Facilitator's Handbook
Ransomware Tabletop Exercise

Version 2.0 – January 17, 2020

Table of Contents

Notes for Facilitator (Facilitator's Handbook Only)

Background (Facilitator's Handbook Only)

This ransomware scenario is designed to unfold throughout the day testing an organization's ability to digest threat intelligence, react to an incident's initial consequences, and manage long-term fallout from the incident. The broader concepts of the exercise are business resiliency, disaster recovery, and continuity of operations. Participants should focus on these concepts throughout the exercise in order to determine what gaps may exist in these processes, and how they can be filled.

For most effective results, the designers of the exercise suggest bringing together a small group of 8-10 stakeholders from IT, Operations, HR, Communications, and Senior Leadership. One participant should facilitate the exercise using this book, the others should use the accompanying participant handbook. The exercise takes approximately 4-5 hours to complete, including lunch and breaks throughout the exercise. The suggested timing for each inject, or exercise event, is included at the beginning of each session. A summary of each session is located at the end of this section.

This facilitator's guide is designed for use in conjunction with the participant handbook. Information that is restricted to facilitators only is noted by the parenthetical comment (Facilitator's Handbook only) and is noted in a boxed, light gray background such as this one. Information that has been provided for both participants and facilitators is noted by the parenthetical comment (Participant's Handbook), and appears with a standard white background.

Before the exercise, print out a copy of the participant book for each player but do not distribute full copies of the participant's handbook at the start of the day. Distribute the table of contents and Session 1 – Background & Introductions section only. Red prompts such as this one indicate when to pass out the next piece of information. Facilitators may want to set timer reminders to prompt the distribution of injects and keep the session on track.

The exercise is guided through the use of "Injects" which serve as prompts for the players. Each inject has discussion questions at the end for the players to discuss. The facilitator's handbook includes suggested inject times at the start of each session, along with a summary of all inject discussion questions. When the suggested time occurs, or the players are ready to move on to the next inject, pass it out to each player at the same time, and assign one of the players to read the inject. Some of the timings are intentionally clustered together to simulate the confusion and rapid evolution of an incident in progress.

The scenario will unfold over the course of 3 sessions, outlined below

- Session 1 (960 minutes) – This session will give the players a chance to introduce themselves and their familiarity or exposure to ransomware and information security concepts. The injects will start out slowly: there are vague hints in the InfoSec information sharing community that there is a ransomware outbreak targeting transportation logistics companies. The participants will explore proactive measures they can take.
- Session 2 (9045 Minutes) – This session is the most frantic. The players will explore institutional response to a rapidly escalating and sophisticated ransomware incident. Malware affects the players, and ransomware takes root in operational servers. As a result, organizations lose internal sites and

operations information systems. The players will need to explore operational resiliency, continuity of operations and communications strategies to maintain critical functionality.

- Session 3 – (690 Minutes) – This session explores the next few days after the incident. A remediation becomes available from a partner (EG US-CERT, FBI or similar). The players will explore implementing the patch/solution and restoring customer confidence damaged by incident.

The beginning of each session has suggested timing for each inject, some of which come at a much more frequent pace than others in order to add a level of realism.

Objectives (Facilitator's Handbook only)

Overall objectives of the tabletop

- Objective 1 - Examine internal information sharing roles and responsibilities during a ransomware outbreak (such as when to escalate)
- Objective 2 - Examine what steps players have taken to reduce risk of ransomware
- Objective 3 - Examine operational resilience, including what to do when the logistics information system is unavailable
- Objective 4 - Examine communications protocols during an incident with external parties, such as customers and news media

Notes on Attack Timeline / Impacts (Facilitator's Handbook only)

Notes on the attack

- Sneaky/quiet attack at first
- Finds its way from enterprise workstations (e.g., phishing) to backend and production servers
- Online backups are encrypted, logistics databases are encrypted. Logistics and maintenance software is stops working.
- Loading staff are unable to print/load shipment cargo manifests and destinations.
- Operations team is unable to view real-time truck location/tracking information.
- Internal and External sites are not working (returning 404 error)
- Terminals begin to show ransom messages.
- Email will stop working in session 2 and mobile phones still work but Email address books are encrypted.
- Paying the ransom doesn't get anything back.

1. Session I – Introductions & Background

Facilitator Instructions (Facilitator Only)

Facilitator Note: This section will give the players an opportunity to introduce themselves and their roles at their organization. Read the following aloud:

"Welcome to the Ransomware tabletop exercise, I <your name here> will be the facilitator. We will start by reading the introductions and background section below"

After reading assigning a player (or soliciting a volunteer) to read the background text below. Rotate reading responsibilities around the table throughout the exercise.
Time Budget for Background and Introductions: ~~Less than 20~~30 minutes

Introductions and Role Assignment (Participant Handbook)

Facilitator Note: Assign a reader for the text below. Make sure that each player chooses a role or roles, but do not let them get sidetracked. If players identify additional roles which are necessary throughout the exercise, they can assume those identities, but make sure they take note of them in their participant books. Suggested roles include: Senior Leadership, IT Operations, Senior IT, Logistics, and Communications.
Introductions and role assignment should take less than 5~~2~~ minutes per player.
After the introductions assign a reader for the background section below

Please briefly introduce yourselves to the group by name, title and area of responsibility within your organization. If your group believes that any important organizational component for incident response is not represented, assign those roles amongst yourselves. If at any point during this exercise you feel another organizational component should be present, make a note of it and assign that position in your group.

Background (Participant Handbook)

Ransomware is an emerging threat to a variety of industries, and is characterized by The National Institute of Standards and Technology as a type of malware that attempts to deny access to a user's data usually by encrypting it with a key known only to the hacker who deployed the attack until a ransom is paid.

The purpose of this tabletop exercise is to test your organization's preparedness to respond to a ransomware incident in a no-fault environment and to develop a better understanding of how incident response works.

Group Discussion (Participant's Handbook)

Facilitator Note: Make sure each participant gets an opportunity to share. This section should take approximately ~~2~~5 minutes per player.
After the last question, pass out Inject #0 to the players and read the facilitator notes on the next page

Please briefly describe your and your organization's familiarity with ransomware using the questions below:

1. What steps have your groups' organizations taken to improve their resiliency to ransomware attacks?
2. Does your organization have somebody at the organization responsible for tracking the news/threat intelligence?
   Name:
   Position:
   Reports to:
3. What news feeds or organizations is your organization subscribed to?

