SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Simone **Soderi**

M3.1 - Cybersecurity Operations and Management

Contents (1/2)

Contents (2/2)

Contents

Human Resource Security (1/2)

SECURITY REQUIREMENTS BE EMBEDDED INTO EACH STAGE OF THE EMPLOYMENT LIFE CYCLE

- **Human resource security includes** all security aspects involving employees:
  - hiring new employees
  - training employees
  - monitoring employee behavior
  - handling employee departure/termination
- Cybersecurity is **not exclusively a technical challenge** to be relegated to the work of IT and security professionals
- In the case of cybersecurity the **actions of any one employee can compromise security for the entire organization**
- **Technical fixes cannot remove vulnerabilities inherent in the workforce itself**, including social engineering, poor credential management, and use of insecure or poorly configured devices and applications
- Employees, through **awareness** training, should **learn basic security practice**

Human Resource Security (2/2)

SECURITY REQUIREMENTS BE EMBEDDED INTO EACH STAGE OF THE EMPLOYMENT LIFE CYCLE

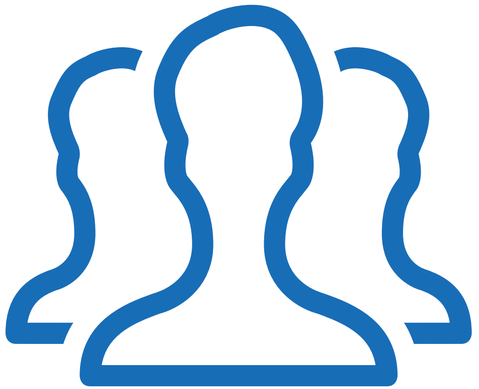
- **Security problems caused by employees** fall into two categories:
  - Non-malicious
  - Malicious
- Some **people unintentionally aid in the commission of security incidents** by failing to follow proper procedure, by forgetting security considerations, and by not understanding what they are doing
  - If an organization **does not have effective awareness and training programs, a problem could occur** because an employee was never told what constitutes proper procedure in terms of security
  - Such behaviour does not involve an intention to cause harm
  - It may be either accidental, when there is no decision to act inappropriately, or it may be negligent, when there is a conscious decision to act inappropriately
- Other people **knowingly violate controls and procedures to cause or aid in security incidents**
  - The security problems caused by **such persons can exceed those caused by outsiders**, as **employees with privileged access** are the ones who know the controls and know what information of value may be present

Hiring Process Objectives

SUGGESTED BY ISO 27002

ISO 27002 *"Code of Practice for Information Security Controls"*, **lists** the following security **objective** of the **hiring process**:

"to ensure that employees and contractors **understand their responsibilities** and are suitable for the roles for which they are considered"



Hiring Process: Background Checks and Screening

SUGGESTED BY ISO 27002

- The Computer Security Handbook points out that growing evidence suggests that **many people inflate their resumes with unfounded claims**
- Compounding this problem is that a significant number of employers have a **corporate policy that forbids discussing a former employee's performance** in any way, positive or negative; the employer may limit information to the dates of employment and the title of the position held
- Despite these obstacles, employers must make a significant effort to do background checks and otherwise screen applicants
- Such checks are done to **ensure that the prospective employee is competent to perform the intended job** and poses no security risk
- In addition, employers should be aware of the concept of **"negligent hiring"** that applies in some jurisdictions. Essentially, an **employer can be held responsible for negligent hiring if an employee** causes harm to a third party (individual or company) while acting as an employee

General Guidelines for Checking Applicants

- Ask an applicant for **as much detail as possible** about employment and educational history
- Investigate the accuracy of the applicant's details to a reasonable extent
- **Arrange for experienced staff members** to interview candidates and discuss discrepancies

For **highly sensitive positions**, more intensive investigation is warranted
The *Information Technology Security Handbook* gives **the following examples** of measures that may be warranted in some circumstances:

- Have an **investigation agency** do a background check
- Get a **criminal record check** of the individual
- Check the applicant's **credit record** for evidence of large personal debt and inability to pay it
- Consider conducting a polygraph examination of the applicant (if legal)
- Ask the applicant to obtain bonding for his or her position

the application of these checks depends on the country!

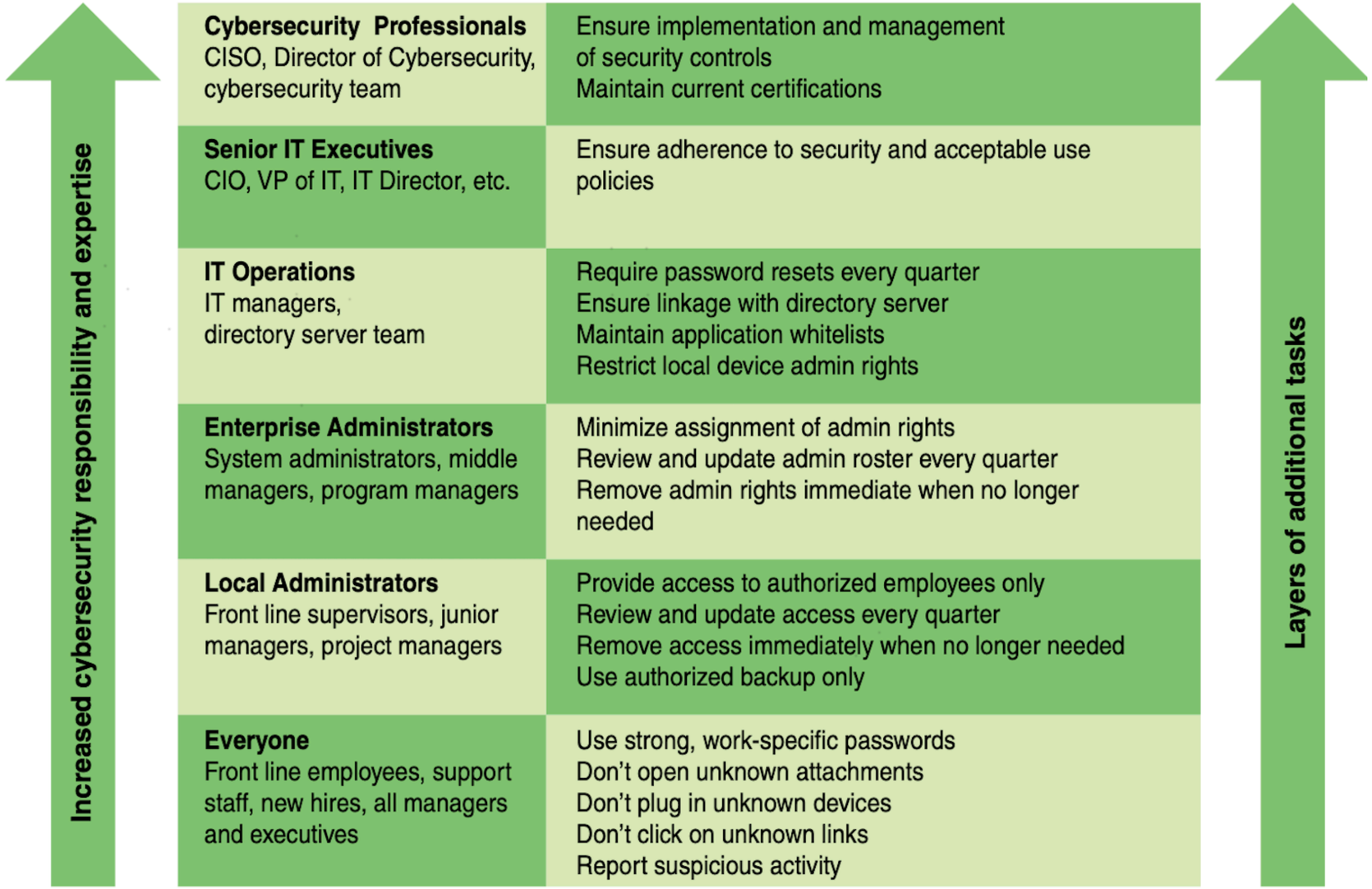
Employment Agreement

- As part of their contractual obligation, **employees should agree and sign the terms and conditions of their employment contract**, which should state their and the organization's responsibilities **for information security**
- The agreement **should include a confidentiality and non-disclosure agreement that accomplishes** specifically that the organization's information **assets are confidential** unless classified otherwise and that the employee must protect that confidentiality
- **Confidentiality agreements put all parties on notice that the organization owns its information**, expects strict confidentiality, and prohibits information sharing except for that required for legitimate business needs
- The agreement should also reference the organization's security policy and indicate that the employee has reviewed and **agrees to respect by the policy**

Job Descriptions

FOR SECURITY ROLES

A **key aspect** of clarifying the security responsibilities attached to a particular job description **is to specify the cybersecurity tasks associated with each type of job**.



