GMU cyber resilience center

Dr. Jean-Pierre Auffret

Vu Nguyen

Tabletop Exercise Package: Ransomware & Water and Wastewater Incident

Overview:

Exercise name: Cybersecurity desktop exercise.

Purpose:

They are designed to test if the organization's Incident response capabilities are up to a real attack. It is a cyber security drill scenario, and you will be able to see how well your key Incident Response stakeholders will handle and response to a real attack situation.

Focusing on 2 aspect:

- Cyberattack on IT administration system
- Cyberattack on operation system

Objective

1. Examine the **response capabilities** of cybersecurity team during a significant cyber incident.

2. Evaluate the ability for cyber threat response team to **coordinate information** sharing during a significant cyber incident.

3. Identify **areas of improvement** in cyber incident response plans and overall organizational resilience during and following a significant cyber incident.

4. Explore the organizations **plans to recover** and restore services, mission critical assets, or systems.

5. Highlight for the **water utility** cybersecurity team

General Information

- Increase organization’s resilience by assessing and validating capabilities and identifying areas for improvement.

- Define cyber resilience as “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources”.

Structure: Module

Module 1: Threat and Initial Incident

Module 2: Incidents

- Administrative system
- Operation system

Module 3: Post Incidents

- Company Recovery
- Customer Recovery

Structure: Appendix

_**Appendix A:** Additional discussion questions that can replace or augment the existing Module 1 and 2 discussion questions.

_**Appendix B:** Reference section for acronyms used within this situation manual.

_**Appendix C**: Case studies that provide real-world examples of the threats presented in this scenario.

_**Appendix D:** An explanation of the threats presented in this scenario.

_**Appendix E**: Additional cybersecurity preparedness and response resources

Let’s Get started: Guideline

- This exercise is intended to be held in an open, no-fault environment. Varying viewpoints are expected.

- Respond to the scenario utilizing your knowledge of existing plans and capabilities, along with the valuable insights derived from your training and experience.

- 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, possible solutions, and suggested actions to resolve or mitigate a problem.

- There is no hidden agenda, and there are no trick questions. The resources and written materials provided are the basis for discussion. In any exercise, assumptions and artificialities are necessary to complete play within the given time, achieve training objectives, and account for logistical limitations. Please do not allow these factors to negatively impact your participation in the exercise.

Module 1: Day 1

_The Cybersecurity and Infrastructure Security Agency (CISA) issues an Alert regarding a new ransomware variant.

_This ransomware is being used in a campaign targeting local water utility.

Module 1: Day 2

_It has been one year since the developer of your current operating system announced that they will no longer develop security patches for your operating system.

_The final security patch was installed last week. This vulnerability was identified in your recently completed annual risk assessment.

Module 1: Day 3 - 4

_An employee informs their manager that their work laptop was stolen from their car overnight. The laptop contained sensitive organizational information.

Module 1: Day 5 - 6

_Members of your Financial department receive an email that appears to be from the Vice President of the department.

_It instructs them to access a PDF containing details about an unpaid bill from a third-party vendor supporting your organization.

_Several employees call the Vice President to verify the email’s authenticity.

_They replies that they did not send it, and that there is no outstanding vendor bill. Nevertheless, some employees still open the PDF

Module 1: Questions

1. What are the greatest cyber threats to your organization?

2. What information technology (IT) systems or processes are the most critical to your organization?

3. What cybersecurity threat information does your organization receive?
   a. What cyber threat information is most useful?
   b. How is information disseminated across your organization and by whom?
   c. What actions would your organization take following an alert like the one presented in the scenario?

Module 1: Questions

4. Has your organization conducted a risk assessment to identify specific cyber threats, vulnerabilities, and critical assets?

   a. What information technology (IT) systems or processes are the most critical to your organization?

   b. Describe your organization’s asset management plan and how you prioritize critical assets.

   c. What improvements have been implemented to enhance cyber resilience following recent risk assessments?

   d. Does your organization have a vulnerability management program dedicated to mitigating known exploited vulnerabilities in internet-facing systems?

