MEASURES TO PROTECT AGAINST POTENTIAL CRITICAL THREATS

Joe Frohlich
Cybersecurity Advisor, Montana
Cybersecurity and Infrastructure Security Agency

Heightened Cybersecurity Posture

- Objective: Adopt a Heightened Cybersecurity Posture
- Near-Term Actions:
  - Minimize Attack Surface
  - Monitor and Protect Network
  - Incident Response: Exercise Your Plan
  - Operational Resilience: Backups & Redundancy
  - See Something, Report Something

https://www.cisa.gov/shields-up

Minimize Attack Surface

- Minimize Attack Surface and Harden Assets
  - Implement Multi-Factor Authentication
  - Stop Bad Practices
    - EoL Software, Default Accounts, Single-Factor Authentication
  - Update Software
    - Prioritize known exploitable vulnerabilities identified by CISA
  - System Hardening
  - Adopt CISA's Cloud Services Security Best Practices
    - CISA's Cloud Service Guidance
  - Signup for CISA's Cyber Hygiene Services
    - Vulnerability Scanning
    - Web Application Scanning
  - CISA Automated Indicator Sharing Program

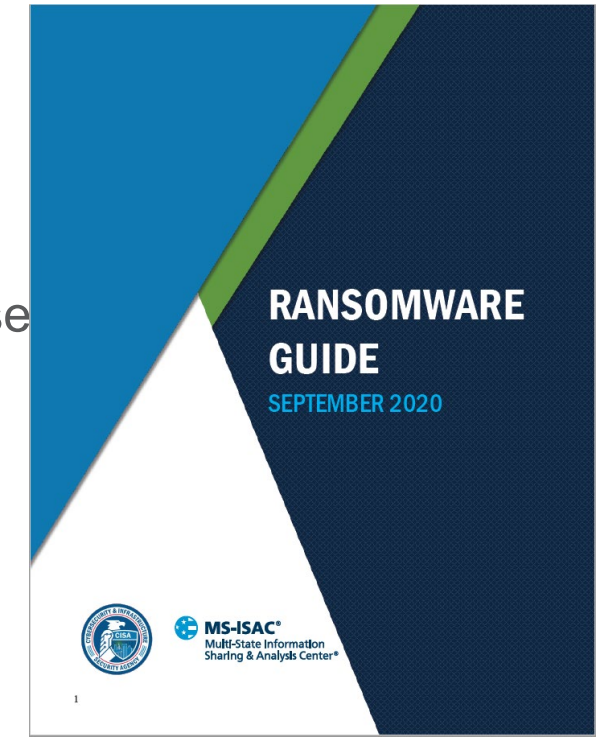
https://www.cisa.gov/cyber-hygiene-services

Monitor and Protect

- Monitor and Protect the Network
  - Monitor your network for unusual behavior
    - Enable logging
    - Monitor hosts
    - Monitor network traffic
  - Deploy host- and network-based antivirus/antimalware controls
    - Keep the signatures updated

Incident Management

- Incident Response/Management
  - Designate an incident response team
  - Assure availability of key personnel
  - If you have an incident response plan – assess it with a tabletop exercise
  - If you DO NOT have an incident response plan – create one now
    - CISA Ransomware Guide
    - Federal Government Cybersecurity Incident and vulnerability response playbooks
- CISA Ransomware Guide
  - Part 1: Ransomware Prevention Best Practices
  - Part 2: Ransomware Response Checklist