2. Session I – Inject #0

Facilitator Note: Read aloud:

"This is an example of an inject, and will be how the flow of the exercise is executed throughout the exercise."

Assign someone to read the inject.

You arrive at work. All indications are that it will be a normal day.

Facilitator Note: Read aloud:
"Normally there will be discussion questions that follow each inject. I will now pass out Inject #1"
Pass out Inject #1 and allow the players about 5 minutes to read the news article. While they are reading, familiarize yourself with the following exercise information.

Facilitator Directions (Facilitator's Handbook only)

The injects will start out slowly: There are vague hints in the InfoSec information sharing community that there is a ransomware outbreak targeting transportation logistics companies. The participants will explore proactive measures they can take. All of the discussion questions and timing information is in the box below.

At the beginning of each inject, assign a reader and have them read the prompt. Have each player take turns leading one of the discussion questions.

Each session will have a Facilitator's notes/discussion prompts section like the one below. This gives an at-a-glance summary of the key injects, timing, and discussion questions for each session. Each inject is provided for facilitator convenience.

The exercise and discussion should be **Player-driven** although if players are getting too far off topic, or having difficulty keeping up step in as facilitator to get them back on track.

Facilitator's notes/discussion prompts (Facilitator's Handbook only)

Preliminary information / baseline
Inject 1 – News Article – Recommended Time: 5-10 Minutes to Read // ~~10~~ 15-20 Minutes Discussion

- What are the important takeaways from the article?
- How does your organization react to this news?
- Who is likely to read or be forwarded this information first?

Inject 2 – FBI PIN - Recommended Time: 10~~5~~ minutes to read // ~~20~~ 25-30 minutes to discuss

- FBI Shares technical bulletin about a European trucking company being affected by ransomware
- Go over the PIN with your group. What are the significant findings?
- Who receives this information? (Name, Position, Reports to) Do they know it is their responsibility?
- What should they do after they read it?
- Which internal/external parties is the information shared with?
- What technical steps does the IT team take in this case?
- Is there any additional information your organization would request at this time? How would they get this information?
- What information does the IT team share with the Operations team?
- What does Operations do when they learn about a "heightened cyber security risk?"

3. Session I – Inject #1

High-level scenario

After a normal day, you receive an article about a ransomware incident affecting a European transportation company. Please take 5 minutes to read the article and answer the discussion questions below.

NOTE: Real news articles/social media posts about a ransomware attack on Spanish company Everis have been included throughout as examples of how ransomware attacks have been reported by companies, company employees and the media. For this tabletop exercise, please imagine that the embedded articles relate to transportation companies as described in the high-level scenario.

https://www.cbronline.com/news/spain-ransomware-attacks

BREAKING – Spanish Businesses Hit by Wave of Ransomware Attacks

- **Ed Targett** **Editor** 4th November 2019

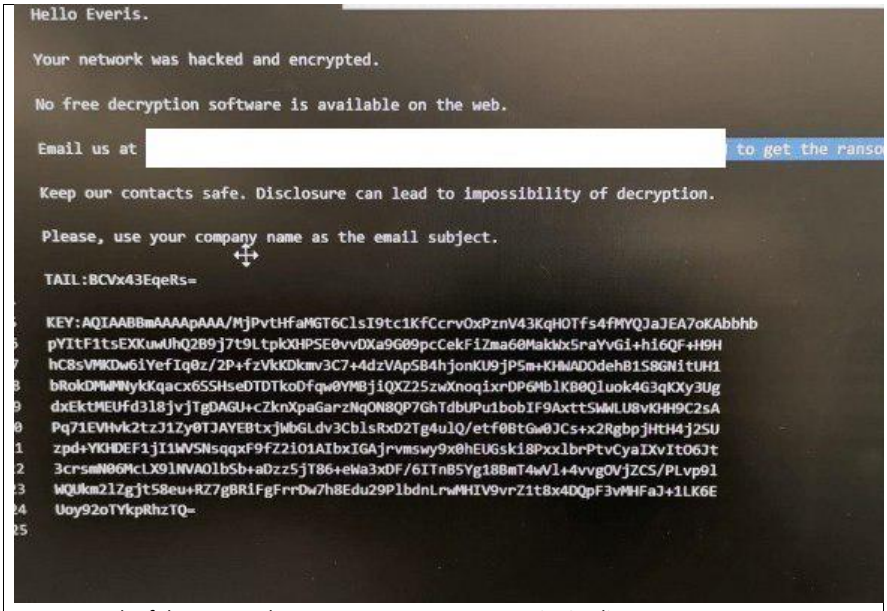
Numerous companies hit, ransomware details not yet known

UPDATED 13:50 BST 4/11/19 with more details, government comment.

Spain has been hit by a wave of ransomware attacks today, with NTT Data-owned Everis – a major IT consultancy – and national radio station SER among those reported to be affected.

Embarrassingly for Everis, it apparently offers its own "seamlessly integrated" cybersecurity services, including "security auditing, pentesting, vulnerability analysis and any other service focused on the proactive identification of vulnerabilities and weaknesses."

The company has yet to respond to requests for comment.



A screengrab of the reported ransomware message at Everis. Credit: https://bitcoin.es/actualidad/everis-se-encuentra-sufriendo-un-hackeo-cryptografico/

"We are in hysteria mode" a technician from one of the companies hit told Spanish news media this afternoon.

The specific type of ransomware payload or the vulnerability they are exploiting have not yet been reported, but has various been named as Ryuk and Bitpaymer. Speculation is rife that the attack involves the exploitation of the so-called Bluekeep vulnerability, after an explosion of Bluekeep malware was detected over the weekend.

#everis #Ransomware pic.twitter.com/HR9iIkxWAc

— Miguel (@Dormidera) November 4, 2019

Spain's largest radio station SER (Sociedad Española de Radiodifusión) confirmed it had been hit in a statement this afternoon saying it had suffered an attack "of the ransomware type… which has had a serious and widespread effect on all of all its computer systems."

Aena @aena, biggest airport operator in Spain, also reporting they're taking down their networking services (LAN & VPN) due to cyberattack. pic.twitter.com/8b7QxrFVSV

— Sound (@Sound1618) November 4, 2019

UPDATED 14:35 BST 4/11/19 with Aena comment.

