INFORMATION SECURITY TIPS 2026

Developed by the Indiana Executive Council on Cybersecurity's Finance Committee

CYBER RISK FRAMEWORK

Adhere to a Structured Cybersecurity Framework

Adopt a recognized framework (e.g., **NIST CSF 2.0**) to structure cyber risk outcomes; align policies, controls, and reporting to the **Govern, Identify, Protect, Detect, Respond, Recover** functions. One example is the NIST Framework. https://www.nist.gov/cyberframework

Define Roles and Responsibilities

Name an **Information Security Officer** responsible for the program; make **senior management accountable** for implementation and effectiveness; provide periodic, risk-based reporting to the Board or appropriate committee.

Management Accountability for the Cyber Risk Framework Utilized

Senior management and a Board of Directors should be responsible for implementing and periodically reviewing the cybersecurity program in conjunction with the Information Security Officer.

Information Security Oversight

The **Information Security Officer** should periodically report the status of the cyber program to the appropriate governing body. In addition to the report, they should also provide regular security training to the Board & Executives, and training on the organizations risk posture, material threats, and readiness for any cybersecurity threats. A framework such as the NIST will help greatly in organizing this.

POLICIES AND PROCEDURES

Policy Relevance and Purpose

Maintain **concise, purpose-driven policies** that directly support the cyber risk management framework (avoid "policy for policy's sake"). Keep them **accessible**, versioned, and **approved at the appropriate level** on a defined cadence.

Evaluation of Impact

Each policy should be assessed for its effects on business operations and employee workflow to avoid negative consequences.

Accessibility and Review

Policies need to be simple, accessible to all stakeholders, and regularly reviewed and approved at appropriate levels.

Exception Management & Policy Attestation:

Implement **exception management** and **policy attestation** processes to track deviations and accountability. (CIS Controls v8.1 aligns governance with CSF 2.0.)

https://www.cisecurity.org/controls/v8

ASSET MANAGEMENT

Comprehensive Asset Inventory

Maintain detailed inventory of **physical devices**, **hardware**, and **network resource maps** for both cybersecurity and network technicians.
Utilize a **Ticketing Software** for **Requesting** any **New Hardware** or **Software** that is being requested by the users.

Software Inventory and Allow List

Keep a Software inventory and implement an allowed applications list to control installations.

Ensure that you have a policy for your Help Desk & IT staff who installs software so that they know what software is or isn't allowed.

Prioritizing Asset Protection

Identify **systems**, **operating systems**, **open ports**, and **user accounts** to prioritize protection by sensitivity.

Offboarding Policy

Ensure there is a policy in place to remove software, service accounts, and user accounts that are no longer needed. Have a process in place to disable them in a timely manner.
https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools

https://www.cisa.gov/resources-tools/resources/foundations-ot-cybersecurity-asset-inventory-guidance-owners-and-operators

RISK ASSESSMENTS

Threat Identification and Analysis

Regularly identify and analyze internal and external threats to ensure effective risk assessments.

Evaluating Likelihood and Impact

Assess the likelihood and impact of cyber risks to prioritize mitigation strategies effectively.

Using Threat Intelligence

Leverage cyber threats, vulnerabilities, and intelligence data to determine overall cyber risk.

Communication to Management

Share cyber risk information promptly with senior management for informed decision-making.

URL:
https://www.cisa.gov/risk-assessments

MANAGE ACCESS TO ASSETS AND INFORMATION

Role-Based Access Control

Use role-based access controls to restrict access to assets based on job functions and responsibilities.

https://www.cisa.gov/resources-tools/resources/enhanced-visibility-and-hardening-guidance-communications-infrastructure

Strong Password Practices

Enforce long, complex passwords and randomize service account passwords for increased security. Training users on how to create a passphrase will make this much easier on having them create new secure passwords.

https://www.cisa.gov/resources-tools/training/cyb3rsmrt-use-password-manager-create-and-remember-strong-passwords

