early in the morning?” he muses. Just then his cell phone rings, and he sees his girlfriend’s number displayed. Grinning, he spins in his chair and chats for 10 minutes or so before realizing he is about to be late, again, for the 8 a.m. IT staff call. He quickly wraps up the call, hangs up and dials into the meeting, logs and emails forgotten.

**Discussion**
*Training, training, and more training!*

* Does your organization provide basic cybersecurity and/or IT security awareness training to all IT users (including managers and senior executives)?
	+ How often is training provided?
	+ Does it cover:
		- The county’s information security program and cyber incident response plan.
		- Roles and responsibilities
		- Password procedure
		- Whom to contact and how to report suspected or suspicious activities?
* What security-related training does your organization provide to, or contractually require of:
	+ IT Managers
	+ System and Network Administrators
	+ Vendors
	+ Other IT personnel having access to system-level software
* Discuss your organization’s suspected or suspicious cyber activity reporting mechanism.
* Discuss your organization’s intrusion detection capabilities and analytics that alert you to a cyber incident.

**Inject 4 - Friday, November xx, 2022 – 8:00 a.m.**

During the morning IT staff call, an IT employee reports that he received five reports of potential suspicious emails allegedly from HR asking employees to update their medical beneficiary information.

Further investigation reveals that the “HR emails” were phishing emails and were sent to 30 employees across all ABC County departments over a two-day period. The emails directed users to a spoofed website designed to capture usernames, passwords, and deliver a payload. It is unknown how many employees opened the email, entered their credentials, and clicked the link to “…review and update their medical beneficiary information...”.

**Discussion**
*Multiple indicators of compromise over the last 3 days*

* Do you conduct regular IT/executive cybersecurity meetings?
* Does the IT department assign severity levels or tiers to cyber incidents?
* What is the incident severity level or tier of this incident once multiple spoofed emails are reported?
* What immediate remediation and protective actions would be taken at your organization?
	+ Who is responsible for those actions?
	+ Are these actions and responsibilities documented in plans?
	+ How are they activated?
* Would any additional reports or notifications be made? If so, where are primary, secondary, and tertiary points of contact identified?
* What are the requirements and/or processes to notify organization leadership of a cyber incident at each severity tier?
* What resources and capabilities are available to analyze the intrusions?
	+ Internally?
	+ Externally through government partners?
	+ Through the private sector?
* Are cybersecurity roles and responsibilities defined in contracts with third-party IT support vendors and crucial suppliers.
	+ Have you discussed these types of concerns and risks with them?
* What mechanism(s) is used to share cyber threat information within your organization and external to your organization?

**Module 2: Ransomware Attack**

**Inject 1 - Friday, November xx, 2022 – 11:15 a.m.**

A few months have passed, John continues to gain IT experience and make progress with reviewing the logs. The HR phishing email seemed to resolve itself after IT alerted all users to delete the suspicious email and not click on any links or open any attachments.

The IT Department, though, has been receiving a higher volume of calls and emails lately about the file shares not opening and users receiving an error when attempting to “Open a Word document I have always been able to open.”

The IT Department continues to investigate the problem, but for now it would have to wait until Tuesday because it is a long holiday weekend there is an early out scheduled on the Friday before the holiday.

**Saturday, November xx, 2022 - 8:45 a.m.**

A county employee, Bob, from the finance department had some work to catch up on over the weekend and uses the county Virtual Private Network (VPN) to log in to the network from home. He tries logging on to his work email but keeps getting error messages. He also tries accessing his databases and finance software, but no luck. He calls the IT help desk number, which was forwarded to an IT tech cell phone since it was the weekend. Mary from IT answers.

Bob and Mary talk about what was going on and whether there was weekend maintenance happening. Mary confirms that she was not aware of any scheduled or unscheduled network maintenance occurring this weekend. Mary tries to remote in to look around and gets an ‘Unable to complete this request, try again’ error three times in a row. She tells Bob that she will do some research into the issue and call him back.

Mary calls her boss, Joe, the Chief Information Officer (CIO), to discuss what was happening and he tries remoting in as well with no success. They conference in the remaining IT staff to determine whether this issue would require someone to go in and see firsthand what the potential issue is.

**Discussion**
*What is the county policy for afterhours IT support?*

* What is the county IT policy on afterhours help desk requests and customer support?
* Who makes the decision on whether IT staff need to go on site after hours? How are IT staff employees compensated for this work?
* Is there a process in place to notify the appropriate stakeholders of an IT “outage” or event?
* As it relates to your county executives and elected officials, what cybersecurity information do they regularly request, if any? What kind of cybersecurity information do they receive from the IT department, if any?
* What priorities have county executives and elected officials set related to the cybersecurity of county assets?
	+ Are those priorities documented?

