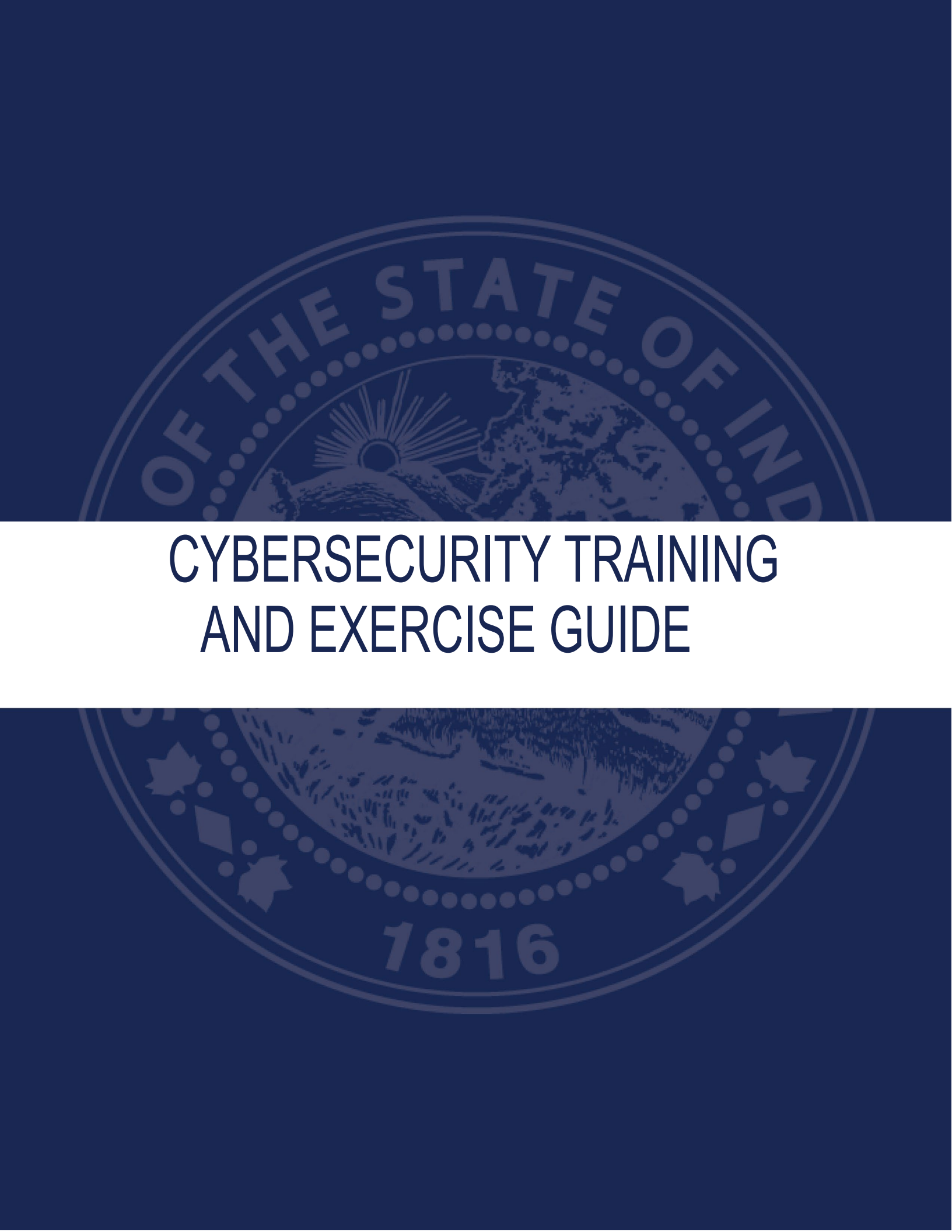

CYBERSECURITY TRAINING AND EXERCISE GUIDE

CYBERSECURITY TRAINING AND EXERCISE GUIDE

Table of Contents

I. Introduction

A. Purpose

As part of an all-hazards approach to emergency management, the *Cybersecurity Training and Exercise Guide* provides general information and instructions for establishing and implementing an effective cybersecurity training and exercise program.

The contents of this Guide are intended to align state and federal emergency management training and exercise requirements with cybersecurity training and education standards established by the National Institute of Standards and Technology (NIST). In addition to NIST, this Guide incorporates concepts and elements from the Homeland Security Exercise and Evaluation Program (HSEEP), National Incident Management System (NIMS), Emergency Management Accreditation Program (EMAP), and National Fire Protection Association (NFPA).

B. Scope

The Guide is intended for emergency managers in municipal, county, and local government agencies. It may also be useful to individuals responsible for emergency preparedness and business continuity functions in other public sector, private sector, healthcare, and academic organizations. Moreover, this guide can be a good primer for technology directors who are working with emergency managers or are put in charge of their organization's cyber incident response planning, training, and exercising.