Two-Factor Authentication

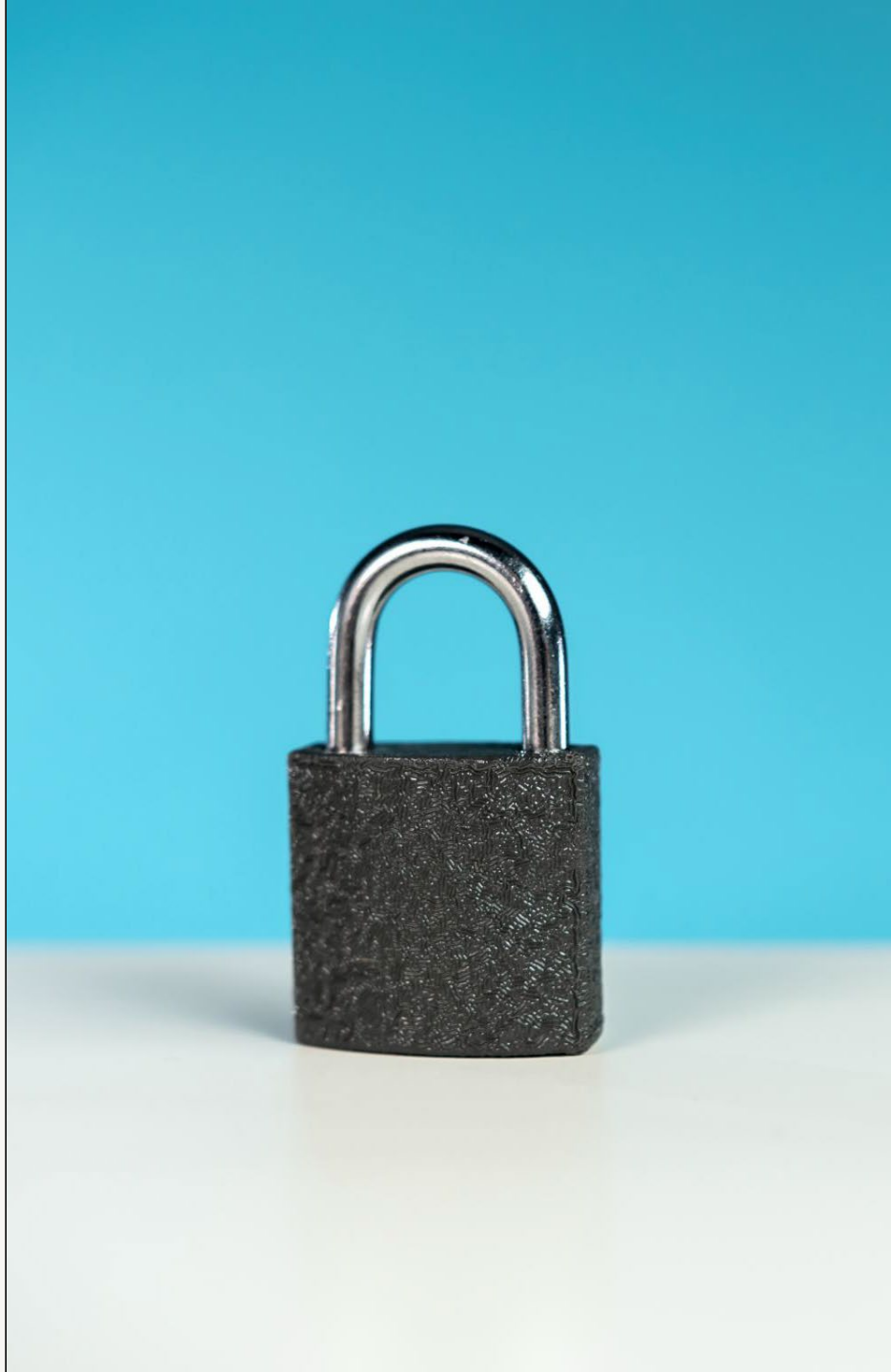
Implement two-factor authentication combining something you have, are, or know to enhance security.

