America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

FACT SHEET

Level Up Your Defenses—Four Cybersecurity Best Practices for Businesses

Publish Date: August 29, 2025

RELATED TOPICS: CYBERSECURITY BEST PRACTICES </topics/cybersecurity-best-practices>

Strengthening your cybersecurity is crucial to protecting your business from threats that impact customers, the community, and critical infrastructure. Level up your policies by implementing these critical behaviors:

- **Use logging on business systems**
- **Back up business data**
- **Encrypt business data**
- **Share cyber incident information with CISA**

Use Logging on Business Systems

Cyber threats are rising, but you can effectively and affordably strengthen defenses by logging and monitoring your systems. **Logging** refers to automatically recording events on your systems. **Monitoring** means reviewing and analyzing those logs to spot suspicious activity, system misuse or early signs of attack.

1. Set up logging.

Determine what to log, such as admin actions, network traffic, system events and more. **Enable logging** on servers, firewalls, endpoint devices, and cloud services. **Centralize your logs** to make it easier to detect unusual activity.

2. Monitor logs regularly.

Set up alerts for high-risk events such as failed login attempts, privilege escalation. **Review logs** manually or with automated tools where possible.

3. Establish policies and procedures.

- **Follow** best practices when setting up logging and monitoring.
- **Protect logs** from unauthorized access/deletion (restrict/monitor access, store securely).
- **Retain logs** in accordance with your policies and compliance needs.
- **Designate a crisis-response team** including responsibilities for technology, communications, legal and business continuity.

RETURN TO TOP

Back Up Business Data

A backup is a secure copy of your business's critical data, stored separately from your primary systems. Regularly backing up your data is a critical part of your cybersecurity strategy. This is especially important for businesses in the critical infrastructure supply chain, since many systems rely on your services to maintain operations.

1. **Know what to back up.**

   Take inventory of what important information resides on your network. This will give you an understanding of what you are protecting and who has access. Identify what data your business can't operate without, like proprietary research, development files or financial records, and prioritize those for protection.

2. **Follow the 3-2-1 backup rule.**

   Once you know what needs to be protected, protect your data with 3 copies of important files on 2 different types of storage media (like a hard drive and the cloud) with 1 copy stored off-site, away from your location.

3. **Secure, test and train.**

   Test backup procedures to make sure your team can rapidly restore data up to at least seven days. If using industrial control systems or operational technology, conduct a test of manual controls to ensure that critical functions remain operable if the organization's network is unavailable. Finally, train your team on these policies and procedures.

RETURN TO TOP

Encrypt Business Data

Encryption is one of the most powerful tools you can use to protect your business data. It scrambles sensitive information—like customer details, financial records and business communications—into unreadable coded language so that only authorized users with the key can access it.

1. Understand the different types of encryption.

System encryption protects a device's entire hard drive, including operating system. **Drive encryption** protects data stored in on-premises servers or removable media. **File encryption** prevents threat actors from accessing the contents of a document.

2. Identify what to encrypt.

Prioritize what type information to secure, such as personally identifiable information (PII), protected health information (PHI), criminal justice/law enforcement data, financial/tax information, operational/infrastructure data, education records, internal communications.

3. Apply encryption best practices.

- Encrypt all devices, hard drives, removable media and relevant documents. Encrypt data both at rest and in transit.
- Back up data to a vetted cloud service or external hard drive and encrypt your backups. Maintain offline, encrypted backups of data and regularly test them.
- Develop a culture of cybersecurity that trains staff on data protection and include encryption in cybersecurity policies.

RETURN TO TOP

Report Cyber Incident Information to CISA

Sharing cyber incident information with CISA helps protect not just your organization, but others across the country. CISA can then analyze the threat, alert other businesses and share actionable guidance to help prevent similar attacks. The sooner you report, the sooner CISA and others can act.

What is cyber incident information sharing?

Cyber incident information sharing means reporting suspected or confirmed cyberattacks, system vulnerabilities or suspicious activity to CISA. In return, CISA shares threat intelligence, mitigation tips and technical assistance.

Why does it matter?

When you share this information, you protect your network *and* help defend interconnected infrastructure across your state, region and the nation. It helps you respond more quickly to current threats, warn peers, prevent repeat attacks, and get federal expertise/assistance.

How do you report to CISA?

Don’t wait for a major breach to share with CISA. Even suspected activity can be valuable.

- **Use CISA’s Cyber Incident Reporting System** <https://myservices.cisa.gov/irf>**.**
- **Report incidents early**—don’t wait until full investigation.
- **Include relevant details** like indicators of compromise, system impacts and attacker behavior.
- **Designate a point of contact** on your IT or emergency management team.

RETURN TO TOP

CISA has free resources, tools and guidance to help businesses implement these best practices. Share these tips with your team!