There are a wide variety of potential cyber threats and a constantly evolving list of methods and tactics used to conduct cyberattacks. The training and exercise activity outlined here is focused on cyber incidents that may:

- Pose an immediate threat to public health, safety, and security;
- Impact or disrupt the delivery of essential government and social services; or
- Require a coordinated, multi-agency, multi-disciplinary response

C. Situation

Cybersecurity incidents and cyberattacks on computers, information networks, and communications systems are now part of the complex threat environment emergency managers must face.

In the State of Indiana, numerous high-profile cyberattacks have occurred in recent years. Targets of these attacks included government agencies, healthcare facilities, community organizations, businesses, school systems, and universities. Attacks have occurred in every region of the state and affected communities and organizations large and small, rural, and urban.

Most of these incidents have involved the theft of sensitive data or ransomware attacks. These incidents had significant financial and public relations impacts but did not pose an immediate safety threat. However, cyberattacks are increasingly targeting critical infrastructure sectors. A successful cyberattack on critical infrastructure could cause real-world operational damage and trigger cascading impacts that threaten public safety.

Nationally, in the vast majority of cybersecurity incidents, it was a lack of awareness and coordination that allowed the attacks to occur and delayed the response to the incidents. The problem was a failure to train and educate all people who are access points to information and operations systems, not a failure of technology or lack of resources.

Collaborating with information technology (IT) professionals and integrating cybersecurity training into a comprehensive emergency management program can help reduce the risk of a cyberattack, improve incident response, and limit the impacts should an attack occur.

This Guide is being used to address training gaps identified in a formal cybersecurity risk assessment and/or incident response planning process.

D. Assumptions

In developing this document, it was assumed the government entity or organization intending to use the Guide had the following measures and practices in place:

- The Guide is being used to address training gaps identified in a formal cybersecurity risk assessment and/or incident response planning process.
- An individual, group, department, agency, or third-party vendor is assigned and is responsible for managing information technology resources and information security for the government agency or organization.
- There are established organizational rules and policies in place for the safe and secure use of computers, tablets, mobile devices, personal devices, and any other internet-capable electronic devices issued to or used by an employee.
- Employees are made aware of device usage rules and IT incident reporting procedures.
- The user of this Guide is familiar with the concepts and practices outlined in the Homeland Security Exercise and Evaluation Program (HSEEP).
- Emergency managers have a basic awareness of cybersecurity threats and intend to include information technology professionals in cyber incident response planning, training, and exercise activity.

II. Training

Training is essential for protecting information and operation network systems and effectively responding to a cybersecurity incident. Training recommendations and suggested online, classroom, and resident training courses for emergency managers, IT professionals, and cybersecurity stakeholders are included in this section.

These courses can provide a basic understanding and awareness for both cybersecurity and emergency management concepts. The goals are for emergency managers and IT professionals to "speak each other's language" and promote joint planning, training, and exercise activity.

A. Essential Cybersecurity Awareness Training for All Users

People in an organization are both the greatest vulnerability and best line of defense in regard to cybersecurity. Training can be delivered as part of formal or ad hoc new employee training, ongoing in-service training, or as-needed at the direction of IT managers, supervisors, or executives.

Recommended best practices for cyber hygiene and critical information security training content are outlined in this section. Additional cybersecurity training can be found on Indiana's Cybersecurity Hub at https://www.in.gov/cybersecurity/trainingevents/.

1. Basic Device and System Usage: Training that provides all users of an organization's information technology resources, including staff, managers, executives, and contract employees, awareness of policies and rules regarding the acceptable use of information devices and systems. This could include:
    - Mobile telephone, device, and application use
    - Computer use and portable data storage
    - Access to data networks, servers, drives, and folders
    - Internet browsing and social media restrictions
    - Approved use of official email and messaging applications
    - Personal mobile device and computer use for official business
2. Information Security Awareness: Instruction regarding the need and importance of information security, privacy measures, and cyber hygiene within an organization to protect valuable data, devices, and network systems. Examples include:
    - Physical security and protective measures for computers and mobile devices
    - Use of strong passwords for computers, mobile devices, email, and network access
    - Secure use of external data storage devices such as flash drives and external hard drives
    - Employee role in maintaining and supporting routine software updates, antivirus software, and firewall protections
    - Requirements for remote network access and use of virtual private networks
    - Use of public, personal, or unsecured Wi-Fi networks
    - Cyberattack methods, vectors, and tactics
    - Recognizing social engineering attempts, phishing emails, and malicious websites
    - Awareness of cybersecurity threats to mobile devices including location services, USB charging devices, mobile apps, malicious QR codes and texts messages

3. Incident Response Procedures: Internal processes and procedures for reporting and initially responding to unexplained computer or system malfunctions, unusual or suspicious network activity, loss of data or data access, detection of malicious software, or a confirmed cyberattack. Information provided in training could include:

    - Primary and alternate points of contact and methods for reporting a suspected or confirmed cybersecurity incident.
    - Essential information to provide when reporting an incident.
    - Immediate actions the user must take to help contain a suspected or confirmed cybersecurity threat.
    - The user's role in supporting an incident response including analysis, containment, eradication, evidence gathering, and recovery.