https://cheatsheetseries.owasp.org/cheatsheets/Multifactor_Authentication_Cheat_Sheet.html

Account Monitoring and Deactivation

Regularly inventory inactive accounts and disable them; identify accounts accessed by terminated employees.

https://www.cisa.gov/resources-tools/services/account-management



OFFBOARDING & ONBOARDING SECURITY

Employment Screening

Ensure that proper Employment screening is put into place for new hires, especially when it comes to remote positions.
https://www.cisa.gov/resources-tools/resources/resources-onboarding-and-employment-screening-fact-sheet

Secure User Onboarding

Grant access only as required, educate new users on security policies, and enforce strong password requirements for all accounts.

Thorough Offboarding Process

Immediately remove all access for departing users, confirm proper asset handling, and document offboarding steps during exit interviews.

Regular Access Audits

Regularly review access logs and update inventories to make sure no residual access remains after users leave.

SENSITIVE DATA

Inventory Sensitive Data

Identify all locations of sensitive data as the foundational step in data protection.

Use Strong Encryption

Apply strong encryption techniques for data both in motion and at rest to ensure confidentiality.

Isolate Sensitive Data

Separate sensitive data areas from the rest of the infrastructure to reduce exposure risks.

Implement Data Loss Prevention

Use DLP technology to detect, prevent, and alert on unauthorized access or breaches.

Manage Data Retention

Develop a data retention policy to control the removal and lifecycle of sensitive information.

https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/encrypt-business-data

CONDUCT REGULAR BACKUPS

3-2-1-1-0 Backup Rule

Maintain three copies of data on two different media types, one backup stored offsite for disaster recovery, one immutable air-gapped copy (cannot be altered or deleted), ensures 0 recovery errors through regular restore testing.
This modern enhancement is used as Ransomware targets backups as well.

Backup Security Measures

Backups must be encrypted and isolated from unauthorized infrastructure access to ensure data safety.

Monitoring and Testing

Regularly test backups and include backup devices in log monitoring systems like SIEM for security oversight. Ensure all parties are available for testing so everyone is comfortable with the process.

https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/back-up-business-data

SECURELY PROTECT YOUR DEVICES

Endpoint Protection Management

Centralized endpoint protection secures devices against threats and enforces security policies consistently.