Cybersecurity Professionals CISO, Director of Cybersecurity, cybersecurity team	Ensure implementation and management of security controls Maintain current certifications
Senior IT Executives CIO, VP of IT, IT Director, etc.	Ensure adherence to security and acceptable use policies
IT Operations IT managers, directory server team	Require password resets every quarter Ensure linkage with directory server Maintain application whitelists Restrict local device admin rights
Enterprise Administrators System administrators, middle managers, program managers	Minimize assignment of admin rights Review and update admin roster every quarter Remove admin rights immediate when no longer needed
Local Administrators Front line supervisors, junior managers, project managers	Provide access to authorized employees only Review and update access every quarter Remove access immediately when no longer needed Use authorized backup only
Everyone Front line employees, support staff, new hires, all managers and executives	Use strong, work-specific passwords Don't open unknown attachments Don't plug in unknown devices Don't click on unknown links Report suspicious activity

During Employment

Employees and contractors should:

- Be aware **of information security threats and concerns**
- Be aware of **their responsibilities with regard to information security**
- Be equipped **to support organizational security policy** in the course of their normal work

Two essential elements of personnel security during employment are:

- Comprehensive **security policy and acceptable** use documents
- An **ongoing awareness and training program** for all employees

Principles for Personnel Security

IN ADDITION WE SHOULD APPLY

LEAST PRIVILEGE

- Give each person the **minimum access necessary** to do his or her job
- This **restricted access is both logical** (access to accounts, networks, programs) and **physical** (access to computers, backup tapes, peripherals)

SEPARATION OF DUTIES

Separate duties so that people involved in checking for inappropriate use are not also capable of perpetrating such inappropriate use

MANDATORY VACATIONS

Mandatory vacation policies **help reveal employees involved in malicious activity** such as fraud or misappropriation

LIMITED RELIANCE ON KEY EMPLOYEES

- Some employees are key to the operation of an organization, **which creates risk**
- Organizations should have written policies and **plans established for unexpected illness or departure**
- There should be **no single employee with unique knowledge or skills**

DUAL OPERATOR POLICY

- In some cases it may be possible to define **specific tasks that require two people**
- A similar policy is **two-person control**, which requires that **two employees approve each other's work**

Termination of Employment

ISO 27002 LISTS THE FOLLOWING SECURITY OBJECTIVE

ISO 27002 security objective with respect to termination of employment:
“To protect the organization’s interests as part of the process of changing or terminating employment”

From **a security point of view the following actions** are important in the termination process:

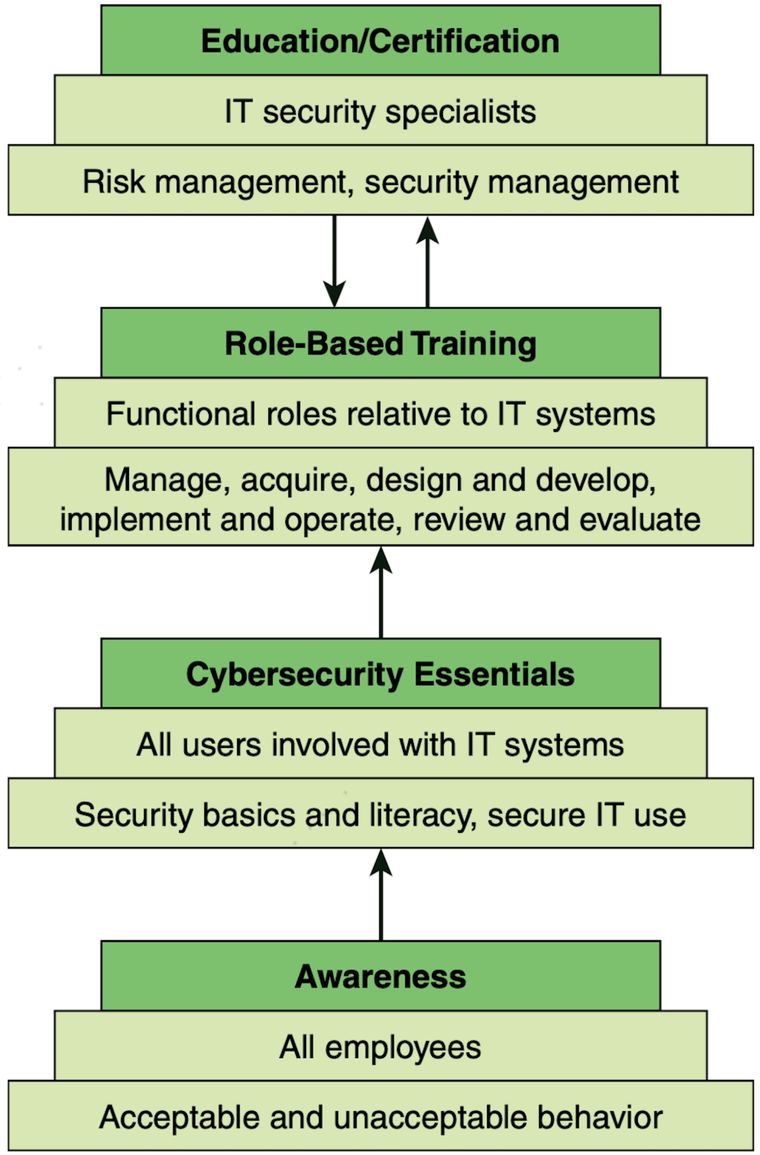
- **Removing the person’s name** from all lists of authorized access to applications and systems
- For IT personnel, ensuring that **no rogue admin accounts were created**
- Explicitly **informing guards that the ex-employee is not allowed into the building** without special authorization by named employees
- **Removing all personal access codes**
- If appropriate, **changing lock combinations, reprogramming access card systems**, and replacing physical locks
- Recovering all assets, including employee ID, disks, documents, and equipment
- **Notifying**, by memo or **email**, appropriate departments so that **they are aware of the change in employment status**
- If appropriate, escorting the ex-employee off the premises

Security Awareness and Eduction

A CRITICAL ELEMENT

- A **critical element** of an information security program is the **security awareness** and **training program**.
- A workforce that has a **high level of security awareness and appropriate security training** for each individual's role is as **important as**, if not more important than, **any other security countermeasure or control.**

Cybersecurity learning continuum that depicts a progression of learning across the spectrum of roles throughout the organization



Continuous Cybersecurity Learning

FOUR PHASES

Awareness

Set of activities

A set of activities that **explains** and **promotes security**, establishes accountability, and informs the workforce of security news.

Cybersecurity essentials

Secure practices

Intended to **develop secure practices** in the use of IT resources. Role-based training by providing a universal baseline of key security terms and concepts

Role-based training

Knowledge and skills

Intended to provide **knowledge and skills specific to an individual's roles and responsibilities relative to information systems.** Training supports competency development and helps personnel understand and learn how to perform their security roles.

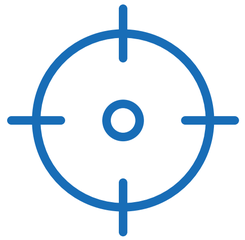
Education/certification

Functional specialties

Integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge and adds a multidisciplinary study of concepts, issues, and principles (technological and social).

Security Awareness

WHAT IS IT?



- **All employees have security responsibilities** and therefore all employees must have suitable awareness training
- Awareness seeks to focus an individual's attention on an issue or a set of issues
- **Awareness is a program that continually pushes the security message** to users in a variety of formats
- A security awareness program **must reach all employees**, not just those with access to IT resources
- Such topics as physical security, protocols for admitting visitors, social media rule, and social engineering threats are concerns with all employees
- The awareness program **must be ongoing, focused on the behavior of various categories of people**, monitored, and evaluated

What the Security Awareness Program Should Include

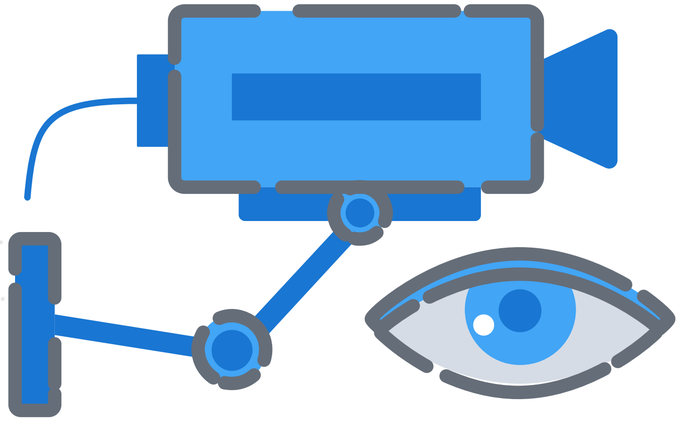
SPECIFIC GOALS

Education

Providing a focal point and a driving force for a range of awareness, training, and educational activities related to information security.

Communication

Communicating important **recommended guidelines** or practices required to secure information resources



Security Culture

Creating a **stronger culture of security, with a broad understanding** and commitment to information security

Behavior

Providing employees with an **understanding of the different types of inappropriate behavior and how to avoid negligent behavior** or accidental behavior and recognize malicious behavior in others.

