PUBLIC NOTICE

Federal Communications Commission
45 L Street NE
Washington, DC 20554

News Media Information 202-418-0500
Internet: www.fcc.gov

DA 26-96
Released: January 29, 2026

PUBLIC SAFETY AND HOMELAND SECURITY BUREAU HIGHLIGHTS BEST PRACTICES FOR DEFENDING AGAINST RANSOMWARE ATTACKS

By this Public Notice, the Public Safety and Homeland Security Bureau (Bureau) of the Federal Communications Commission (Commission) urges communications providers to implement cybersecurity best practices to protect their networks from the introduction of malware, including ransomware. Recent events show that some U.S. communications networks are vulnerable to cyber exploits that may pose significant risks to national security, public safety, and business operations.[1] Specifically, over the past year, the Commission has become aware of ransomware incidents involving small-to-medium sized communications companies that disrupted service, exposed information, and locked providers out of critical files.

What is Ransomware?

Ransomware is malicious code designed to encrypt files on a device, rendering them and the systems on which they rely unusable. In some instances, it can involve the theft of exfiltrated data from the targeted devices and systems.[2] Threat actors can launch ransomware attacks after gaining initial access by various methods, including: (1) engaging in social engineering;[3] (2) hiding malware in downloads of software; (3) creating fake or compromised websites that prompt the user to download ransomware; (4) exploiting vulnerabilities in remote access or management software; and (5) using stolen credentials obtained from access brokers or other unlawful sources. After obtaining initial access, cyber criminals establish persistent access; conduct network reconnaissance; and use privilege escalation, lateral movement, and defensive evasion to plant ransomware.[4] Once ransomware is successfully executed on a device or in a system, malicious actors typically demand a ransom in exchange for decrypting the files targeted or for preventing the release of stolen data.[5] Ransomware incidents can severely impair an organization's ability to conduct operations, leaving it unable to access data or systems necessary to

[1] *See* Cyble Inc., Telecommunications Sector: Threat Landscape Report 2025 (2025), https://cyble.com/resources/research-reports/telecommunications-sector-threat-landscape-report-2025. Notably, the report cites a four-fold increase in ransomware attacks against communications providers since 2021, notes the value of provider-held data, and specifies that ransomware attacks are not limited to major carriers, but also affect, among others, regional operators and vendors. *Id.* at 7, 10.

[2] CISA, *#StopRansomware Guide*, https://www.cisa.gov/stopransomware/ransomware-guide (last visited Jan. 29, 2026); NIST, *Ransomware*, https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware (last visited Jan. 29, 2026).

[3] Social engineering can include phishing or sharing links on popular user sites where users share comments and tips.

[4] Dept. of Health and Human Services, Health Sector Cybersecurity Coordination Center, HC3: Analyst Note, Akria Ransomware at 2-3 (2024), https://www.hhs.gov/sites/default/files/akira-randsomware-analyst-note-feb2024.pdf.

[5] CISA, *#StopRansomware Guide*, https://www.cisa.gov/stopransomware/ransomware-guide (last visited Jan. 29, 2026); NIST, *Ransomware*, https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware (last visited Jan. 29, 2026).

provide service to the public.[6] The time and services that entities lose responding to a ransomware attack—as well as the ransom itself, if paid—can be both costly and disruptive.[7] Depending on their effects, ransomware attacks may also require reporting the attack to the Commission or federal law enforcement.

Communications providers should review the below resources related to ransomware attacks, including best practices designed to prevent such attacks and steps to take if you are the target of an attack. Adopting these measures can help secure the nation's critical infrastructure by preventing and mitigating communications network outages, protecting sensitive information, and promoting the continuity of business operations.

Best Practices for Preventing and Mitigating Ransomware Attacks

(1) *Develop a Cybersecurity Risk Management Plan*. Referencing best practices and industry standards will assist communications providers in developing a plan for their organizations to respond to a ransomware attack. Having a plan in place that creates incident response teams, assigns clear responsibilities to key employees, and includes response planning can provide concrete steps to follow if an attack occurs and help minimize stress or panic in reacting to attacks.

(2) *Regularly Update and Patch Software and Disable Unnecessary Features*. Using the most recent software updates and promptly applying applicable security patches can provide critical defenses against viruses, malware, and other online threats.

(3) *Enable Multi-Factor Authentication (MFA)*. Implementing MFA as part of an authentication and access management strategy helps guard against unauthorized network access.