Access Control and Privilege Restriction

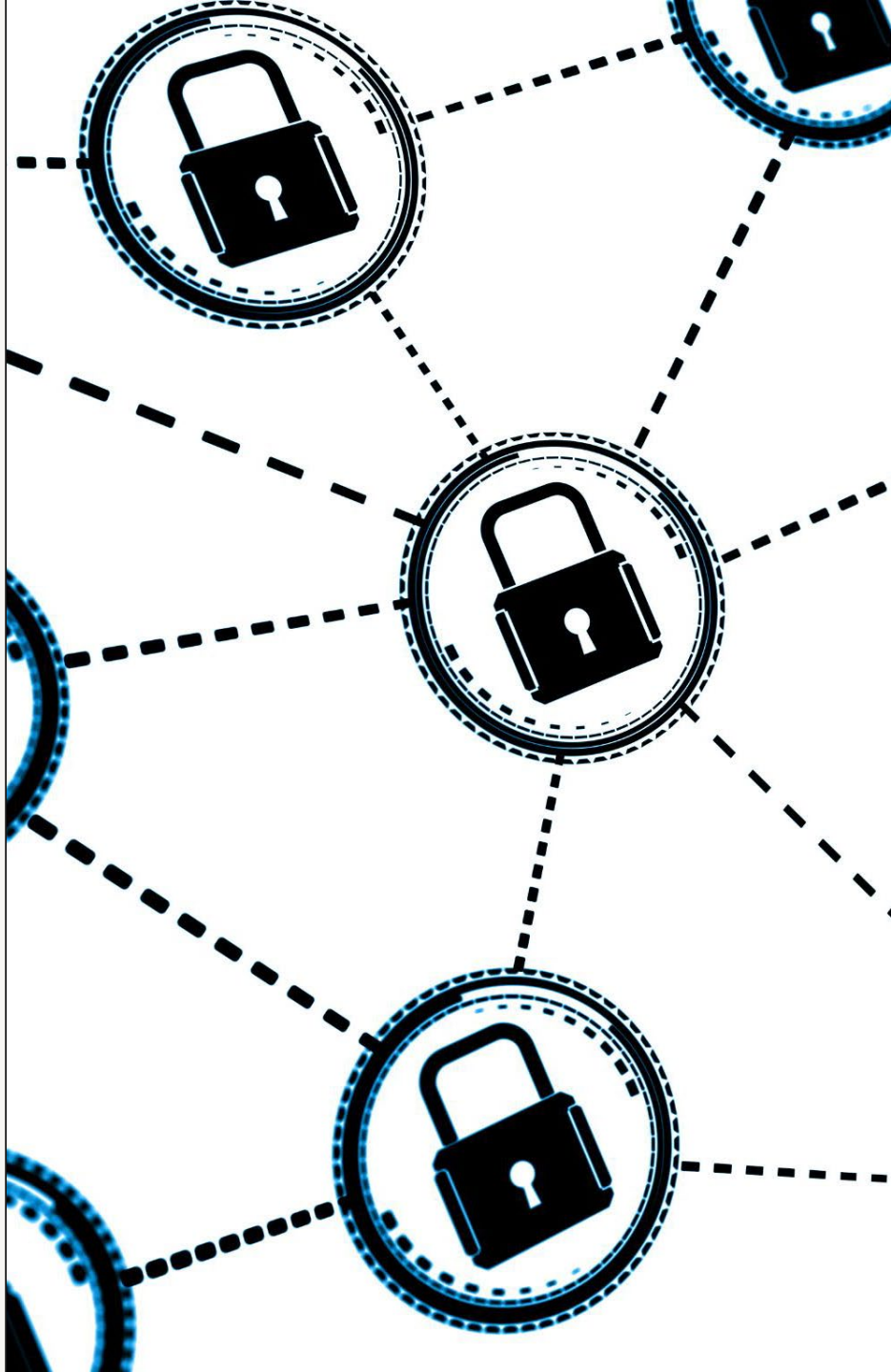
Restrict privileged and administrative accounts, applying least privilege and disabling inactive accounts.

Device Encryption and Isolation

Encrypt devices with strong protocols and isolate them upon detecting unnecessary communication.

Disabling Vulnerable Services

Disable unneeded services and vulnerable authentication protocols to reduce security risks.



END USER SECURITY AWARENESS

Security Awareness Training

Implement training programs to educate employees on company security policies and secure asset handling.

Recognizing Cyber Threats

Train staff to identify social engineering, phishing, smishing, and vishing attacks to reduce risks.

Data Handling Practices

Educate on proper identification, storage, transfer, and destruction of sensitive data to ensure security.

Ongoing Cybersecurity Resources

Provide monthly cybersecurity tips and use resources like newsletters to keep awareness current.

https://www.cisa.gov/cybersecurity-awareness-training
https://www.sans.org/newsletters/ouch

TRAIN USERS ON BEST SECURITY PRACTICES

Security Updates and Patching

Train users to identify missing security updates and understand the importance of regular device restarts for security. Ideally, in an Enterprise Environment, you will want to have a Patch Management Program in place to have automated updates.

