Threat Mitigation Workshop – Cybersecurity Overview

Dan Costa

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM22-0035

Agenda

Cybersecurity Overview

Cybersecurity Requirements

Role of the CISO in Enterprise Risk

Role of the Human in Cybersecurity

Fundamental Concepts in Cybersecurity

What Is Cybersecurity?

“Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.”

-Merriam-webster.com

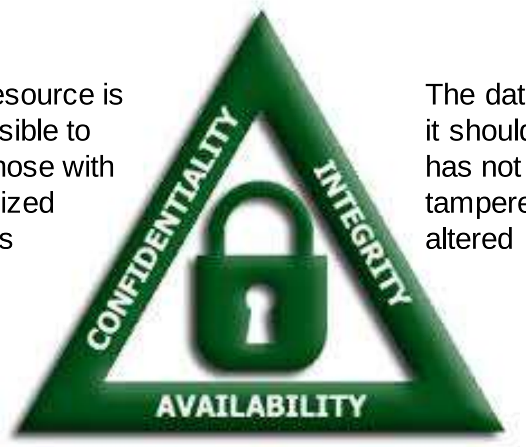
“Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work.

- Thus, the healthy functioning of cyberspace is essential to our economy and our national security.”

-The National Strategy to Secure Cyberspace, 2003

Confidentiality, Integrity, Availability

The resource is accessible to only those with authorized access



The data is what it should be – has not been tampered with or altered

The ability to use the resource when it is needed

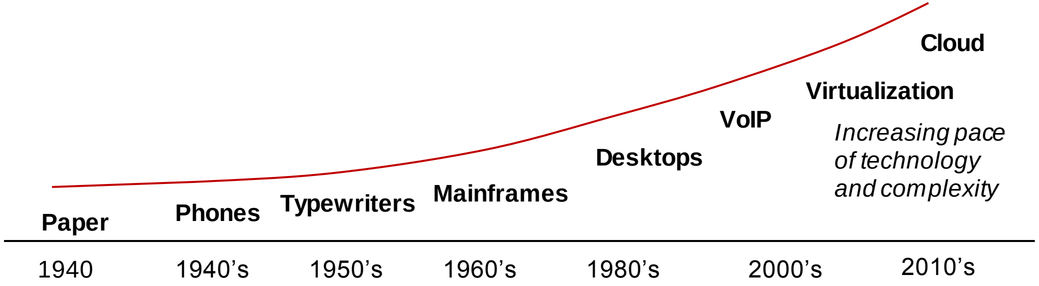
Increasing Pace

Information is an indispensable component of virtually all organizations and their ability to conduct business.

Information security (IS) is becoming an increasingly critical program.

It has become an integral part of enterprise management.

- affects an organization’s leadership, structure, and processes
- is now a responsibility of executive management, with oversight from the board of directors



Information Security vs. Information Technology Security

IT security is a component of information security

Information security

- Encompasses ALL aspects of information: content, meaning, knowledge
- includes all aspects of risks, benefits, and processes involving information
- is governed by executive management

Information technology security

- focuses on the security of information within the boundaries of the technological domain
- is governed at the chief information officer (CIO) level

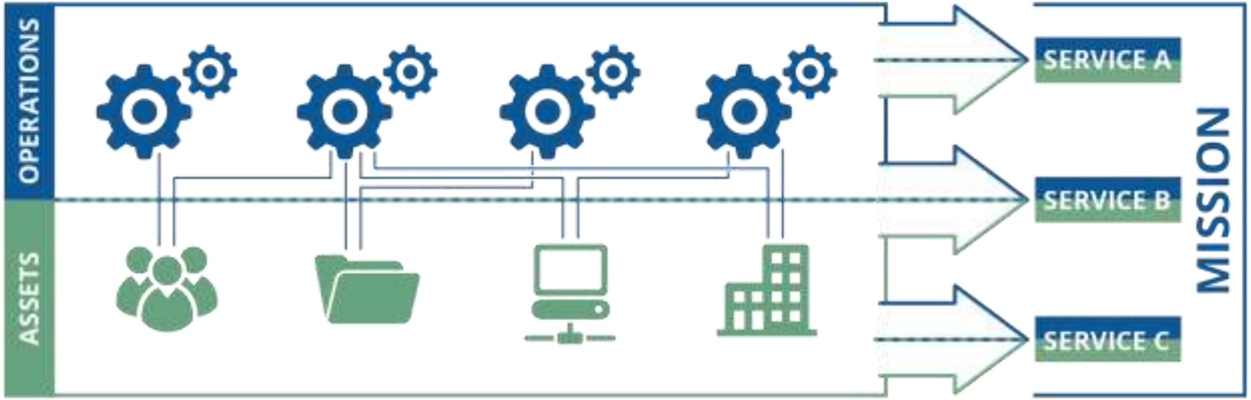
Operational Balance

The security of these functions cannot override the ability to operate them.

