

# Contents

<b>1</b>	<b>Chapter 1 - Security and Risk Management</b>	<b>6</b>
1.1	Fundamental Principles of Security . . . . .	6
1.1.1	AIC Triad: . . . . .	6
1.1.2	Risk Definitions: . . . . .	6
1.1.3	Control Types: . . . . .	7
1.1.4	Defense in Depth - layered . . . . .	7
1.1.5	Control Functionalities: . . . . .	7
1.2	Security Frameworks . . . . .	7
1.2.1	Security Program Development: . . . . .	7
1.2.2	Enterprise Architecture Development: . . . . .	8
1.2.3	Security Controls Development: . . . . .	8
1.2.4	Process Management Development: . . . . .	9
1.2.5	Security Program Lifecycle . . . . .	10
1.2.6	Functionality vs. Security . . . . .	10
1.3	Crime Laws . . . . .	10
1.3.1	Computer-assisted - crime could take place even without a computer . . . . .	10
1.3.2	Computer-targeted - crime could not take place . . . . .	10
1.3.3	Computer is incidental - computer just happened to be involved . . . . .	10
1.4	Complexities: . . . . .	10
1.4.1	Evolution of attacks . . . . .	10
1.4.2	International issues . . . . .	11
1.4.3	Types of Legal Systems . . . . .	12
1.5	Intellectual Property . . . . .	12
1.5.1	International Protection of Intellectual Property . . . . .	13
1.5.2	Software Piracy . . . . .	14
1.6	Privacy . . . . .	14
1.6.1	Definitions . . . . .	14
1.6.2	Increasing Need for Privacy Laws . . . . .	15
1.6.3	Laws, Directives and Regulations . . . . .	15
1.6.4	Employee Privacy Issues . . . . .	17
1.6.5	Additional Material . . . . .	17
1.7	Data Breaches . . . . .	18
1.7.1	Verizon Data Breach Report: <a href="http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/">http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/</a> . . . . .	18
1.7.2	Reporting . . . . .	18
1.7.3	US Laws pertaining to data breaches . . . . .	18

1.7.4	Other Nation's Laws . . . . .	18
1.8	Policies, Standards, Baselines, Guidelines and Procedures . .	19
1.8.1	Policy - high level of requirement - typically should have a 3-5 year life . . . . .	19
1.8.2	Standards . . . . .	19
1.8.3	Baselines . . . . .	19
1.8.4	Guidelines . . . . .	19
1.8.5	Procedures . . . . .	20
1.8.6	Implementation . . . . .	20
1.9	Risk Management . . . . .	20
1.9.1	InfoSec risk types . . . . .	20
1.9.2	Risk Assessment Additional Readings: . . . . .	20
1.9.3	Holistic . . . . .	21
1.9.4	Process . . . . .	22
1.9.5	Threat Modeling . . . . .	22
1.9.6	Vulnerabilities . . . . .	22
1.9.7	Information . . . . .	22
1.9.8	Processes . . . . .	22
1.9.9	People . . . . .	22
1.9.10	Threats . . . . .	23
1.9.11	Attacks . . . . .	23
1.9.12	Reduction Analysis . . . . .	23
1.10	Risk Assessment and Analysis . . . . .	23
1.10.1	Identifying risks . . . . .	23
1.10.2	Generic process (NIST) . . . . .	23
1.10.3	Facilitated Risk Analysis Process (FRAP) . . . . .	24
1.10.4	OCTAVE . . . . .	24
1.10.5	AS/NZS 4360 . . . . .	24
1.10.6	ISO/IEC 27005 . . . . .	24
1.10.7	Failure Modes and Effect Analysis (FMEA) . . . . .	24
1.10.8	Fault tree analysis . . . . .	24
1.10.9	Central Computing and Teecmmunications Agency Risk Analysis and Management Method (CRAMM) . . . .	24
1.10.10	Difference: . . . . .	25
1.10.11	Approaches . . . . .	25
1.10.12	Quantitative . . . . .	25
1.10.13	Qualitative . . . . .	25
1.10.14	Control Selection . . . . .	25
1.10.15	Risk terms: . . . . .	25
1.10.16	Handling Risk: . . . . .	26