Responsibility

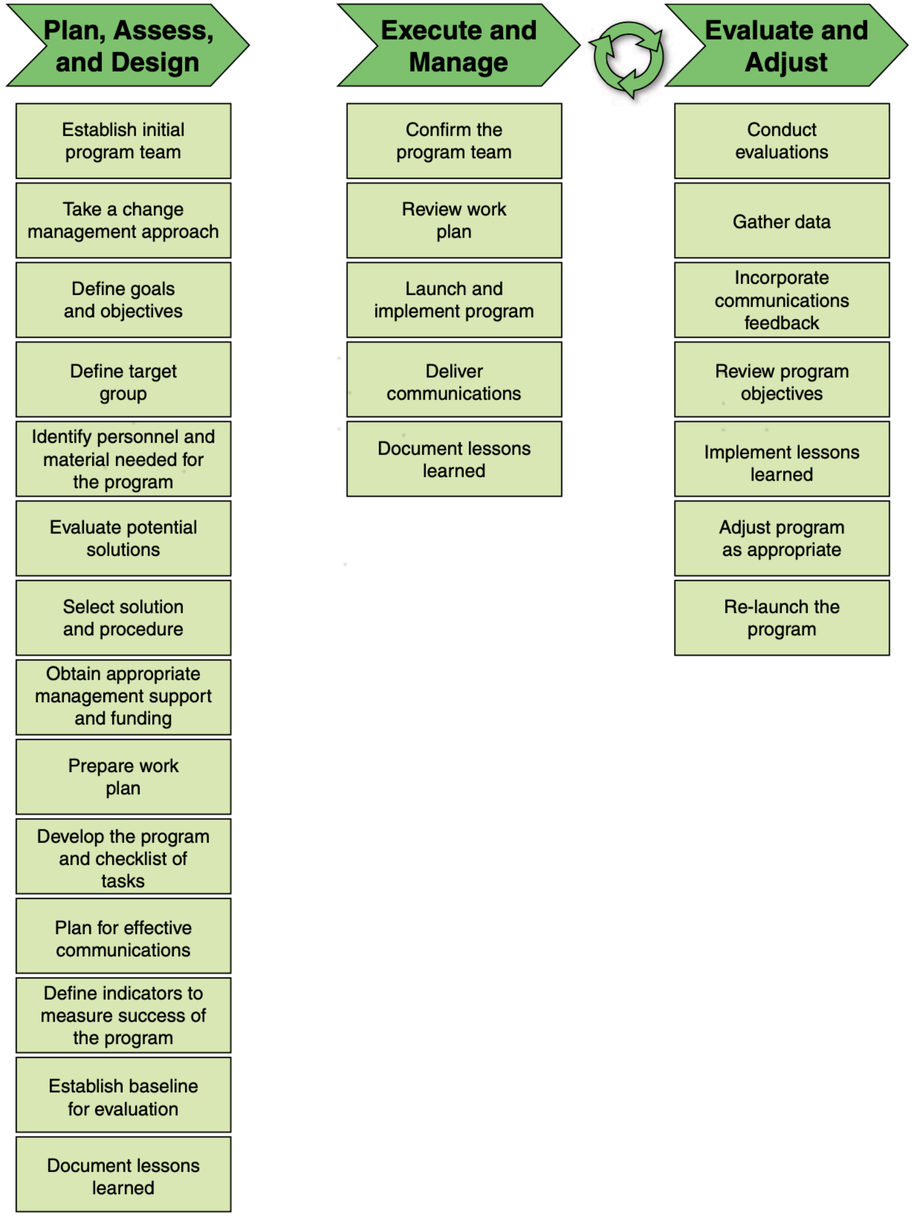
Making individuals **aware of their responsibilities** in relation to information security.

Help

Helping enhance the **effectiveness of existing information security controls** and minimize the number of information security breaches

Security Awareness Process by ENISA

The European Union Agency for Network and Information Security (**ENISA**) **has identified three main processes** in the development of an information security awareness program



Plan, assess, and design: Awareness programs **must be designed with the organization mission in mind.** In the design step of the program, the awareness needs are identified.

Execute and manage: This process includes **activities necessary to implement an information security** awareness program.

Evaluate and adjust: Formal **evaluation** and feedback mechanisms are **critical components of any security awareness program**. The feedback mechanism must be designed to address objectives initially established for the program.

Awareness Program Communication Materials

Communication materials and methods used to convey security awareness **are at the heart of an awareness training program**

There **are two options for the awareness program** and a well designed program should have materials **from both sources!**

Use in-house materials

- Brochures, leaflets, fact sheets
- Security handbook
- Regular email or newsletter
- Distance learning
- Workshop and training sessions
- Formal classes
- Video
- Website

Use externally obtained materials

- Email advisories issued by industry-hosted news groups, academic institutions, or the organization's IT security office
- Professional organizations and vendors
- Online IT security daily news websites
- Periodicals, Conferences, seminars, and courses

Education and Certification

An **education and certification program is targeted at those who have specific security responsibilities.**

Often, this type of education is **provided by outside sources**, such as college or university courses or **specialized training programs**. Examples are:

- **Global Information Assurance Certification (GIAC) Security Essentials (GSEC):** Designed for IT pros who want to **demonstrate skills in IT system hands-on roles** with respect to security tasks. Ideal candidates for this certification possess an understanding of information security beyond simple terminology and concepts

- **International Information System Security Certification Consortium (ISC)² Certified Information Systems Security Professional (CISSP):** Ideal candidates for this certification are information assurance pros who know **how to define the information system architecture, design, management, and controls** to ensure the security of business environments

- **International Information System Security Certification Consortium(ISC)² Systems Security Certified Practitioner (SSCP):** Designed for those with proven technical skills and practical security knowledge in hands-on operational IT roles. **The SSCP provides confirmation of a practitioner's ability to implement, monitor, and administer IT infrastructure** in accordance with information security policies and procedures that ensure data confidentiality, integrity, and availability

- **Information Systems Audit and Control Association (ISACA) Certified Information Security Manager (CISM):** For candidates who have an **inclination toward organizational security and want to demonstrate the ability to create a relationship between an information security program and broader business goals** and objectives. This certification ensures knowledge of information security and development and management of an information security program

- **SANS computer security training and certification:** The SANS Institute provides intensive **immersion training designed to an organization's staff master the practical steps necessary for defending systems and networks against the most dangerous threats**—the ones being actively exploited

Role-based Training

TRAINING IS TARGETED AT INDIVIDUALS WHO HAVE FUNCTIONAL

The nature of the training depends on the role of the individual in the organization

NIST SP800-16 develops **training recommendations** based on **differentiation of four major roles**:

- **Manage**

  The individual's job functions **include overseeing a program or technical aspect** of a security program; overseeing the life cycle of a computer system, network, or application; or having responsibilities for the training of staff

- **Design**

  The individual's job functions **include scoping a program or developing procedures, processes, and architectures**; or designing a computer system, a network, or an application

- **Implement**

  The individual's functions include **putting programs, processes, or policies into place**; or operation/maintenance of a computer system, a network, or an application

- **Evaluate**

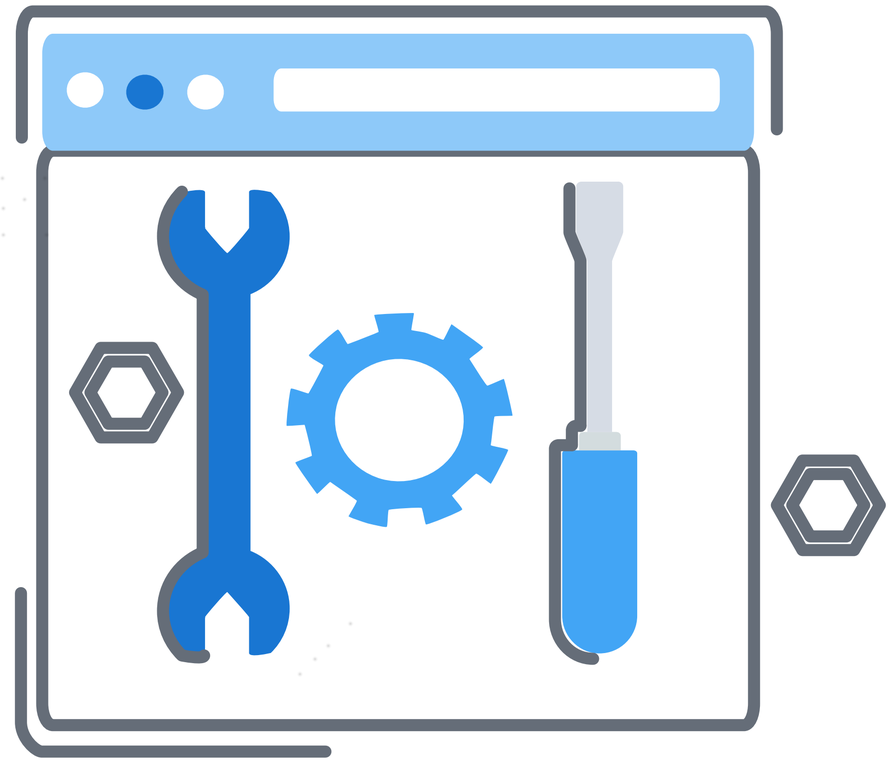
  The individual's functions **include assessing the effectiveness of any of the above actions**