(4) *Regularly Back Up Data*. Having robust backup data processes in place is essential to facilitating data restoration in the event of an attack.

(5) *Train Employees in Cybersecurity Awareness and Security Principles*. Educating employees and conducting periodic cyber-hygiene training reduces vulnerabilities and fosters increased network security to help prevent breaches.

(6) *Segment Network Appropriately While Implementing a "Zero Trust" Architecture*. Network segmentation helps minimize the impact of an attack by establishing important controls on network access.

(7) *Deploy Detection and Protection Processes and Regularly Scan for Vulnerabilities*. Maintaining awareness of network conditions and proactively monitoring for suspicious activities enables companies to more quickly identify and respond to potential threats. Monitoring approaches include implementing intrusion detection and prevention systems (IDS/IPS), endpoint detection and response (EDR), running regular vulnerability scans, monitoring logs and setting alerts for unusual login attempts or network activity, and staying up to date on threat intelligence by subscribing to threat monitoring sources.

(8) *Evaluate Third-Party Risk*. Evaluating the cybersecurity practices and monitoring the vulnerability of third-party vendors reduces the risk of threats that occur outside the provider's controlled infrastructure.

The attached Appendix contains a sample of best practices that address some of these measures in greater detail.

[6] CISA, *#StopRansomware Guide*, https://www.cisa.gov/stopransomware/ransomware-guide (last visited Jan. 29, 2026).

[7] *Id.*

Responding to an Attack

It is important to respond quickly and effectively to a ransomware attack. When responding, providers should take steps to mitigate the effects of the attack. These include:

(1) *Follow Your Cybersecurity Risk Management Plan*. Resist an attacker's attempts to sow chaos or create false urgency, and follow the cybersecurity risk management plan your organization developed before the attack. Engage incident response teams to understand how to mitigate, respond to, and recover from the incident.

(2) *Identify and Isolate*. Identify the scope/impact of the intrusion and immediately isolate affected systems to stop the spread of the ransomware.

(3) *Preserve Evidence*. Take system images and conduct memory capture of affected devices. Collect and preserve any relevant logs.

(4) *Patch and Harden Systems*. Patch and update systems and software to address the vulnerability that enabled the ransomware. In many cases, harden systems by issuing password reset to all affected accounts and enabling additional security controls, as applicable.

(5) *Restore Data*. Restore enterprise and customer data from clean backups (which were ideally stored offline and encrypted).

(6) *Report the Incident to the FCC and Law Enforcement as Appropriate*.

a. If a ransomware attack results in the compromise of Customer Proprietary Network Information (CPNI), the breach must be reported as soon as practicable, and in no event later than seven business days after reasonable determination of the breach, to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) via the reporting portal accessible at https://www.cpnireporting.gov.[8]

b. If the attack results in a network outage subject to the Commission's reporting rules, providers are required to submit notifications and reports to the Commission, 911 special facilities, and/or 988 special facilities on the required timelines.[9]

c. If the attack results in the unauthorized transmission of Emergency Alert System codes or Attention Signal, it must be reported to the FCC Operations Center at FCCOPS@fcc.gov within 24 hours.[10]

d. Even if the attack does not trigger any of the above reporting requirements, consider reporting it to the FCC and federal law enforcement for their situational awareness and assistance. Relevant contact information is below:

- ***FCC Operations Center***: Available 24 hours a day, 365 days a year, the FCC Operations Center is available to assist public safety, government, and communications industry stakeholders with emergency communications needs. The FCC Operations Center can be reached at FCCOPS@fcc.gov or 202-418-1122.
- ***Federal Law Enforcement Resources***: These agencies conduct law enforcement and national security investigations of cyber incidents.
    - **Internet Crime Complaint Center (IC3)**: IC3 is the central hub for reporting cybercrime. The IC3's website is designed to provide information about the latest and most harmful cyber threats and scams:

[8] *See* 47 U.S.C. § 222; 47 CFR § 64.2011(b). Following law enforcement notification, the Commission's rules also require notification to affected customers of a breach of those customers' CPNI. 47 CFR § 64.2011(c).

[9] *See* 47 CFR § 4.9.

[10] 47 CFR § 11.45(b).

https://www.ic3.gov/Home/Index. The website also receives complaints and reports that help the FBI and its partners to bring cyber criminals to justice: https://complaint.ic3.gov/.