B. Cybersecurity Training for Emergency Managers

These course recommendations are intended to familiarize emergency managers with cybersecurity terminology, core concepts, and best practices.

Training providers include the FEMA Emergency Management Institute (EMI), Texas A&M Engineering Extension Service (TEEX), Norwich University (NUARI), University of Texas San Antonio (UTSA), and the Criminal Justice Institute (CJI).

Detailed course information is available in the FEMA National Preparedness Course Catalog.

Basic

- AWR-136: Essentials of Community Cyber Security (TEEX, Classroom or Virtual)
- AWR-169-W: Introduction to Cyber Incident Management (TEEX, Online)
- AWR-367: Understanding Social Engineering Attacks (CJI, Online)
- AWR-395-W: Cybersecurity in the Workplace (TEEX, Online)
- AWR-397-W: Cybersecurity for Everyone (TEEX, Online)
- AWR-399-W: Detecting and Responding to a Cyber Attack (TEEX, Online)

Intermediate

- AWR-176-W: Disaster Recovery for Information Systems (TEEX, Online)
- AWR-177: Information Risk Management (TEEX, Online)
- AWR-353-W: Using the Community Cyber Security Maturity Model (CJI, Online)
- AWR-366-W: Developing a Cyber Security Annex for Incident Response (NUARI, Online)
- AWR-383: Cybersecurity Risk Awareness for Officials and Senior Management (NUARI, Virtual or Classroom)
- MGT-465: Recovering from Cybersecurity Incidents (TEEX, Classroom)

Advanced

- MGT-384: Community Preparedness for Cyber Incidents (TEEX, Virtual or Classroom)
- MGT-452: Physical & Cybersecurity for Critical Infrastructure (TEEX, Classroom)
- MGT-456: Integration of Cybersecurity Personnel into the EOC for Cyber Incidents (NUARI/TEEX, Classroom)
- MGT-473: Organizational Cybersecurity Information Sharing (CJI, Classroom)
- MGT-478: Community Cybersecurity Information Sharing Integration (NUARI, Classroom or Virtual)
- E8515: Cybersecurity Symposium (EMI, Virtual or Classroom)

C. Emergency Management Training for IT Professionals

These course recommendations are intended to provide IT professionals and cybersecurity stakeholders with foundational knowledge of emergency management. This includes Incident Command System, NIMS, emergency operations centers, exercise planning, and how IT professionals can be integrated into a coordinated response to a major cybersecurity incident.

Basic

- IS0908: Emergency Management for Senior Officials (EMI, Online)
- IS0100.c: ICS 100 Introduction to the Incident Command System (EMI, Online)
- IS0200.c: ICS 200 Basic Incident Command for Initial Response (EMI, Online)
- IS0700.b: National Incident Management System (EMI, Online)
- IS0235.c: Emergency Planning (EMI, Online)

Intermediate

- IS0546.a: Continuity of Operations Awareness (EMI, Online)
- IS0120.c: An Introduction to Exercise (EMI, Online)
- IS0775: Emergency Operations Center Management and Operations (EMI, Online)
- AWR-366-W: Developing a Cyber Security Annex for Incident Response (NUARI, Online)
- AWR-388-W: Cyber Awareness for Municipal, Police, Fire and EMS IT Personnel (CJI, Online)

Advanced

- MGT-456: Integration of Cybersecurity Personnel into the EOC for Cyber Incidents (NUARI/TEEX, Classroom)
- PER-256: Comprehensive Cybersecurity Defense (CJI, Classroom)
- PER-257: Cyberterrorism First Responder (UTSA, Classroom)
- PER-371: Cybersecurity Incident Response for IT Personnel (CJI, Classroom)
- E8515: Cybersecurity Symposium (EMI, Virtual or Classroom)

III. Exercise

Cybersecurity incidents are complex. The response to these incidents is often equally complex, involving groups which are not traditional disaster response or emergency support function partners. Conducting exercises with IT professionals, private sector representatives, and community stakeholders is critical to ensure an effective, coordinated response to a cyberattack.

The nature of cybersecurity threats makes them unique. However, conducting exercises to test and evaluate response capabilities can be accomplished using well-established practices familiar to emergency managers. This section will provide best practices, planning considerations, and suggestions drawn from HSEEP to plan and conduct cybersecurity exercises.