Module 1: Questions

5. Does your organization have backups of vital records stored in a location separate from your primary working files/copies?
    a. How frequently do you run backups?
    b. How long do you keep copies of archived files backed up?
    c. How long would it take to restore primary files from backups?
6. Discuss your risk management strategy.
    a. How is it developed/maintained?
    b. Does your organization apply Zero Trust Architecture (ZTA)/zero-trust concepts?
    c. What considerations are addressed in your risk management strategy (e.g., extended downtime, impaired functionality, loss of data, etc.)?

Module 1: Questions

7. Describe your organization’s cybersecurity training program for employees.

   a. How often are employees required to complete this training?

   b. Is training required during employee onboarding before granting system/network access?

   c. What additional training is required for employees who have system administrator-level privileges?

   d. What type of training methods or approaches have you found most beneficial?

8. How do employees report suspected phishing attempts or other possible cybersecurity incidents?

   a. What actions does the IT department take when suspicious emails are reported?

   b. What feedback do employees receive after reporting a suspicious email or event?

Module 2: Day 7

_An increase in **Domain Name System** (DNS) traffic outside of standard business hours is flagged by your organization’s intrusion detection system and an alert is sent to your Security Operation center.

_Upon further investigation of the system logs, they discover that a significant amount of data was sent from known HR employee IP addresses to external IP addresses.

Module 2: Day 8 - 9

_Computers throughout your organization display a blank red screen. A ransom message then appears demanding **$53,000.00 worth of Bitcoin** for the decryption key and a warning that the key will expire unless payment is received within 48 hours.

Module 2: Day 10

_A security researcher uncovers a series of posts from a well-known **hacker** group on the Dark Web and contacts your organization.

_The researcher believes that the posts are genuine, and the threat actors gained access to PII, including employee social security numbers, bank account and routing number information.

_The hacker group shared a limited number of data records to substantiate their claims and assert their intention to **sell the data**.

Module 2: Questions

1. Discuss your organization’s cyber resilience planning.

    a. What information technology (IT) infrastructure has been identified to support mission essential functions in continuity of operations and incident response plans?

    b. How has your organization prioritized IT infrastructure for restoration?

    c. How has cybersecurity been integrated into your continuity plans?

Module 2: Questions

2. How does your organization baseline network activity?

    a. How can you distinguish between normal and abnormal traffic?

3. Utilizing your organization’s cyber incident response plan (CIRP), describe the actions that your organization would take at this time.

    a. Describe the training your employees receive on this plan.

    b. What guidance does the plan include on assessing the severity of the incident?

    c. How does incident severity level dictate response?

    d. How are critical systems and processes incorporated within your CIRP?

Module 2: Questions

4. What redundant systems exist for when primary systems are compromised?
    a. What alternative systems or manual processes are implemented to continue operations if a critical system is unavailable for a significant period?
    b. Who can authorize use of alternate systems or procedures?
    c. How long can you perform manual or alternate processes on your critical systems?
5. Explain your organization’s decision-making process regarding ransomware payment.
    a. Are ransomware policies/procedures included in your CIRP?
    b. Explain how your response partners, such as your cyber insurance provider or third-party vendors, are involved in your procedures.
    c. Discuss the advantages and disadvantages of either agreeing or refusing to pay.
    d. Discuss potential legal and reputational ramifications of paying or not paying the ransom.

Module 2: Questions

7. What capabilities and resources are required for responding to this scenario?

   a. What additional resources outside of your organization would be necessary for responding to the cyber incident?

   b. What are the processes or procedures for requesting additional resources?

   c. What external partners (e.g., CISA, FBI, etc.) would you contact for assistance?

Module 2: Day 11 - 12: **The Second Attack !!!**

_Media outlet in US report that an unknown group calling themselves “**Universal Adversary**”(UA) implemented a series of cyberattack against drinking water treatment facilities throughout UK.

