LECTURE SUMMARY. PLEASE GO THROUGH THE MATERIAL IN THE PRESCRIBED BOOKS FOR THIS LESSON.

2023/02/22

1

Agenda

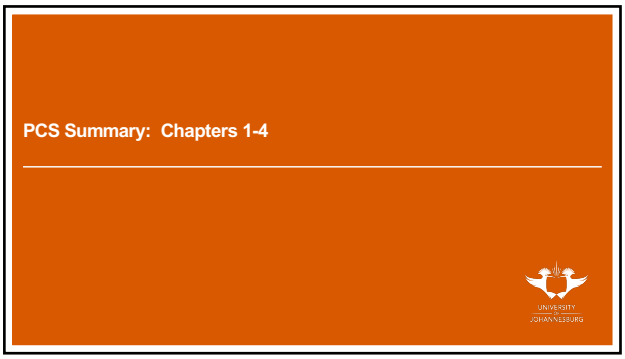
Outcome: Examine why critical infrastructure attacks are a concern in the current economic and political context

PCS (*Principles of Computer Security: CompTIA Security+ and Beyond (PCS). Sixth Edition.*)
Chapter 1: Introduction and Security Trends
Chapter 2: General Security Concepts
Chapter 3: Operational and Organizational Security
Chapter 4: The Role of People in Security

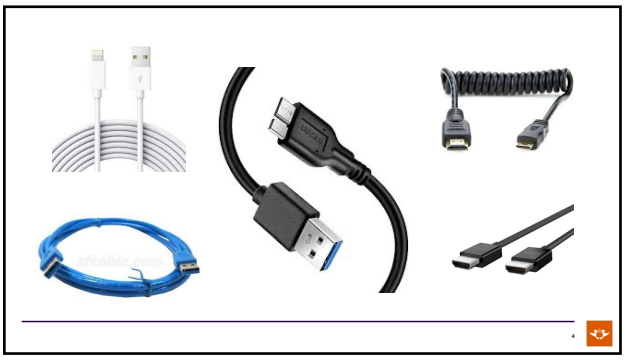
PIR&DR (*Principles of Incident Response & Disaster Recovery*)
Chapter 1: An Overview of Information Security and Risk Management.

Sources: PCS and PIR&DR 2

2



3



4

Threats to Information Security

Category of Threat	Attack Examples
Compromises to intellectual property	Piracy, copyright infringement
Deviations in quality of service	Internet service provider (ISP), power, or WAN service problems
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, floods, earthquakes, lightning
Human error or failure	Accidents, employee mistakes
Information extortion	Blackmail, information disclosure
Sabotage or vandalism	Destruction of systems or information
Software attacks	Viruses, worms, macros, denial of service
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of equipment or information

5

Information Security

- CIA Triad
- Confidentiality
- Integrity
- Availability
- Non-repudiation
- PAIN ?

6

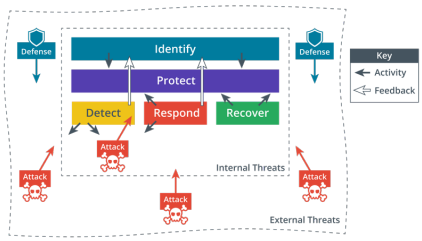
What is Information Security?

- Information security (InfoSec) is the protection of the confidentiality, integrity, and availability of information assets, whether in storage, processing, or transmission, via the application of policy, education, training and awareness, and technology.

7

7

Cyber Security Framework (CSF)



8

8

Information Security Competencies

- Risk *assessments* and testing
- Specifying, sourcing, installing, and *configuring* secure devices and software
- Access control and user privileges
- Auditing logs and events
- Incident reporting and *response*
- Business continuity and disaster recovery
- Security *training* and education programs

9

9

Information Security Roles and Responsibilities

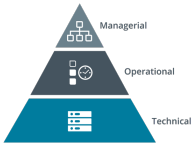
- Overall responsibility
  - Chief Security Officer (CSO)
  - Chief Information Security Officer (CISO)
- Managerial
- Technical
  - Information Systems Security Officer (ISSO)
- Non-technical
- Due care/liability

10

10

Security Control Categories

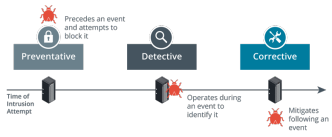
- Technical
  - Controls implemented in operating systems, software, and security appliances
- Operational
  - Controls that depend on a person for implementation
- Managerial
  - Controls that give oversight of the system



11

11

Security Control Functional Types (1)



Other Control Functional Types:

Physical | Compensating | Deterrent

Images © 123rf.com.