A. Exercise Planning

1. **Exercise Participants:** Those taking part in an exercise will vary depending on the nature, scope, and scale of the exercise being planned. This will likely include both traditional and non-traditional partners. Participants to consider could include:

    a) Emergency Support Function (ESF) organizations

    b) Chief Information Officer/IT Director for jurisdiction or organization

    c) IT /Data/Cybersecurity contractor for jurisdiction or organization

    d) Attorney or general counsel for jurisdiction or organization

    e) County Commissioners/County Council Members

    f) Municipally-elected officials/Mayors/Town Manger

    g) City/Town Council members

    h) Auditor, Treasurer, Assessor, Recorder, Surveyor

i) Prosecutor, Clerk/Clerk of Courts

j) Township Trustees or designee

k) Human resources/Personnel department for jurisdiction or organization

l) Electric power utility or electric cooperative

m) Water/Wastewater/Stormwater utilities

n) Natural gas utility

o) Telecommunications provider or telephone cooperative

p) Hospitals, healthcare facilities, and providers

q) School district representatives

r) Cooperative extension service program representative

s) Chamber of Commerce/Local economic development stakeholders

t) Zoning/Building/Area planning commission members

u) Americans with Disabilities Act/Accessibility Office representative

v) Mass transit/rural transit service providers

w) Vendor-managed and contract service representatives

x) County insurance coverage provider

2. **Exercise Planning Team:** The composition of the Exercise Planning Team should reflect the agencies, groups, and organizations participating in the exercise. Incorporating subject-matter experts involved in incident planning, response, and recovery will help ensure the exercise scenarios are realistic, challenging, and adequately test key response functions.

    a) Planning Meetings: The complex nature of cybersecurity exercise design and development requires well organized meetings to ensure exercise success. In some situations, participants may be unfamiliar with exercise planning methodology and may never have taken part in a disaster exercise.

    b) Concept and Objectives Meeting: Identify the type, scope, objectives, and purpose.

    c) Initial Planning Meeting: Lay the foundation for exercise development.

    d) Midterm Planning Meeting: A forum for discussing organization, staffing concepts, and exercise logistics.

    e) Master Scenario Events List (MSEL) Meeting: A forum for creating and reviewing the scenario injects and timeline.

    f) Final Planning Meeting: Forum for reviewing exercise logistics, processes, and procedures.

    g) After-Action Meeting: Feedback for participating jurisdictions on their performance and plans for improvement.

3. **Documentation:** The requirement for exercise documentation will vary depending on the type and size of exercise being conducted, as well as the number and variety of participants.

Seminar, Workshop, or Game:

a) Budget

b) Required pre-exercise meeting sign-ins and agendas

c) Presentations (if applicable)

d) Agenda for exercise event

e) Exercise participant rosters/sign-in sheets

f) Executive summary

Tabletop Exercise:

a) Budget

b) Required pre-exercise meeting sign-ins and agendas

c) Agenda for exercise event

d) Situation manual

e) Exercise evaluation guides

f) Exercise participant rosters/sign-in sheets

g) After action report/improvement plan

Drill, Functional, and Full-Scale Exercise:

a) Budget

b) Required pre-exercise meeting sign-ins and agendas

c) Agenda for exercise event

d) Exercise plan

e) Master scenario events list

f) Controller and evaluator handbook

g) Exercise evaluation guides

h) Exercise participant rosters/sign-in sheets

i) After action report/improvement plan

B. Special Considerations

Private-sector organizations and critical infrastructure stakeholders may require additional documentation before and after an exercise. There may be legal, regulatory, or internal policy compliance documentation requirements.

These may include memorandums of understanding, sector-specific reporting forms, or non-disclosure agreements.

C. Discussion-Based Exercises

- **Seminars:** Orient participants or provide an overview of plans, policies, and procedures. Example: Review of Cybersecurity Incident Response Plan with cybersecurity stakeholders, emergency responders, or elected/appointed officials.
- **Workshops:** Focus on development of a planning product by the attendees. Example: Develop annexes, standard operating procedures, or checklists to support the activation of an incident response plan. These could be notification checklists, response and containment processes, or recovery procedures.
- **Games:** Simulation of operations that often involves two or more teams designed to depict an actual or hypothetical situation. Example: Groups of participants test their abilities to recognize and report phishing emails.
- **Tabletop Exercise:** Guided discussion following an incident scenario used to assess response plans, policies, and procedures. Example: Senior officials, ESF representatives, and IT professional are presented with a series of simulated network system failures and information injects. Participants talk through their coordinated response to a ransomware attack scenario.

D. Operations-Based Exercises

- **Drills:** Test of a single operation or function in a single agency or organization. Example: Incident notification procedures and systems are tested to ensure all cyber incident response stakeholders receive alert messages.

- **Functional Exercises:** Tests individual capabilities, multiple functions, or activities within a function; however movement of personnel and equipment is simulated. Example: Emergency operations center is activated and ESF representatives respond to a simulated cyberattack scenario. Participants manage command, control, and coordination functions in real-time.

- **Full-Scale Exercises:** Combines command and control elements of a functional exercise with the actual deployment of operational personnel and resources to test incident response capabilities under realistic conditions. Example: IT professionals, public safety officials, and ESF agencies respond to a large-scale cyberattack which impacts critical infrastructure. This would include the deployment of resources and personnel in response to immediate and cascading community impacts of the attack.

