Information Security Tips 2023

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

Governance: Cyber Risk Framework

- Adhere to a cybersecurity framework:
  - Establishes processes to identify, monitor, and report cyber risk.
  - Informed by applicable industry standards and guidelines.
  - Establish and clearly define cybersecurity roles and responsibilities.
- Approved by the Board of Directors or one of its committees
  - Senior Management held accountable for implementation.
  - Periodically updated and reviewed.
- Designates an Information Security Officer that is responsible and accountable for developing, implementing, and overseeing the cybersecurity program.
  - Periodically reports status of the cyber program to the appropriate governing body.

Governance: Policies and Procedures

- Cybersecurity policies should support the Cyber Risk Management Framework.
- Determine what policies are needed.
  - Do not have a policy just for the sake of having a policy.
    - Is this relevant?
    - How does it help the organization?
    - Does it negatively impact the business or employees?
- Keep it simple.
- Ensure policies and procedures are always accessible to employees and stakeholders.
- Regularly review and approve policies at the appropriate level.

Identify: Asset Management

- Maintain asset inventory that includes:
  - Physical devices and hardware.
  - Maps of network resources.
  - External information systems.
- Maintain software inventory.
  - Implement an allowed list of applications that can be installed.
- Identify systems, OS, software, open ports, and user accounts.
- Organizational resources should be prioritized for protection based on sensitivity, criticality, business value, etc.

Identify: Risk Assessments

- Internal and external threats are regularly identified and analyzed.
- Assessment approach includes likelihood and impact of cyber risks being exploited.
- Use cyber threats, vulnerabilities, and threat intelligence to determine overall cyber risk.
- Share cyber risk with appropriate levels of senior management in a timely manner.

Protect: Manage Access to Assets and Information

- Implement role-based access.
- Service / local account password randomization and very complex.
- Use passwords that are long and complex.
- 2FA wherever possible.
  - Something you have, you are, or you know.
  - For more information on 2FA visit fidoalliance.org.
- Change passwords based on organizational and regulatory requirements.
- Inventory and disable inactive accounts based on predefined time of inactivity.
- Develop a process to identify all accounts a terminated employee has (or had) access to.

Protect: Protect Sensitive Data

- Create an inventory of all sensitive data locations.
- Use strong encryption on all sensitive data in motion and at rest.
- Isolate areas of sensitive data from the rest of the infrastructure.
- Implement Data Loss Prevention (DLP) technology that will identify, block, and notify of sensitive data.
- Develop a data retention policy for the process of removing sensitive data.

Protect: Conduct Regular Backups

- Develop a disaster recovery policy that adheres to:
  - Backups Utilize 3-2-1 Rule:
    - Keep 3 copies of your data.
    - Utilize 2 different backup media.
    - Keep 1 backup offsite.
  - Encrypt your backups.
  - Develop retention plans.
  - Test backups regularly.
- Isolate backup devices from infrastructure that does not need access.
- Do not join backup devices to Active Directory.
- Include your backup devices in log monitoring such as a SIEM.

Protect: Securely Protect Your Devices

- Implement a centrally managed end-point protection.
- Restrict access to privileged accounts and groups.
  - Role-based access.
  - Limit administrative accounts.
- Vendor Accounts.
  - How do they have access to your network?
    - Site-to-site VPN / Remote access VPN?
  - Principle of Least Privilege.
  - Disable when not in use.
- Encrypt devices utilizing strong encryption.
- Isolate devices that do not need to communicate with each other.
- Disable unneeded services and vulnerable authentication protocols.

Protect: Securely Protect Your Devices

- Enable strong authentication such as SMB signing.
- Mobile Devices
  - Enable DNS filtering.
  - Require devices to lock with a pin or password.
  - Implement the ability to remotely wipe the device.
- Implement a well-defined patch management program.
  - Install OS and firmware security updates regularly.
- Implement system hardening of all devices on the infrastructure.
  - Create OS and systems baseline configurations.
  - For more information on system hardening visit: https://www.cisecurity.org/cis-benchmarks/

Protect: End User Security Awareness

- Implement a security awareness program.
  - Train new hires on company security policies.
  - Train employees how to interact with assets and data in a secure manner.
  - Train employees how to report any unusual activity or security incidents.
  - Periodically review and update content on a regular basis.

