“First 48”: What to Expect When a Cyber Incident Occurs

Advice from Public Safety Colleagues

Publication: 2022
Cybersecurity and Infrastructure Security Agency

"First 48": What to Expect When a Cyber Incident Occurs

Advice from Public Safety Colleagues

Introduction

Public safety communications are at risk from a multitude of cyber threats and vulnerabilities. Due to the urgent nature of the operations, public safety communications are high-value targets for cyber threat actors.

This document, developed in partnership with public safety officials who have first hand experience with cyberattacks, will inform expectations and provide recommendations on how to proceed after experiencing a cyber incident. A cyber incident will jeopardize the confidentiality, integrity, or availability of digital information or information systems. As responses to specific incidents vary greatly, this document will provide foundational guidance on cyber incident response expectations.

Common themes, insights, and best practices from public safety colleague interviews are presented throughout the document as text boxes and visual aids. Appendices link to additional public safety cyber resources. The "First 48" focuses on cyber incidents, but organizations are encouraged to holistically review their operational posture to ensure that they remain resilient in instances of other human-caused or natural disruptions (e.g., device management, dependencies on non-agency infrastructure and services).

Cyberattacks have increasingly targeted public safety organizations, utilizingattacks such as telephony denial of service (TDoS), malware, and ransomware to cause disruptions of critical operations. In some instances, organizations are unaware that they are experiencing a cyberattack until they are informed by outside entities such as the Federal Bureau of Investigation (FBI). In other instances, it is immediately obvious the organization is under attack.

It is key for organizations to develop a "culture of cyber readiness" and work collaboratively with all stakeholders who influence or impact their cyber posture. It is recommended that organizations examine external resources that could assist in protecting their systems and networks from threats, preserving forensic evidence, mitigating incidents, and recovering from disruptions. Resources to develop a culture of cyber readiness are available in Appendix A: Cybersecurity Planning Resources.

Public safety colleagues stress planning and preparing against cyber incidents and vulnerabilities. It is recommended that organizations regularly review and assess their cybersecurity posture. Resources such as CISA's Cyber Essentials Toolkit, Public Safety Communications and Cyber Resiliency Toolkit, and the Cybersecurity Incident and Vulnerability Response Playbooks are available to assist organizations in understanding the fundamentals of cybersecurity and communications resiliency.

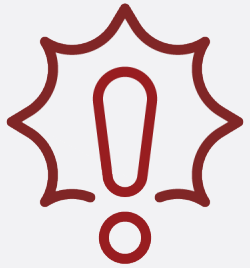
In addition to reviewing guidance, organizations must familiarize themselves with existing available cyber support. Whether with jurisdictional partners or state and federal level technical cyber support, it is recommended that organizations establish and maintain a close relationship with these stakeholders and involve them in the planning and preparation processes. Third-party vendors, public information offices, and other impactful stakeholders could also be involved.

PRE-INCIDENT

What to Expect:

- There are daily cyberattack campaigns against public safety networks; some colleagues have observed eight to 12 campaigns at any given moment against their systems
- It could take 18 months to discover a cyberattack; some malware could dwell on the network from 70 to 200 days before launching the attack
- Often, there are more minor incidents leading to a significant, more damaging incident
- Backups connected to the live production system may be impacted during a cyber incident
- Staff may be unfamiliar with potential signs of a cyber incident
- Staff may unknowingly cause cyber incidents via everyday routines (e.g., checking personal email, accessing the internet at a workstation that is connected to the Computer-Aided Dispatch system)
- Unless strictly written in agreements and policies, third-party vendors may neglect to perform necessary security upgrades and patching

WHEN TO BE SUSPICIOUS



- Activity on unusual network ports
- Alerts from malware or antivirus protection systems
- Attempts from normal users to gain elevated privledges
- A threat from a group stating that a cyberattack is imminent (ransomware)
- Configuration changes that cannot be tracked to known updates
- Repeated system or application crashes
- Unauthorized creation of new user accounts
- Unexpected user account lockouts
- Unexplained browsing to unauthorized websites
- Unexplained modifications or destruction of user files
- Unusual deviation from typical network traffic flows
- Web server log entries that show the usage of a vulnerability scanner

Advice from Colleagues:

Organizations should develop a cyber incident response plan and ensure that it is reviewed, practiced, and updated on a scheduled basis. In addition, establish an incident communications plan that clearly outlines the chain of command, individual roles and responsibilities, emergency purchasing powers (e.g., hardware, software, services for recovery), and who to contact if an incident should occur to streamline information sharing via unified messaging. Organizations may also consider implementing or updating continuity of operations procedures (COOP) to strengthen overall cyber resiliency. In the event of a cyber incident, COOP ensures the contituation of critical services and could potentially lessen the strain on getting these services back online before they are completely restored.