E. Exercise Scenario Ideas

- **Scenario 1**: **Phishing Trip**

  Target: Elected and Appointed Officials, System Access Credentials

  Attack Method: Spear Phishing

  Triggering Incident Description:

  County commissioners, county sheriff's department, and staff members in the county auditor's office receive emails requesting confirmation of their usernames and passwords for their official email accounts. The message says there has been suspicious activity in their email account and their account will be disabled unless they provide the requested information. In some cases, the username and passwords for other systems and databases were requested. The email appears to come from a current county employee with a legitimate email address. Some staff members report providing their username and password information. No system disruptions or suspicious system activity has been observed or reported.

  Inject Discussion:

  Who within your organization is notified?

  What is your organization's initial response?

  How do you warn and communicate with employees, contractors, and vendors?

What actions are taken to determine if malware is present or if data has been compromised?

Do you require external agencies or vendor-managed services?

Is law enforcement notified?

- **Scenario 2: The Hacktivist**

  Target: Local Government Websites

  Attack Method: SQL Injection, Denial of Service

  Triggering Incident Description:

  A well-known activist group threatens to shut down local government computer networks on social media. The next morning, multiple agency websites are offline. Some sites are defaced with vulgar, anti-government messages and the insignia of a hacking group. Other sites show error messages or are blank. An initial investigation also shows servers are being overloaded by internet traffic from thousands of sources simultaneously.

  Inject Discussion:

  Who within your organization is notified? What is that notification process?

  Are IT disaster recovery and incident response plans in place?

  What is your jurisdiction's initial response to the incident?

  What local, county, and/or state agencies are involved in the response?

  Do you require external or vendor-managed services to restore systems?

  Is law enforcement notified?

  How is public information, social media, and news media messaging managed?

- **Scenario 3: The Break-In**

  Target: Financial Data and Personally Identifiable Information

  Attack Method: Spyware, Data Extracting Malware

  Triggering Incident Description:

  Your jurisdiction is notified by federal and state law enforcement that a large amount of sensitive information from your jurisdiction's databases is being sold on a criminal website. The information included names, social security numbers, addresses, dates of birth, mother's maiden names, checking account, and credit card account information of residents, employees, and contractors. An initial network investigation identified malware that recorded log-in credentials and extracted data from several systems and databases. It is unclear how long the data breach has been in place.

Inject Discussion:

What is your organization's initial response?

Who is the lead response agency? Who are the supporting agencies?

Do you require external agencies or vendor-managed services?

How do you identify and warn those affected by the data breach?

Does your jurisdiction have insurance that covers costs related to the breach?

What legal or regulatory issues may result?

- **Scenario 4: The Lockout**

  Target: Local Government Computers, Networks, and Data

  Attack Method: Ransomware

  Triggering Incident Description:

  County employees in multiple local government offices and agencies report being unable to log in to their computers. Those that are able to log in to their computers are unable to access email, public records, and essential databases. Telephones and fax machines are also reported to be offline at several office locations. Fire, law enforcement, and EMS departments have been affected. Public safety communications has been impacted, but computer aided dispatching and 911 telephone systems are still operating normally. A local school system and several municipalities are also reporting similar problems. A message appears on computer screens declaring the computers and systems are locked and will only be released if the hacker is paid $50,000 in bitcoin currency.

  Inject Discussion:

  What is your organization's response?

  Are IT disaster recovery and incident response plans in place?

  Are business continuity and continuity of operations plans in place?

  How would your organization communicate internally and externally?

  Does your jurisdiction have cybersecurity insurance?

  Does your jurisdiction have access to bitcoin currency?

  Who is authorized to approve or deny the ransom payment?

  What are the potential cascading impacts to local government and community?

- **Scenario 5: False Alarm**

  Target: Outdoor Warning and Mass Notification Systems
  Attack Method: Spyware, Credential Theft, DMTF Signal Spoofing

  Triggering Incident Description:

  At 11:30 PM, outdoor warning sirens across the county begin to sound. There is no severe weather or local emergency. Sirens were not activated by emergency management or other public safety agency. Attempts to access the siren control system and shut off sirens remotely are unsuccessful. Attempts by emergency management to shut off nearby sirens manually are also unsuccessful. Sirens momentarily deactivate, but immediately reactivate. Public safety dispatchers receive dozens of 911 calls from residents in a matter of minutes. Emergency management also receives reports that text messages falsely reporting a train derailment and hazardous chemical spill are being received on cellphones across the county.

  Inject Discussion:

  What is your organization's response?

  What agencies have access to the jurisdiction's outdoor warning and/or emergency mass notification systems?

  How can siren and notification system vendors be engaged to assist?

  How would you quickly communicate accurate information to the public and media outlets?

  What instructions would you provide to the public?