Risk analysis helps identify security requirements based on operational needs, threats, and impact from those threats:

- a database with no outside connectivity could be considered secure, but the operational effect of denying access to it makes the security pointless.
- a cost-benefit analysis can help you avoid "building a $10,000 fence around a stack of quarters."

Focus Cybersecurity on Business Objectives



People: those who operate and monitor the service

Information: data associated with the service

Technology: tools and equipment that automate and support the service

Facilities: where the service is performed

! **Assets derive their value from their importance in meeting the service mission.**

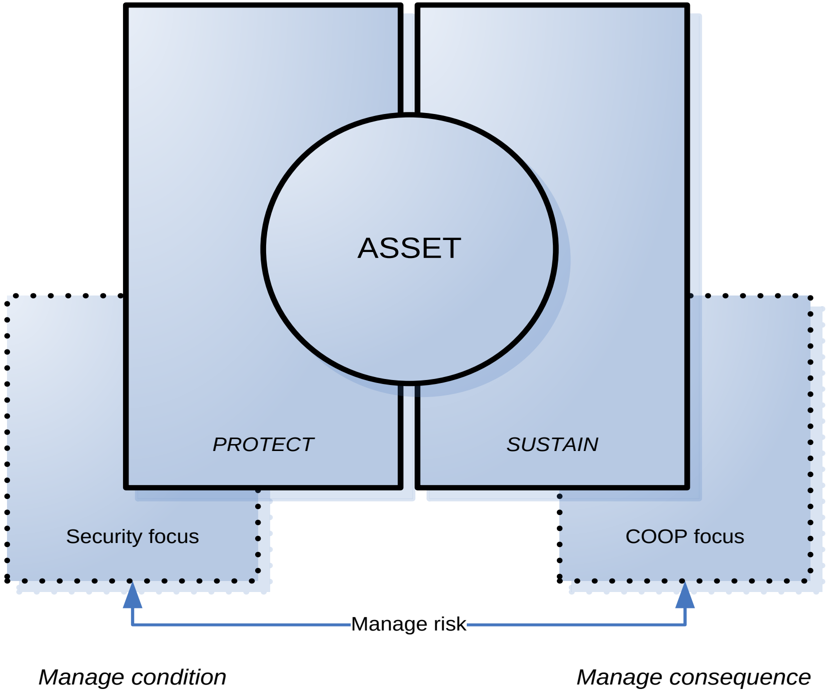
Cybersecurity Goal: Enhance Resilience

Resilience is the physical property of a material when it can return to its original shape or position after deformation that does not exceed its elastic limit. [wordnet.princeton.edu]

Operational resilience is the emergent property of an organization that can continue to carry out its business objectives after disruption that does not exceed its operational limit [CERT-RMM]

The **disruption** comes from realized risk.

Balance Protection and Sustainment



The first principle of risk management is to focus on the critical few.