1.10.17	Outsourcing . . . . .	26
1.11	Risk Management Frameworks . . . . .	26
1.11.1	Categorize Information Systems . . . . .	26
1.11.2	Select Security Controls . . . . .	27
1.11.3	Implement Security Controls . . . . .	27
1.11.4	Assess Security Controls . . . . .	27
1.11.5	Authorize Information Systems . . . . .	27
1.11.6	Monitor Security Controls . . . . .	27
1.12	Business Continuity and Disaster Recovery . . . . .	28
1.12.1	Standards and Best Practices . . . . .	28
1.12.2	Making BCM Part of teh Enterprise Security Program	29
1.12.3	BCP Project Components . . . . .	30
1.12.4	Scope of the Project . . . . .	30
1.12.5	BCP Policy . . . . .	30
1.12.6	Project Management . . . . .	31
1.12.7	BCP Requirements . . . . .	31
1.12.8	Business Impact Analysis . . . . .	31
1.12.9	Interdependencies . . . . .	32
1.13	Personnel Security . . . . .	32
1.13.1	Hiring Practices . . . . .	33
1.13.2	Termination . . . . .	33
1.13.3	Security-Awareness Training . . . . .	33
1.13.4	Degree or Certification? . . . . .	33
1.14	Security Governance . . . . .	33
1.14.1	Metrics . . . . .	33
1.15	Ethics . . . . .	34
1.15.1	The Computer Ethics Institute . . . . .	34
1.15.2	The Internet Architecture Board . . . . .	35
1.15.3	Corporate Ethics Programs . . . . .	35
<b>2</b>	<b>Chapter 2 - Asset Security</b>	<b>35</b>
2.1	Information Life Cycle . . . . .	35
2.1.1	Acquisition . . . . .	35
2.1.2	Used . . . . .	35
2.1.3	Archival . . . . .	36
2.1.4	Disposal . . . . .	36
2.2	Information Classification . . . . .	36
2.2.1	Classifications Levels . . . . .	36
2.2.2	Classifications Controls . . . . .	37
2.3	Layers of Responsibility . . . . .	37

2.3.1	Executive Management . . . . .	37
2.3.2	Data Owner . . . . .	37
2.3.3	Data Custodian . . . . .	37
2.3.4	System Owner . . . . .	38
2.3.5	Security Administrator . . . . .	38
2.3.6	Supervisor . . . . .	38
2.3.7	Change Control Analyst . . . . .	38
2.3.8	Data Analyst . . . . .	38
2.3.9	User . . . . .	38
2.3.10	Auditor . . . . .	38
2.3.11	Why so many roles? . . . . .	38
2.4	Retention Policies . . . . .	38
2.4.1	Developing a Retention Policy . . . . .	38
2.5	Protecting Privacy . . . . .	39
2.5.1	Data Owners . . . . .	39
2.5.2	Data Processors . . . . .	39
2.5.3	Data Remanence . . . . .	39
2.5.4	Limits on Collection . . . . .	40
2.6	Protecting Assets . . . . .	40
2.6.1	Data Security Controls . . . . .	40
2.6.2	Media Controls . . . . .	41
2.7	Data Leakage . . . . .	41
2.7.1	Data Leakage Prevention . . . . .	41
2.8	Protecting Other Assets . . . . .	42
2.8.1	Protecting Mobile Devices . . . . .	42
2.8.2	Paper Records . . . . .	42
2.8.3	Safes . . . . .	42
<b>3</b>	<b>Chapter 3 - Security Engineering</b>	<b>43</b>
3.1	System Architecture . . . . .	43
3.1.1	ISO/IEC 42010:2011 - System Architecture Standard. Establishes a shared vocabulary . . . . .	43
3.2	Computer Architecture . . . . .	43
3.2.1	The Central Processing Unit . . . . .	44
3.2.2	Multiprocessing . . . . .	44
3.2.3	Memory Types . . . . .	44
3.2.4	Buffer Overflow Resources . . . . .	45
3.2.5	Memory Protection Techniques . . . . .	46
3.2.6	Memory Leaks . . . . .	46
3.3	Operating Systems . . . . .	46

3.3.1	Process Management . . . . .	46
3.3.2	Memory Management . . . . .	47
3.3.3	Input/Output Device Management . . . . .	48
3.3.4	CPU Architecture Integration . . . . .	48
3.3.5	Operating System Architectures . . . . .	48
3.3.6	Virtual Machines . . . . .	49
3.4	System Security Architecture . . . . .	49
3.4.1	Security Policy . . . . .	49
3.4.2	Security Architecture Requirements . . . . .	49
3.5	Security Models . . . . .	50
3.5.1	Bell-LaPadula Model . . . . .	50
3.5.2	Biba Model . . . . .	50
3.5.3	Clark-Wilson Model . . . . .	50
3.5.4	Noninterference Model . . . . .	51
3.5.5	Brew and Nash Model . . . . .	51
3.5.6	Graham-Denning Model . . . . .	51
3.5.7	Harrison-Ruzzo-Ullman Model . . . . .	51
3.6	Systems Evaluation . . . . .	52
3.6.1	Common Criteria . . . . .	52
3.6.2	Why Put a Product Through Evaluation? . . . . .	52
3.7	Certification vs. Accreditation . . . . .	53
3.7.1	Certification . . . . .	53
3.7.2	Accreditation . . . . .	53
3.8	Open vs. Closed Systems . . . . .	53
3.8.1	Open Systems . . . . .	53
3.8.2	Closed Systems . . . . .	53
3.9	Distributed System Security . . . . .	53
3.9.1	Cloud Computing . . . . .	53
3.9.2	Parallel Computing . . . . .	54
3.9.3	Databases . . . . .	54
3.9.4	Web Applications . . . . .	54
3.9.5	Mobile Devices . . . . .	55
3.9.6	Cyber-Physical Systems . . . . .	55
3.10	A Few Threats to Review . . . . .	56
3.10.1	Maintenance Hooks . . . . .	56
3.10.2	Time-of-Check/Time-of-Use Attacks . . . . .	56
3.11	Cryptography in Context . . . . .	56
3.11.1	The History of Cryptography . . . . .	56
3.12	Cryptography Definitions and Concepts . . . . .	56
3.12.1	Kerckhoffs' Principle . . . . .	56