**Inject 2 - Saturday, November xx, 2022 - 10:45 a.m.**

Joe and IT staff on the conference call all agree that something is not right. He talks quickly through a mental checklist of possible explanations of what the issue may be, all quickly rejected by the staff. Joe says, “Ok team, I think this needs to be addressed on site so Mary and I will go in and see if we can resolve the network issues.”

Mary is so thrilled to go in to work on a Saturday during a holiday weekend!

**Saturday, November xx, 2022 - 12:00 p.m.**

About an hour later, Joe and Mary arrived at the county office. They figured they would be in and out and back to enjoying their weekend after checking a few settings, and maybe restarting some services.

Mary logged in and tried to access the servers to check for issues and immediately yelled to Joe “come see this!”

Mary had the following message on her screen when she logged in:



After multiple attempts at trying to access each of the county servers and file shares, Joe got the same encryption message for each of them. It appeared that all county servers had been impacted and infected with Ransomware as well as all county data was encrypted.

**Discussion**
*What should Joe and Mary do right now?*

* What should Mary and Joe be doing right now?
* Do they have an incident response checklist that they should be referring to?
* Should infected systems be taken offline right away?
* What about county services?
	+ Which county services would be impacted by taking the systems offline?
	+ What about 911 and other county emergency services?
	+ Who is responsible for making notifications calls to departments and assess the operational impact of the attack?
* Do Joe and Mary need anyone else’s approval before proceeding with any incident response procedures?
* Has county executive level leadership been notified at this point?

**Inject 3 - Saturday, November xx, 2022 – 3:14 p.m.**

Mary and Joe realize this is a significant cyber incident, and starts putting together a list of people that need to be notified and schedule a conference call for 6:30 p.m.

**Discussion**
*Who needs to be notified at this point?*

* Who are the key county stakeholders that need to be notified at this point?
* Who should be invited to the 6:30 conference call?
* What are key questions and initial response actions to discuss tonight on the call? At this point, would they include:
	+ Are 911 or other emergency services affected?
	+ What other critical county services are affected?
	+ What other operational impacts are anticipated because of the attack?
	+ How are hacker demands to be handled?
	+ Does the county have the appropriate manpower and resources to adequately respond on this holiday weekend?

**Inject 4 - Saturday, November xx, 2022 – 9:40 p.m.**

All county servers were pulled off the network. All county services managed by those servers are currently down. The 911 Center seems to be fully functional because they are separated from the main county network. Instructions from the ransomware actor are found and they say:



**Discussion**
*What to do, what to do?*

* From an IT perspective, what remediation actions would be taken?
	+ Who is responsible for those actions?
* Are redundant systems available if critical systems are compromised?
* Is there a priority list of county essential services that need to be restored first?
* Who contacts the hacker? When?
* Has the county IT staff and emergency managers jointly planned for cybersecurity incidents?
* What are the county IT workforce gaps? How does the county recruit, develop, and retain cybersecurity IT staff?
* What other actions or concerns, at the CIO level, should Joe be contemplating?
* At what point in the scenario would you contact law enforcement?
	+ What are your expectations of state and federal government?
	+ Are processes and resources in place for evidence preservation and collection?
* At what point in the scenario would you inform Pennsylvania Emergency Management Agency (PEMA) of the incident?

**Inject 5 – Sunday, November xx, 2022 – 7:48 a.m.**

After all night conference calls with the county commissioners, executive staff, IT staff, and the legal team, everyone is tired, and uncertain as to how to proceed. Joe pushes for, and gets authorization, to get external support.

**Discussion**

* Now that they have agreed to get external help, what is the next step?
* Who needs is available to be called for external support? Other county IT departments?
* Who else needs to be notified?

**Inject 6 - Sunday, November xx, 2022 – 8:07 a.m.**

Joe decides to call Ron, the County Commissioner Association of Pennsylvania (CCAP) CIO to get some advice on how to proceed since he has assisted other counties who have had a ransomware attack. Luckily, Ron answers the call on this Sunday morning.

Ron suggests that Joe report the incident to the FBI and PA State Fusion Center (PaCIC), as well as contact the cyber insurance provider if the county has cyber insurance. Ron also sends Joe a copy of the Pennsylvania Cyber Incident Annex (PCIA), which is part of the Commonwealth Emergency Operations Plan (CEOP). The Annex identifies various federal, out-of-state (EMAC) and in-state resources which may be available to assist the county. These primarily include: PEMA, the PA National Guard, and the Department of Homeland Security’s Cybersecurity and Infrastructure Agency (DHS CISA).