Contents

Hardware

GENERAL DEFINITION

Any **physical asset** that is used to s**upport corporate information or systems** (e.g., a server, network device, mobile device, printer or specialized equipment, such as that used by manufacturing, transport or utility companies), including the **software embedded within them** and the **operating systems** supporting them



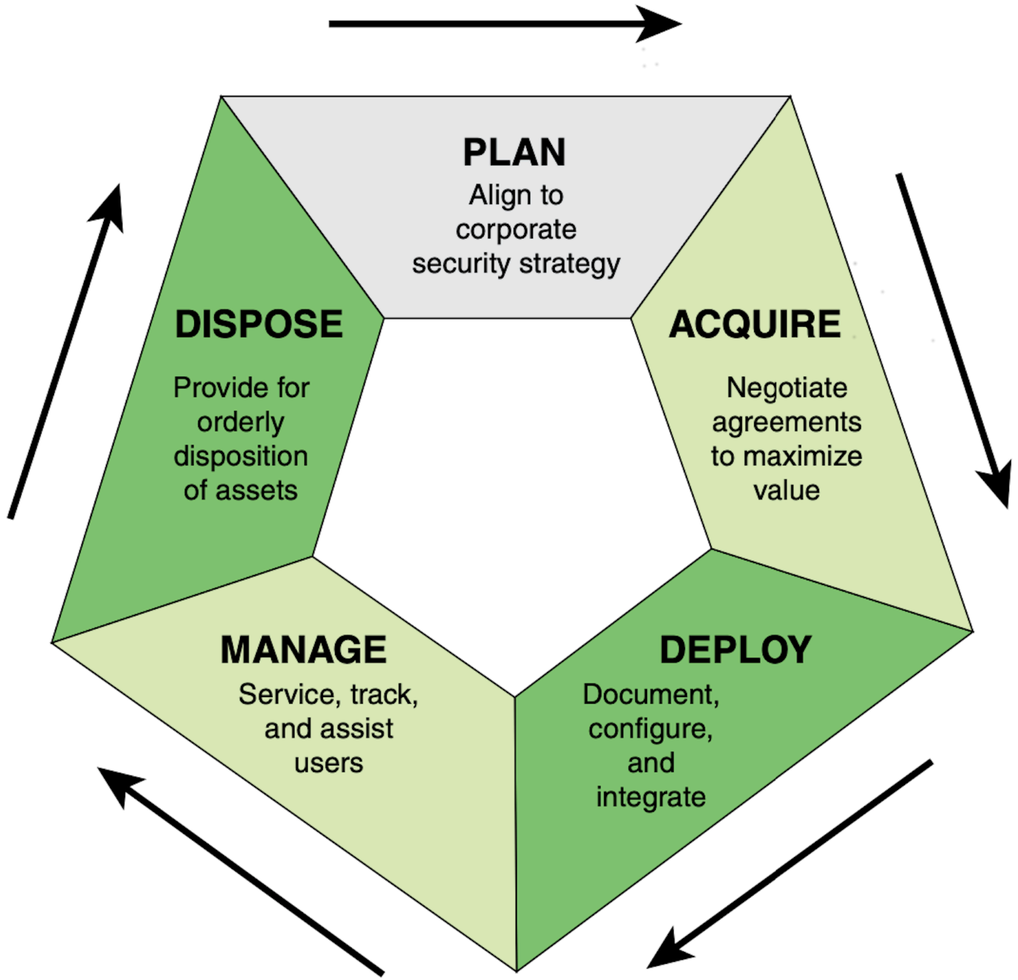
Hardware Life Cycle Management

Hardware life cycle management, also known as **hardware asset management (HAM)**, is a subset discipline of IT asset management, which **deals specifically with the hardware portion of IT assets**.

HAM entails **managing the physical components** of computers, computer networks and systems, beginning with acquisition and continuing through maintenance until the hardware's ultimate disposal.

Hardware Asset Life Cycle

MANAGEMENT OF HARDWARE ASSETS



Planning:

The plan should include guidelines for hardware selection, methods for identifying and controlling for security vulnerabilities, and a classification scheme.

Acquisition:

A number of individuals and groups should be involved in the hardware acquisition process.

Deployment:

The deployment process involves ensuring that any software running on the new hardware is subject to security hardening, such as changing default vendor passwords and applying secure configuration settings.

Management:

Hardware should be serviced/maintained on a regular basis. The simplest approach is to schedule maintenance in accordance with supplier/manufacturer recommendations.

Disposition:

An important part of the IT hardware life cycle is disposition, which may be destruction, recycling, or redeployment.

Hardware Destruction

BEWARE OF INFORMATION INSIDE!

An important part of the life cycle of **IT hardware is disposal, which can be destruction, recycling or redistribution.**

When hardware items are to be destroyed, **it is important to securely destroy all information stored on the hardware**.

Cell phones	2 years
Laptop PC	3 years
Desktop PC	4 years
Server	5 years
Networking gear	5 years
Monitor	8 years

Office Equipment

GENERAL DEFINITION

The SOGP defines **office equipment** as follows:

> Office equipment includes printers, photocopiers, facsimile machines, scanners, and multifunction devices (MFDs). Office equipment often contains the same components as a server (e.g., operating system, hard disk drives, and network interface cards)and runs services such as web, mail, and ftp. As a result, **sensitive information processed by or stored on office equipment is subject to similar threats as to servers**, yet this equipment is often poorly protected.

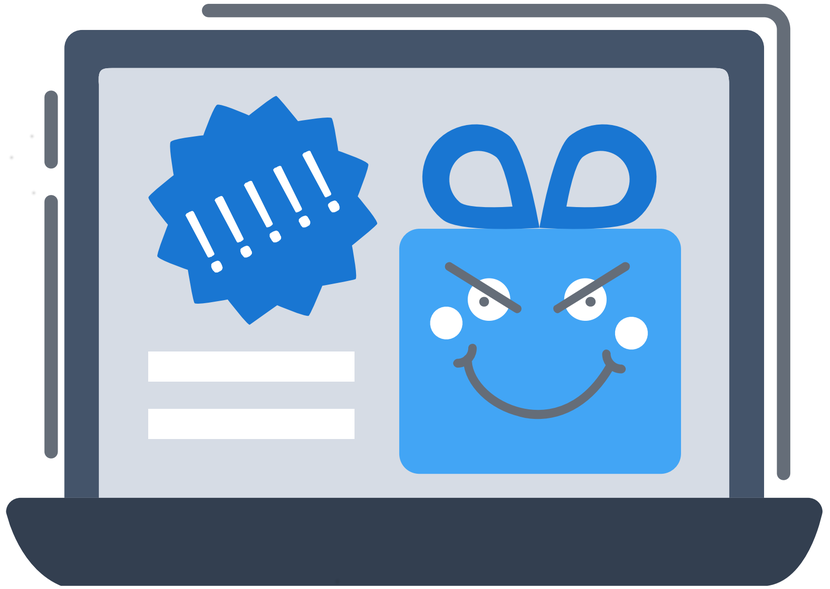
A **multifunction device (MFD)** is generally defined as:

> A network-attached document production device that combines two or more of these functions: copy, print, scan, and fax

Office Equipment: Warning!

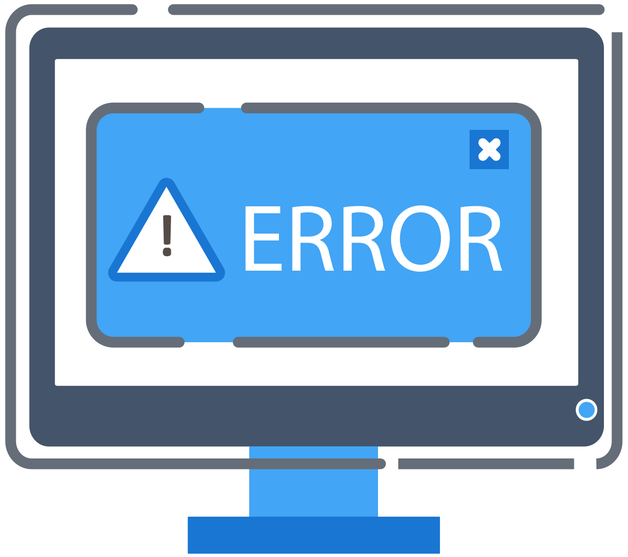
DO SOME FUNCTIONS REALLY HELP US?

- Most office equipment devices contain some **processing** power and storage capability, and in the office setting, such devices are frequently **attached to a network**.
- Thus, most such devices **are both assets to protect and opportunities for threat.** Such **equipment often is not provided with the necessary security controls** to meet risk management objectives.