Major airport operator Aena confirmed to Computer Business Review that it categorically had ***not*** been impacted by the attacks, but had just taken precautionary measures to protect its networking systems. Despite reports to the contrary, Accenture also insisted it had not been affected.

SER, meanwhile, is being "kept running by its headquarters in Madrid, supported by autonomous teams", the company said in a Spanish language statement.

"The technicians are already working for the progressive recovery of the local programming of each of their stations."

The country's Department of Homeland Security played down the attacks, saying in an otherwise detail-free blog post that "this type of attack occurs quite frequently. In 2016, the National Cybersecurity Institute handled some 2,100 similar incidents…

"It does not compromise data security nor is it a data leak."

The department confirmed SER had been hit and that it was a ransomware attack: "The infection path appears to be a file attached to an email (" La vía de infección parece ser un fichero adjunto a un correo electrónico").

Discussion questions

1. What are the important takeaways from the article?

2. How does your organization react to this news?

3. Who is likely to be forwarded this information first?

4. Session I – Inject #2

High-level scenario

The attached EXERCISE MOCKUP of an FBI Private Industry Notification is about an attempt by unknown actors to deploy ransomware malware on European freight carriers. It is based on the real-world Ryuk ransomware PIN which affected hospitals across the globe. Please take 5 minutes to read the PIN and answer the discussion questions below.

EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE

EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

This PIN has been released TLP: GREEN: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

Unknown Cyber Actors Attempted to Deploy Ransomware Malware on European Freight Transportation Carriers

Summary

FOR EXERCISE PURPOSES ONLY

Unknown cybercriminals have targeted more than 100 US and international businesses with EXERCISE ransomware since approximately August 2018. EXERCISE encrypts files on network shares and an infected computer's filesystem. Once the victim has been compromised, the actors encrypt all the network's files and demand sums of up to $5 million worth of Bitcoin (BTC) in exchange for a decryptor program. EXERCISE's targets are varied and indiscriminate, but attacks focus on organizations with high annual revenues in hopes of extracting larger ransoms from the victims. While EXERCISE is generally undiscerning about victims, attacks have had a disproportionate impact on logistics companies, technology companies, and small municipalities.

EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE

EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE

Technical Details

EXERCISE first appeared as a derivative of Ryuk ransomware, which first emerged in late 2018 and available for sale on the open market as of November 2019. Exercise still retains some aspects of Ryuk code. For example, all of Exercises files contain the "RYUK" tag but some of the files have .EXR added to the filename, while others do not. In other parts of the ransomware code, EXERCISE has removed or replaced features of its predecessor, such as the restriction against targeting specific Eurasian-based systems.

FOR EXERCISE PURPOSES ONLY

The exact infection vector remains unknown as EXERCISE deletes all files related to the dropper used to deploy the malware. In some cases, EXERCISE has been deployed secondary to Trickbot and/or Emotet banking Trojans, which use Server Message Block (SMB) protocols to propagate through the network and can be used to steal credentials. In one case, the ransomware appears to have used unsecured or brute forced Remote Desktop Protocols (RDPs) to gain access. After the attacker has gained access to the victim network, additional network exploitation tools may be downloaded, including PowerShell Empire, the Microsoft Sysinternals tool psexec, or the penetration testing tool Cobalt Strike.

Once executed, EXERCISE establishes persistence in the registry, injects into running processes, looks for network connected file systems, and begins encrypting files. EXERCISE utilizes AES-256 to encrypt files and uses an RSA public key to encrypt the AES key. The EXERCISE dropper drops a .bat file which tries to delete all backup files and Volume Shadow Copies (automatic backup snapshots made by Windows), preventing the victim from recovering encrypted files without the decryption program. The “EXERCISEReadMe” file the ransomware places on the system after encryption provides two email addresses, using end-to-end encrypted email providers Protonmail and/or Tutanota, through which the victim can contact the attacker(s). While earlier versions provide a ransom amount in the initial notifications, EXERCISE users are now designating a ransom amount only after the victim makes contact. The attacker(s) tell the victim how much to pay to a specified BTC wallet for the decryptor and will provide a sample decryption of two files.

The FBI does not encourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or may fund illicit activities. More importantly, paying the ransom does not guarantee that a victim’s

EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE

EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE

files will be recovered. For instance, with this variant, testing shows success when running the decryption as 'admin'. Additionally, initial testing reports that the "EXERCISEReadMe" file does not need to be present for the decryption script to run successfully but other reporting advises that some files will not decrypt properly without it. Even if run correctly, there is no guarantee the decryptor will be effective. This is further complicated by the fact that the "EXERCISEReadMe" file is deleted when the script is finished which may affect the decryption script unless it is saved and stored in a different location before running. In all cases, the FBI encourages organizations to contact their local field office immediately to report a ransomware event.

FOR EXERCISE PURPOSES ONLY

EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE

TLP: GREEN

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE

TLP: GREEN

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE

Indicators:

The following indicators of compromise have been observed in samples of EXERCISE malware.

Host Based Indicators:

- Mutex: "efkrm4tgkl4ytg4", "FakeMutex"
- Registry:
  - KeyName: "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run";
  - Value: "EXERCISE";
  - Date Type: "REG_EXR";
- File:
  - Depending on the Windows version, one of the following:
    - "C:\users\Public\sys"
    - "C:\Documents and Settings\Default User\sys"
  - Numerous identical "ransom note" files:
    - "EXERCISEReadMe.txt"
    - Numerous encrypted files, which were not renamed, but have the "EXER" tag followed by an encrypted key at the end of the file;
- Some malware samples add '.EXR' to the end of encrypted filenames

FOR EXERCISE PURPOSES ONLY

Network Indicators (not common):

- HTTP GET request:
  - GET /Lfkgnt5lkgngl3knfl3.php?UI=v9&ID=1140 HTTP/1.1;
- User-Agent string
  - "Microsoft Internet Explorer";
- IP address: 9.999.999.998

EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE

TLP: GREEN

EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE

TLP: GREEN

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE

Information Requested:

If you or your company is found to be a victim of EXERCISE ransomware, the FBI is seeking any information, including:

- Recovered executable file
- Copies of the "read me" file – DO NOT REMOVE the file or decryption may not be possible
- Live memory (RAM) capture
- Images of infected systems
- Malware samples
- Log files
- E-mail addresses of the attackers
- A copy of the ransom note
- Ransom amount and whether or not the ransom was paid
- Bitcoin wallets used by the attackers
- Bitcoin wallets used to pay the ransom (if applicable)
- Names of any other malware identified on your system
- Copies of any communications with attackers

FOR EXERCISE PURPOSES ONLY

Formatted: Centered

EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE

EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE

Recommended Mitigations

Determining the initial point and method of compromise is critical to preventing reoccurrence since there is both the initial network compromise and exploitation and the persistence mechanism of the ransomware itself. There have been victims who experience a second EXERCISE infection after remediation because a single workstation was offline when remediation occurred.

