CYBER RISK TO PUBLIC SAFETY: RANSOMWARE

RANSOMWARE IMPACTS ON PUBLIC SAFETY

If you are experiencing a ransomware attack, please go directly to page 3 for incident reporting resources

Ransomware is a type of malicious software that encrypts information stored on hard drives or network drives and disrupts access to compromised devices or networks. Ransomware applications threaten to erase, lock, or otherwise damage compromised drives and data unless payment is provided. Ransomware programs often elicit a sense of urgency (e.g., a short deadline for payment) to encourage affected organizations to pay. Ransomware applications may threaten to escalate demands (e.g., increase payment) if payment is not provided quickly. Even when payments are provided, malicious actors may steal sensitive information, default on agreements to restore access, or conduct follow-up cyberattacks. While ransomware typically aims to extort money from organizations, malicious actors may also target public safety agencies or critical infrastructure with the goal of disrupting emergency response capabilities.

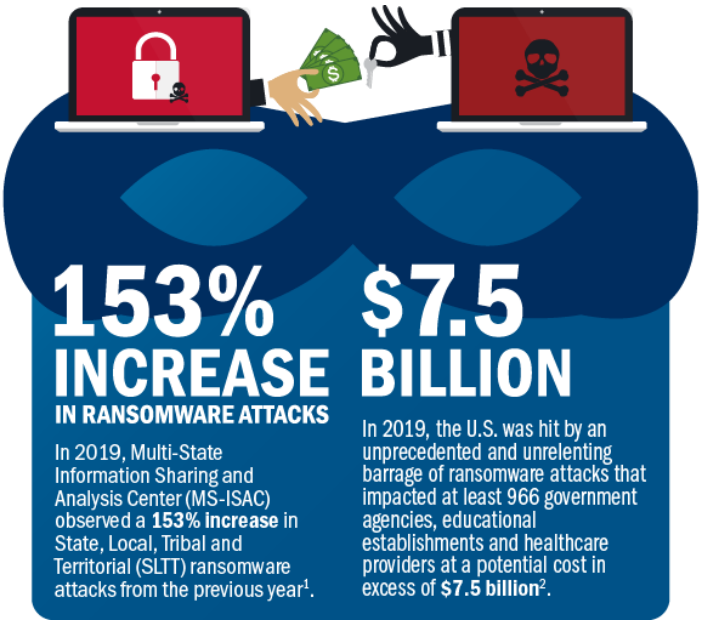

Figure 1. Recent Ransomware Attack Statistics

Ransomware can have a significant impact on public safety operations, including services provided by fire, emergency medical services, law enforcement, emergency communication centers/public safety answering points, and other public safety partners. Disruptions to public safety operations directly and negatively impact the health and safety of the communities they serve. For example, delays dispatching fire and emergency medical services may lead to increased loss of life and property damage. Malicious actors may target public safety agencies specifically to exploit these negative outcomes, creating a strong sense of urgency to accommodate perpetrator demands. Public safety agencies are highly encouraged to plan and prepare for a ransomware event to mitigate service disruptions, conduct effective response operations, and ensure rapid recovery.

CYBER VULNERABILITIES

Malicious actors may use a variety of technical methods to exploit an organization's cyber vulnerabilities and disperse ransomware onto mission critical systems. Common ransomware techniques include social engineering, spreading from interconnected networks, or entering through unauthorized remote access applications.

- **Social engineering attacks** are designed to trick authorized users into granting network access to perpetrators by revealing credentials or downloading malicious software, for example. Social engineering attacks aim to exploit trusted relationships, such as family, friends, coworkers, or familiar organizations (e.g., financial institutions, charities), to provide the illusion of legitimacy.

[1] Center for Internet Security (CIS), "Security Primer – Ransomware," last modified May 2020, https://www.cisecurity.org/white-papers/security-primer-ransomware/.
[2] Emsisoft Malware Lab, "The State of Ransomware in the US: Report and Statistics 2019," last modified December 2019, https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/.

- **Interconnected systems** may expose mission critical capabilities, such as computer aided dispatch, to cyber intrusions in other parts of a network. Malicious actors may exploit cyber vulnerabilities in other state or local agencies (e.g., transportation, public works, finance, criminal justice) to spread malicious software to public safety stakeholders.
- Third-party vendors may use **remote access applications** to provide technology support, such as troubleshooting and software maintenance, to mission critical systems. Malicious actors may exploit unsecured connections to upload ransomware applications using a vendor's access permissions.