Joe reviews the PCIA and secures approval to report the incident to the PEMA, PaCIC and FBI. He then turns his attention to preparing for the upcoming call with the county’s cyber insurance provider.

**Discussion**
*Incident response is starting to get real!*

* What information do county level executives and elected officials need to support their decision-making process?
* The county executives should start thinking about whether to pay the ransom to bring the county back online quickly and avoid more financial turmoil, or work with IT and other resources to try and restore the systems. Both are costly. The following are considerations:
	+ Does the county have data backups? Have the backups been infected with the malware?
* Who will be involved in the decision-making process? How is legal involved?
* Since this happened on a holiday weekend, how will public notification and media response be handled?
* Who maintains communications with the hacker? The insurance company? CIO?

**Inject 7 – Sunday, November xx, 2022 – 9:00 a.m.**

The conference call with the insurance company is scheduled for 11:00 a.m.

County executive staff and the CIO collaborate with the legal team to discuss the questions that need to be discussed with the cyber insurance provider.

**Discussion**
*What is the county getting for their money with their cyber insurance policy?*

* Will the insurance company pay the ransom if that is the course of action the county chooses?
* What is the deductible?
* Does the cyber insurance premium increase if a claim is made? If so, how much?
* Does the insurance company provide onsite subject matter experts for incident response support?
* Does the insurance company provide recovery support and manpower to assist with restoring servers and data?
* Does the insurance company provide forensics analysis?
* Does the insurance company provide a security assessment to identify any remaining vulnerabilities to prevent a follow-on attack from occurring?
* Are there any other questions or concerns will the county need to discuss with the cyber insurance company?

**Module 3: Containment, Eradication, Recovery**

Situation Recap - ABC County is currently handling a ransomware attack that is affecting all the county’s servers and all county data is encrypted. All servers are currently offline, and all county services managed by those servers are down. The 911 Center is still fully functional. County stakeholders hold a conference call to assess the situation and authorization was given to contact external sources for assistance. The CIO reported the incident to PEMA, PaCIC and the FBI. A conference call was scheduled with the cyber insurance company to discuss options.

IT staff are conducting an initial assessment of the incident and determining if backups were affected.

The message from the hacker was found stating they needed to be contacted to discuss decryption. No one at the county has contacted the hackers yet. The hacker demands are unknown as of this time.

**Inject 1 – Sunday, November xx, 2022 – 10:00 a.m.**

The IT Staff on site completed the initial incident assessment and determined that all county files are encrypted. There is no available encryption key and the hackers warned not to try encrypting with 3rd party software or permanent damage may be done.

Access to the encrypted files can only be gained with the appropriate encryption key provided by the hackers (which will likely require ransom to be paid) or to try to restore from county backups. The IT staff determined that all recent county backups have also been impacted and encrypted by the hackers. They looked at backups from 6 months ago and they have not been encrypted so the county can restore from 6-month old backups as an option, but these could take a few weeks to fully restore.

**Discussion**
*What options does the county have at this point?*

* What would the county strategy be if only one day’s worth of data is lost?
	+ Would the existence of cyber insurance affect that decision?
	+ If the recent backup is also not recoverable and the 6-month backup appears to not be impacted, is using a 6-month backup a viable option to pursue considering it will take weeks to recover the data?
	+ What would be the strategy to continue business if recovery took 2 weeks?
* Does the county have a cyber incident response team? Would they be activated?
* What actions should county be considering when performing essential functions without IT support? How will these actions be coordinated with other key partners?
* Discuss overall strategy for ransomware payout.
	+ Would the cyber insurance provider play a part in the various decisions?
* What would the county staff communications look like without availability of e-mails?

**Inject 2 - Sunday, November xx, 2022 – 12:08 p.m.**

The conference call between the cyber insurance provider and ABC county stakeholders just finished up and the insurance company will provide the following assistance:

* Respond to the hackers and gather information about any demands requested, work with them to get an encryption key, and pay any ransom if the county chooses to do so.
* Conduct initial forensic analysis remotely on the network to determine where the hackers got in, how they got in, what data they may have stolen, where they laterally moved across the network, and extent of damage done.
* Forensically image any devices that require it

**Sunday, November xx, 2022 – 12:15 p.m.**

The county IT staff will be responsible to:

* Restore any systems from backups.
* Receive the encryption key from the insurance company and decrypt all files.
* Prioritize and restore all affected county services.
* Change all passwords on all network devices and force all users to change their passwords.
* Conduct a vulnerability assessment and update any outdated systems or software as well as verify configuration management of all network devices.
* Review account management and ensure principle of least privilege to all systems and services is implemented.
* Ensure antivirus and anti-malware software and signatures are up to date and functioning appropriately.