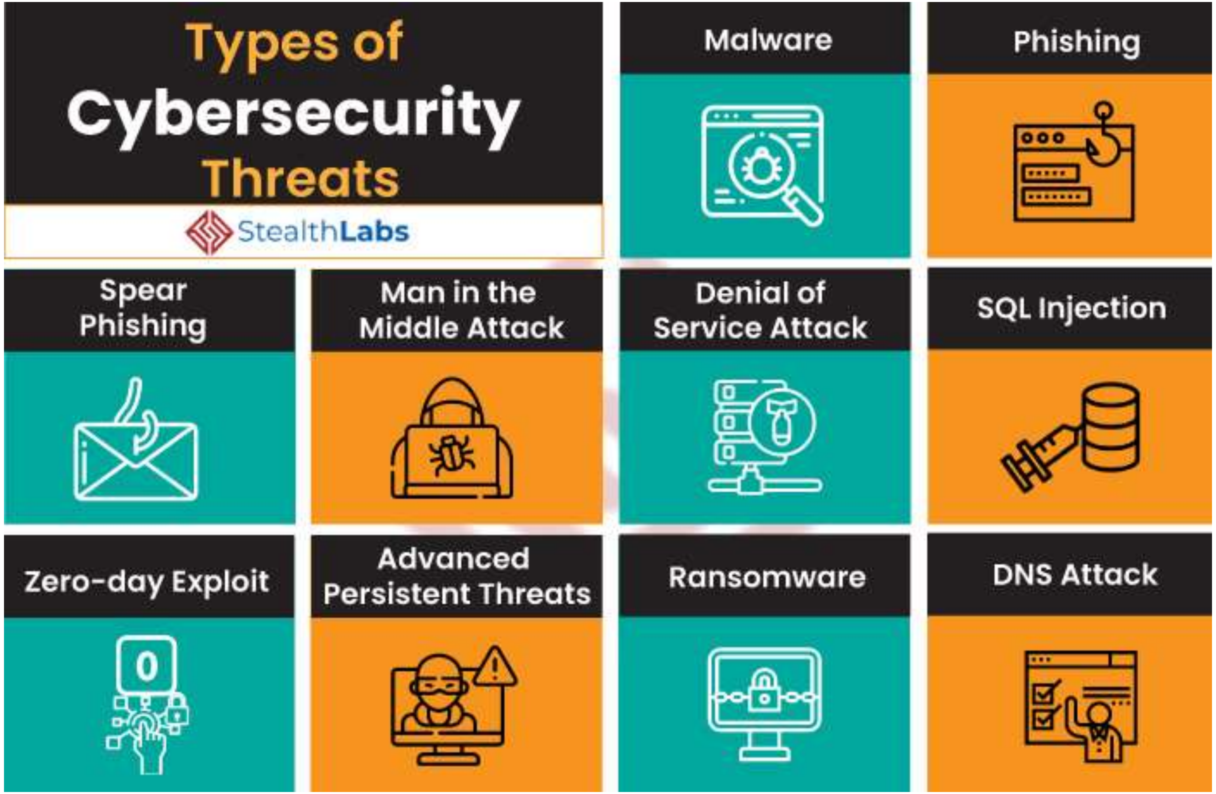
- Find out what is most important to your organization.
- Figure out where it lives.
- Build your strategy around it.

A lack of proper asset management is a key reason organizations cannot get a handle on cybersecurity.