- **Federal Bureau of Investigation (FBI)**: Contact the appropriate local FBI field office by phone or email. Find your local field office here: https://www.fbi.gov/contact-us/field-offices.
- **United States Secret Service (USSS)**: Contact the appropriate local USSS field office by phone or email. Find your local field office here: https://www.secretservice.gov/contact/field-offices.

- ***Federal Asset Response Resources***: These agencies can provide technical assistance to help protect assets, mitigate vulnerabilities, and reduce the impact of the cyber incident.
  - **Cybersecurity and Infrastructure Security Agency (CISA)**. Email: Central@cisa.gov; Phone: 1-844-729-2472.
  - **MS-ISAC for State, Local, Tribal, and Territorial Government entities**. Email: soc@msiac.org; Phone: 866-787-4722.

Additional Resources

In addition to the specific best practices included in the Appendix, the following resources provide broader guidance that your organization can implement to protect against and mitigate malware and ransomware attacks.

(1) *FCC's 10 Cyber Security Tips for Small Businesses*. The Commission's tips provide core guidance to small businesses on establishing a cybersecurity strategy to protect their businesses, customers, and data: https://www.fcc.gov/communications-business-opportunities/cybersecurity-small-businesses.

(2) *Federal Trade Commission (FTC) Ransomware Business Guidance.* The FTC provides cybersecurity guidance for small businesses: https://www.ftc.gov/business-guidance/small-businesses/cybersecurity.

(3) *National Institute of Standards and Technology (NIST) Cybersecurity Framework (Framework).* The NIST Framework helps businesses understand, manage, and reduce their cybersecurity risk and protect their networks and data: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

(4) *CSRIC Industry Best Practices.* CSRIC publishes industry best practices vital to the reliability of the nation's public communications networks and services. Users can select categories of interest, including cybersecurity: https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/about_data.

(5) *CISA's #StopRansomware Guide.* CISA publishes a ransomware guide with input from the Multi-State Information Sharing and Analysis Center (MS-ISAC), the National Security Agency, and the FBI: https://www.cisa.gov/stopransomware/ransomware-guide.

(6) *CISA's Known Exploited Vulnerabilities Catalog*. CISA maintains an authoritative source of vulnerabilities to help organizations keep pace with threat activity and better manage these risks: https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

For more information, contact Jeanne Stockman, Jeanne.Stockman@fcc.gov, or George Weber, George.Weber@fcc.gov, Attorney-Advisors, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau.

APPENDIX

Select Best Practices to Prevent, Respond, and Recover from Ransomware Attacks

(1) *Regularly Update and Patch Software and Disable Unnecessary Features*

- **Communications Security, Reliability, and Interoperability Council (CSRIC) Best Practice 13-8-8020:** Network Operators, Service Providers, and Equipment Suppliers should have special processes and tools in place to quickly patch critical infrastructure systems when important security patches are made available. Such processes should include determination of when expedited patching is appropriate and identifying the organizational authority to proceed with expedited patching. This should include expedited lab testing of the patches and their effect on network and component devices.
- **CSRIC Best Practice 13-8-8566:** Network Operators, Service Providers, and Equipment Suppliers should assure that patching distribution hosts properly sign all patches. Critical systems must only use OSs and applications which employ automated patching mechanisms, rejecting unsigned patches. If a patch fails or is considered bad, restore OS and applications from known good backup media.
- **CSRIC Best Practice 13-9-8037:** Network Operators, Service Providers, and Public Safety should maintain a complete inventory of elements to ensure that patches/fixes can be properly applied across the organization. This inventory should be updated each time a patch/fix is identified and action is taken.
- **CSRIC Best Practice 13-9-8039:** Service Providers, Network Operators, and Public Safety should perform a verification process to ensure that patches/fixes are actually applied as directed throughout the organization. Exceptions should be reviewed and the proper patches/fixes actually applied.
- **CSRIC Best Practice 13-9-8756:** Network Operators and Public Safety should establish and implement procedures to ensure that all security patches and updates relevant to the device or installed applications are promptly applied. The patching process should be automated whenever possible. The system should be rebooted immediately after patching if required for the patch to take effect.