***Discussion*** *How will the county handle restoration of services as well as securing their network?*

* What devices will need to be forensically imaged?
* Do all systems and devices need to be re-imaged?
* What are some other primary areas of concerns that the county IT team should be considering at this point?
* What key actions should they be considering?
* How will the county manage IT staff to continue to move forward with the service restoration, eradication, and recovery process?
* What will the work schedule look like?
* How will tasks be divided amongst employees?
* What will the daily battle rhythm look like? Daily, hourly, update meetings? 24-hour operations? Shifts?

**Inject 3 -** The cyber insurance company contacted the hackers and received the following information:

Hackers are demanding $500,000, paid in bitcoin, within 48 hours or all county personnel data will be exposed on the Internet to the public and files permanently deleted.

The cyber insurance company told the CIO that he would need to make a decision quickly and that the deductible for their policy would be $25,000.

**Discussion**
*What should the county do?*

* Who is the final decision maker or has final approval authority?
* Does the county have the funds to pay the insurance deductible? What will county taxpayers say? Do they have a say in this type of decision?
* Does the county need to notify its employees and residents of a possible data breach? Is there a process in place to conduct this type of widespread notification?

**Inject 4 – Monday, November xx, 2022 – 8:45 a.m.**

After an initial forensic analysis, the cyber insurance provider provides this update:

Patient zero was likely Jane in the County Treasurer’s Department. The stolen user credentials enabled access to the VPN, three network folders, and various servers not configured for Multi Factor Authentication. The hackers were able to laterally move across the entire network with Jane’s elevated privileged credentials.

Log data has been scoured. The phishing emails ceased after the initial wave back in March. The mail server they originated from is no longer visible. The phishing email was opened on 18 endpoints. 11 of those 18 provided their network credentials. Those stolen credentials allowed even greater movement and access in the network.

Privilege escalation was gained by a brute force attack on the Administrator account. Once credentials were stolen, the hacker reconned the network of other accessible hosts (computer and devices). The attacker then moved laterally to those hosts. LockBit (the ransomware) was downloaded from each host with a PowerShell script and compiled. CPU usage exploded on each host during this stage in the attack. Wednesday thru Friday of last week, packets went to and from an IP in Belarus. Numerous Emotet (trojan, malware) and LockBit Indicators of Compromise (IOCs) were noted. This version of LockBit is generation three which gave the attacker enhanced lateral movement, code execution and concealment capability over previous versions.”

An additional forensic analysis of Jane’s computer revealed that she has an unsupported operating system that was not receiving updates and anti-virus software was not functioning.

Her computer is the only computer in the county that has very specific software that managed the county’s dog license database. The software is legacy and no new versions existed after 2007 so Jane was never able to get a new computer with an updated operating system without the software malfunctioning. So, Jane continued to use her outdated Windows 7 computer.

Pockets of missing encrypted files from all county departments were found in hidden folders on Jane’s computer. The hackers likely used Jane’s computer to communicate back and forth to their command and control center, and exfiltrate the county’s stolen files in various batches throughout the last few months (after the computer was comprised during the phishing attack).

**Discussion**

*The recovery work is never-ending!*

* Where does the IT team focus its efforts now?
* What should the CIO be focusing on or coordinating now?
* Would the CIO consider bringing in additional support to assist with remediation and recovery efforts?

**Inject 5 - Monday, November xx, 2022 – 12:00 p.m.**

The team took 6 hours to rest and change clothes Sunday night before going back to Containment work at 7 a.m. on Monday morning. They push through and complete Containment efforts by mid-afternoon.

Eradication efforts get underway around 1:00 p.m. on Monday and continued all day and into the evening.

Forensic analysis and malware scans have been completed on all endpoints, network devices, servers, virtual machines and backup data. Several instances of Emotet and LockBit were discovered and remediated.

Reimaging activities will begin immediately, followed by data restoration.