The FBI recommends that any victims of EXERCISE take the following steps, to include, but not limited to:

- Scan system backups for registry persistence
- Scan system backups for other malware infections, particularly Trickbot and/or Emotet
- Execute a network-wide password reset
- Enact multifactor authentication
- Ensure network segmentation
- Ensure all file backups are located offline

FOR EXERCISE PURPOSES ONLY

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at EXERCISE or by e-mail at EXERCISE. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at EXERCISE@fbi.gov

Formatted: Heading 2

EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE

EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE EXERCISE

Recommended Mitigations

Determining the initial point and method of compromise is critical to preventing reoccurrence since there is both the initial network compromise and exploitation and the persistence mechanism of the ransomware itself. There have been victims who experience a second Ryuk infection after remediation because a single workstation was offline when remediation occurred.

The FBI recommends that any victims of Ryuk take the following steps, to include, but not limited to:

- Scan system backups for registry persistence
- Scan system backups for other malware infections, particularly Trickbot and/or Emotet
- Execute a network-wide password reset
- Enact multifactor authentication
- Ensure network segmentation
- Ensure all file backups are located offline

Reporting Notice

FOR EXERCISE PURPOSES ONLY

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at EXERCISE or by e-mail at EXERCISE. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at EXERCISE@fbi.gov

Formatted: Heading 2, Left

Discussion questions

1. Go over the PIN with your group. What are the significant findings?

2. Who receives this information? Do they know it is their responsibility?

Name:

Position:

Reports to:

3. What should they do after they read it?

4. Which internal/external parties is the information shared with?

5. What technical steps does the IT team take in this case?

6. Is there any additional information your organization would request at this time? How would they get this information?

7. What information does the IT team share with the Operations team?

8. What does Operations do when they learn about a “heightened cyber security risk?”

5. Session II – Background (90 minutes)

Background (Facilitator's Handbook only)

Session 2 "React" - This session is the most frantic. The players will explore institutional response to a rapidly escalating and sophisticated ransomware incident. Malware affects the players, and ransomware takes root in operational servers. Organizations lose internal sites and operations information systems. The players will need to explore operational resiliency, continuity of operations and communications strategies.

The Injects will arrive on a much faster timeline than in the other sessions. The goal is to partially overwhelm the players and they must act quickly.

Facilitator's notes/discussion prompts (Facilitator's Handbook only)

Calls go in to the IT help desk, computers at the loading docks are displaying ransomware messages asking for $500,000 in bitcoin

Inject 3 – Loading dock (George) calls Help desk (janet) calls Pass out at start of Session, 1 minute later pass out Inject #4

- What should Janet do? What should George do?
- What is the escalation protocol for incidents like this? What other business units become involved? Who gets the call?
- What external parties does your organization reach out to?
- Do you contact business partners? What business partners do you reach out to? Do you have an offline backup of critical contacts?
- Do you contact customers at this time? If so, what do you tell them?
- Does your organization have a policy regarding paying the ransom?

Inject 4- Loaders and Drivers at multiple locations are unable to access navigation data, route planning information, or cargo manifests. Operations have ground to a halt. Pass out 1 minute after Inject #3

- What do you tell the drivers and loaders?
- Do you have a continuity of operations or operations resiliency plan?
- What are the essential services needed to maintain a diminished operating capacity?
- Do you have a plan to procure hardware and software services to maintain critical functionality?

Inject 5 – Enterprise Servers are affected. Internal/external sites are not functioning properly. Email is no longer working. Pass out 5 minutes after Inject 4

- ~~Ransomware has taken hold in enterprise systems, external and internal sites are not functioning.~~
- How does your organization communicate and coordinate containment and recovery?
- What is the first string of response? Who makes the call? At what point is senior management informed?
- What external parties (if any) does your organization reach out to? (EG AUTO-ISAC, FBI ...)
- What law enforcement organizations does your company reach out to?
- Who does your organization appoint to manage parallel efforts and prioritize the response process?
- Does your organization take systems offline? Which systems?

Injects 6 & 7 – Social Media and Customer Complaints Pass out Injects #6 and #7 at the same time, 15 minutes after Inject #5.

Customers are calling and complaining that they are unable to view tracking information and/or that packages are not arriving (inject 6)

- Does your organization have a prepared communications statement for the customer services department?
- What should the operations team tell the customer?
- As the calls become more frequent, call centers are having difficulty handling the volume of calls coming in. Do you have a plan to expand call center capacity?

A picture of the ransomware screen on a company device goes public on social media. A news agency contacts your organization asking for a comment. (Inject 7)

- Does your organization have a prepared communications statement for the media representative?
- Who is authorized to speak on behalf of the company?
- What should folks authorized to speak to the news agency say?

Inject 8 – News Article & loss of phone systems and corporate website – Pass out 15 Minutes after Injects 6 & 7.

- How you communicate with the teams to find out status and provide situation report/update?
- How do you communicate with your customers?
- ~~Does your organization have a prepared communications statement for the news agent?~~
- ~~Who is authorized to speak on behalf of the company?~~
- What should folks authorized to speak to the news agency say?

Background (Participant's Handbook)

The Help Desk receives a report of a system issue.

6. Session II – Inject #3

High-level scenario

Janet at the help desk receives a call from George who works at a loading dock. George is reporting that workstations in the loading docks are displaying messages asking for $500,000 in bitcoin.

Discussion questions

1. What should Janet do? What should George do?

2. What is the escalation protocol for incidents like this? What other business units become involved? Who gets the call?

3. What external parties does your organization reach out to?

4. Do you contact business partners? What business partners do you reach out to? Do you have an offline backup of critical contacts?

5. Do you contact customers at this time? If so, what do you tell them?

6. Does your organization have a policy regarding paying the ransom?

7. Session II – Inject #4

High-level scenario

Loaders and drivers at multiple locations are reporting that they are unable to access navigation data, route planning information, or cargo manifests. Operations have stalled and ground to a halt.