_The attack cause errors and in some instance the incorrect application of chemicals to the water being treated.

_They declare that this is a **trial run** in preparation for larger attack against the area surround the **US Water Utilities.**

Module 2: The Second Attack: Questions

1. What is the process by which your organization would receive intelligence and protective measure information given the threat:
    a. What organiza to communicate (local law enforcement agencies, Joint Terrorism Task Force)
    b. Does your organization use Homeland Security Information Network
2. What internal information sharing and dissemination processes does your organization currently have in place
3. What resources are used to disseminate information
    a. What notification capabilities do you use to share information and communicate protective measures for implementation
4. If there is identified “suspicious behavior” observed at a water or wastewater facility, how do the facilities report this information locally.
5. What protective security measures or recommendation, if any, will be employed at your

Module 2: Day 13 :The Second Attack

_Wastewater treatment plants and potable water treatment plants across the US receive an **alert** from the U.S. Computer Emergency Response Team after domestic intelligence agencies report i**ncreased activity** on several hacker site.

_In early afternoon, several wastewater treatment plants report computer system **outrage** after an apparent power surge

_Automated operations at water treatment facilities are placed on hold until the nature of the power outage can be determined

_Several industry partners are observing unusual activity on the networks, and the pumps at a high capacity sewage pumping station cannot be reset remotely.

Module 2:The Second Attack: Question

1. What is the overall response to the water situation:
    a. What plans and procedures does your stakeholder group active when the water situation occurs
    b. How soon an utilities provide government agencies with an estimate of the number of customers that are affected by the large-scale disruption
    c. How soon an utilities provide government agencies with an estimate of the extend of the potential damage to their own systems.
    d. How are your organization cyber incident response and water emergency response plan linked? Are they linked to state and local response plans
2. Does your facility incident response plan contain protocols for properly responding to this and similar incidents described in the scenario update? What other protocols are included in the plan?

Module 2: The Second Attack: Question

3. What are the key messages that need to be communicated to the public from the organization’s perspective? From a government perspective?

4. What federal, state, local resources are available to support you response

   a. What coordination is occurring a the federal, state, local levels?

   b. What assets or resources are available to help you?

   c. Do you have mutual aid or other types of agreement with federal, state, local agencies to provide resource for emergency?

   d. How are information and updates communicated

Module 3: The Aftermath

_News outlets report on the cyber incident. Several news outlets contact your organization for comments on the ransomware infection and data breach.

_And the water companies are forced to issue “**Do no drink**” and “**Do not use**” order and to ask customers to limit flushing of toilets and greywater use until the outages can be resolve.

_Media report the public is **growing frustrated** with the water restrictions and are **losing faith** in the public water supply. Bottle water is selling out as soon as the shelves are stocked

_In some area the **fire department** has not had sufficient water pressure to combat structure fire

_Property damage has been significant as a result

Module 3: Question

1. Discuss your organization’s cyber resilience planning.

    a. What information technology (IT) infrastructure has been identified to support mission essential functions in continuity of operations and incident response plans?

    b. How has your organization prioritized IT infrastructure for restoration?

    c. How has cybersecurity been integrated into your continuity plans?

2. How does your organization baseline network activity?

    a. How can you distinguish between normal and abnormal traffic.

Module 3: Question

3. Utilizing your organization’s cyber incident response plan (CIRP), describe the actions that your organization would take at this time.

   a. Describe the training your employees receive on this plan.

   b. What guidance does the plan include on assessing the severity of the incident?

   c. How does incident severity level dictate response?

   d. How are critical systems and processes incorporated within your CIRP?

4. Explain your organization’s decision-making process regarding ransomware payment.

   a. Are ransomware policies/procedures included in your CIRP?

   b. Explain how your response partners, such as your cyber insurance provider or third-party vendors, are involved in your procedures.

   c. Discuss the advantages and disadvantages of either agreeing or refusing to pay.

   d. Describe the impact the sale or release of sensitive information or PII would have on your response and recovery activities.

   e. Discuss potential legal and reputational ramifications of paying or not paying the ransom.