- **Scenario 6: Dispatch Flood**

  Target: Public Safety Answering Points

  Attack Method: Botnet, Telephony Denial of Service

  Triggering Incident Description:

  Public safety dispatchers begin receiving numerous 911 calls which immediately disconnect when answered. Police officers are initially dispatched to the hang-up call locations as the volume of calls grow over several minutes. Nearly 200 calls appear to be originating from the same 20 to 30 mobile telephones in the local area. When arriving on scene, police officers investigating the hang-up calls find residents are unaware of the 911 calls. Upon inspection, the cellphones making the calls appear to be locked with blank screens. Owners are unable to unlock the telephones or power them off. Owners reported that the cellphones "froze" when they clicked on a link in a social media app. similar incidents were reported by public safety agencies in adjacent counties.

Inject Discussion:

What is your organization's initial response?

What back-up systems, processes, facilities, or mutual aid agreements are in place? How would you quickly communicate accurate information to the public and media outlets?

What instructions would you provide to the public?

How would commercial telecommunications and cellular telephone service providers assist? How can vendor assistance be requested?

Is state or federal assistance required? How is assistance requested in this situation?

- **Scenario 7: Flu Season**

  Target: Hospital Information Network

  Attack Method: Ransomware

  Triggering Incident Description:

  It is the height of a very severe flu season. Below zero temperatures and heavy snow are straining local emergency medical services and fire department resources. The emergency department in the community's largest hospital is experiencing a high volume of patients. The hospital is operating at near capacity. The hospital goes on full diversion due to patient volume and reported information network issues. Hospital staff are unable to access the electronic medical records system. The email system also experienced intermittent outages before going completely offline. Facilities staff are unable to access and control heating and ventilation systems. Temperature, air pressure, and humidity in the hospital can no longer be controlled. The system issues are initially blamed on the weather, until a ransomware message appears on multiple computer screens. The message demands $100,000 in bitcoin to restore the hospital's computer systems.

  Inject Discussion:

  How would public safety and public health agencies assist?

  Does the hospital have business continuity and emergency operations plans in place?

  What vendor-managed services would be required to maintain safe patient care activity at the hospital?

  Can other hospitals in the area manage the additional patient volume diverted from the affected hospital?

  Does the hospital have cybersecurity insurance?

Is the hospital willing to pay the ransom?

At what point would partial or full evacuation of the hospital be required?

- **Scenario 8: From Bad to Worse**

  Target: Emergency Management, Emergency Support Functions

  Attack Method: Email Extortion, Ransomware, Distributed Denial of Service

  Triggering Incident Description:

  A major flood has been impacting large areas of the state for several days and there is widespread damage across the county. The county emergency operations center has been activated to coordinate local response operations. There has been extensive local and national media coverage of the flood and the community's response. Mid-morning on the 5th day of operations, the emergency management director and several other county officials receive an email threatening to shut down the county's information networks unless a payment of $300,000 in bitcoin is made by the end of the day. Similar threats are received via the county's official social media sites. Shortly after the threats are received, the county government's email system and websites go offline for exactly 30 minutes, then come back online. Access to critical information databases is also lost, then restored. The hackers claim responsibility for the outage and threaten to increase the ransom amount and severity of attacks if the ransom payment is not received.

  Inject Discussion:

  Are IT disaster recovery and incident response plans in place? How are these plans activated?

  Are continuity of operations plans in place? How are these plans activated?

  How would an alternate EOC location be activated?

  Does the jurisdiction have cybersecurity insurance?

  Who has the authority to approve or deny the ransom payment? What is that process?

  What state or federal notifications or requests for assistance would be made?

  How is public information, social media, and news media messaging managed?

- **Scenario 9: Troubled Waters**

  Target: Water Utility Control Systems

  Attack Method: Industrial Control System Malware

  Triggering Incident Description:

  A local fire department responds to a large fire at the community's primary water treatment plant. Plant personnel report the fire started in an area of the plant that houses high lift water pumps. These pumps discharge treated drinking water into water mains and storage tanks for distribution. They also stated that just before the fire began, they were unable to access the computer system that controlled the pumps. The pumps began to cycle on and off, running at very high RPMs, then quickly shutting down. Attempts to access the control systems on site and from remote computer terminals failed. After several minutes, all of the pumps in the plant burned out and failed, with one pump catching fire. The plant can no longer maintain pressure within the system, which provides water to most of the county and large portions of adjacent counties. Water sampling of storage tanks also showed dangerously high levels of chemicals used to disinfect water at the plant. During a detailed analysis of the control systems, highly sophisticated malware was detected. The malware had caused the pumps to malfunction, altered the amount of disinfectant used to treat the water, and locked operators out of the system. The water supply for residents, hospitals, schools, manufacturing, and firefighting is now unavailable, and will likely be offline for weeks.

  Inject Discussion:

  How would the county's response be activated and coordinated?

  How would the community be notified of the incident and warned of water contamination?

  How could InWARN mutual aid resources be requested?