Discussion questions

1. What do you tell the drivers and loaders?

2. Does your organization have a continuity of operations or operations resiliency plan?

3. What are the essential services needed to maintain a diminished operating capacity?

4. Does your organization have a plan to procure hardware and software services to maintain critical functionality?

8. Session II – Inject #5

High-level scenario

Ransomware has taken hold in enterprise servers. Internal and external sites are experiencing major disruptions and not functioning. Enterprise email is no longer functioning.

Discussion questions

1. How does your organization communicate and coordinate containment and recovery?

2. What is the first string of response? Who makes the call? At what point is senior management involved?

3. What external parties (if any) does your organization reach out to? What law enforcement organizations does your company reach out to?

4. Who does your organization appoint to manage parallel efforts and prioritize the response process?

5. Does your organization take any systems offline? Which systems?

9. Session II – Inject #6

High-level scenario

Disgruntled customers are calling in to your customer support office and complaining that deliveries are not arriving and tracking information is no longer available.

Discussion questions

1. Does your organization have a prepared communications statement for the customer services department?

2. What should the operations team tell the customer?

3. As the calls become more frequent, call centers are having difficulty handling the volume of calls coming in. Do you have a plan to expand call center capacity?

10. Session II – Inject #7

High-level scenario

A picture of a ransomware screen on a company branded device goes public on social media and a news agency contacts your organization seeking a comment.

NOTE: For this portion of the exercise, please imagine that the embedded articles below relate to transportation companies and the screen shots appear as in the high-level scenario described. Sometimes, particularly for organizations with global reach, the first social media or media reports may not be posted in English.

Twitter post by a Cyber Security Consultant of a screen shot reportedly taken by an Everis employee

Discussion questions

1. Does your organization have a prepared communications statement for the customer services department?

2. Who is authorized to speak on behalf of the company?

3. What should folks authorized to speak to the news agency say?

11. Session II – Inject #8

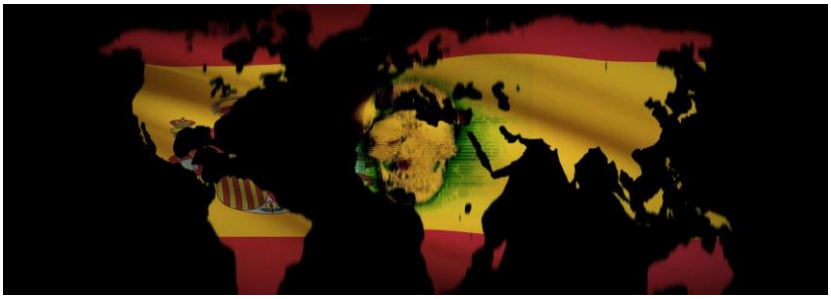
High-level scenario

A social media report of an alleged ransomware attack on your company is picked up by mainstream media before your company has decided whether the attack should be publicly acknowledged. At this time, the attack is still spreading across multiple departments and locations, the infection mechanism remains unknown and the impact cannot be fully assessed. Your company is still deciding who, if anyone, is authorized to speak on this issue. A news agency contacts your organization seeking a comment. Phone systems and the corporate website are no longer available.

NOTE: For this portion of the tabletop exercise, please assume that a news story was released based on the initial social media post above as the source report of the alleged ransomware infection. Please assume the story is updated throughout the day and is picked up by other media sources.

https://www.bleepingcomputer.com/news/security/ransomware-attacks-hit-everis-and-spains-largest-radio-network/

Ransomware Attacks Hit Everis and Spain's Largest Radio Network
By Sergiu Gatlan
November 4, 2019 12:56 PM



Everis, an NTT DATA company and one of Spain's largest managed service providers (MSP), had its computer systems encrypted today in a ransomware attack, just as it happened to Spain's largest radio station Cadena SER (Sociedad Española de Radiodifusión).

While the ransomware attacks were not yet publicly acknowledged by the company, the ransom note left on Everis' encrypted computers has already leaked and BleepingComputer can confirm that the MSP's data was infected using the BitPaymer ransomware.

BitPaymer used in MSP attack
After the attack began, Everis sent an internal notification saying that they "are suffering a massive virus attack on the Everis network. Please keep the PCs off."

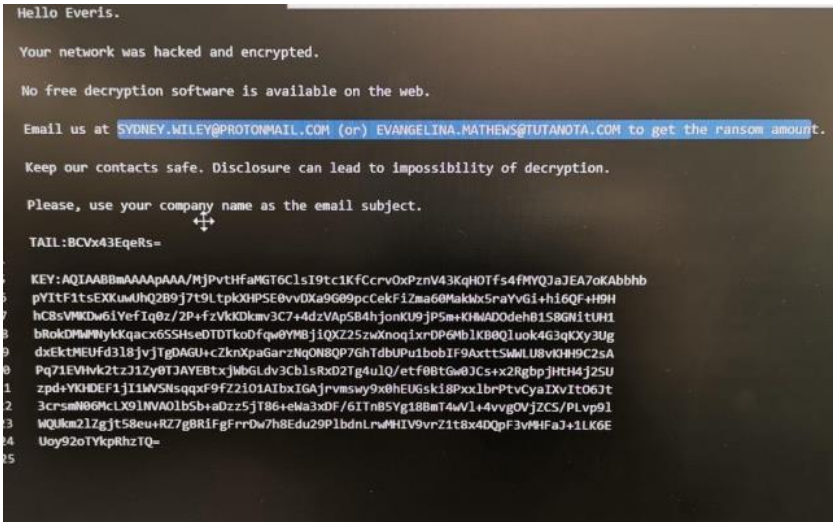
"The network has been disconnected with clients and between offices. We will keep you updated. Please, send urgently the message directly to your teams and colleagues due to standard communication problems," Everis added.

> Esta parece ser la nota que everis ha mandado a sus trabajadores.
> #ransomware pic.twitter.com/1UOT8jDO4s
> — Arnau Estebanell Castellví (@ArnauEstebanell) November 4, 2019

The ransomware encrypted files on the company's systems using the .3v3r1s extension, further exposing the targeted nature of this attack against the MSP.

The ransom note that got planted on Everis' encrypted systems warns the company against disclosing the incident while also providing it with contact details "to get the ransom amount." The email contacts listed in the ransom note are sydney.wiley@protonmail.com and evangelina.mathews@tutanota.com, but these change per targeted attack.