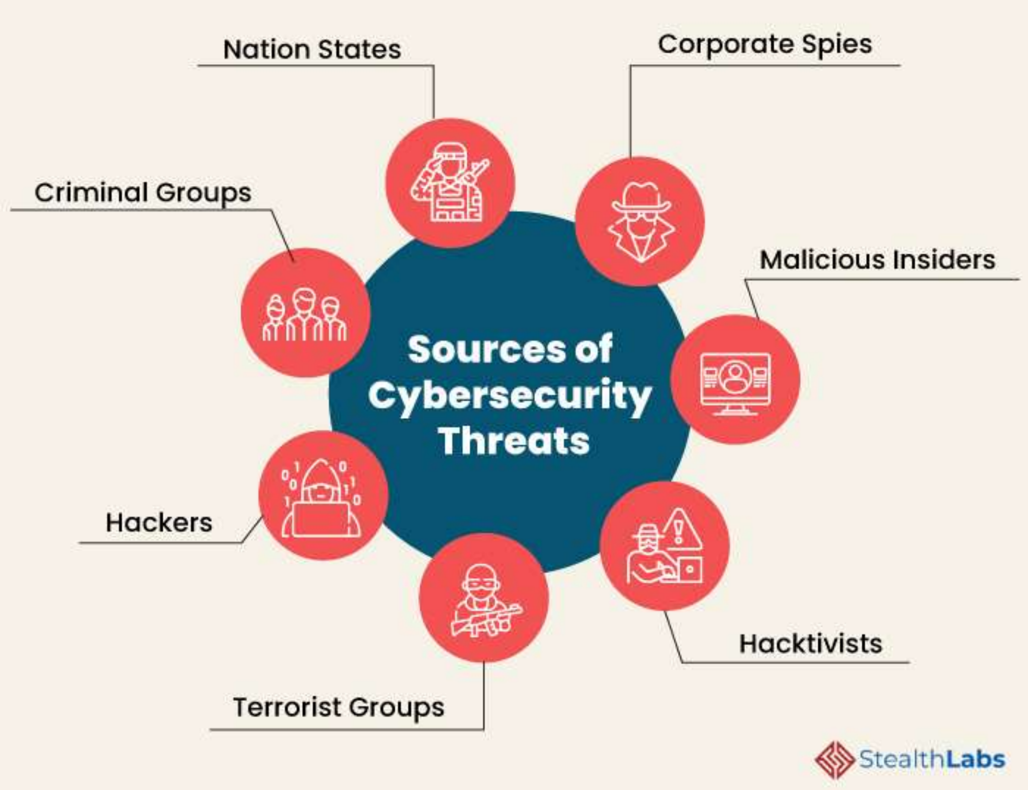
Security vs. Survivability

Security	Survivability
Focus on protecting information	Focus on continuity of operations
Systems are seen as bounded and under central administrative control.	Are seen as open, unbounded, with distributed administrative control.
Considered an overhead expense	Considered an investment; essential to the business of the organization
Narrow technical specialty with technology-based solutions	Part of enterprise risk management; business driven, management-based solutions
Protect system components	No component is immune; ensure business objectives sustained