Module 3: Question

5. Who are the key organizations involved in overseeing response and water restoration efforts, as well as the cyber incident?

a. What is the overall coordination or organizational structure for the response
b. Who are the key private stakeholders involved?
c. Who are the key government stakeholders involved?
d. How to utilities set up coordination and information exchange with response agencies?
e. How do government agencies roll up information about the incident across the region? Are there fusion centers available to facilitate information sharing?
f. What established procedures ensure the critical information is getting to the right decision makers
g. How would regional coordination begin between utilities?
h. How would regional coordination begin between jurisdictions across the region?

Appendix A: Additional Discussion Questions

The following section includes supplemental organizational resilience discussion questions designed to guide exercise play. Quick question about **your organization** and how it was/has been.

Appendix A: Cyber Resilience

1. What is your cyber incident management structure?

2. How often are your cybersecurity plans, policies, and procedures externally reviewed or audited?

    a. What were the most recent results and action items that followed?

3. Describe your organization’s review process for your CIRP.

    a. How often is the CIRP reviewed?

    b. Which individual(s) and department(s) are responsible for reviewing and updating the plan?

Appendix A: Employee Accounts & Privileges

1. Describe your organization’s employee off-boarding process

2. Describe your organization’s bring your own device (BYOD) policy

3. What are your organization’s policies or procedures for IT account management?

    a. What are the protocols for establishing, activating, modifying, disabling, and removing accounts?

Appendix A: Incident Identification

1. How are cyber incidents reported within your organization?
2. Discuss your organization’s intrusion detection capabilities and analytics that alert you to a potential cyber incident.

   a. What type of hardware/ software used?
3. Describe your organization’s ability to monitor the Dark Web.
4. How often is your organization’s data reviewed?

Appendix A: Incident Response

1. What are your processes for collecting evidence and maintaining the chain of custody during a cyber incident?

2. At what point in the scenario would you contact law enforcement?

    a. How would a law enforcement investigation impact containment, eradication, and recovery efforts?

    b. What are the processes and resources for evidence preservation and collection?

3. What are the processes for contacting critical personnel outside of core hours?

    a. How do you proceed if critical personnel are unreachable or unavailable?

4. Who is responsible for coordinating information across different organizational-level incidents?

Appendix A: Recovery

1. When does your organization determine a cyber incident is over?
    a. Who makes this decision?
2. What actions would your organization take if your IT/incident response staff could not confirm the integrity of your systems/data?

Appendix A: Training & Exercises

1. What training does your cybersecurity incident response team undergo to detect, analyze, and report malicious activity?
2. How often does your organization exercise its CIRP?
    a. What agencies are involved in the exercise?
    b. What level of the organization is required to participate?
3. How does your organization's training and exercise efforts address both physical and cyber risks?
    a. Have senior staff participated in a cybersecurity exercise?