Ensure operating systems and applications are up-to-date and fully patched. Develop and maintain images of servers, workstations, and operating systems. Regularly back up data and operating systems and ensure such backups are maintained so that information remains accessible and up to date. Coordinate with IT department to ensure that backups are stored offline. Consider network segmentation as a physical and virtual architectural approach as emergency communications should operate separately from the municipality administrative network.

Staff with technical knowledge and skills and an understanding of organizational network and system architecture could reduce cyber incidents or expedite incident response time. Other resources such as diagrams and other visual aids could also be helpful. Regularly train all staff to practice good cyber hygiene and frequently exercise operating under manual mode to help prevent, discover, and respond to cyber incidents better.

THE FIRST EIGHT HOURS

What to Expect:

- Organizations may not be aware that they are being targeted and attacked until an outside organization notifies them (e.g., FBI, neighboring jurisdictional partner, third-party vendor)
- Organizations may be unfamiliar with existing reporting channels and resources available to them; the incident may also cause established communications channels and reporting mechanisms to become unavailable (e.g., Internet/phone unavailable)
- Resources may not be available to organizations at the onset of an incident (e.g., IT department is not available on a 24/7 365 schedule; other incidents of higher precedent consuming national or regional resources; cyber incidents may rank lower on the risk registers, thus not warranting immediate assistance)
- Personnel may be confused as to what occurred and may unknowingly destroy forensic evidence and exacerbate the incident
- Information will change rapidly as new evidence is discovered; it is recommended to establish a point of contact to act as the response coordinator to ensure a continuity of information and response efforts

EXAMPLE INCIDENT RESPONSE ESSENTIAL ACTIONS

- Leverage assessments and evaluate mission impacts to prioritize resources and identify which systems must be recovered
- Establish and maintain internal reporting structure
- Block and log unauthorized access
- Change system admin passwords and access
- Direct the cyber threat to a sandbox or another form of containment to monitor the threat's activity, gather additional evidence, and identify attack vectors

Advice from Colleagues:

It is recommended that organizations deploy the cyber incident response plan as soon as they observe signs of compromise. A part of incident response includes contacting relevant local (e.g., organizational leadership, emergency management), state (e.g., state chief information officer, governor), and federal authorities (e.g., FBI field office, CISA) and assembling the incident response team (e.g., municipal IT team, vendors). The incident response team and appropriate resources must work together to isolate affected networks and systems. Removing affected devices from the network in the event of a cyber incident may stop or slow the spread of the incident. However, this step will impact operational continuity, which should be considered in the plan. In the process of removing the devices from the network, do not turn them off as doing so may lose valuable information contained in the flash memory. Attackers will often place items in the flash memory to hide their tracks, turning off affected devices may lose these indicators. It is also crucial to capture and preserve forensic evidence to the greatest extent possible, while ensuring system logs are also available for review. Designate physical and virtual meeting space to conduct and document all response activities.

Example Contact List
• Local Leadership and Partners (e.g., Office of Public Information, Budget Office)
• State Leadership
• Jurisdictional Partners
• Federal Partners (e.g., FBI Field Office, CISA)
• Additional Partners

After initial triage and response, organizations should consider implementing the previously established communications plan to keep the public, media, and other peripheral stakeholders informed and updated.

THE FIRST DAY

What to Expect:

- Organizations may need to procure new devices and machines immediately, which may be outside of the limits of existing budgets or policies
- Forensic evidence associated with the incident may be damaged and crucial information may be lost
- Physical components not directly related to the communications systems may be impacted (e.g., HVAC)
- Staff and external stakeholders may be unaware of the latest decisions and updates, thus becoming doubtful and reluctant, potentially leading to low morale
- External subject matter experts may be unfamiliar with the organization's architecture; they may also be challenged to collaborate if there is not an established chain of authority

EXAMPLE INCIDENT RESPONSE/RECOVERY ESSENTIAL ACTIONS:

- Remediate all infected IT environments and reimage all affected systems
- Rebuild hardware
- Replace compromised files with clean versions
- Install patches
- Reset passwords on compromised accounts
- Monitor for signs of adversary responding to containment activities
- Develop response scenarios for threat actors using alternative attack vectors
- Allow adequate time to ensure all systems are clear of all possible cyber threat persistence mechanisms
- Ensure all adversary activity is contained prior to rebuilding and reconnecting to the network; if not contained, adversaries could reinfect the rebuilt system

Advice from Colleagues:

During the first day, it is important to locate any remaining backdoor access to the organization and secure these vulnerabilities to prevent further damage. While removing affected devices from the network, if possible, organizations should simultaneously review and authenticate the integrity of backups. This integrity review is crucial to ensure the network is not reinfected. After the authentication process, apply appropriate backups to unaffected or new machines.

Organizations could consider employing outside organizations with subject matter experts to examine networks and systems to remove the remaining cyber threat. However, outsourcing some or all of the responses could be burdensome based on the organization’s size, budget, location, and resources available. In addition, the initial response period may be intense and lengthy, spanning more than 24 hours. Accordingly, organizations may need to implement work shifts to alleviate fatigue, maintain continuous coverage, and manage scarce resources.

Should organizations elect to employ third-party support, ensure that access is granted only to those with “need-to-know.” Organizations should review contracts and agreements with third-party support to define data and infrastructure management, security practices, and roles and responsibilities during incident response.

Organizations should continue to communicate and update relevant stakeholders. Some victims are reluctant to notify because they do not want to advertise what happened. Organizations may need to consider if sharing specific incident details judiciously and securely could prevent similar attacks.

TWO DAYS AND BEYOND

What to Expect:

- Incident response may take more than 48 hours; personnel may become fatigued, and resources strained
- Staff may be unfamiliar with operating in manual mode, causing delays in response and services
- Municipal administrative functions (e.g., timesheet, payroll) may be impacted in addition to public safety operations
- Jurisdictional partners may experience similar incidents or attacks
- There may be pressure from leadership, media, and the public demanding incident details and immediate mitigation solutions

EXAMPLE INCIDENT RESPONSE/RECOVERY ESSENTIAL ACTIONS:

- Ensure root cause has been eliminated or mitigated
- Identify infrastructure problems to address
- Identify organizational policy and procedural problems to address
- Review and update roles, responsibilities, interfaces, and authority to ensure clarity
- Identify technical or operational training needs
- Improve tools required to perform protection, detection, analysis, or response actions

Advice from Colleagues:

As the response operation continues, organizations should maintain previously established procedures unless they discover additional issues. For example, if the cyber response has transitioned to cyber recovery, organizations need to maintain strategic coordination to keep bringing sanitized devices and systems back online. If the incident remains in eradication and containment phase, organizations should continue to deploy and manage resources to maintain coverage while avoiding fatigue.

Organizations could also consider conducting a hotwash to discuss initial after-action lessons and insights while the response and recovery process continues. Documentation of crucial observations and findings should include:

- Indicator of compromise
- Adversary tactics, techniques, and procedures
- Log data and technical artifacts
- Indication of additional victims (in cases of malicious cyberattacks)
- Safeguard or mitigation that would prevent a similar incident from occurring in the future

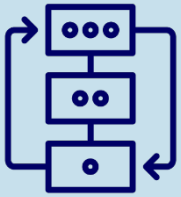
Reviews and discussions of incident artifacts and documentation could impact response and recovery in real-time. In addition, such discussions could assist external investigative organizations, such as the FBI and CISA, to better analyze the incident and develop leads.

Conclusion

As highlighted in the numerous interviews that helped build the expertise in this document, the preparation before any cyber incident occurs will determine actual response success. Cybersecurity is a shared responsibility; identifying, coordinating, and cementing relationships with all partners will impact the success of the incident response.