The attackers asked Everis for a €750,000 ($835,923) ransom to get a decryption key to unlock their files as reported by bitcoin.es.



Everis ransom note (*Alex Barredo*)

Unknown ransomware encrypts radio's systems

Everis was not alone in getting hit by a ransomware attack today as Cadena SER, the largest radio station network in Spain, was also hit by an unknown ransomware.

"The SER chain has suffered this morning an attack of computer virus of the ransomware type, file encrypter, which has had a serious and widespread affectation of all its computer systems," Cadena SER says in a notification published today.

Following the attack that used an unknown ransomware strain, the radio station had to disconnect all of its computers from the Internet and it is currently continuing activity with the help of equipment at its Madrid headquarters.

"The technicians are already working for the progressive recovery of the local programming of each of their stations," Cadena SER adds.

Spain's Department of Homeland Security (Departamento de Seguridad Nacional) also confirmed the ransomware attack that impacted Cadena SER as did Spain's INCIBE (Instituto Nacional de Ciberseguridad).
INCIBE is currently helping the radio station to restore their encrypted data and get their systems back online.

Possible MSP downstream attacks
A tactic more commonly being used by ransomware attackers is to target MSPs and use their management software to push the ransomware down to the MSPs' clients.

While it is not known if these are unrelated cyberattacks, cybersecurity consultant Arnau Estebanell Castellví implied that Everis may have been the source. According to a tweet by Castellví, Orange cut off Everis' access to the network in order to prevent the ransomware attack from affecting them.

> Trabajadores de @orange_es me confirman que ellos tampoco han sido afectados por el ataque. Lo único que se ha hecho es cortar acceso a @everis y se estan tomando medidas preventivas. De momento las cosas funcionan con normalidad.
> — Arnau Estebanell Castellví (@ArnauEstebanell) November 4, 2019

BleepingComputer has not been able to independently corroborate this statement.

BlueKeep potentially exploited in the attacks
BleepingComputer has learned from a source close to one of the attacks who wishes to remain anonymous that the BlueKeep vulnerability is reportedly involved in these attacks.

Furthermore, in light of the BlueKeep mass exploitation discovered over the weekend, some say [1, 2] that this vulnerability was leveraged in today's ransomware attacks against Spanish organizations but there is no clear evidence to support this theory.

The BlueKeep exploitation attempts have been recorded by security expert Kevin Beaumont's honeypots that expose only the 3389 port used for remote assistance connections via the Remote Desktop Protocol (RDP).
Beaumont also found today that Everis has hundreds of servers directly exposed to Internet connections, something that hints at the possibility of the rumors of BlueKeep exploitation in today's ransomware attacks being true.

> Oh boy, these guys appear to have hundreds of RDP servers directly on the internet HT @binaryedgeio data pic.twitter.com/d7wGjP4J6S
> — Kevin Beaumont (@GossiTheDog) November 4, 2019

Castellví told BleepingComputer that, while "nothing is confirmed right now", Everis' internal network being down could be explained through exploiting BlueKeep or the other two RDP vulnerabilities patched some time ago.

"I think the initial vector might be email. That is what the Spanish National Security Center has said," he added. "But after patient 0, I also think it is RDP-based. If not, there is no explanation of why the internal network of Everis is down."

Whether BlueKeep was actually involved is not yet clear at this point.

Bleeping Computer asked CERT Spain, Everis, and SER for more details but did not hear back at the time of publication.

Update November 04, 13:07 EST: Added comments from cybersecurity consultant Arnau Estebanell Castellví.

Discussion questions

1. How you communicate with the teams to find out status and provide situation report/update?

2. How do~~s~~ you communicate with your customers?

~~3. Does your organization have a prepared communications statement for the news agent?~~

~~4. Who is authorized to speak on behalf of the company?~~

~~5~~3. What should folks authorized to speak to the news agency say?

12. Session III – Background (90 minutes)

Background (Facilitator's Handbook only)

Session 3 "Restore" – This session explores the next few days after the incident. A remediation solution becomes available from a partner (EG US-CERT, FBI or similar). The players will explore implementing the patch/solution and restoring customer confidence damaged by incident.

Time Budget = 15-30 minutes per discussion area based on participant engagement and overall session time constraints. Suggested times in red below.

Facilitator's notes/discussion prompts (Facilitator's Handbook only)

Inject 9 - Online backups are encrypted and it is not possible to roll-back to a previous version Pass out at beginning of session

- Do you have cold offline backups? Who manages them?
- Do you have a continuity of operations site?
- Has your organization identified the most critical systems to prioritize for recovery? Does your organization have a procedure to get the most critical systems up and running?
- Does your company have access to backups of critical firmware for devices? Who has it and where can you get it?

Inject 10 - Next Day Communications Strategy Pass out 20 minutes after Inject #9

- How does the organization respond to ongoing inquiries? Who is the point person for messaging?
- ~~Who is authorized to speak for the organization? Do you assign different people from multiple parts of the organization?~~
- How do you ensure the messaging is consistent across the organization both internally and externally? How are updates communicated?

Inject 11 - NCCIC / FBI / Vendor releases a remediation of some kind Pass out ~~25~~5 minutes after Inject #10 of exercise

- How does this information get to your organization? What information sharing channels do you have available?
- What changes has your organization made since the attack? Were any temporary measures put in place during attack or recovery that have been made or should be made permanent? Who is involved in the decision-making?
- Who is responsible for determining a deployment schedule?
- When does the deployment start? What are the operational impacts of patching?
- When does your management learn about the remediation?

Inject 12 - After you have recovered, sales informs you that long-time clients have begun to use competitors citing a lack of confidence Pass out with 30 minutes remaining (~15 minutes after Inject #11)

- How does your organization respond? Who is involved in assessing the impact of the attack?
- Who is involved in deciding what messaging should be communicated internally and externally? How is the response coordinated?
- How do you track ongoing impacts of the attack on your business?
- Are any changes made to the IT budget or other investment decisions, such as cyber insurance?

Background (Participant's Handbook)

The attack has been contained. The organization is now focused on recovery.

13. Session III – Inject #9

High-level scenario

Online backups are encrypted by the ransomware and your organization is unable to roll back workstations or servers to a prior good configuration.