  Is local, state, and/or federal law enforcement notified?

  What state and federal resources could be requested?

  How could drinking water be distributed to the community?

  How would water for healthcare facilities be provided?

  Would evacuation of hospitals be necessary?

  How would schools be affected?

  How could water for firefighting be supplied?

  How would wastewater treatment be

  impacted?

  What are the potential sanitation and public health hazards?

Are there legal and regulatory issues that must be addressed?

How could weather conditions affect potential impacts and response operations? (i.e. Winter vs. Summer)

- **Scenario 10: The Blackout**

  Target: Electric Power Utilities

  Attack Method: Advanced Persistent Threat, Industrial Control System Malware

  Triggering Incident Description:

  It is late Monday afternoon, the day before Election Day. Weather is fair across the Midwest with no severe weather or extreme temperatures. At 4:45 PM EST, multiple cable news networks begin to report a major power outage in the City of Detroit. Within 30 minutes of the initial news reports, widespread power outages are reported across Michigan, Wisconsin, Minnesota, and northern Ohio. At 5:40 PM power outages begin to occur across Central Illinois and Northwest Indiana.

  At 6:15 PM, power outages occur across your entire county. Simultaneously, adjacent counties experience widespread outages. All fire stations, police stations, and healthcare facilities in the county are on generator power. The county public safety answering point and emergency operations center are also operating on generator power. 911 service is operational, but is quickly being overwhelmed by emergency calls and inquiries from the public. County Emergency Management is notified the Indiana State Emergency Operations Center is activated.

  By 8:00 PM, multiple power companies and regional transmission organizations confirm massive power outages in seven states across the Midwest. The cause of the blackout, as well as when power will be restored, is unknown. Locally, nearly all traffic lights in the county are out. Numerous vehicle accidents and major traffic backups are reported. Grocery stores, gas stations, hardware, and home improvement stores are frantically requesting law enforcement assistance to deal with security and crowd control problems. Fire departments are responding to multiple fires at electric power substations and pole-mounted transformers across the county. EMS response is delayed due to the volume of calls and traffic congestion. Water and wastewater treatment plants remain operational, but are on emergency generator power. There are sporadic landline telephone and internet service outages, but cellular telephone systems are operating normally.

  At 10:00 PM, the U.S. Department of Homeland Security (USDHS) confirms the power outages were caused by a massive cyberattack against power companies and regional power management organizations. The identity of the attacker and the method of attack are not announced.

  In Indiana, it is estimated 90 % of the state is without electricity. Only a few counties in Northeastern Indiana have power. Areas of the Midwest not affected by the blackout include the City of Chicago and areas of Northern Illinois, Southwestern Michigan, and

most of Central and Southern Ohio. The State of Kentucky is not impacted by the power outage. The Governor of Indiana formally declares a state of emergency, activates the National Guard, and requests federal assistance.

24 hours after the attack began, USDHS officials confirm the attack is sophisticated, coordinated, and consistent with the capabilities of a nation state. The President of the United States issues a Major Disaster Declaration. Cyber incident response operations have isolated and contained the impacts to the Midwest. Electrical power in the rest of the U.S. is unaffected. Across the Midwest, major physical damage to power generation plants, power transmission, and power distribution infrastructure has occurred. Due to the extent of the damage and compromise of control systems, the local electric power utility reports repair and power restoration in the county may not begin for two to three weeks. Full restoration of power to all areas of the county may take up to three months.

Inject Discussion:

How would the county's incident response be activated and coordinated?

How would Emergency Support Functions be mobilized and staffed?

How would situational awareness be established and maintained?

What are your jurisdiction's incident priorities, goals, and objectives?

What emergency response and continuity of operations plans are in place? How would these plans be implemented?

What are the immediate public safety, security, and health concerns?

How would critical county information networks and telecommunication systems be maintained and protected during an extended power outage. How would county and/or contract IT professionals be integrated into the incident response?

How would local elected officials be engaged? What emergency orders would need to be issued?

How would the county EOC establish and maintain communications with local, county, district, volunteer, state, and federal partners during a prolonged power outage?

How would resource needs be assessed and requests for assistance communicated?

How long can critical public safety, healthcare, water/wastewater utility, and telecommunications facilities operate on emergency generator power without refueling?

What are the anticipated fuel needs for vehicles and generators? What type of fuel is required?

How would public information, warnings, and alerts be managed and communicated?

How would critical staffing needs be met? (i.e. public safety, healthcare, mass care)

How would potable water be provided to the community if water utility systems fail?

How would natural gas utilities in your area be affected?

How would wastewater treatment and community waste management services be maintained?

How would transportation infrastructure and services be affected? (i.e. streets, highways, rail, airports, public transportation)

During a prolonged power outage lasting weeks or months, how would fuel distribution and fuel use be prioritized? How could community fuel rationing be implemented and maintained?

What could be done to help maintain retail food and fuel services at grocery stores and gas stations?