12

12

Operational and Org Security

13

Policies, Procedures, Standards and Guidelines

- Policies (high level)
- Procedures (step by step)
- Stds (mandatory elements)
- Guidelines (Recommendations)

See Ch3 for types of HR and other policies and what they are for.

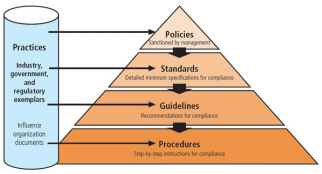


Figure 1-3 Policies, standards, practices, procedures, and guidelines

14

Guidelines for Effective Policy Development and Implementation

- For policies to be effective and legally defensible, they must be properly:
  - Development
  - Distribution
  - Reading
  - Comprehension
  - Compliance
  - Uniform Enforcement

15

NIST Cybersecurity Framework

- Importance of frameworks
  - Objective statement of current capabilities
  - Measure progress towards a target capability
  - Verifiable statement for regulatory compliance reporting
- National Institute of Standards and Technology (NIST)
  - Cybersecurity Framework (CSF)
  - Risk Management Framework (RMF)
  - Federal Information Processing Standards (FIPS)
  - Special Publications

16

16

ISO and Cloud Frameworks

- International Organization for Standardization (ISO)
  - 21 000 information security standards
  - 31 000 enterprise risk management (ERM)
- Cloud Security Alliance
  - Security guidance for cloud service providers (CSPs)
  - Enterprise reference architecture
  - Cloud controls matrix
- Statements on Standards for Attestation Engagements (SSAE) Service Organization Control (SOC)
  - SOC2 evaluates service provider
    - Type I report assesses system design
    - Type II report assesses ongoing effectiveness
  - SOC3 public compliance report

17

17

Benchmarks and Secure Configuration Guides

- Center for Internet Security (CIS)
  - The CIS Critical Security Controls
  - CIS-RAM (Risk Assessment Method)
- OS/network platform/vendor-specific guides and benchmarks
  - Vendor guides and templates
  - CIS benchmarks
  - Department of Defense Cyber Exchange
  - NIST National Checklist Program (NCP)
- Application servers and web server applications
  - Client/server
  - Multi-tier—front-end, middleware (business logic), and back-end (data)
  - Open Web Application Security Project (OWASP)

18

18

Regulations, Standards, and Legislation

- Due diligence
  - Sarbanes-Oxley Act (SOX)
  - Computer Security Act (1987)
  - Federal Information Security Management Act (FISMA)
- General Data Protection Regulation (GDPR)
- National, territory, or state laws
  - Health Insurance Portability and Accountability Act (HIPAA)
  - California Consumer Privacy Act (CCPA)
  - Protection of Personal Information Act (POPIA)
  - Cybercrimes Act of 2020
- Payment Card Industry Data Security Standard (PCI DSS)

19

19

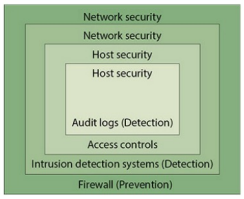
Security Approaches

UNIVERSITY OF JOHANNESBURG

20

Security approach and principles

- Approach
  - Host security
  - Network security
- Principles
  - Least privilege
  - Separation of duties
  - Fail safe defaults
  - Security through obscurity
  - Defense in depth/layered



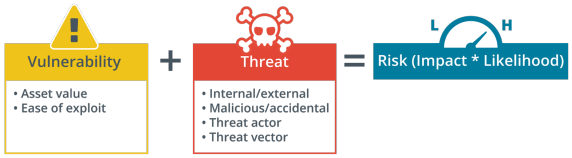
21

21

Explaining Threat Actors and Threat Intelligence

22

Vulnerability, Threat, and Risk



23

Attributes of Threat Actors

- Known threats versus adversary behaviors
- Internal/external
- Intent/motivation
  - Maliciously targeted versus opportunistic
  - Accidental/unintentional
- Level of sophistication
  - Resources /funding
  - Adversary capability levels