- Train employees to recognize social engineering attacks.
  - Train users on how to recognize a phishing attack. Reinforce this training by phishing them.
  - Train users on Smishing and Vishing.

- Train users on how to identify, store, transfer, and destroy sensitive data.
  - Include addressing the causes of sensitive data exposure.

- Post cyber security tips on your internal website monthly. (SANS is a good resource for this)
  - https://www.sans.org/newsletters/ouch/

Protect: Train Users

- Train users on identifying missing security updates and the importance of restarting their devices.
- Train users appropriately for their role and responsibility, including privileged users and high-risk groups.
- Ensure key cybersecurity personnel maintain current knowledge, training, and certifications.
- Train IT in secure system administration, vulnerability awareness, etc.
- Ensure that senior management and Board of Directors receive cybersecurity situational awareness training and have access to adequate cybersecurity expertise.

Detect: Anomalies and Events

- Develop baseline mapping of expected connections and data flows of network resources.
- Ensure event data from across the organization is collected, analyzed, and correlated.
- Real-time central aggregation and correlation of anomalous activities, alerts, and threat intelligence is performed.
- Establish and validate cyber alert parameters and thresholds.
- Create relevant system logging retention policies.

Detect: Continuous Monitoring

- The environment is monitored to include unauthorized physical access to high-risk systems.
- Authorized and unauthorized access, authentication, usage, connections, and devices are actively monitored.
- Privileged user activities are monitored, logged, and reviewed.
- All third-party connections are authorized and monitored.
- Malicious code and unauthorized mobile code is detected.
- Unauthorized and unsupported software is detected.
- Web-filtering tools are used to block access to malicious sites.

Detect: Vulnerability Management

- Implement a vulnerability program:
  - Implement automated vulnerability scanning for Operating Systems (OS) and third-party applications.
  - Perform vulnerability scanning on at least a monthly basis after patching is complete.
  - Perform vulnerability scanning after network changes and on systems before entering production.
  - Develop prioritization and remediation timelines that fit your organization.
    - Risk-based vs criticality/CVSS
  - Perform remediation scans to verify vulnerability is remediated.
  - Document all vulnerability remediation efforts.
- Develop vulnerability metrics to measure the effectiveness of your vulnerability management program.
- Test for weak or compromised passwords.
- Perform Penetration testing and remediation.

Respond: Incident Response

- Incident response, disaster recovery, and business continuity plans are activated to ensure timely response to incidents.
- Ensure an incident response plan is in place, and includes:
  - Clearly defined roles and responsibilities.
  - Documentation, notification, escalation, and reporting requirements.
  - Incident prioritization and categorization.
  - Containment strategies.
  - Requirements for remediation of identified weaknesses.
  - Lessons learned.
- The Incident Response Plan and response strategies are periodically reviewed, updated and tested.

Respond: Analysis

- Forensic investigation planning should be considered.
  - Internal capabilities verse 3rd party support.
- Vulnerabilities identified as part of a cyber incident should be analyzed and addressed as part of the vulnerability management program, including:
  - Evaluating vulnerabilities received from public sources, forums, third parties, and internal teams.
  - Analyze vulnerabilities to determine validity, scope, severity, impact, and response options.
  - Create mitigation and validation plans.

Recover: Resiliency

- Incident response, disaster recovery, and business continuity plans are executed to resume critical services and core business functions.

- Ensure that communication plans are in place to include:
  - Internal and external stakeholder incident notification.
  - Timely response and recovery updates to senior management.
  - Status of recovery activities to regulatory authorities.
  - Mitigation techniques to address reputation after an incident.

- Refine IR, DR, and BCP by reviewing and incorporating ‘lessons learned’ from:
  - Cybersecurity incidents.
  - Cybersecurity assessments and testing.
  - Widely reported incidents and industry reports.

For more Information:

NIST CSF

https://nist.gov/cyberframework

Cyber Risk Institute “Profile”

https://cyberriskinstitute.org/the-profile/

FFIEC Cyber Resource Guide

https://ffiec.gov/press/pdf/FFIECCybersecurityResourceGuide2022ApprovedRev.pdf