How would food be provided to the community if grocery stores could not remain open?

What are the anticipated long-term mass care and sheltering needs?

How would access and functional needs populations, residents of long-term care facilities, and those in home healthcare programs receive assistance?

What is the impact on local school systems?

How would volunteers and donations be managed?

What are the potential financial issues that would need to be addressed? (i.e. county employee payroll, purchasing, cost tracking, damage costs, documentation, bank closures)

What government and social services could be maintained? (i.e. courts, county offices, WIC)

How would the election, scheduled for the day after the attack occurred, be affected?

How would local government assist power companies in repairing damaged infrastructure?

Once damaged equipment was repaired and control systems brought back online, how would local government agencies support the safe reenergizing of the local power grid and restoration of power?

How would economic impacts to the community be mitigated? How would long-term recovery activities be managed?

How would county and/or contract IT professionals be integrated into long-term recovery activity?

F. CISA Tabletop Exercise Packages

CISA Tabletop Exercise Packages (CTEPs) are a comprehensive set of resources designed to assist stakeholders in conducting their own exercises. Partners can use CTEPs to initiate discussions within their organizations about their ability to address a variety of threat scenarios.

Each package is customizable and includes template exercise objectives, scenarios, and discussion questions as well as a collection of references and resources. Available scenarios cover a broad array of physical security and cybersecurity topics, such as natural disasters, pandemics, civil disturbances, industrial control systems, election security, ransomware, vehicle ramming, insider threats, active assailants, and unmanned aerial systems. CTEPs also provide scenario and module questions to discuss pre-incident information and intelligence sharing, incident response, and post-incident recovery.

With more than 100 CTEPs available, stakeholders can easily find resources to meet their specific exercise needs. More information visit https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages.

Cybersecurity Scenarios

These CTEPs include cybersecurity-based scenarios that incorporate various cyber threat vectors including ransomware, insider threats, phishing, and Industrial Control System (ICS) compromise. There are also sector-specific cybersecurity scenarios for elections infrastructure, local governments, maritime ports, water, and healthcare.

Cyber-Physical Convergence Scenarios

Physical impacts resulting from a cyber threat vector, or cyber impacts resulting from a physical threat vector. While CTEPs within the cyber and physical sections may touch on these subjects, convergence CTEPs are designed to further explore the impacts of convergence and how to enhance one's resiliency.

CTEP Documents

Leverage pre-built templates to develop a full understanding of roles and responsibilities for exercise planners, facilitators / evaluators, and participants. Additionally, the documentation includes templates for the initial invitation to participants, a slide deck to use for both planning meetings and conduct, a feedback form to distribute to participants post-exercise, and an After Action Report. In conjunction with selecting one of the above situation manuals, your exercise planning team will be able to fully develop your own tabletop exercise and update information sharing processes; emergency response protocols; and recovery plans, policies, and procedures.

For more information or to request an exercise, please contact cisa.exercises@cisa.dhs.gov and CISA Cybersecurity Advisor Chetrice Romero at Chetrice.romero@cisa.dhs.gov.

G. Evaluation and Improvement

The evaluation phase for all exercises includes a formal exercise evaluation, an integrated analysis, and an After Action Report/Improvement Plan (AAR/IP) that identifies strengths and areas for improvement of an agency's preparedness, based on exercise performance. Recommendations developed during evaluation are used in improvement planning phase.

During improvement planning, the corrective actions identified in the evaluation phase are assigned, with due dates, to responsible parties; tracked to implementation; and then validated during subsequent exercises.

The importance of applying lessons learned, from both successes and failures, cannot be overstated. True cybersecurity preparedness can only be accomplished through a constant cycle of effective planning, training, exercise, and improvement

IV. Information Resources for Training and Exercise

Indiana Cybersecurity Hub
www.in.gov/cyber

Indiana Cybersecurity Hub – Emergency Response and Recovery
https://www.in.gov/cybersecurity/3813.htm

Cybersecurity & Infrastructure Security Agency
https://www.cisa.gov/

CISA Tabletop Exercise Packages
https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

Indiana Information Sharing and Analysis Center (IN-ISAC)
https://www.in.gov/cybersecurity/in-isac/

FEMA National Training and Education Division (NTED)
https://www.firstrespondertraining.gov/frts/npccatalog

Homeland Security Exercise and Evaluation Program (HSEEP) Toolkit
https://preptoolkit.fema.gov/hseep-resources

National Institute of Standards and Technology (NIST) Cybersecurity Framework
https://www.nist.gov/cyberframework

V. Guide Development and Maintenance

This Guide was developed by the Response and Resiliency Subcommittee of the State of Indiana Governor's Executive Council on Cybersecurity. The Subcommittee was chaired by the Adjutant General of the Indiana National Guard and the Executive Director of the Indiana Department of Homeland Security. Subcommittee members included multi-disciplinary representatives from public sector, private sector, and academic organizations.