Appendix A: Senior Leaders

1. As a leader in your organization, what cybersecurity resilience goals have you set?

2. What critical infrastructure does your organization own, operate, and/or regulate?

3. What cybersecurity training is required for senior leadership?

4. What is your role during a cyber incident?

Appendix A: Public information

1. What information are you sharing internally (e.g., employees, leadership)?

2. What information are you sharing externally (e.g., residents, customers, vendors)?

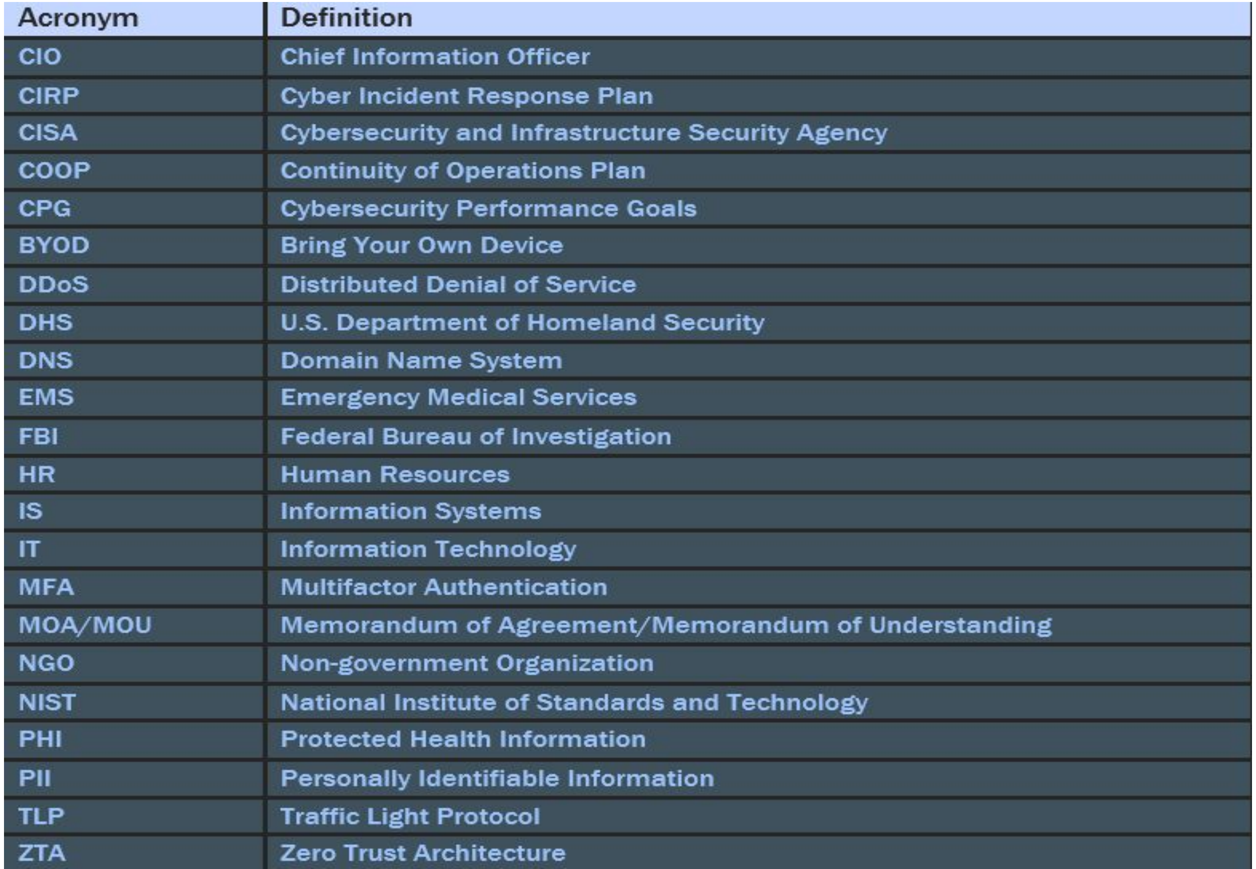
3. What training are employees given on reporting any contact with the media to the appropriate public information personnel?

4. How do you build and maintain trust with your customers and constituents?

Appendix A: Legal

1. What is the role of the legal department during a cyber incident?
    a. What issues need to be addressed based on the scenario?
2. What legal documents should your organization have for cyber incidents?