24

Hackers, Script Kiddies, and Hacktivists

- The "Lone Hacker"
  - White/Grey/Black hats
  - Authorized versus non-authorized versus semi-authorized
- Script kiddies
- Hacker teams and hacktivists

25

25

State Actors and Advanced Persistent Threats

- State-backed groups
  - Attached to military/secret services
  - Highly sophisticated
- Advanced Persistent Threat (APT)
- Espionage and strategic advantage
- Deniability
- False flag operations

26

26

Criminal Syndicates and Competitors

- Criminal syndicates
  - Operate across legal jurisdictions
  - Motivated by criminal profit
  - Can be very well resourced and funded
- Competitors
  - Cyber espionage
  - Combine with insider threat

27

27

Insider Threat Actors

- Malicious insider threat
  - Has or has had authorized access
  - Employees, contractors, partners
  - Sabotage, financial gain, business advantage
- Unintentional insider threat
  - Weak policies and procedures
  - Weak adherence to policies and procedures
  - Lack of training/security awareness
  - Shadow IT

28

28

Attack Surface and Vectors

- Attack surface
  - Points where an attacker can discover/exploit vulnerabilities in a network or application
- Vectors
  - Direct access
  - Removable media
  - Email
  - Remote and wireless
  - Supply chain
  - Web and social media
  - Cloud

29

29

Threat Research Sources

- Counterintelligence
- Tactics, techniques, and procedures (TTPs)
- Threat research sources
  - Academic research
  - Analysis of attacks on customer systems
  - Honeypots
  - Dark nets and the dark web

30

30

Tactics, Techniques, and Procedures and Indicators of Compromise

- Tactics, Techniques, and Procedures (TTPs)
  - Generalized statement of adversary behaviour
  - Campaign strategy and approach (tactics)
  - Generalized attack vectors (techniques)
  - Specific intrusion tools and methods (procedures)
- Indicator of compromise (IoC)
  - Specific evidence of intrusion
  - Individual data points
  - Correlation of system and threat data
  - AI-backed analysis
  - Indicator of attack (IoA)

31

31

Threat Intelligence Providers

- Narrative analysis and commentary
- Reputation/threat data feeds—cyber threat intelligence (CTI)
- Platforms and feeds
  - Closed/proprietary
  - Vendor websites
  - Public/private information sharing centres
  - Open source intelligence (OSINT) threat data sources
- OSINT as reconnaissance and monitoring

32

32

Other Threat Intelligence Research Sources

- Academic journals
- Conferences
- Request for Comments (RFC)
- Social media

33

33

Threat Data Feeds

- Structured Threat Information exchange (STIX)
- Trusted Automated Exchange of Indicator Information (TAXII)
- Automated Indicator Sharing (AIS)
- Threat maps
- File/code repositories
- Vulnerability databases and feeds

34

34

Artificial Intelligence and Predictive Analysis

- Correlation between security intelligence/event monitoring and threat data
- Artificial intelligence (AI) and machine learning (ML)
  - Expert systems
  - Artificial neural networks (ANN)
    - Inputs, outputs, and feedback
    - Objectives and error states
- Predictive analysis
  - Threat forecasting
  - Monitor "chatter"

35

35

People - A Security Problem

36

Social Engineering

- "Hacking the human"
- Purposes of social engineering
  - Reconnaissance and eliciting information
  - Intrusion and gaining unauthorized access
- Many possible scenarios
  - Persuade a user to run a malicious file
  - Contact a help desk and solicit information
  - Gain access to premises and install a monitoring device

37

37

Social Engineering Principles

- Reasons for effectiveness
- Familiarity/liking
  - Establish trust
  - Make request seem reasonable and natural
- Consensus/social proof
  - Exploit polite behaviours
  - Establish spoofed testimonials or contacts
- Authority and intimidation
  - Make the target afraid to refuse
  - Exploit lack of knowledge or awareness
- Scarcity and urgency
  - Rush the target into a decision

