Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches

OVERVIEW

Over the past several years, the Cybersecurity and Infrastructure Security Agency (CISA) and our partners have responded to a significant number of ransomware incidents, including recent attacks against a U.S. pipeline company and a U.S. software company, which affected managed service providers (MSPs) and their downstream customers.

> Ransomware is a serious and increasing threat to all government and private sector organizations, including critical infrastructure organizations. In response, the U.S. government launched StopRansomware.gov, a centralized, whole-of-government webpage providing ransomware resources, guidance, and alerts.

Ransomware is malware designed to encrypt files on a device, rendering files and the systems that rely on them unusable. Traditionally, malicious actors demand ransom in exchange for decryption. Over time, malicious actors have adjusted their ransomware tactics to be more destructive and impactful. Malicious actors increasingly exfiltrate data and then threaten to sell or leak it—including sensitive or personal information—if the ransom is not paid. These data breaches can cause financial loss to the victim organization and erode customer trust.

All organizations are at risk of falling victim to a ransomware incident and are responsible for protecting sensitive and personal data stored on their systems. This fact sheet provides information for all government and private sector organizations, including critical infrastructure organizations, on preventing and responding to ransomware-caused data breaches. CISA encourages organizations to adopt a heightened state of awareness and implement the recommendations below.

PREVENTING RANSOMWARE ATTACKS

1. **Maintain offline, encrypted backups of data and regularly test your backups**. Backup procedures should be conducted on a regular basis. It is important that backups be maintained offline as many ransomware variants attempt to find and delete or encrypt accessible backups.

2. **Create, maintain, and exercise a basic cyber incident response plan, resiliency plan, and associated communications plan.**

    - The cyber incident response plan should include response and notification procedures for ransomware incidents. See the CISA and Multi-State Information and Sharing Center (MS-ISAC) Joint Ransomware Guide for more details on creating a cyber incident response plan.

    - The resilience plan should address how to operate if you lose access to or control of critical functions. CISA offers no-cost, non-technical cyber resilience assessments to help organizations evaluate their operational resilience and cybersecurity practices.

3. **Mitigate internet-facing vulnerabilities and misconfigurations** to reduce risk of actors exploiting this attack surface.

    a. **Employ best practices for use of Remote Desktop Protocol (RDP) and other remote desktop services.** Threat actors often gain initial access to a network through exposed and poorly secured remote services and later propagate ransomware.

        i. Audit the network for systems using RDP, closed unused RDP ports, enforce account lockouts after a specified number of attempts, apply multi-factor authentication (MFA), and log RDP login attempts.

b. **Conduct regular vulnerability scanning** to identify and address vulnerabilities, especially those on internet-facing devices. CISA offers a range of no-cost cyber hygiene services, including vulnerability scanning, to help critical infrastructure organizations assess, identify, and reduce their exposure to cyber threats, such as ransomware. By taking advantage of these services, organizations of any size will receive recommendations on ways to reduce their risk and mitigate attack vectors.

c. **Update software**, including operating systems, applications, and firmware, in a timely manner. Prioritize timely patching of critical vulnerabilities and vulnerabilities on internet-facing servers—as well as software processing internet data, such as web browsers, browser plugins, and document readers. If patching quickly is not feasible, implement vendor-provided mitigations.

d. **Ensure that devices are properly configured and security features are enabled**, e.g., disable ports and protocols that are not being used for a business purpose.

e. **Disable or block inbound and outbound Server Message Block (SMB) Protocol** and remove or disable outdated versions of SMB.

4. **Reduce the risk of phishing emails** from reaching end users by:

   a. **Enabling strong spam filters.**

   b. **Implementing a cybersecurity user awareness and training program** that includes guidance on how to identify and report suspicious activity (e.g., phishing) or incidents. CISA offers a no-cost Phishing Campaign Assessment for organizations to support and measure the effectiveness of user awareness training.

5. **Practice good cyber hygiene** by:

   a. **Ensuring antivirus and anti-malware software and signatures are up to date.**

   b. **Implementing application allowlisting.**

   c. **Ensuring user and privileged accounts are limited** through account use policies, user account control, and privileged account management.

   d. **Employing MFA** for all services to the extent possible, particularly for webmail, virtual private networks (VPNs), and accounts that access critical systems.

   e. **Implementing cybersecurity best practices** from CISA's Cyber Essentials and the CISA-MS-ISAC Joint Ransomware Guide.

Note: organizations relying on MSPs for remote management of IT systems should take into consideration the risk management and cyber hygiene practices of their MSP. Refer to CISA Insights: Mitigations and Hardening Guidance for MSPs and Small- and Mid-sized Businesses for additional guidance on hardening systems against cyber threats, including ransomware.

PROTECTING SENSITIVE AND PERSONAL INFORMATION

Organizations storing sensitive or personal information of customers or employees are responsible for protecting it from access or exfiltration by malicious cyber actors. CISA recommends that organizations:

1. **Know what personal and sensitive information is stored on your systems and who has access to it**. Limit the data by only storing information you need for business operations. Ensure data is properly disposed of when no longer needed.