Appendix B: Acronyms



Acronym	Definition
CIO	Chief Information Officer
CIRP	Cyber Incident Response Plan
CISA	Cybersecurity and Infrastructure Security Agency
COOP	Continuity of Operations Plan
CPG	Cybersecurity Performance Goals
BYOD	Bring Your Own Device
DDoS	Distributed Denial of Service
DHS	U.S. Department of Homeland Security
DNS	Domain Name System
EMS	Emergency Medical Services
FBI	Federal Bureau of Investigation
HR	Human Resources
IS	Information Systems
IT	Information Technology
MFA	Multifactor Authentication
MOA/MOU	Memorandum of Agreement/Memorandum of Understanding
NGO	Non-government Organization
NIST	National Institute of Standards and Technology
PHI	Protected Health Information
PII	Personally Identifiable Information
TLP	Traffic Light Protocol
ZTA	Zero Trust Architecture

Appendix C: Case study

Iranian hacker group "CyberAv3ngers" allegedly breach Municipal Water Authority of Aliquippa (November 27, 2023)

In January 2022, a large county in the United States experienced a ransomware attack that took office computers and several department websites offline. This led to the closure of county offices for several days, during which the sheriff's department and Emergency Medical Services (EMS) relied on backup contingencies.[1] Notably, due to the ransomware attack, the local detention center lost access to its automated door and camera systems. Adding to the impact, a sum of $191,000 worth of employee laptops was reported as damaged.[2]

County representatives declared their decision not to pay the ransom demands. Instead, they utilized their cyber insurance coverage to aid in recovery processes.[3] Subsequently, the county's Chief Information Officer (CIO) announced the implementation of multifactor authentication (MFA) for all users, aiming to enhance security controls. In response to the incident, the county commission purchased a new cybersecurity policy.

Appendix D: Attacks and Threat

Ransomware

Ransomware is a type of malware that denies access to victims' data or systems through encryption with a key only known by the malicious actor who deployed the malware. Once encrypted, the ransomware directs the victim to pay the attacker, typically in the form of cryptocurrency, so the victim can receive a decryption key. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website. Ransomware and associated data breach incidents can severely impact business processes, leaving organizations unable to access data necessary to function. The economic and reputational impacts of ransomware and data extortion have proven challenging and costly for organizations of all sizes throughout the initial disruption and, at times, extended recovery. Recovery can be an arduous process and there is no guarantee the victim will receive access to their data or systems if the ransom is paid. For more information on best practices to protect users from the threat of ransomware, as well as recent Alerts on specific ransomware threats, see the resource list below.

Social Engineering and Phishing

One of the most prominent tactics attackers use to exploit network and system vulnerabilities is social engineering, which is the manipulation of users through human interaction and the formation of trust and confidence to compromise proprietary information. Techniques for uncovering this information largely involve the use of phishing, i.e., email or malicious websites that solicit personal information by posing as a trustworthy source. Social engineering is effective for breaching networks and evading intrusion detection systems without leaving a log trail, and it is completely dependent on the operating system platform. While technical exploits aim to bypass security software, social engineering exploits are more difficult to guard against due to the involvement of human emotions. Organizations should take steps towards strengthening employee cybersecurity awareness training by incorporating trainings on identifying suspicious emails, instructing personnel on how to report them, and emphasizing the importance of keeping software systems up to date.

Appendix E: Preparation

1. Data Security

How secure is your data? Whether it's financial information, employee data, or your customers' sensitive health information, attackers want access. This is why it's so critical for organizations to take data security seriously.

Follow data security best practices like:

- Encryption
- Anti-virus, firewall, and anti-malware solutions
- Archiving or deleting data

… to prevent attackers from accessing personally identifiable information and sensitive organizational data.

2. Backups and Disaster Response

_It’s always a good idea to have backups and a disaster response playbook in place to minimize the damage of a cyberattack.

_Backup all of your data, both in online and offline formats. These backups should run on a regular basis and cover all of your data, applications, and servers. Your IT team should also practice how to restore that data, so you’re sure that your backup protocols actually work.

_Beyond regular backups, it’s essential to have a disaster response plan in place. This should cover situations such as ransomware or a data breach, as well as natural disasters.

_If you already have a disaster response plan, make sure it follows the new reporting requirements of the Cyber Incident Reporting for Critical Infrastructure Act.