SUMMARY OF RECOMMENDATIONS

Build a culture of cyber readiness



Engage with leadership and review organizational cyber incident response planning

Establish and maintain close relationships and maintain points of contact with cybersecurity partners and involve them in the planning and preparation process, such as:

- Organization leadership and staff
- Network system providers (including internal and external interfaces)
- Identity management administrators
- Cyber threat intelligence sources
- Entities with potential mission impacts (e.g., jurisdictional partners)
- Response, investigative, and recovery resources
- Third-party vendors
- Public information offices

Review cyber resources (Appendix B: Cybersecurity Planning Resources)

Regularly review and assess cybersecurity posture

Holistically review operational posture to remain resilient in instances of non-cyber human-caused or natural disruptions

Appendix A: Common Cyber Incident Response Pitfalls and Solutions

Below is a list of common cyber incident response pitfalls and corresponding solutions presented throughout the document. Please note the lists are not comprehensive. Organizations are recommended to review guidance, requirements, and relevant legislature to ensure solutions are appropriate and tailored to meet their mission needs.

THE FIRST 8 HOURS	THE FIRST DAY	TWO DAYS AND BEYOND
Pitfall: Lack of planning and resources	**Pitfall:** Lack of authority and communication	**Pitfall:** Recovery fatigue
SOLUTIONS: • Ensure the cyber incident response plan is reviewed, practiced, and updated on a scheduled basis • Deploy the cyber incident response plan as soon as signs of compromise are observed • Contact relevant local, state, and federal authorities • Assemble the incident response team • Remove affected devices from the network • Capture and preserve forensic evidence to the greatest extent possible • Ensure system logs are also available for review • Conduct meetings and document all response activities	SOLUTIONS: • Locate remaining backdoor access to the organization and secure these vulnerabilities • Review and authenticate the integrity of backups; once authenticated, apply appropriate backups to unaffected or new machines • Consider collaborating with outside organizations with the subject matter expertise to examine networks and systems to remove the remaining cyber threat • Implement work shifts to alleviate fatigue and maintain continuous coverage • Communicate and keep stakeholders, leadership, the public, and the media informed	SOLUTIONS: • Maintain previously established procedures unless additional issues are discovered • Maintain strategic coordination to continue to bring sanitized devices and systems back online • Conduct a hotwash to discuss initial after-action lessons and insights while the response and recovery process continues

Appendix B: Cybersecurity Planning Resources

- Public Safety Communications and Cyber Resiliency Toolkit: An interactive directory of resources that assist public safety agencies and others responsible for communications networks in evaluating current resiliency capabilities, identifying ways to improve resiliency, and developing plans for mitigating the effects of potential resiliency threats.
- Cyber Resiliency Resources for Public Safety Fact Sheet: A compilation of cyber resiliency assessment tools and programs provided by the federal government, industry, and trade associations designed to assist agencies in taking proactive measures to enhance their overall cybersecurity posture.
- Guide to Getting Started with a Cyber Risk Assessment: Public safety organizations may use this customizable guide to learn about and document organizational networks, components, risk levels, and vulnerabilities.
- Cyber Essentials: A guide for leaders of small and local government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices. The Cyber Essentials Starter Kit contains the basics for building a culture of cyber readiness.
- Federal Government Cybersecurity Incident and Vulnerability Response Playbooks: Operational procedures for planning and conducting cybersecurity incident and vulnerability response activities in Federal Civilian Executive Branch (FCEB) Information Systems that can also be used by critical infrastructure entities; state, local, territorial, and tribal government organizations; and private sector organizations to benchmark their vulnerability and incident response practices. The playbooks provide illustrated decision trees and detail each step for both incident and vulnerability response.
- CISA Interoperable Communications Technical Assistance Program (ICTAP): The ICTAP serves all 56 states and territories and provides direct support to state, local, and tribal emergency responders and government officials through the development and delivery of training, tools, and onsite assistance to advance public safety interoperable communications capabilities. Example public safety communications resiliency-specific services include public safety answering point cyber awareness webinar, Statewide Communication Interoperability Plan workshop, Next Generation 911 strategic planning, and other cybersecurity technical assistance offerings.
- Incident Response Training: CISA offers a no-cost cybersecurity incident response training for government employees and contractors across federal, state, local, tribal, and territorial government, and is also open to educational and critical infrastructure partners.
- Detection and Prevention: CISA rapidly notifies relevant critical infrastructure stakeholders of elevated risk exposure, conducts incident management operations, provides vulnerability assessments, and directly deploys risk management information, tools, and technical services to mitigate risk, including regulatory enforcement where authorized.
- Subscribe to Cybersecurity and Infrastructure Security Agency (CISA) Alerts: Sign up to receive CISA-curated alerts and notifications.
- Report Cyber Issue: Report incidents, phishing attempts, malware, and vulnerabilities through CISA's secure mechanism.