Cybersecurity Threats



Cybersecurity Threat Actors

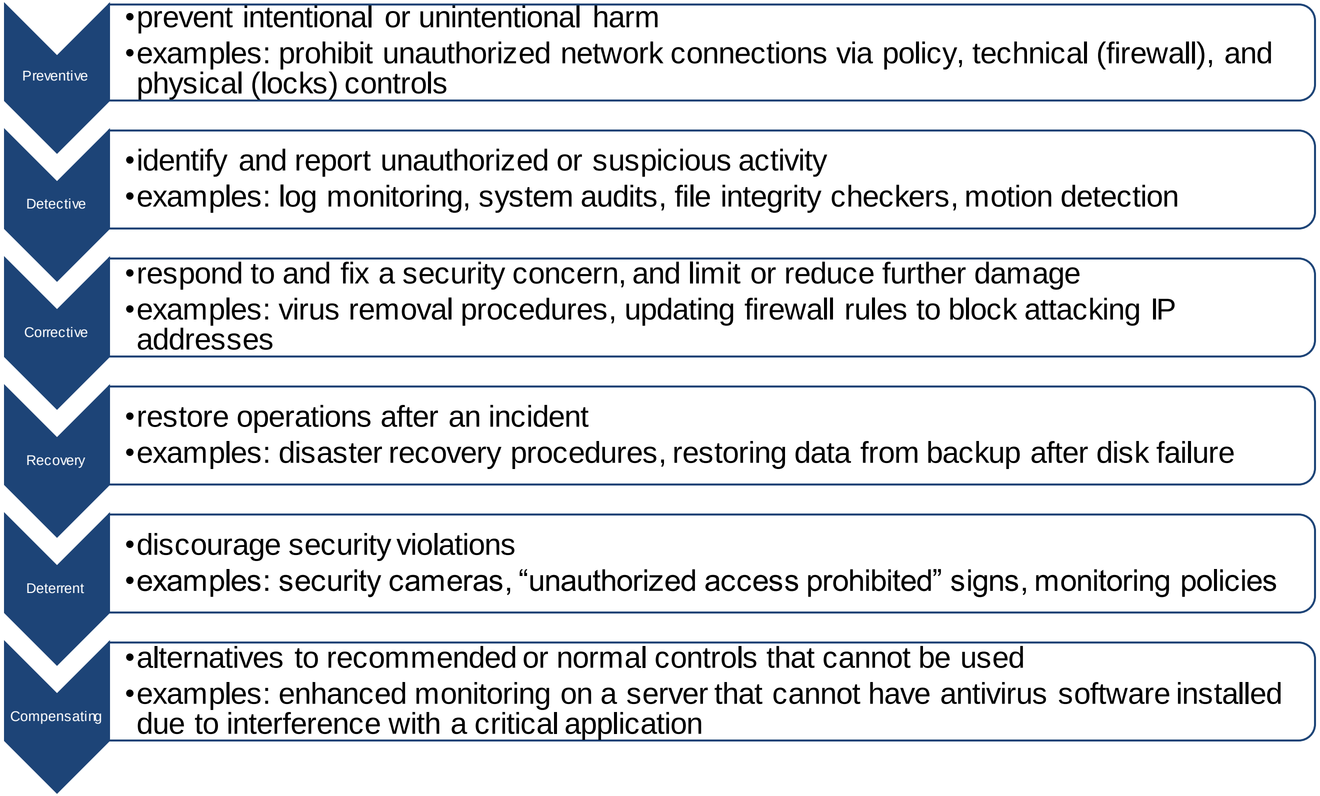


Classes of Cybersecurity Controls

Class	Family
Management	Certification, Accreditation, and Security Assessments
	Planning
	Risk Assessment
	System and Services Acquisition
Operational	Awareness and Training
	Configuration Management
	Contingency Planning
	Incident Response
	Maintenance
	Media Protection
	Personnel Security
	Physical and Environmental Protection
	System and Information Integrity
Technical	Access Control
	Audit and Accountability
	Identification and Authentication
	System and Communications Protection

Source: NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems”

Control Function Categories



Preventive
- prevent intentional or unintentional harm
- examples: prohibit unauthorized network connections via policy, technical (firewall), and physical (locks) controls

Detective
- identify and report unauthorized or suspicious activity
- examples: log monitoring, system audits, file integrity checkers, motion detection

Corrective
- respond to and fix a security concern, and limit or reduce further damage
- examples: virus removal procedures, updating firewall rules to block attacking IP addresses

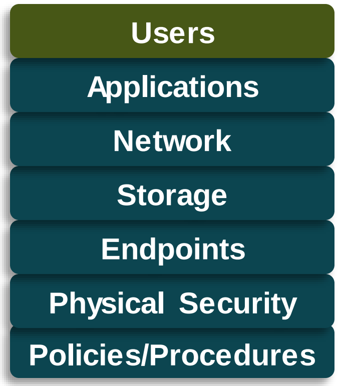
Recovery
- restore operations after an incident
- examples: disaster recovery procedures, restoring data from backup after disk failure

Deterrent
- discourage security violations
- examples: security cameras, “unauthorized access prohibited” signs, monitoring policies

Compensating
- alternatives to recommended or normal controls that cannot be used
- examples: enhanced monitoring on a server that cannot have antivirus software installed due to interference with a critical application

Defense in Depth

There is no cyber "silver bullet." Security must be applied in layers.



- strong passwords, backup and restore strategy
- application hardening
- operating system hardening, authentication, security update management, antivirus updates, auditing
- network segments
- firewalls, virtual private networks
- guards, locks, tracking devices

Cybersecurity Requirements

Cybersecurity Requirements Overview

Federal Information Security Management Act (FISMA)

Federal Acquisition Regulation (FAR)

Defense Federal Acquisition Regulation (DFAR)

Executive Order on Improving the Nation’s Cybersecurity

Standards and Frameworks

NIST Cybersecurity Framework

NIST 800 Series Special Publications

Control Objectives for Information and Related Technologies (COBIT)

ISO 27000 and 31000 Standards Families

CERT Resilience Management Model (RMM)

Common Cybersecurity Roles

Cybersecurity Roles and Responsibilities

Executive Committee

- Provides oversight; sets tone at the top

Senior Management

- Implements effective governance and defines strategic information security objectives
- Sets cultural “acceptance” of information security

Information Security Steering Committee

- Ensures all stakeholders impacted by security considerations are involved

Chief Information Security Officer

- Commonly reports directly to senior management
- Managers who have security responsibilities as their core focus, working with appropriate business/operations personnel

Senior Management Commitment

Senior management should have a commitment to

- Treat cybersecurity as a critical business issue and create a positive environment regarding security
- Demonstrate to third parties that the organization deals with cybersecurity professionally
- Apply fundamental principles such as
  - Assuming ultimate responsibility for cybersecurity
  - Implementing controls that are proportionate to risk
  - Achieving accountability

Information Security Steering Committee

Used to ensure that all stakeholders impacted by security considerations are involved

Normally comprised of senior representatives of affected groups

- Facilitates achieving consensus on priorities and tradeoffs
- Serves as an effective communications channel
- Ensures alignment of the security program with business objectives
- Is instrumental in achieving modification of organizational behavior toward a conducive security culture

Chief Information Security Officer

CISO or equivalent executive position

- Ensures security risks are appropriately communicated to executive management
- Establishes and manages a budget to conduct all infosec activities
- Ensures appropriate and timely development of security policies, procedures, baselines, standards, and guidelines
- Develops and provides a security awareness training program
- Ensures compliance with applicable regulations
- Remains current on emerging technologies and threats