38

38

Dumpster Diving and Tailgating

- Dumpster diving
- Tailgating
- Piggy backing

39

39

Identity Fraud and Invoice Scams

- Identity fraud
  - Impersonation with convincing detail and stolen or spoofed proofs
  - Identity fraud versus identity theft
- Invoice scams
  - Spoofing supplier details to submit invoices with false account details
- Credential theft and misuse
  - Credential harvesting
  - Shoulder surfing
  - Lunchtime attack

40

40

Phishing, Whaling, and Vishing

- Trick target into using a malicious resource
- Spoof legitimate communications and sites
- Spear phishing
  - Highly targeted/tailored attack
- Whaling
  - Targeting senior management
- Vishing
  - Using a voice channel
- SMiShing
  - Using text messaging

41

41

Spam, Hoaxes, and Prepending

- Spam
  - Unsolicited email
  - Email address harvesting
  - Spam over Internet messaging (SPIM)
- Hoaxes
  - Delivered as spam or malvertising
  - Fake A-V to get user to install remote desktop software
  - Phone-based scams
- Prepending
  - Tagging email subject line
  - Can be used by threat actor as a consensus or urgency technique
  - Can be added by mail systems to warn users

42

42

Social Engineering Techniques

43

Malware Classification

- Classification by vector or infection method
- Viruses and worms
  - Spread within code without authorization
- Trojans
  - A malicious program concealed within a benign one
- Potentially unwanted programs/applications (PUPs/PAPs)
  - Pre-installed "bloatware" or installed alongside another app
  - Not completely concealed, but installation may be covert
  - Also called grayware
- Classification by payload

44

Computer Viruses

- Rely on some sort of host file or media
  - Non-resident/file infector
  - Memory resident
  - Boot
  - Script/macro
- Multipartite
- Polymorphic
- Vector for delivery

45

Computer Worms and Fileless Malware

- Early computer worms
  - Propagate in memory/over network links
  - Consume bandwidth and crash process
- Fileless malware
  - Exploiting remote execution and memory residence to deliver payloads
  - May run from an initial script or Trojan
  - Persistence via the registry
  - Use of shellcode to create backdoors and download additional tools
  - "Living off the land" exploitation of built-in scripting tools
- Advanced persistent threat (APT)/advanced volatile threat (AVT)/ low observable characteristics (LOC)

46

46

Spyware, Adware, and Keyloggers

- Tracking cookies
- Adware (PUP/grayware)
  - Changes to browser settings
- Spyware (malware)
  - Log all local activity
  - Use of recording devices and screenshots
  - Redirection
- Keylogger
  - Software and hardware

47

47

Rootkits

- Local administrator versus SYSTEM/root privileges
- Replace key system files and utilities
- Purge log files
- Firmware rootkits

48

48

Ransomware, Crypto-Malware, and Logic Bombs

- Ransomware
  - Nuisance (lock out user by replacing shell)
- Crypto-malware
  - High impact ransomware (encrypt data files or drives)
- Cryptomining/crypojacking
  - Hijack resources to mine cryptocurrency
- Logic bombs

49

49

Risk Management

50

Definition

- **Risk management** is the process of identifying vulnerabilities in an organization's information systems and taking carefully reasoned steps to ensure the confidentiality, integrity, and availability of all the systems' components.
- Risk management involves discovering and understanding answers to some key questions with regard to the risk associated with an organization's information assets:
  - Where and what is the risk (risk identification)?
  - How severe is the current level of risk (risk analysis)?
  - Is the current level of risk acceptable (risk evaluation)?
  - What do I need to do to bring the risk to an acceptable level (risk treatment)?

51

51

Components of Risk Management

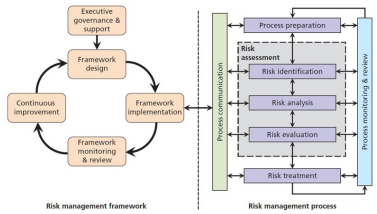


Figure 1-4 The risk management framework and process

52

52

53