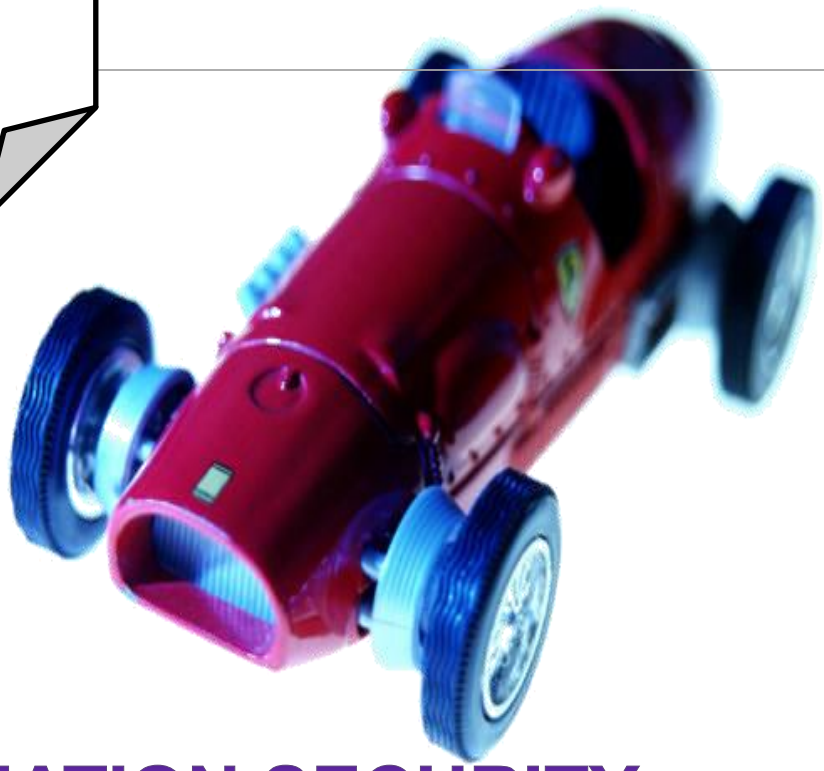
Mora Montasser Khalf
Section"7"

Mariam Mahmoud Mohamed
Section"6"

Mariam Khaled Ramadan
Section"6"

Mariam Ashraf Mohammed
Section"6"

Mariam Salman Sedky
Section"6"



IS INFORMATION SECURITY CONTROLS

What are Information Security Controls?

Information security controls are measures taken to reduce information security risks such as information systems breaches, data theft, and unauthorized changes to digital information or systems. These security controls are intended to help protect the availability, confidentiality, and integrity of data and networks, and are typically implemented after an information security risk assessment.

Types of information security controls include security policies, procedures, plans, devices and software intended to strengthen cybersecurity. There are three categories of information security controls:

Preventive security controls, designed to prevent cyber security incidents

Detective security controls, aimed at detecting a cyber security breach attempt (“event”) or successful breach (“incident”) while it is in progress, and alerting cyber security personnel

Corrective security controls, used after a cyber security incident to help minimize data loss and damage to the system or network, and restore critical business systems and processes as quickly as possible (“resilience”)

Security controls come in the form of:

Access controls including restrictions on physical access such as security guards at building entrances, locks, and perimeter fences

Procedural controls such as security awareness education, security framework compliance training, and incident response plans and procedures

Technical controls such as multi-factor user authentication at login (login) and logical access controls, antivirus software, firewalls

Compliance controls such as privacy laws and cyber security frameworks and standards.

The most widely used information security frameworks and standards include:

The National Institute of Standards and Technology (NIST) Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. This document lists security requirements useful not only for federal agencies but for all organizations' information security risk management programs.

The International Organization for Standardization (ISO) standard ISO 27001, *Information Security Management,* which provides guidance on information technology security and computer security.

The Payment Card Industry Data Security Standard (PCI DSS), which establishes security requirements and security controls for the protection of sensitive data associated with personal credit card and payment card information

The Health Insurance Portability and Accountability Act (HIPAA), a federal law regulating information security and privacy protections for personal health information

Frameworks and standards are systems that, when followed, help an entity to consistently manage information security controls for all their systems, networks, and devices, including configuration management, physical security, personnel security, network security, and information security systems. They define what constitutes good cybersecurity practices and provide a structure that entities can use for managing their information security controls.

Information Security Controls

Insurance Requirements

UC Irvine has an insurance program to cover liability in the event of a data breach.

To ensure full insurance protection the follow security requirements must be met: Cyber Security Insurance Requirements (pdf)

Minimum Network Connectivity Requirements

Any computer or device connected to UCInet must, at minimum, meet the following security configuration requirements: Security Guidelines for Computers and Devices Connected to UCInet.

Security Control Baseline

To ensure appropriate steps are taken to protect the confidentiality, integrity, and availability of data, the following controls must be addressed for any UC Irvine information system.

Adopted from the SANS Top 20, these are the minimum steps required to protect against the most obvious, persistent, and exploited threats.

Information systems with higher risk should perform a risk assessment to create a detailed information security plan: Security Risk Assessment Questionnaire

1. Inventory of Authorized and Unauthorized Devices

Reduce the ability of attackers to find and exploit unauthorized and unprotected systems: Use active monitoring and configuration management to maintain an up-to-date inventory of devices connected to the enterprise network, including servers, workstations, laptops, and remote devices.