Business and Operations Personnel

- Are critical in implementing business operations that meet security needs as well as identifying, escalating security incidents, and handling other concerns
- Must recognize and meet their responsibilities in ensuring day-to-day operational security
- Should be represented on the information security steering committee

Four Key Functions of CISO Responsibilities

Protect, shield, defend, and prevent: Ensure that the organization's staff, policies, processes, practices, and technologies proactively protect, shield, and defend the enterprise from cyber threats, and **prevent the occurrence and recurrence of cybersecurity incidents** commensurate with the organization's risk tolerance.

Monitor, detect, and hunt: Ensure that the organization's staff, policies, processes, practices, and technologies **monitor ongoing operations and actively hunt for and detect adversaries;** report instances of suspicious and unauthorized events as expeditiously as possible.

Respond, recover, and sustain: When a cybersecurity incident occurs, minimize its impact and ensure that the organization's staff, policies, processes, practices, and technologies are rapidly deployed to **return assets to normal operations as soon as possible**. Assets include technologies, information, people, facilities, and supply chains.

Govern, manage, comply, educate, and manage risk: Ensure that the organization's leadership, staff, policies, processes, practices, and technologies provide **ongoing oversight, management, performance measurement, and course correction of all cybersecurity activities**. This function includes ensuring compliance with all external and internal requirements and mitigating risk commensurate with the organization's risk tolerance.

Source: Allen, J., Crabb, G., Curtis, P., Fitzpatrick, B., Mehravari, N. and Tobar, D. (2015). *Structuring the Chief Information Security Officer Organization*. [online] Software Engineering Institute - Carnegie Mellon University - CERT Division of Carnegie Mellon's Software Engineering Institute. http://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf

Role of the Human in Cybersecurity

Security Awareness and Training Programs

People, who are all fallible, are usually recognized as one of the weakest links in securing systems.

The purpose of computer security awareness, training, and education is to enhance security by

- improving awareness of the need to protect system resources
- developing skills and knowledge so computer users can perform their jobs more securely
- building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems

Security awareness and training programs may also be required by law.

Employees need to understand the value of the company's information assets.

The State of Information Security Policy Awareness

According to a 2018 Kaspersky survey of over 8,000 full-time employees:

- 12% claimed to be fully aware of their organization’s information security policies.
- 24% of employees indicated that they believe their organization does not have any established security policies.

https://www.techrepublic.com/article/88-of-employees-have-no-clue-about-their-organizations-it-security-policies/

Developing Awareness and Training Program

Security teams should be methodical in developing and implementing the education and awareness program.

Consider various aspects:

- Who is the intended audience?
  - management, business managers, IT staff, users
- What is the intended message?
  - policies, procedures, recent events
- What is the intended result?
  - improved policy compliance, behavioral change, and better practices
- What communication method will be used?
  - computer-based training (CBT), all-hands meeting, intranet, newsletters, etc.
- What is the organizational structure and culture?

Training by “Target”

Training is most effective when it is targeted to a particular group.

Organizations should segment user populations into groups based on threats specific to those groups; for example

- Executives: prevalent use of mobile devices, targets of spear phishing (whaling)
- Administrators; privileged accounts, potential for insider abuse
- End users; heavy Internet usage with no awareness of “dangers”; targets of phishing and social engineering

For maximum effectiveness, build training targeted to each group.

End-User Training

Appropriate employee training can have significant impact in mitigating risks.

End-user training should include

- purpose, explanation, and importance of adhering to security policies/procedures
- clean desk policy
- response to emergencies
- requirements of privacy/confidentiality
- significance of logical access in the IT environment

Training should be initial, periodic, and ongoing, and should include assessments and quality assurance on training and trainers.

In an organization, information systems security is the responsibility of all personnel.

Key Takeaways

- Cybersecurity is NOT a technical or IT issue -> it is an enterprise risk issue
- Threats and technology will change much more rapidly than business strategies
- Executives need to have a solid understanding of cybersecurity principles in order to provide effective oversight

Q&A

Presenter Contact Information

Dan Costa

Technical Manager, Enterprise Threat and Vulnerability Management

CERT Division | Carnegie Mellon University Software Engineering Institute

dlcosta@sei.cmu.edu

www.sei.cmu.edu