Discussion questions

1. Does your organization have cold offline backups? Who manages them?

2. Does your organization have a continuity of operations hot site?

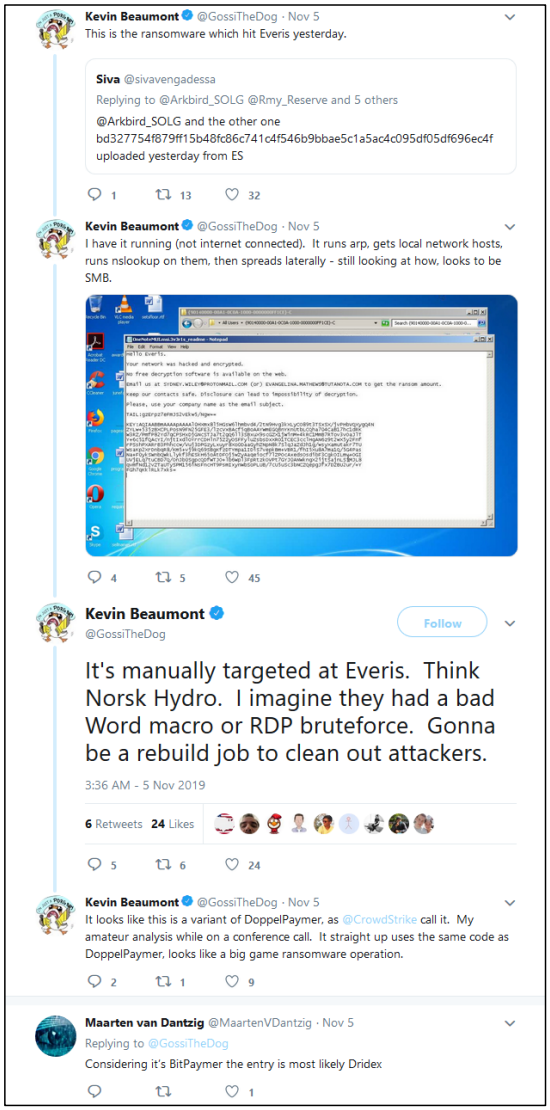
3. Has your organization identified the most critical systems to prioritize for recovery? Does your organization have a procedure to get the most critical systems up and running?

4. Does your company have access to backups of critical firmware for devices? Who has it and where can you get it?

14. Session III – Inject #10

High-level scenario

The next day, some functionality has been restored. The attack has been contained. Impact is still being assessed. The ransomware attack has been widely reported on social media and in mainstream news. Awareness of the attack is spreading among customers, suppliers and industry competitors. Many professional and amateur cyber security experts and hackers are speculating about the attack – entry methods, impact, ransomware variant, current state of recovery, etc.



Discussion questions

1. How does the organization respond to ongoing inquiries? Who is the point person for messaging?

~~2. Who is authorized to speak for the organization? Do you assign different people from multiple parts of the organization?~~

3. How do you ensure the messaging is consistent across the organization both internally and externally? How are updates communicated?

15. Session III – Inject #11

High-level scenario

Time skip ahead 3 days. A federal partner has discovered and published a remediation for the ransomware which affected your organization.

Discussion questions

1. How does this information get to your organization? What information sharing channels do you have available?

2. What changes has your organization made since the attack? Were any temporary measures put in place during attack or recovery that have been made or should be made permanent? Who is involved in the decision-making?

3. Who is responsible for determining a deployment schedule for the remediation?

4. When does the deployment begin? What are the operational impacts of patching?

5. When does your management team learn about the remediation?

16. Session III – Inject #12

High-level scenario

Jordan from Sales informs the Board at a quarterly meeting that long time clients have started to use competitors, citing a lack of confidence in the organization and disruptions to their business as a result of shipping interruptions during the recent ransomware attack. News reporters continue to follow up to ask about the impact of the attack on your organization and the total cost of the attack.

Discussion questions

1. How does your organization respond? Who is involved in assessing the impact of the attack?

2. Who is involved in deciding what messaging should be communicated internally and externally? How is the response coordinated?

3. How do you track ongoing impacts of the attack on your business?

4. Are any changes made to the IT budget or other investment decisions, such as cyber insurance?

17. Hotwash/ Debrief (90 Minutes)

Background (Participant's Handbook)

Exercises afford organizations the opportunity to evaluate capabilities and assess progress toward meeting capability targets in a controlled, low-risk setting. After the evaluation phase concludes, organizations should reach consensus on identified strengths and areas for improvement and develop a set of improvements that directly assess core capability gaps. This information is recorded in the AAR/IP [After Action Report/Improvement Plan] and resolved through the implementation of concrete correction actions, which are prioritized and tracked as part of a corrective action program. This process constitutes the improvement planning phase and the final step in conducting an exercise.[1]

Discussion questions (Participant's Handbook)

1. What went right?

2. What changes need to be made to plans and procedures to improve incident response?

3. What changes to equipment or resources are needed to improve performance?

4. What training is needed to improve performance?

5. What are the lessons learned for approaching similar problems in the future?

Follow-up (Participant's Handbook)

The identification of strengths, areas for improvement and corrective actions that result from exercises help organizations build capabilities as part of a larger continuous improvement process.[2]

Each identified improvement should be turned into an organizational goal/action item for the group responsible for delivering the solution. When developing solutions, consider:

1. What are the possible short- and long-term steps that can be taken to resolve this?

2. What will yield the best results?

3. What will work the fastest?

4. What will use the least resources?[3]

[1] https://www.fema.gov/media-library-data/20130726-1914-25045-8890/hseep_apr13_.pdf
[2] https://www.fema.gov/media-library-data/20130726-1914-25045-8890/hseep_apr13_.pdf
[3] https://trainingtools.files.wordpress.com/2010/04/ebook-hotwash.pdf

18. Template: FEMA Hot Wash Form

The below template may be useful to participants to record notes from the hotwash/debrief discussion and/or to record follow-up actions for their own organizations following the tabletop exercise.

See
https://training.fema.gov/is/flupan/references/02_course%20forms%20and%20templates/02_hot%20wash%20form-508.pdf

This form is to be used by the Facilitator to conduct the Hot Wash for the exercise Determined Accord tabletop exercise (TTX). Use this form to record the top three strengths and the top three items requiring improvement as observed during the exercise.

Additional comments and discussions recorded during the Hot Wash will be recorded on in the comments section of the form.

Upon completion of the exercise, combine this form with the Participant Questionnaires, the completed AAR/IP, and attendance rosters. This post exercise packet is used as support documentation in Test, Training, and Exercise (TT&E) files and the Corrective Action Program.