Office Equipment: Threats and Vulnerabilities

There are **numerous potential threats** to office equipment.



Network Services

MFDs often come with a number of services enabled, many of which are not required in a given environment and should be disabled.

Management Protocols (HTTP/HTTPS, SNMP,…)

Service Protocols (FTP, SMTP)

Information Disclosure

Three **potential sources** of vulnerability are:

- Print, fax, and copy/scan logs
- Address books
- Mailboxes

DoS Attacks

These types of attacks include:

- Sending multiple **fake print jobs** to exhaust paper resources
- Modifying settings to make the device **unusable**
- Stopping or deleting jobs
- Setting the IP address of the MFD to be the same as a router, causing routing confusion

Physical Security

Proper physical security is needed to guard against:

- Making **modifications to the global configuration** via the console interface
- Obtaining printouts that do not belong to them
- Physically removing the hard disk, which might contain print spool file and other information

Operating System Security

Many **office devices run an embedded commercial OS**, which have the same threats and vulnerabilities as any other devices running the same OS

Manufacturers may embed versions of OS for which functionality to install **patches or updates is not available**

Examples of these vulnerabilities include:

- Buffer overflows
- Execution of arbitrary code
- Taking control of the device using remote administration capabilities

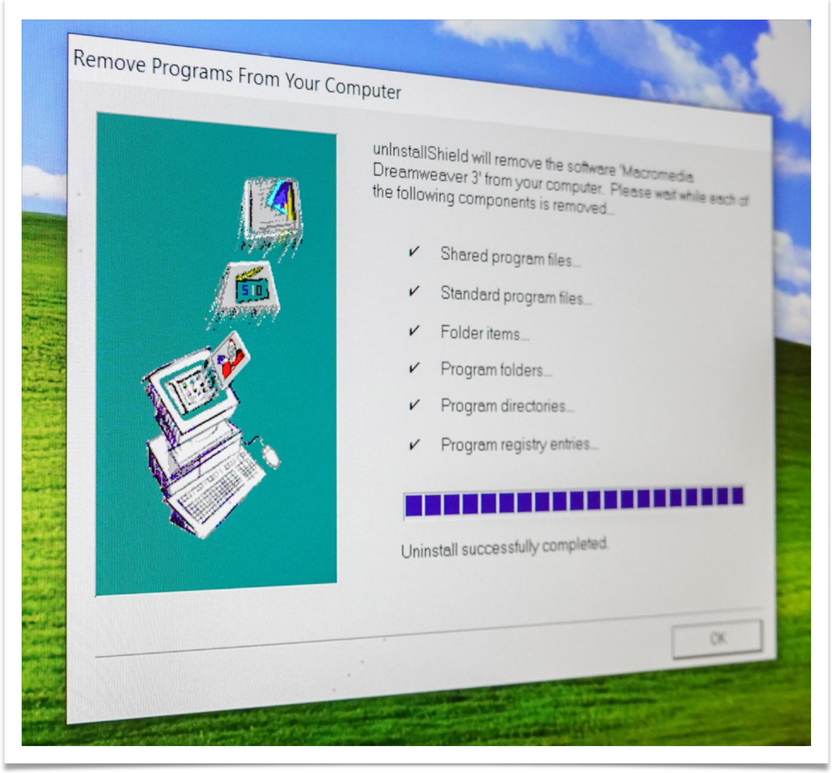
MultiFunction Device Hardening Checklist

A useful checklist of security **measures an organization can take to protect MFDs** is provided in the **SANS** Institute article *"Auditing and Securing Multifunction Devices"*

Category	Action
Network Protocols and Services	Disable unused network protocols other than TCP/IP.
	Disable unused network services (print/fax/scan and management).
	Assign the MFD a static IP address.
	Restrict access to MFD services (print/fax/scan and management) to the minimum number of hosts that require these functions.
	Use encrypted communications protocols (e.g. HTTPS), where available, and disable insecure protocols.
Management	Set a strong administrator password.
	Change default SNMP community strings to strong passwords.
	Ensure that logging is enabled on the MFD.
	Ensure that logs are monitored on a regular basis.
	Restrict access to address books, mailboxes, and logs using your current password policy.
Security updates	Monitor CVEs and vendor for security bulletins and patches.
	Upgrade firmware in a timely manner, using your current change control process.
Physical security	Place the device in an area with physical security controls consistent with the sensitivity data it processes.
	Set an administrator password on the console.
	Require that users authenticate to scan, fax, or copy from the console.
	If the MFD has a removable hard drive, ensure that it is locked into the device.
	If possible, implement measures to encrypt or secure-wipe print spool files.
	Ensure that your security policy specifies what to do with MFD drives that are decommissioned or sent back to the manufacturer or leasing company (e.g. retained, secure wiped, destroyed, etc.).

Equipment Disposal (1/3)

The **SOGP recommends that sensitive information stored on office equipment be securely destroyed** before the equipment is decommissioned, sold, or transferred to an external party. This is an important security area that should not be overlooked as part of an organization's security program for office devices.



Equipment Disposal (2/3)

NIST SP 800-88 *“Guidelines for Media Sanitization”* defines **three actions:**

CLEAR

Applies logical techniques to **sanitize data in all user-addressable storage locations** for protection against simple non-invasive data recovery techniques; typically applied through the standard read and write commands to the storage device, such as by **rewriting with a new value or using a menu option to reset the device to the factory state** .

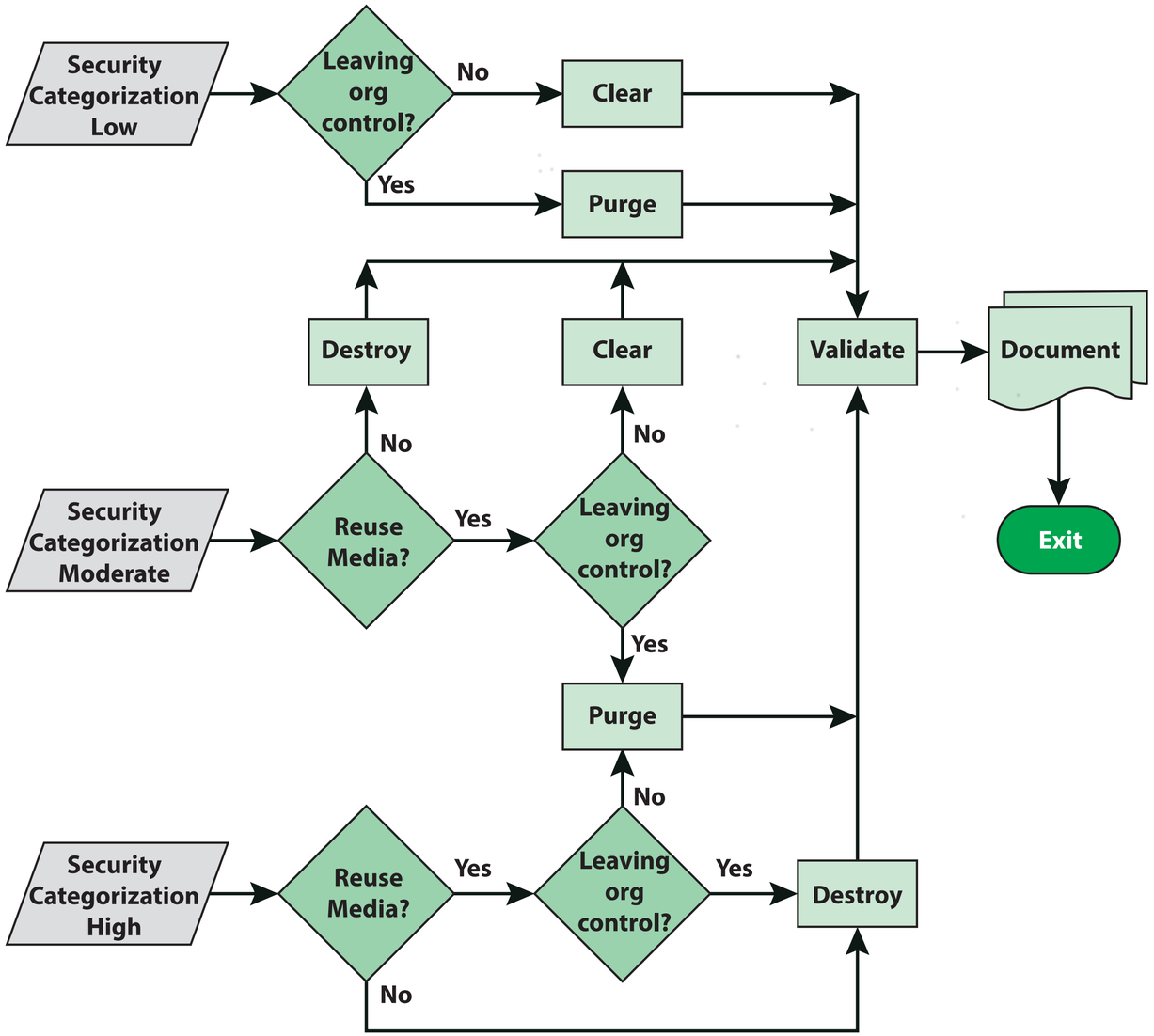
PURGE

Applies physical or logical techniques that render target data recovery infeasible using state-of-the-art laboratory techniques. This can be achieved by **performing multiple overwrites**. For a self-encrypting drive (SED), cryptographic erasure can be used. If the drive automatically encrypts all user-addressable locations, **then all that is required is to destroy the encryption key**, which could be done by multiple overwrites

DESTROY

Renders target data recovery infeasible using state-of-the-art laboratory techniques and results in the subsequent inability to use the media for storage of data. Typically, the medium is pulverized or **burned at an outsourced metal destruction** or licensed incineration facility.