2. **Implement physical security best practices** from the Federal Trade Commission (FTC): Protecting Personal Information: A Guide For Business and FTC: Cybersecurity for Small Business. (See CISA: Cybersecurity and Physical Security Convergence Guide for more information on the importance of physical security for IT assets.)
3. **Implement cybersecurity best practices** by:
    a. **Identifying the computers or servers where sensitive personal information is stored. Note:** do not store sensitive or personal data on internet-facing systems or laptops unless it is essential for business operations. If laptops contain sensitive data, encrypt them and train employees on proper physical security of the device.
    b. **Encrypting sensitive information** at rest and in transit.
    c. **Implementing firewalls** to protect networks and systems from malicious or unnecessary network traffic.
    d. **Considering applying network segmentation** to further protect systems storing sensitive or personal information.
4. **Ensure your cyber incident response and communications plans include response and notification procedures for data breach incidents.** Ensure the notification procedures adhere to applicable state laws. (Refer to the National Conference of State Legislatures: Security Breach Notification Laws for information on each state's data breach notification laws.)

For more information and guidance on protecting sensitive and personal information, refer to FTC: Protecting Personal Information: A Guide for Business and FTC: Start With Security: A Guide for Business. For more cybersecurity best practices, refer to CISA's Cyber Essentials.

RESPONDING TO RANSOMWARE-CAUSED DATA BREACHES

Should your organization become a victim of a ransomware incident and associated data breach, CISA strongly recommends implementing your cyber incident response plan and taking the following actions.

> CISA strongly discourages paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or may fund illicit activities. Paying the ransom also does not guarantee that a victim's files will be recovered.

1. **Secure network operations and stop additional data loss** by using the following checklist, moving through the first three steps in sequence. Note: CISA recommends including this checklist as a ransomware-specific annex in cyber incident response plans. See the CISA-MS-ISAC Joint Ransomware Guide for a full ransomware response checklist.
    a. **Determine which systems were impacted and immediately isolate them.** If several systems appear impacted, take the network offline at the switch level. If taking the network temporarily offline is not immediately possible, locate the network (e.g., Ethernet) cable and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.
    b. **If—and only if—affected devices cannot be removed from the network or the network cannot be temporarily shut down, power infected devices down to avoid further spread of the ransomware infection. Note:** this step should be carried out only if necessary because it may result in the loss of infection artifacts and potential evidence stored in volatile memory.
    c. **Triage impacted systems for restoration and recovery.** Prioritize based on criticality.
    d. **Confer with your team to develop and document an initial understanding** of what has occurred based on preliminary analysis.

e. **Engage your internal and external teams and stakeholders** to inform them of how they can help you mitigate, respond to, and recover from the incident. Strongly consider requesting assistance from a reputable third-party incident response provider with experience in data breaches.

2. **If no initial mitigation actions appear possible, take a system image and memory capture of a sample of affected devices.** Additionally, collect any relevant logs as well as samples of any "precursor" malware binaries and associated observables or indicators of compromise. **Note:** do not destroy forensic evidence, and take care to preserve evidence that is highly volatile in nature—or limited in retention—to prevent loss or tampering.

3. **Follow notification requirements** as outlined in your cyber incident response plan.

   - If personal information stored on behalf of other businesses is stolen, notify these businesses of the breach.
   - If the breach involved personally identifiable information, notify affected individuals so they can take steps to reduce the chance that their information will be misused. Tell people the type of information exposed, recommend actions, and provide relevant contact information.
   - If the breach involved electronic health information, you may need to notify the FTC or the Department of Health and Human Services, and, in some cases, the media. Refer to Federal Trade Commission's Health Breach Notification Rule and U.S. Department of Health and Human Services: Breach Notification Rule for more information.

     Refer to FTC: Data Breach Response: A Guide for Business for more guidance on notifying affected businesses and individuals.

4. Report the incident to CISA, your local Federal Bureau of Investigation (FBI) field office, the FBI Internet Crime Complaint Center, or your local U.S. Secret Service office.

For additional information and guidance on responding to data breaches, refer to FTC: Data Breach Response: A Guide For Businesses.

ADDITIONAL RESOURCES

- For more information and resources on protecting against and responding to ransomware, refer to StopRansomware.gov.
- CISA's Ransomware Readiness Assessment (RRA) is no-cost self-assessment based on a tiered set of practices to help organizations better assess how well they are equipped to defend and recover from a ransomware incident.
- CISA Tip: Protecting Against Ransomware
- CISA Tip: Preventing and Responding to Identity Theft
- National Institute of Standards and Technology, National Cybersecurity Center of Excellence: Data Confidentiality: Detect, Respond to, and Recover from Data Breaches
- MS-ISAC: Ransomware: The Data Exfiltration and Double Extortion Trends
- FTC's Ransomware Fact Sheet, Quiz, and Video from Cybersecurity For Small Business.