2. Inventory of Authorized and Unauthorized Software

Identify vulnerable or malicious software to mitigate or root out attacks: Devise a list of authorized software for each type of system, and deploy tools to track software installed (including type, version, and patches) and monitor for unauthorized or unnecessary software.

3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers

Prevent attackers from exploiting services and settings that allow easy access through networks and browsers: Build a secure image that is used for all new systems deployed to the enterprise, host these standard images on secure storage servers, regularly validate and update these configurations, and track system images in a configuration management system.

4. Continuous Vulnerability Assessment and Remediation

Proactively identify and repair software vulnerabilities reported by security researchers or vendors: Regularly run automated vulnerability scanning tools against all systems and quickly remediate any vulnerabilities, with critical problems fixed within 48 hours.

5. Malware Defenses

Block malicious code from tampering with system settings or contents, capturing sensitive data, or spreading: Use automated anti-virus and anti-spyware software to continuously monitor and protect workstations, servers, and mobile devices. Automatically update such anti-malware tools on all machines on a daily basis. Prevent network devices from using auto-run programs to access removable media.

6. Application Software Security

Neutralize vulnerabilities in web-based and other application software: Carefully test internally developed and third-party application software for security flaws, including coding errors and malware. Deploy web application firewalls that inspect all traffic for high risk applications, and explicitly check for errors in all user input (including by size and data type).

7. Wireless Device Control

Protect restricted information from being transmitted over unencrypted wireless or through unauthorized access points: Encrypt wireless traffic. Ensure that all wireless access points are manageable

using enterprise management tools. Configure scanning tools to detect wireless access points.

8. Data Recovery Capability

Minimize the damage from an attack: Implement a trustworthy plan for removing all traces of an attack. Automatically back up all information required to fully restore each system, including the operating system, application software, and data. Back up all systems at least weekly; back up sensitive systems more often. Regularly test the restoration process.

9. Security Skills Assessment and Appropriate Training to Fill Gaps

Find knowledge gaps, and fill them with exercises and training: Develop a security skills assessment program, map training against the skills required for each job, and use the results to allocate resources effectively to improve security practices.

10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Preclude electronic holes from forming at connection points with the Internet, other organizations, and internal network segments: Compare firewall, router, and switch configurations against standards for each type of network device. Ensure that any deviations from the standard configurations are documented and approved and that any temporary deviations are undone when the business need abates

11. Limitation and Control of Network Ports, Protocols, and Services

Allow remote access only to legitimate users and services: Apply host-based firewalls and port-filtering and port-scanning tools to block traffic that is not explicitly allowed. Properly configure web servers, mail servers, file and print services, and domain name system (DNS) servers to limit remote access. Disable automatic installation of unnecessary software components. Move servers inside the firewall unless remote access is required for business purposes.

12. Controlled Use of Administrative Privileges

Protect and validate administrative accounts on desktops, laptops, and servers to prevent two common types of attack: (1) enticing users to open a malicious e-mail, attachment, or file, or to visit a malicious website; and (2) cracking an administrative password and thereby gaining access to a target machine. Use robust passwords.

13. Boundary Defense

Control the flow of traffic through network borders, and police content by looking for attacks and evidence of compromised machines: Establish multilayered boundary defenses by relying on firewalls, proxies, demilitarized zone (DMZ) perimeter networks, and other network-based tools. Filter inbound and outbound traffic, including through business partner networks (“extranets”).

14. Maintenance, Monitoring, and Analysis of Security Audit Logs

Use detailed logs to identify and uncover the details of an attack, including the location, malicious software deployed, and activity on victim machines: Generate standardized logs for each hardware device and the software installed on it, including date, time stamp, source addresses, destination addresses, and other information about each packet and/or transaction. Store logs on dedicated servers, and run biweekly reports to identify and document anomalies.

15. Controlled Access Based on the Need to Know

Prevent attackers from gaining access to highly sensitive data: Carefully identify and separate critical data from information that is readily available to internal network users. Establish a multilevel data classification scheme based on the impact of any data exposure, and ensure that only authenticated users have access to nonpublic data and files.

16. Account Monitoring and Control

Keep attackers from impersonating legitimate users: Review all system accounts and disable any that are not associated with a

business process and owner. Immediately revoke system access for terminated employees or contractors. Disable dormant accounts and encrypt and isolate any files associated with such accounts. Use robust passwords.

17. Data Loss Prevention

Stop unauthorized transfer of sensitive data through network attacks and physical theft: Scrutinize the movement of data across network boundaries, both electronically and physically, to minimize the exposure to attackers. Monitor people, processes, and systems, using a centralized management framework.

18. Incident Response Capability

Protect the organization's reputation, as well as its information: Develop an incident response plan with clearly delineated roles and responsibilities for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

19. Secure Network Engineering

Keep poor network design from enabling attackers: Use a robust, secure network engineering process to prevent security controls from being circumvented. Deploy network architecture with at least three tiers: DMZ, middleware, private network. Allow rapid deployment of new access controls to quickly deflect attacks.

20. Penetration Tests

Use simulated attacks to improve organizational readiness: Conduct regular internal and external penetration tests that mimic an attack to identify vulnerabilities and gauge the potential damage.

Thank you

With best wishes for success