https://www.cisa.gov/news-events/news/understanding-patches-and-software-updates

Role-Specific Training

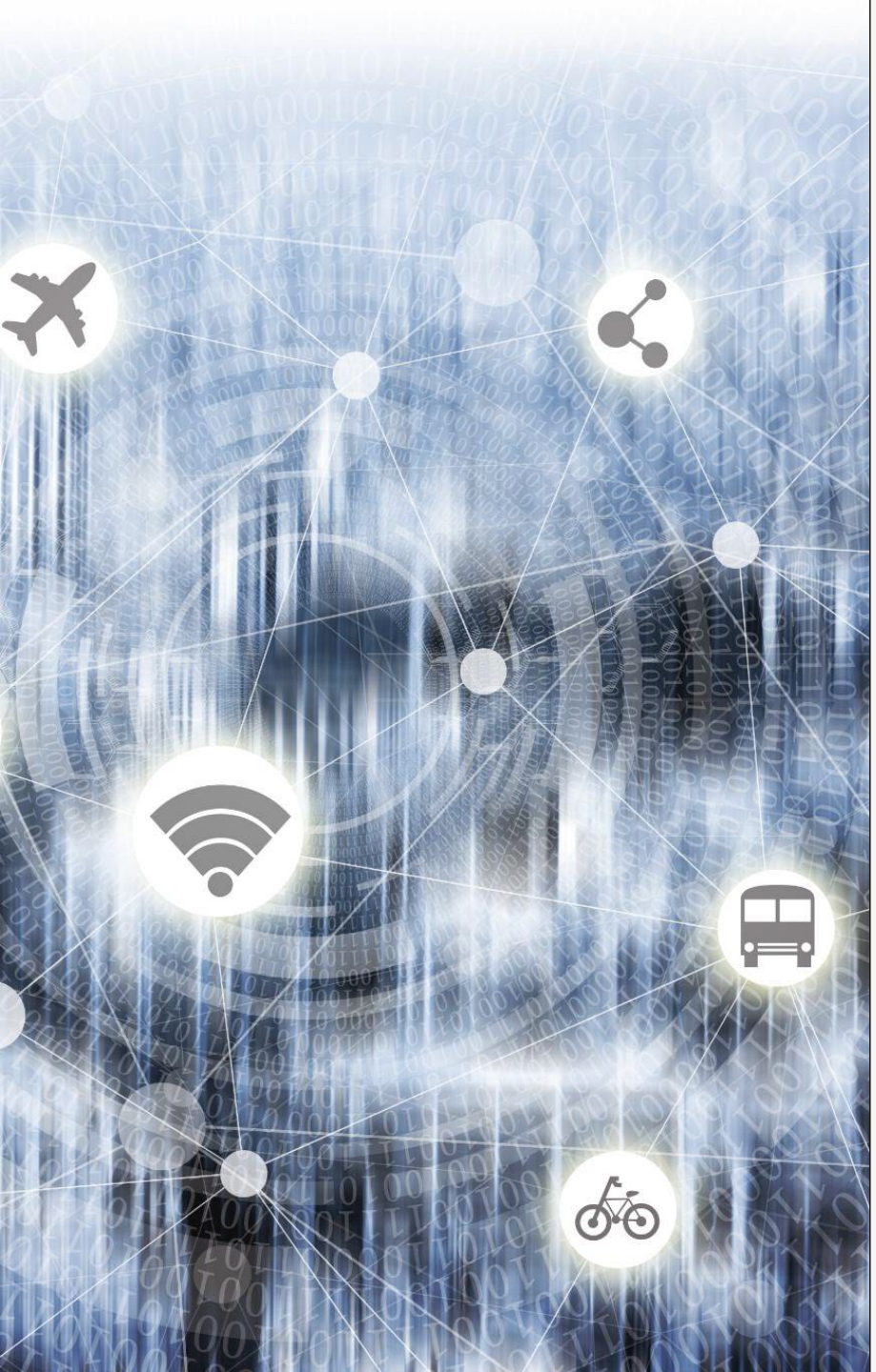
Provide tailored training for privileged users and high-risk groups to address unique security challenges. It is important that users with administrative access get a different more tailored level of training as they have increased risk of being attacked or targeted by threat actors due to their elevated permissions. HIPAA, NCUA, PCIDSS, GDPR, & FISMA are a few examples of regulations that require this additional privileged user training.
https://www.sans.org/information-security-policy/privileged-account-management-policy

Up-to-Date Cybersecurity Knowledge for IT Staff

IT professionals should maintain current certifications and knowledge to effectively protect organizational data. In addition, they should be required to take an advanced privileged security training course in addition to the normal cybersecurity training courses that are mandatory on an annual basis that gets more in-depth than regular users due to their access.