Equipment Disposal (3/3)



Based on the **risk assessment for an office device**, an organization can assign a **security category** to the data on the device and then use this flowchart to determine **how to dispose of the memory associated with the device.**

Industrial Control System (ICS)

GENERAL DEFINITION

An ICS is used to used to **control industrial processes** such as manufacturing, product handling, production, and distribution

Includes **supervisory control and data acquisition (SCADA)** systems used to control geographically dispersed assets, as well as distributed control systems (DCSs) and smaller control systems, using programmable logic controllers to control localized processes

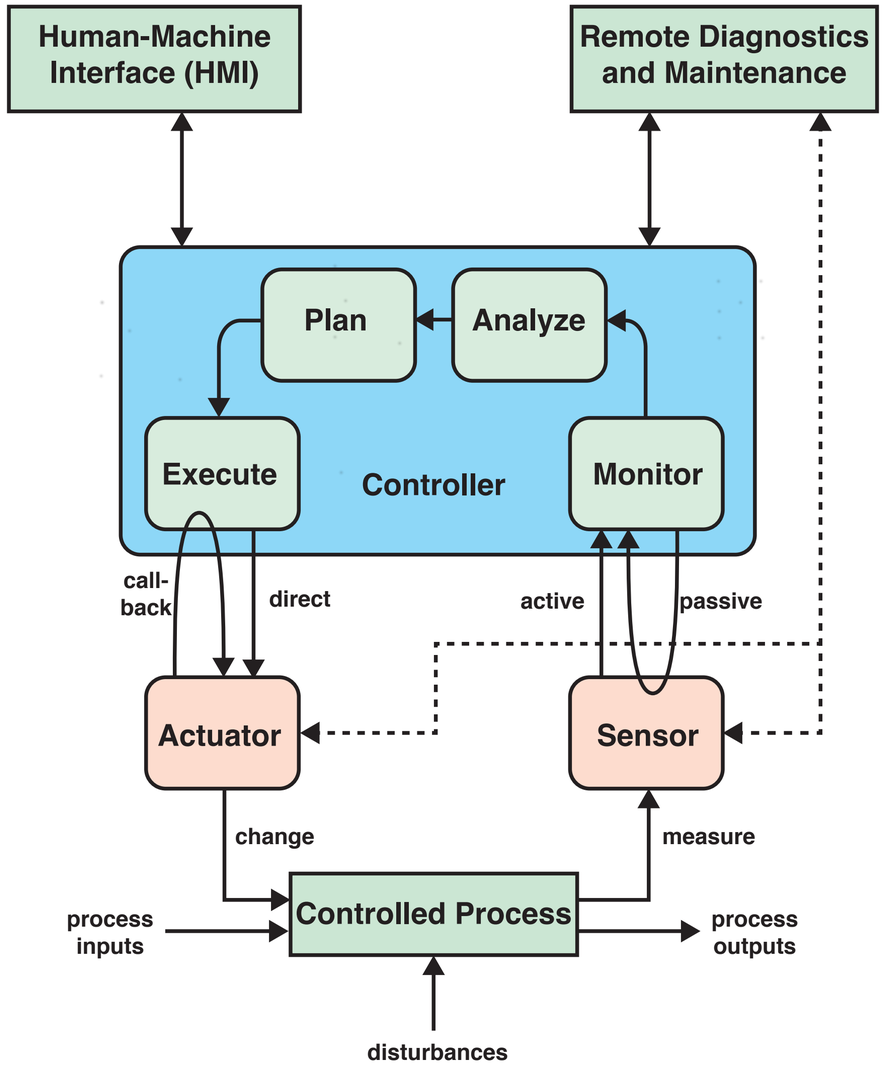
An ICS consists of **combinations of control components** that act together **to achieve an industrial objective**

Principal Elements of an ICS (1/2)

NIST SP 800-82

"Guide to Industrial Control Systems Security"

illustrates the principal elements of an industrial control system and their operational interaction.



Principal Elements of an ICS (2/2)

SENSOR

Measures some parameter of a physical, chemical, or biological entity and delivers an electronic signal proportional to the observed characteristic, either in the form of an analog voltage level or a digital signal

ACTUATOR

Receives an electronic signal from a controller and responds by **interacting with its environment to produce an effect** on some parameter of a physical, chemical, or biological entity

CONTROLLER

Interprets the signals and generates corresponding manipulated variables, based on a control algorithm and target set points, which it transmits to the actuators

HUMAN-MACHINE INTERFACE (HMI)

Operators and engineers use **human interfaces to monitor and configure** set points, control algorithms, and adjust and establish parameters in the controller

REMOTE DIAGNOSTICS AND MAINTENANCE

Utilities used to prevent, identify, and recover from **abnormal operation or failures**

Security for IT and ICS

Just as there are **differences** in the operation and environment between ICSs and IT systems, there are also differences in security risks and countermeasures.

An **ICS** often **involves widely distributed devices that may be in insecure locations**. In many cases, these are embedded devices containing **microcontrollers with limited processing power and limited human interface functionality**.

Security Area	Information Technology (IT)	Control Systems (ICS)
Anti-virus and Mobile Code	Very common; easily deployed and updated. Users have control over customization and can be asset-based or enterprise-based	Memory requirements can impact on ICS; organizations can only protect legacy systems with after-market solutions; usually requires "exclusion" folders to avoid programs quarantining critical files
Patch Management	Easily defined; enterprise-wide; remote and automated	Long timeline to successful patch installation; OEM-specific; may "break" ICS functionality; asset owners required to define acceptable risk
Technology Support Lifetime	2-3 years; multiple vendors; ubiquitous upgrades	10-20 years; usually same vendor over time; product end-of-life creates new security concerns
Testing and Audit Methods	Use modern methods; systems usually resilient and robust to handle assessment methods	Tune testing to the system; modern methods can be inappropriate; equipment may be susceptible to failure during testing
Change Management	Regular and scheduled; aligned with minimum-use periods	Strategic scheduling; nontrivial process due to impact on production
Asset Classification	Common and performed annually; results drive expenditure	Only performed when obligated; accurate inventories uncommon for nonvital assets; disconnect between asset value and appropriate countermeasures
Incident Response and Forensics	Easily developed and deployed; some regulatory requirements; embedded in technology	Focused on system resumption activities; forensics procedures immature (beyond event re-creation); requires good IT/ICS relationships
Physical and Environmental Security	Can range from poor (office systems to excellent (critical IT operations systems)	Usually excellent for critical areas, maturity varies for site facilities based on criticality/culture
Secure Systems Development	Integral part of development process	Historically not an integral part of development process; vendors are maturing but at slower rate than IT; core/flagship ICS solutions difficult to retrofit with security
Security Compliance	Definitive regulatory oversight depending on sector (and not all sectors)	Specific regulatory guidance depending on sector (and not all sectors)

Typical Security Threats to ICSs

According to NIST SP 800-82, **possible threats ICSs** may face include the following:

- **Blocked or delayed flow of information** through ICS networks, which could disrupt ICS operation
- **Unauthorized changes to instructions**, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life
- **Inaccurate information sent to system operators**, either to disguise unauthorized changes or to cause the operators to initiate inappropriate actions, which could have various negative effects
- **ICS software or configuration settings modified**, or ICS software infected with malware, which could have various negative effects
- **Interference with the operation of equipment protection systems**, which could endanger costly and difficult-to-replace equipment
- **Interference with the operation of safety systems**, which could endanger human life

Mobile Device

GENERAL DEFINITION

NIST SP 800-53 **defines a mobile device** as a

"**Portable computing and communications device** with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices"

Mobile Device Security

Prior to the widespread use of smartphones, there was a dominant paradigm for computer and network security. Corporate IT was tightly controlled.

User devices were typically limited to Windows PCs. Business applications were controlled by IT and either run locally on endpoints or on physical servers in data centers.