**Discussion**
*Containment and eradication efforts wrap up.*

* Before beginning eradication activities, what steps would the county take to ensure all infected or impacted systems and infrastructure were identified?
* What actions and processes would you focus on in the Eradication phase?
* Do you have the manpower to complete eradication?
* Would you consider bringing in an external resource(s) to assist with recovery and eradication?
* How are the county departments kept updated on restoration progress? How is the public staying informed on the progress?
* What is the priority of effort needed to efficiently accomplish reimaging and restore operations?

**Inject 6 –**

Re-imaging is completed, current patches verified on all operating systems.

Documentation of new controls (temporary and permanent), forensic analysis and evidence is being collected and secured.

CIO announces Eradication efforts are a success and gives the green light to start data restoration. The team is now in the Recovery Phase.

What are some areas of concern or emphasis during the Recovery phase?

**Tuesday, November xx, 2022 – 5:15 p.m.**

Affected entity configurations were validated using approved configuration baselines.

Vulnerability testing was completed to ensure they are not susceptible to various methods of attack, prior to being placed into production.

Server operating systems, domain controllers, virtual machines and backup systems have been restored, tested and validated.

Data restoration went smoothly, managers or subject matter experts in the major county departments verified and validated the restored data is ‘good’.

Recovery is successful.

**Discussion**
*Final thoughts*

* Who declares the incident is over?
* What are the criteria for declaring the response complete?
* What should county staff be planning and preparing for next?
* What do you need to work on for an actual attack?
	+ Gaps in response / resources
* What will you change within the county to further protect yourself from a ransomware attack and help recover easier / quicker if you are hit?

**After Action Review Considerations**

* What gaps were identified in the cyber incident response plan?
* List the top three organizational strengths.
* List the top three organizational items requiring improvement.
* Are there training or educational efforts needed moving forward?
* What documents, processes and plans may need to be updated from the lessons learned exercise?
* Set a date and time to meet to discuss improvement strategies
	+ Develop highest needs.
	+ Create an actionable list of all improvements needed.
	+ Assign tasks and set expectations, goals, and timelines.
	+ Consider funding needed, funding sources

# Appendix A: Suggested Exercise Schedule

Please modify this suggested schedule to meet your needs.

| Date | November 2022 |
| --- | --- |
| 0900-1200 |
| 0830-0900 | Registration |
| 0900-0915 | Welcome and Introductions |
| 0915-0945 | Module 1: Phishing |
| 0945-1030 | Module 2: Ransomware Attack |
| 1030-1045 | Break |
| 1045-1130 | Module 3: Containment, Eradication, Recovery  |
| 1130-1200 | Hot Wash and Closing Comments |

# Appendix B: Acronyms

| **Acronym** | **Term** |
| --- | --- |
| AAR | After-Action Report |
| BOE | Board of Education  |
| CISA | Cybersecurity and Infrastructure Security Agency |
| DDoS | Distributed Denial of Service |
| DHS | U.S. Department of Homeland Security |
| FBI | Federal Bureau of Investigation |
| HSEEP | Homeland Security Exercise and Evaluation Program |
| HVAC | Heating, Ventilation, and Air Conditioning |
| MS-ISAC | Multi-State Information Sharing & Analysis Center |
| IS | Information Systems |
| IT | Information Technology |
| NIST | National Institute of Standards and Technology |
| PII | Personally Identifiable Information |
| SitMan | Situation Manual  |
| TTX | Tabletop Exercise  |
| TLP | Traffic Light Protocol |

**Appendix C: Participant Feedback Form**

Please enter your responses in the form field or check box after the appropriate selection.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name:** |  | **Title:** |  |
| **Agency:** |  |  |  |  |
| **Role:**  | Player [ ]  | Facilitator *[ ]*  | Observer *[ ]*  | Evaluator *[ ]*  |

**Part I: Recommendations and Corrective Actions**

1. Based on the discussions today and the tasks identified, list the top three strengths and/or areas that need improvement.

|  |  |
| --- | --- |
| 1.
 |  |
|  |  |
|  |  |

1. Identify the action steps that should be taken to address the issues identified above. For each action step, indicate if it is a high, medium, or low priority.

| **Corrective Action** | **Priority** |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

1. Describe the corrective actions that relate to your area of responsibility. Who should be assigned responsibility for each corrective action?

| **Corrective Action** | **Recommended Assignment** |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

1. List the policies, plans, and procedures that should be reviewed, revised, or developed. Indicate the priority level for each.

| **Item for Review** | **Priority** |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Part II: Participant Feedback**

What changes would you make to this exercise? Please provide any recommendations on how this exercise or future exercises could be improved or enhanced.

|  |
| --- |
|  |
|  |
|  |
|  |
|  |