(2) *Enable Multi-Factor Authentication (MFA)*

- **CSRIC Best Practice 13-13-8768:** Network Operators, Service Providers, Equipment Suppliers, Public Safety and Government should support multi-factor authentication to increase confidence in the identity of an entity.
- **CSRIC Best Practice 13-12-8081**: Network Operators, Service Providers, Equipment Suppliers and Public Safety should develop an enforceable password policy, which considers different types of users, requiring users to protect, as applicable, either (a) the passwords they are given/create or (b) their credentials for two-factor authentication.
- **CSRIC Best Practice 13-12-8126**: Network Operators, Service Providers, Equipment Suppliers and Public Safety should employ authentication methods commensurate with the business risk of unauthorized access to the given network, application, or system. For example, these methods would range from single-factor authentication (e.g., passwords) to two-factor authentication (e.g., token and PIN) depending on the estimated criticality or sensitivity of the protected assets. When

two-factor authentication generates one-time passwords, the valid time-duration should be determined based on an assessment of risk to the protected asset(s).

(3) *Regularly Back Up Data*

- **CSRIC Best Practice 13-10-1047**: Network Operators, Service Providers, and Public Safety should develop a process to routinely archive critical system backups and provide for storage in a secure off-site facility which would provide geographical diversity.
- **CSRIC Best Practice 13-9-0415**: Network Operators, Service Providers, and Public Safety should test the restoral process associated with critical data back-up, as appropriate.

(4) *Train Employees in Cybersecurity Awareness and Security Principles*

- **CSRIC Best Practice 13-10-0511**: Network Operators, Service Providers, Equipment Suppliers, and Public Safety should ensure that appropriate operations personnel involved in the direct operation, maintenance, provisioning, security, troubleshooting, repair, and support of network elements are provided periodic training.
- **CSRIC Best Practice 13-13-8970**: Network Operators, Public Safety and Government should ensure that staff is well trained, in reporting of security incidents, weaknesses and suspicious activity and are equipped with intrusion detection capability, response tools, and processes linking operations alarms with security alerts that would support rapid response and mitigation capability.
- **CSRIC Best Practice 13-13-8946**: Public Safety, Government should provide cyber hygiene training to staff that includes informing end users on proper email and web usage, highlighting current information and analysis, and including common indicators of phishing.

(5) *Segment Network Appropriately While Implementing a "Zero Trust" Architecture*

- **CSRIC Best Practice 13-13-8947:** Network Operators, Service Providers, Equipment Suppliers, Public Safety and Government should implement the "least-privilege-principle" for security in all public safety systems; meaning, provide access only to those resources that an individual should have access to.
- **CSRIC Best Practice 13-13-8955**: Network Operators, Service Providers, Public Safety and Government should provide a well-architected, segmented network.
- **CSRIC Best Practice 13-13-8948:** Network Operators, Service Providers, Public Safety and Government should log, monitor, and audit all employee electronic activity.
- **CSRIC Best Practice 13-13-8943**: Public Safety, Government should segment any critical networks or control systems from administrative systems and networks.

(6) *Deploy Detection and Protection Processes and Regularly Scan for Vulnerabilities*

- **CSRIC Best Practice 13-9-8103:** Network Operators, Service Providers, and Public Safety should deploy malware protection tools where feasible, establish processes to keep signatures current, and establish procedures for reacting to an infection.
- **CSRIC Best Practice 13-6-8023:** Network Operators and Service Providers should regularly scan infrastructure for vulnerabilities/exploitable conditions. Operators should understand the operating systems and applications deployed on their network and keep abreast of vulnerabilities, exploits, and patches.

- **CSRIC Best Practice 13-8-8913:** Service Providers should maintain methods to detect likely bot/malware infection of customer equipment. Detection methods will vary widely due to a range of factors. Detection methods, tools, and processes may include but are not limited to: external feedback, observation of network conditions and traffic such as bandwidth and/or traffic pattern analysis, signatures, behavior techniques, and forensic monitoring of customers on a more detailed level.
- **CSRIC Best Practice 13-8-8060:** Network Operators and Service Providers should ensure strong separation of data traffic from management/signaling/control traffic, via firewalls. Network operators should ensure strong cellular network backbone security by employing operator authentication, encrypted network management traffic and logging of security events. Network operators should also ensure operating system hardening and up-to-date security patches are applied for all network elements, element management system and management systems.
- **CSRIC Best Practice 13-13-8965:** Network Operators, Service Providers, Public Safety and Government should continuously monitor IP traffic for scanning, phishing attacks, and other suspicious cyber activity.
- **CSRIC Best Practice 13-13-8936:** Network Operators, Service Providers, Equipment Suppliers, Public Safety and Government should exercise third-party vulnerability testing on a regular basis.