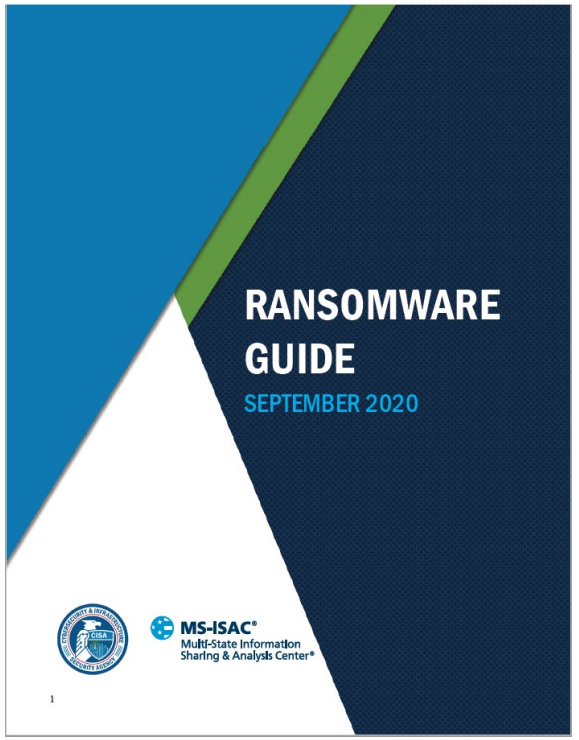


https://www.cisa.gov/stopransomware/ransomware-guide

https://www.cisa.gov/cisa-tabletop-exercises-packages

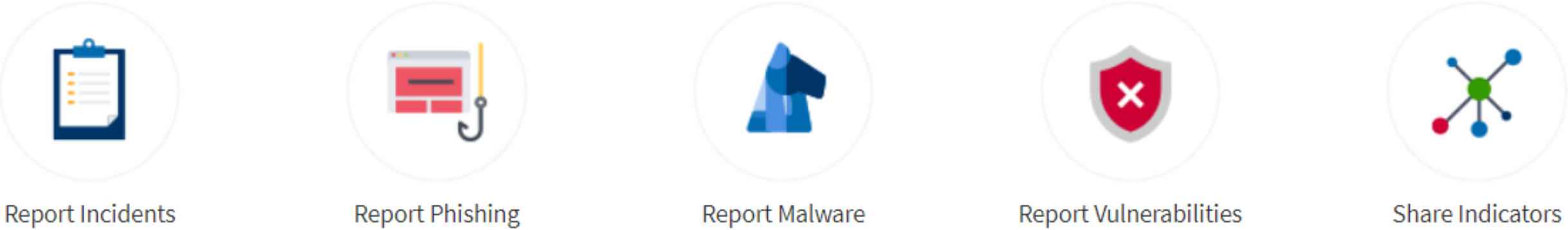
Operational Resilience

- Operational Resilience
  - Backup mission-critical data, software, and “gold images”
  - Store off-line (preferably encrypted)
  - Test these backups
  - Assess the readiness of your alternative/recovery site



https://www.cisa.gov/stopransomware/ransomware-guide

See Something – Report Something



https://www.cisa.gov/uscert/report

Additional Resources

- ***CISA Shields Up Webpage***
- CISA Shields Up Technical Guidance
- Alert (AA22-057A) Destructive Malware Targeting Organizations in Ukraine (revised March 1, 2022)
- Alert (AA22-047A): Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology (February 2022)
- CISA Insights: Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats (January 2022)
- Alert (AA22-011A): Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure (January 2022)
- CISA Insights: Preparing for and Mitigating Potential Cyber Threats (December 2021)
- Reminder for Critical Infrastructure to Stay Vigilant Against Threats During Holidays and Weekends (November 2021)
- Russian Cyber Threat Overview and Advisories
- CISA Automated Indicator Sharing
- CISA Cyber Resource Hub
- CISA's Free Cybersecurity Services and Tools Webpage
- Federal Government Cybersecurity Incident and Vulnerability Response Playbooks
- CISA / MS-ISAC Ransomware Guide
- CISA Cloud Services Guidance
- CISA KNOWN EXPLOITED VULNERABILITIES CATALOG AND Top 10 Routinely Exploited Vulnerabilities | CISA

CISA REGION 8

Joe Frohlich

Cybersecurity Advisor, Montana
Cybersecurity & Infrastructure Security Agency

EMAIL: joseph.frohlich@cisa.dhs.gov
CELL: (406) 461-2651

CISA INCIDENT REPORTING SYSTEM
https://us-cert.cisa.gov/forms/report

CISA CENTRAL - 24/7 Watch
(888) 282-0870;Central@cisa.dhs.gov

FBI's 24/7 Cyber Watch (CyWatch)
(855) 292-3937; CyWatch@fbi.gov