FEMA

HOT WASH REPORT FORM

Exercise Determined Accord

DATE: _____

Name:		**Evaluated Organization:**	
Email:		**Staff/Section:**	
Telephone:		**Role in Exercise:**	

List the top three (3) organizational strengths:
1.)
2.)
3.)

FEMA

List the top three (3) items requiring improvement:
1.)
2.)
3.)

FEMA

Hot Wash Remarks/Comments:

19. Template: After Action Report (Facilitator's Handbook only)

See https://www.in.gov/dhs/files/AAR-IP_Template_Apr-13-2_Clean.docx

Exercise Name]

After-Action Report/Improvement Plan

[Date]

The After-Action Report/Improvement Plan (AAR/IP) aligns exercise objectives with preparedness doctrine to include the National Preparedness Goal and related frameworks and guidance. Exercise information required for preparedness reporting and trend analysis is included; users are encouraged to add additional sections as needed to support their own organizational needs.

Exercise Overview

Exercise Name	[Insert the formal name of exercise, which should match the name in the document header]
Exercise Dates	[Indicate the start and end dates of the exercise]
Scope	This exercise is a [exercise type], planned for [exercise duration] at [exercise location]. Exercise play is limited to [exercise parameters].
Mission Area(s)	[Prevention, Protection, Mitigation, Response, and/or Recovery]
Core Capabilities	[List the core capabilities being exercised]
Objectives	[List exercise objectives]
Threat or Hazard	[List the threat or hazard (e.g. natural/hurricane, technological/radiological release)]
Scenario	[Insert a brief overview of the exercise scenario, including scenario impacts (2-3 sentences)]
Sponsor	[Insert the name of the sponsor organization, as well as any grant programs being utilized, if applicable]
Participating Organizations	[Insert a brief summary of the total number of participants and participation level (i.e., Federal, State, local, Tribal, non-governmental organizations (NGOs), and/or international agencies). Consider including the full list of participating agencies in Appendix B. Delete Appendix B if not required.]
Point of Contact	[Insert the name, title, agency, address, phone number, and email address of the primary exercise POC (e.g., exercise director or exercise sponsor)]

Analysis of Core Capabilities

Aligning exercise objectives and core capabilities provides a consistent taxonomy for evaluation that transcends individual exercises to support preparedness reporting and trend analysis. Table 1 includes the exercise objectives, aligned core capabilities, and performance ratings for each core capability as observed during the exercise and determined by the evaluation team.

Objective	Core Capability	Performed without Challenges (P)	Performed with Some Challenges (S)	Performed with Major Challenges (M)	Unable to be Performed (U)
[Objective 1]	[Core capability]				
	[Core capability]				
[Objective 2]	[Core capability]				
[Objective 3]	[Core capability]				

Ratings Definitions:

- Performed without Challenges (P): The targets and critical tasks associated with the core capability were completed in a manner that achieved the objective(s) and did not negatively impact the performance of other activities. Performance of this activity did not contribute to additional health and/or safety risks for the public or for emergency workers, and it was conducted in accordance with applicable plans, policies, procedures, regulations, and laws.
- Performed with Some Challenges (S): The targets and critical tasks associated with the core capability were completed in a manner that achieved the objective(s) and did not negatively impact the performance of other activities. Performance of this activity did not contribute to additional health and/or safety risks for the public or for emergency workers, and it was conducted in accordance with applicable plans, policies, procedures, regulations, and laws. However, opportunities to enhance effectiveness and/or efficiency were identified.
- Performed with Major Challenges (M): The targets and critical tasks associated with the core capability were completed in a manner that achieved the objective(s), but some or all of the following were observed: demonstrated performance had a negative impact on the performance of other activities; contributed to additional health and/or safety risks for the public or for emergency workers; and/or was not conducted in accordance with applicable plans, policies, procedures, regulations, and laws.
- Unable to be Performed (U): The targets and critical tasks associated with the core capability were not performed in a manner that achieved the objective(s).

Table 1. Summary of Core Capability Performance

The following sections provide an overview of the performance related to each exercise objective and associated core capability, highlighting strengths and areas for improvement.

[Objective 1]

The strengths and areas for improvement for each core capability aligned to this objective are described in this section.

[Core Capability 1]

Strengths

The [full or partial] capability level can be attributed to the following strengths:

Strength 1: [Observation statement]

Strength 2: [Observation statement]

Strength 3: [Observation statement]

Areas for Improvement

The following areas require improvement to achieve the full capability level:

Area for Improvement 1: [Observation statement. This should clearly state the problem or gap; it should not include a recommendation or corrective action, as those will be documented in the Improvement Plan.]

Reference: [List any relevant plans, policies, procedures, regulations, or laws.]

Analysis: [Provide a root cause analysis or summary of why the full capability level was not achieved.]

Area for Improvement 2: [Observation statement]

Reference: [List any relevant plans, policies, procedures, regulations, or laws.]

Analysis: [Provide a root cause analysis or summary of why the full capability level was not achieved.]

[Core Capability 2]

Strengths

The [full or partial] capability level can be attributed to the following strengths:

Strength 1: [Observation statement]

Strength 2: [Observation statement]

Strength 3: [Observation statement]

Areas for Improvement

The following areas require improvement to achieve the full capability level:

Area for Improvement 1: [Observation statement. This should clearly state the problem or gap; it should not include a recommendation or corrective action, as those will be documented in the Improvement Plan.]

Reference: [List any relevant plans, policies, procedures, regulations, or laws.]

Analysis: [Provide a root cause analysis or summary of why the full capability level was not achieved.]

Appendix A: Improvement Plan

This IP has been developed specifically for [Organization or Jurisdiction] as a result of [Exercise Name] conducted on [date of exercise].

Core Capability	Issue/Area for Improvement	Corrective Action	Capability Element[4]	Primary Responsible Organization	Organization POC	Start Date	Completion Date
Core Capability 1: [Capability Name]	1. [Area for Improvement]	[Corrective Action 1]					
		[Corrective Action 2]					
		[Corrective Action 3]					
	2. [Area for Improvement]	[Corrective Action 1]					
		[Corrective Action 2]					

[4] Capability Elements are: Planning, Organization, Equipment, Training, or Exercise.

Appendix B: Exercise Participants

Participating Organizations
Federal
State
[Jurisdiction A]
[Jurisdiction B]