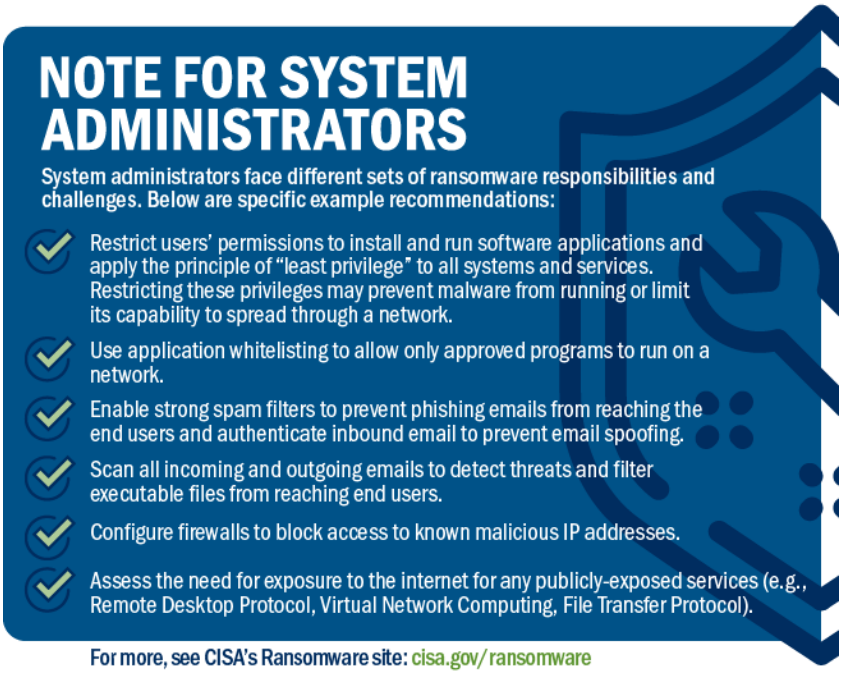

Figure 2. Example Recommendations for System Administrators

Additionally, operational weaknesses may exacerbate the severity of ransomware events, including insufficient systems analysis, lack of pre-incident response or recovery planning, and inadequate access management controls.

PUBLIC SAFETY RESILIENCY AND RESPONSE TO RANSOMWARE

To reduce cyber risk and impacts on operations, public safety organizations should adopt best practices to protect against, respond to, and recover from ransomware events. Instituting cybersecurity risk management best practices, as detailed in the **Appendix**, can establish a strong cybersecurity posture. The following sections build upon that foundation and provide best practices explicitly for the ransomware threat.

Protect

To protect the network from a ransomware attack, organizations should:

- Backup all mission critical data and applications on a consistent basis to a non-networked storage medium, verifying their integrity and restoration process, and securely store the backups.
- Implement resilient network designs (e.g., segmenting mission critical functions, strong access controls, two-factor authentication for staff logins) to limit the impact of a ransomware event, and implement continuous network monitoring solutions to identify suspicious network traffic and analyze threats.
- Apply strong access controls, such as limiting administrator access and requiring unique staff logins, to narrow the scope of a ransomware intrusion.
- Maintain mission critical systems, apply all manufacturer software patches, and secure legacy equipment; if possible, remove unsupported legacy systems to prevent easy infiltration.[3]
- Conduct regular cybersecurity gap analysis of networks to proactively identify and mitigate security vulnerabilities.

[3] CIS, ibid.

Respond

As soon as reports of a potential ransomware attack are received, or signs of an attack become evident, public safety organizations should:

- Execute response plan activities to isolate the cyber intrusion and mitigate impacts; remove the infected system from all networks; disable the computer's wireless, Bluetooth, and any other potential networking capabilities; disconnect all shared and networked drives, whether wired or wireless.
- Power-off and segregate the infected computer(s) and any other computers or devices that shared a network with the infected computer(s) that have not been fully encrypted by ransomware; collect and label all infected and potentially infected equipment and secure them in a central location.
- Report incident to the organization's legal counsel, federal law enforcement, and the cybersecurity insurer, if insured; alert the organization's personnel, share alternate assistance routes for mission critical functions, and also alert the public; activate mutual aid agreements or memoranda of understanding with partner organizations to ensure continued emergency service operations.
- Share incident data with information technology (IT) staff, federal cybersecurity partners, and relevant state, local, tribal, or territorial stakeholders (e.g., Statewide Interoperability Coordinator [SWIC], Cybersecurity and Infrastructure Security Agency [CISA] Emergency Communications Coordinator, CISA Cybersecurity Advisor, other government agencies, mutual aid signatories).