Leadership Cyber Awareness

Senior management and board members need situational awareness and access to cybersecurity expertise to guide decisions. It would be recommended to have additional security courses or training sessions with your Board or Senior Leadership Teams as well to ensure they have a greater understanding.



ANOMALIES AND EVENTS

Baseline Mapping

Mapping expected network connections and data flows is crucial for identifying anomalies effectively.

Event Collection and Correlation

Collecting and correlating event data across the organization enables comprehensive anomaly detection.

Real-Time Aggregation

Centralized real-time aggregation and correlation of alerts improves detection of anomalous activities.

Alert Parameters and Logging

Establishing alert thresholds and logging retention policies ensures effective cyber threat management.

CONTINUOUS MONITORING

Access Monitoring

Monitor physical and network access to detect both authorized and unauthorized activities promptly.

Privileged User Logging

Log and review activities of privileged users to ensure accountability and detect anomalies.

Third-Party Connection Oversight

Authorize and continuously monitor all third-party connections to prevent unauthorized access.

Malware and Software Control

Detect malicious and unauthorized software, and use web-filtering tools to block harmful sites.

VULNERABILITY MANAGEMENT

Automated Vulnerability Scanning

Implement automated scanning for operating systems and third-party applications regularly to detect vulnerabilities effectively.

Prioritization and Remediation

Develop remediation timelines based on risk and criticality to address vulnerabilities in a timely manner.

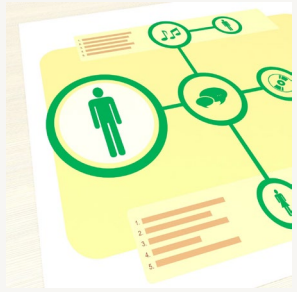
Verification and Documentation

Perform remediation scans to verify fixes and document all efforts to maintain accountability and program integrity.

Program Effectiveness Metrics

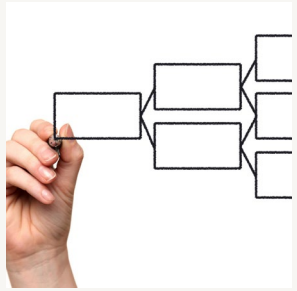
Develop metrics to measure the effectiveness of the vulnerability management program and perform penetration testing.

INCIDENT RESPONSE



Comprehensive Incident Plan

A well-defined incident response plan includes roles, documentation, notification, escalation, and reporting procedures.



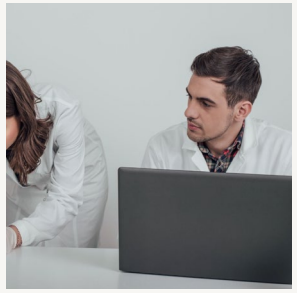
Incident Prioritization and Containment

Incidents must be prioritized and categorized, with strategies to contain and remediate effectively.

Continuous Improvement

Plans and strategies should be regularly reviewed, updated, tested, and lessons learned applied for improvement.

ANALYSIS



Forensic Investigation Planning

Plan forensic investigations considering internal and third-party capabilities to ensure thorough analysis.

Vulnerability Evaluation

Evaluate vulnerabilities from public sources, forums, third parties, and internal teams for comprehensive risk assessment.

Mitigation and Validation

Create mitigation and validation plans based on analysis of severity, impact, and response options.

RESILIENCY

Incident Response & Recovery

Execute response and recovery plans to resume critical services and core business functions swiftly.

Communication Strategies

Include stakeholder notifications, senior management updates, and regulatory status reports in communication plans.

Reputation Management & Mitigation

Apply mitigation techniques to protect organizational reputation after cybersecurity incidents.

Continuous Improvement

Refine plans by integrating lessons learned from incidents, assessments, testing, and industry insights.