3. Employee Cyber Awareness Training

More than 40% of all data breaches happen because of employee oversight. Even the most sophisticated security infrastructure can't work if your employees click on a malicious link.

To prevent cyber attacks, it's critical to train employees on IT security best practices, including:

- How to spot phishing
- How to report suspicious activity
- Mobile security and remote access protocols
- Physical security measures, like locking laptops at night

While many of these measures sound like common sense, breaches commonly happen because of employee behavior. It's also a good idea to conduct phishing tests to keep your employees on their toes at all times.

Appendix E: Preparation

4. Access Management

_Who has access to your information? If an attacker gains access to an employee's account, how much damage can they do?

_Access management is essential for protecting your organization. This means granting access on a need-to-know basis. Only a handful of employees should have access to your organization's critical data.

_It's also important to do proper credential management with your team. Ask employees to frequently change their passwords. You can also require them to create a unique, strong password for every login. Do a complete audit of your organization to ensure that no employees are sharing logins or passwords.

Appendix E: Preparation

5. Updates and Patches

_Every software solution will develop some type of vulnerability over time, and hackers have made it their mission to find these weaknesses.

_This is why it's so critical for organizations to regularly patch their software and check for updates. Work with a provider like Dice to automatically update your solutions so attackers can't exploit known vulnerabilities.

6. Use the Microsoft Secure Score Tool

There are so many robust tools available to your organization for preventing cyber attacks.

Microsoft Secure Score is an effective tool that’s perfect for organizations using Office 365. Keep in mind that your users will need global admin rights in Office 365 to fetch results from Secure Score.

With Secure Score, you can:

- Access a high-level report on your security posture
- Set benchmarks and KPIs
- Discover potential vulnerabilities

With scoring tools, you can stay active and mitigate risks, reducing your attack surface at every turn.

Appendix F: Contact and Resource

Federal Government Resources

- CISA (contact: central@cisa.gov, https://www.cisa.gov)
- United States Secret Service (USSS) Field Offices and Electronic Crimes Task Forces (ECTFs) (contact https://www.secretservice.gov/contact/field-offices, https://www.secretservice.gov/investigation/cyber)
- Federal Bureau of Investigation (FBI)
- Field Office Cyber Task Forces (contact: https://www.fbi.gov/contact-us/field-offices)
- Internet Crime Complain Center (IC3) (contact: http://www.ic3.gov)
- National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center (contact: cywatch@ic.fbi.gov; 855-292-3937)

Appendix F: Contact and Resource

State Level Resources

- Multi-State Information Sharing and Analysis Center (MS-ISAC) (contact: info@msisac.org; 518-266-3460)
- National Governors Association (NGA) (https://www.nga.org/)
- NGA Center for Best Practices (https://www.nga.org/bestpractices/divisions/hsps/)
- DHS Cybersecurity Fusion Centers (https://www.dhs.gov/state-and-major-urban-area-fusion-centers)
- National Association of State Chief Information Officers (NASCIO) (https://www.nascio.org/)

Appendix F: Contact and Resource

Private Sector/Business Resources

- InfraGard (https://www.infragard.org/Files/InfraGard_Redesign_2-24-2022.pdf)
- Internet Security Alliance (https://isalliance.org/)
- Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) (https://www.isao.org/information-sharing-groups/)
- International Association of Certified ISAOs (http://www.certifiedisao.org; contact: operations@certifiedisao.org)
- National Council of ISACs (https://www.nationalisacs.org)

Appendix F: Contact and Resource

Preparedness Resources

- CISA Cross-sector Cybersecurity Performance Goals (https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist)
- NIST Cybersecurity Framework Tools (https://csf.tools/)
- Ransomware:
- CISA Stop Ransomware Website (https://www.cisa.gov/stopransomware)
- CISA Stop Ransomware Guide (https://www.cisa.gov/resources-tools/resources/stopransomware-guide)
- Protecting Against Ransomware (https://www.cisa.gov/news-events/news/protecting-against-ransomware)