Recover

During the recovery period, public safety organizations should:

- Use system backups to restore pre-incident data; prior to restoration, if possible, inspect the backups for latent ransomware applications and restore to a more resilient system that is fully patched and updated.
- Conduct an after-action analysis to identify vulnerabilities and mitigate gaps (e.g., technology, operational procedures, training).
- Revise response and recovery plans using lessons learned; reevaluate mutual aid agreements to ensure continued emergency operations in the future.
- Evaluate cybersecurity insurance requirements and the benefits and risks of third-party vendor services.

RESOURCES

If your organization is experiencing a ransomware event, immediately contact IT, legal counsel, cybersecurity partners, state or regional coordinators (e.g., SWICs), and federal stakeholders for assistance. In addition, alert the public and share alternate assistance routes. The table below identifies federal organizations for assistance and reporting guidance:

Federal Partner	Component	When to Report
CISA	CISA Central	Suspected or confirmed cyber incidents that may impact critical infrastructure and require technical response or mitigation assistance
Federal Bureau of Investigation (FBI)	FBI Field Offices Cyber Task Forces Law Enforcement Enterprise Portal	Cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity
United States Secret Service	Secret Service Field Offices Electronic Crimes Task Forces	Cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card and other financial payment information

For more information on ransomware, visit the CISA Ransomware portal for training resources, mitigation best practices, and cybersecurity alerts. These resources include CISA's Ransomware Security Publication, technical guidance on How to Protect Your Networks from Ransomware, Awareness Briefings on Combating Ransomware, CISA Insights – Ransomware Outbreak, and the CISA Protect Your Center from Ransomware poster. Additional cybersecurity resources for 911 and Next Generation 911 systems can be found at cisa.gov/safecom/next-generation-911.

Additional resources such as the MS-ISAC Security Primer on Ransomware, National Governor's Association Disruption Response Planning Memo, and the National Association of State Chief Information Officers' Cyber Disruption Response Planning Guide could assist in preparing comprehensive ransomware response policies and procedures.

APPENDIX: CYBER RISK MANAGEMENT BEST PRACTICES

Consistent practice of cyber risk management best practices can help public safety organizations maintain or improve their cybersecurity posture:

- Establish a cybersecurity risk management process[4] to holistically address cyber gaps; provide cybersecurity training and direct cybersecurity awareness campaigns for all personnel.
- Adopt National Incident Management System resource typing for cybersecurity assets; standardize response resources and operational principles between partner organizations.
- Conduct cybersecurity vulnerability assessments to proactively identify and resolve risk; employ routine audits of network activity to identify suspicious behavior. See cisa.gov/cyber-resource-hub for a list of free CISA assessment services that can help with these practices.
- Obtain cybersecurity insurance and identify emergency funding mechanisms to cover cyber incident costs.
- Coordinate with third-party vendors to limit network access and identify cybersecurity vulnerabilities from interconnected services.

A critical part of any cybersecurity risk management process is a cyber incident response plan. As part of this plan, organizations should:

- Incorporate how to respond to ransomware and other cyber events, outline operational procedures to detect suspicious network traffic, analyze threats, respond to incidents, and maintain critical functions during recovery.
- Define the responsibilities of staff and partner organizations, incident notification requirements, and alternate assistance routes for the public, including all relevant public and private sector partners in the planning process; ensure incident response plans align with state and federal guidelines, such as the National Cyber Incident Response Plan.
- Engage state and local decision-makers to ensure that cyber legislation, regulations, authorities, and policies clearly support rapid ransomware response.
- Establish mutual aid agreements or memoranda of understanding with other public safety partners to ensure continued operations during a ransomware incident.

As the nation's risk advisor, the CISA offers a variety of support to the public safety community. Visit cisa.gov/emergency-communications to see CISA's full suite of tools, guidance, and resources.

[4] The National Institute of Standards and Technology Cybersecurity Framework is a flexible, risk-based approach to improving the security of critical infrastructure and is designed to complement an existing risk management process or to help develop a credible program if one does not exist. Public safety cyber risk programs should be coordinated with existing and future DHS Threat and Hazard Identification and Risk Assessment (THIRA)/Stakeholder Preparedness Review (SPR) requirements.