Ransomware

Ransomware is a type of malicious software designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption.

Serious Risks to Paying the Ransom

- Paying the ransom **does not guarantee** an organization will regain access to its data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom.
- Some victims who paid the demand have reported being **targeted again** by cyber actors.
- After paying the originally demanded ransom, some victims have been **extorted to pay more**.
- **Decide before** an incident occurs as to whether you will pay or not and include in Cyber Incident Response Plans.
- Paying could inadvertently encourage this **Criminal Business Model**.

Vectors of Attack

- Escalation of **big game hunting** increasing the demand amounts.
- **Ransomware as a Service (RaaS)** allowed for an expansion of criminal enterprises.
- **Remote access software** and **email/phishing** are consistently the most common infection vectors.
- Leveraging trusted relationships, **managed service providers (MSPs)** are used to target multiple entities.

CISA RECOMMENDS THAT YOU DO NOT PAY THE RANSOM

Key Messages

- Keep Calm and Patch On
- Backing Up Is Your Best Bet
- Suspect Deceit? Hit Delete
- Always Authenticate
- Prepare and Practice Your Plan
- Your Data Will Be Fine if It's Stored Offline
- Secure Your Service Message Block (SMB)
- Paying Ransoms Doesn't Pay Off

As the nation's **risk advisor**, the Cybersecurity and Infrastructure Security Agency's (CISA) mission is to **ensure the security and resiliency of our critical infrastructure.**

Contact CISA at **Central@CISA.gov** for assistance with:

- Phishing Campaign Assessment (PCA)
- Vulnerability Scanning
- Remote Penetration Test (RPT)

Register for the EI-ISAC at **learn.cisecurity.org/ei-isac-registration**.

Visit **cisa.gov/election-security** to learn about CISA's role in election security.

Risk Mitigation

- ☐ **Create backups** of your critical systems and data.
- ☐ Implement **multi-factor authentication**.
- ☐ **Patch systems and software**.
- ☐ Develop **Incident Response Plan(s)** and **Business Continuity of Operations Plans**.
- ☐ Conduct a **cybersecurity risk analysis**.
- ☐ **Segment critical systems**.
- ☐ Implement **application allowlisting**.
- ☐ Perform **penetration tests** on your systems.

Incident Detection and Response

Use CISA's Cyber Incident Detection and Notification Planning Guide templates to develop protocols and to build your team: **cisa.gov/publication/protect2020-cyber-incident-guide**

Ransomware Guide

This Ransomware Guide includes recommendations, best practices, recommended incident response policies and procedures, cyber hygiene services, and several checklists that organizations can use to help protect against or response to ransomware attacks: **cisa.gov/publication/ransomware-guide**

Reporting: Important Contacts

Report to CISA
us-cert.cisa.gov/report

Find Your Local FBI Field Office
fbi.gov/contact-us/field/field-offices

Find Your Local Secret Service Field Office
secretservice.gov/contact/field-offices/