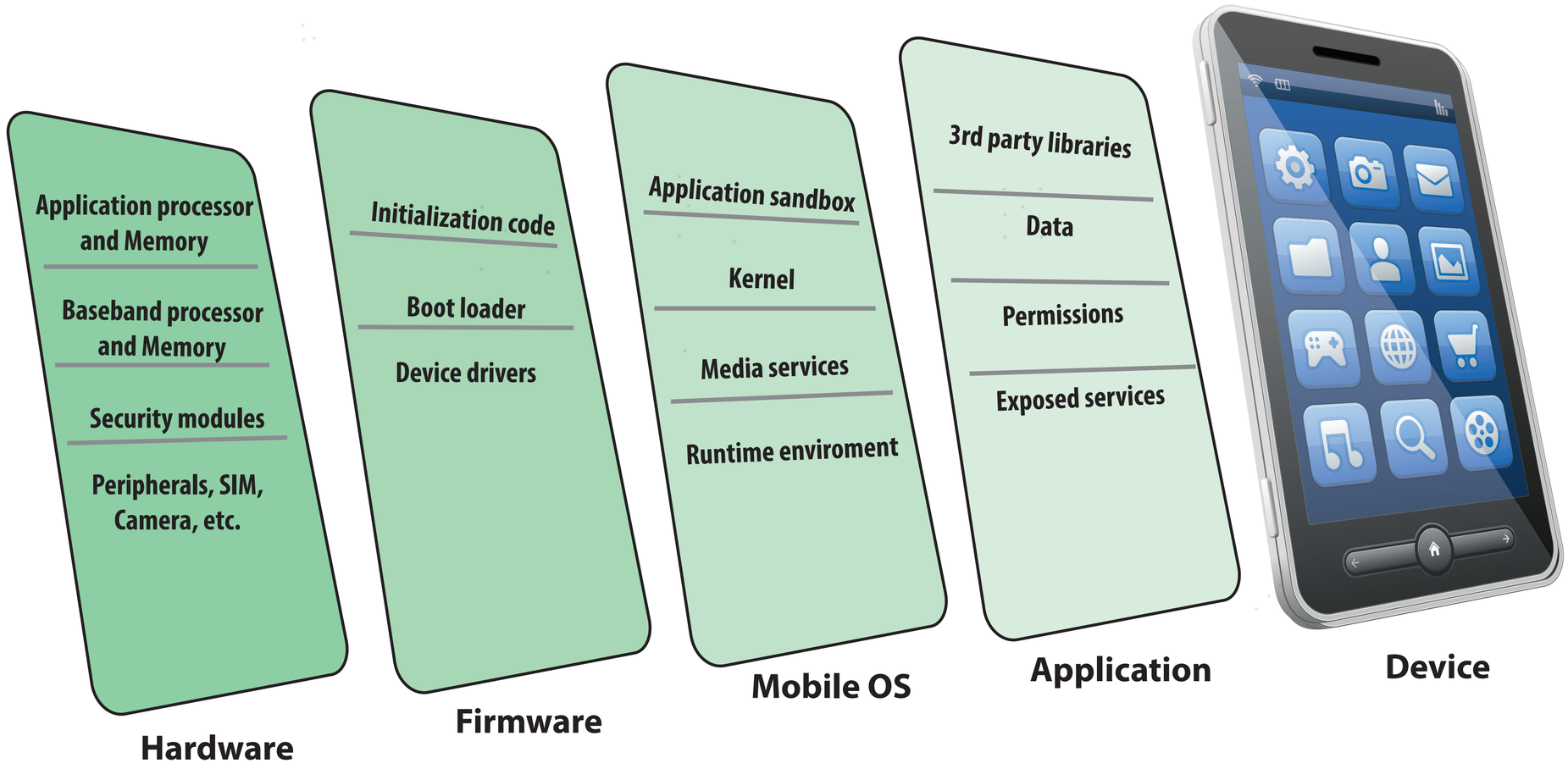
Network security was based on clearly defined perimeters that separated trusted internal networks from the untrusted Internet.

Today, with the introduction of **mobiles**, there have been **massive changes** in these assumptions.

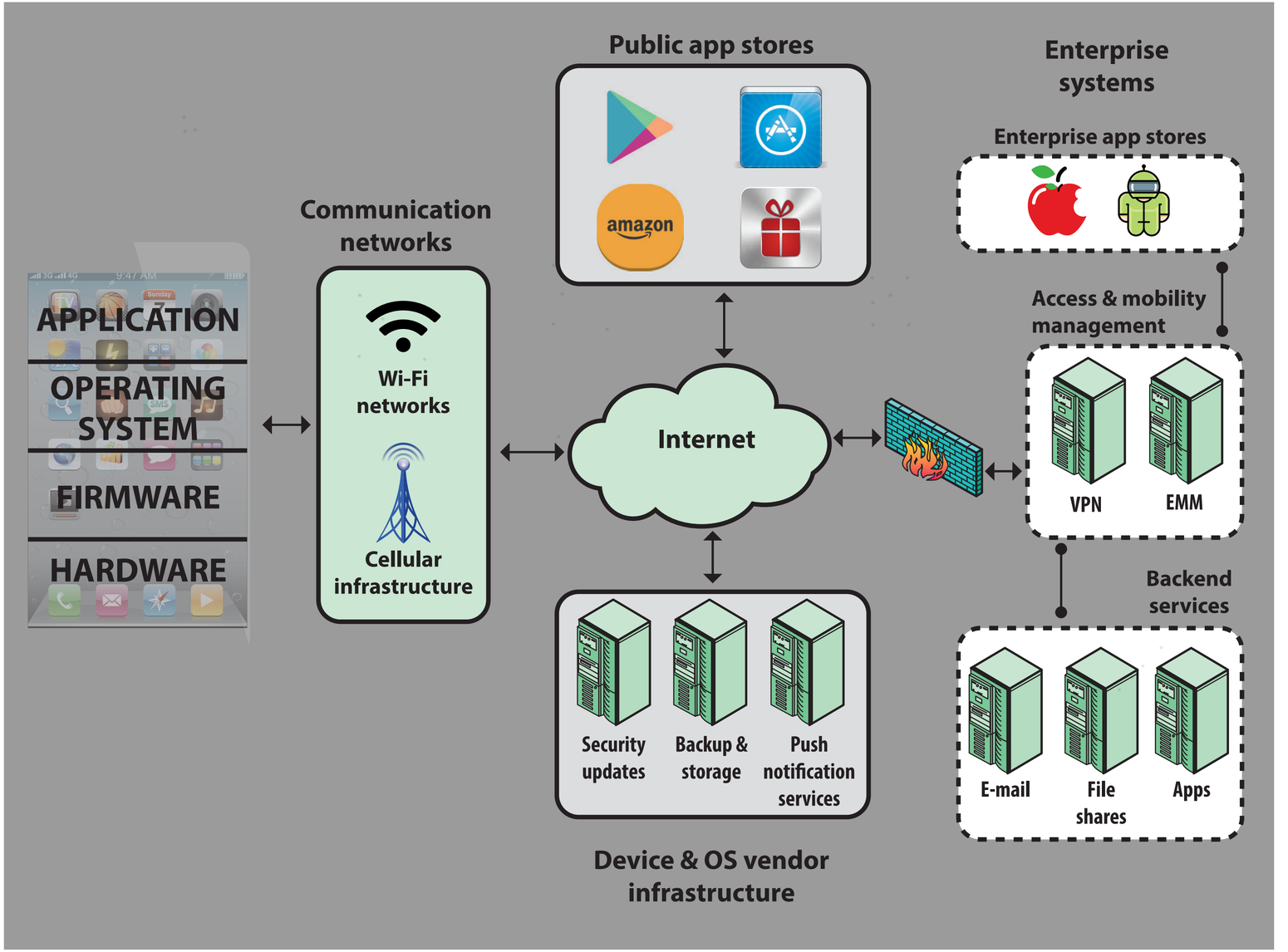
An organization's networks must accommodate the following:

- **Growing use of new devices:** *significant growth in employee use of mobile devices.*
- **Cloud-based applications:** *Applications no longer run solely on physical servers in corporate data centers.*
- **De-perimeterization:** *Multitude of network perimeters around devices, applications, users, and data.*
- **External business requirements:** *guests, third-party contractors, and business partners network access*

Mobile Device Technology Stack



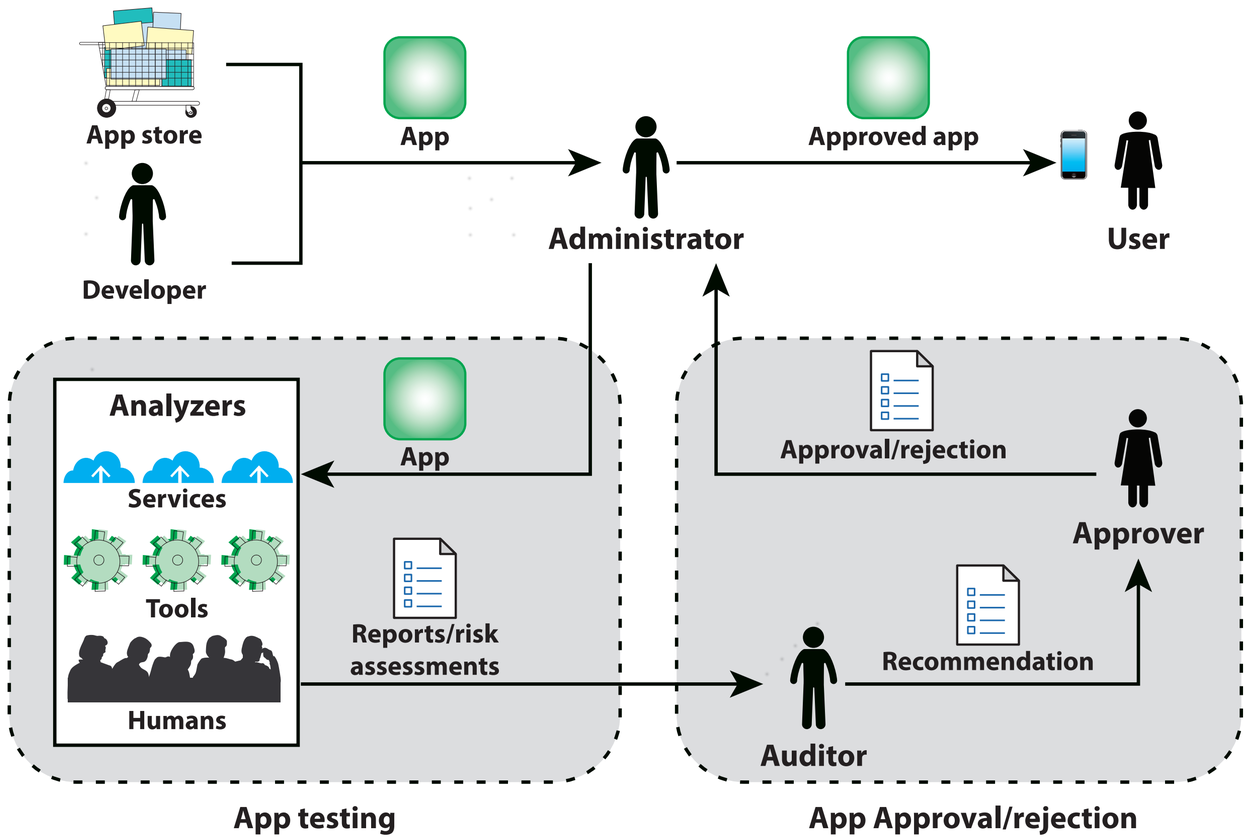
Mobile Device Ecosystem



Mobile Device App

Millions of apps are available from the two major stores, the Apple App Store and Google Play, and millions more can be obtained from other public app stores. The reliability and **security of apps may vary widely**, and the control process may be opaque or insufficiently robust, particularly for apps from outside the two major stores.

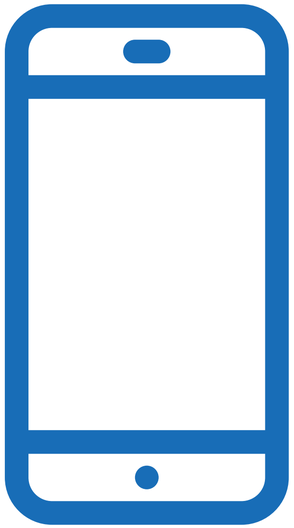
Regardless of the source of an app, **an enterprise should perform its own evaluation of the security of the app to determine if it conforms to the organization's security requirements.** The requirements should specify how data used by the app should be secured, the environment in which the app will be deployed, and the acceptable level of risk for the app.



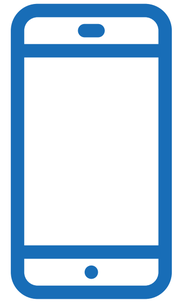
Bring You Own Device (BYOD) (1/2)

Many organizations **supply mobile devices for employee use and preconfigure those devices** to conform to the enterprise security policy. However, many organizations find it convenient or even necessary to **adopt a bring your own device (BYOD) policy** that allows the personal mobile devices of employees to have access to corporate resources.

IT managers should be able to inspect each device before allowing network access. IT should establish configuration guidelines for operating systems and applications. For example, **rooted or jailbroken devices are not permitted on the network, and mobile devices cannot store corporate contacts on local storage.**



Bring You Own Device (BYOD) (2/2)



Whether a device is owned by the organization or an employee, **the organization should configure the device with security controls, including taking the following measures**:

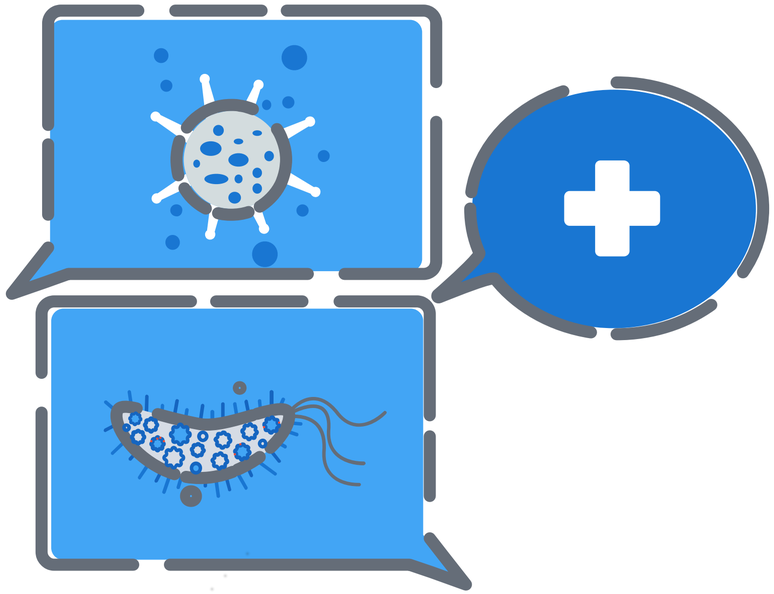
- **Enable auto-lock**, which causes the device to lock if it has not been used for a given amount of time.
- **Enable password or PIN protection**. The PIN or password is needed to unlock the device.
- **Enable remote wipe**.
- Ensure that Transport Layer Security/Secure Sockets Layer (TLS/SSL) protection is enabled, if available.
- Make sure that software, including operating systems and applications, is up to date.
- Install antivirus software as it becomes available.
- Either **prohibit users from storing sensitive data on mobile devices or require users to encrypt sensitive data**.
- Ensure that **IT staff have the ability to remotely access devices,** wipe devices of all data, and disable devices in the event of loss or theft.
- Possibly prohibit installation of third-party applications, implement whitelisting to prohibit installation of all unapproved applications.
- Implement and enforce restrictions on what devices can synchronize and on the use of **cloud-based storage**.

Mobile Device Vulnerabilities

Mobile devices **need additional specialized protection measures** beyond those implemented for other client devices, such as desktops and laptops, **precisely because they are often used outside the corporate perimeter.**

NIST SP 800-124, *"Guidelines for Managing and Securing Mobile Devices in the Enterprise"*, lists **seven major security concerns for mobile devices**

- Lack of physical security controls
- Use of untrusted mobile devices
- Use of untrusted networks
- Use of applications created by unknown parties
- Interaction with other systems
- Use of untrusted content
- Use of location services



Mobile Device Threats

Rooting/Jailbreaking

The act of **removing a restricted mode of operation**. For example, **rooting may enable content with digital rights** to be used on any computer, or it may allow enhanced third-party operating systems or applications to be used on a mobile device. While rooting is the term used for Android devices, jailbreaking is the equivalent term used for Apple's devices

Sideloading

The act of **downloading an app to a device without going through the official app store**, via links or websites. While enterprises often use sideloading as a method for distributing home-grown apps, **malicious actors also use sideloading** (via enterprise certificates in many cases bought on the black market) **to distribute their malware**

Mobile Ecosystem Element	Threats
Mobile device technology stack	Delays in security updates Zero-day exploits against software and firmware, particularly the baseband Bootloader exploitation Jailbreak/rooting Supply chain compromise Trusted Execution Environment (Android) or Secure Enclave (iOS) exploitation Compromised cloud system credentials
Mobile applications	Malware (including backdoors, ransomware, and privilege escalation) Vulnerable third-party libraries Exploitation of vulnerable app Insecure app development practices Exploit public mobile app store
Mobile networks	Rogue cellular base stations and Wi-Fi access points Man-in-the-middle attacks on communications Data/voice eavesdropping Data/voice manipulation Device and identity tracking Denial of service/jamming
Device physical systems	Loss or theft of a mobile device Physical tampering Malicious charging station
Mobile enterprise	Compromised EMM/MDM system or admin credentials Compromised enterprise mobile app store or developer credentials Bypass app vetting

SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Simone **Soderi**

simone.soderi@unipd.it

M3.1 - Cybersecurity Operations and Management

Thanks for your attention!