3.12.2	The Strength of the Cryptosystem . . . . .	56
3.12.3	Services of Cryptosystems . . . . .	57
3.12.4	One-Time Pad . . . . .	57
3.12.5	Running and Concealment Ciphers . . . . .	57
3.12.6	Steganography . . . . .	57
3.13	Types of Ciphers . . . . .	57
3.13.1	Substitution Ciphers . . . . .	57
3.13.2	Transposition Ciphers . . . . .	58
3.14	Methods of Encryption . . . . .	58
3.14.1	Symmetric vs. Asymmetric Algorithms . . . . .	58
3.14.2	Symmetric Cryptography . . . . .	58
3.14.3	Asymmetric Cryptography . . . . .	58
3.14.4	Block and Stream Ciphers . . . . .	59
3.14.5	Hybrid Encryption Methods . . . . .	59

# 1 Chapter 1 - Security and Risk Management

## 1.1 Fundamental Principles of Security

### 1.1.1 AIC Triad:

1. Availability - reliable and timely access Controls: eg. RAIDs, clustering, load balancing, redundancy, backups, secondary facilities, rollback, failover
2. Integrity - assurance of accuracy and reliability Controls: eg. Hashing, Configuration Mgmt., Change controls, Access controls, Software digital signing, CRC checks
3. Confidentiality - necessary level of secrecy Controls: eg. Encryption, Access controls

### 1.1.2 Risk Definitions:

**Vulnerability** weakness in a system

**threat** potential danger

**risk** likelihood of threat source exploiting a vulnerability X the business impact

**exposure** an instance of being exposed to losses

**control** countermeasure, safeguard, to mitigate risk

### 1.1.3 Control Types:

**Administrative** security documentation, risk management, training

**Technical** logical controls, software, hardware, firewalls, IDS, encryption

**Physical** guards, locks, fencing, lighting

### 1.1.4 Defense in Depth - layered

- We use a slide to represent this concept across all control types

### 1.1.5 Control Functionalities:

**Preventative** avoid incident

**Detective** Identify an incident

**Corrective** Fix

**Deterrent** Discourage an attack

**Recovery** Bring back to regular operations

**Compensating** Provide an alternative measure of control

1. Note that NIST CSF is closely organized along these lines, although slightly different
2. There is significant argument as to where companies should focus: preventative, or detective and recovery?
  - You should be able to voice when one approach is better than another.
  - See Table 1-1 for Control Types X Control Functionalities

## 1.2 Security Frameworks

### 1.2.1 Security Program Development:

- ISO/IEC 27000 series – Understand history and how series docs are related

### 1.2.2 Enterprise Architecture Development:

- Zachman Framework - enterprise architecture
- TOGAF - Open Group - enterprise architecture - probably the most relevant to large corporations
- DoDAF - US military
- MODAF - British MoD
- SABSA - security architecture focus

1. An architecture is a set of different organizational views (Figure 1-4)
2. An ISMS is implemented through a Security Architecture - it helps prevent the issues listed in this section
  - our risk framework is a version of a security architecture. Compared risk framework to Table 1-3.
  - "The architecture is a tool used to ensure that what is outlined in security standards is implemented throughout the different layers of an organization" - this is where the applicability matrix start to come into play.

3. Successful security architecture requires:

**Strategic alignment** business drivers, regulatory and legal requirements are being meta

**Business enablement** security supports business, risk is necessary

**Process Enhancement** security tools can offer the opportunity to automate and streamline processes

**Security Effectiveness** metrics, SLA, ROI

### 1.2.3 Security Controls Development:

1. COBIT 5 - IT Management Framework - ISACA
  - Focuses on optimizing Value of IT - beyond just security
  - Key feature is a separation of governance from management, and goal breakdown
  - Goals: 17 enterprise and 17 IT-related goals (clearly very generic to apply to all companies)



- COBIT introduced the concept of "control objectives", "controls", and "control tests".
- COBIT 5 got rid of "controls objectives".
- The Audit industry is largely based off COBIT.

## 2. NIST SP 800-53 - NIST controls

- NIST lives in the Dept. of Commerce
- FISMA (Federal Information Security Management Action) requires agencies to follow NIST

## 3. COSO Internal Control-Integrated Framework - financial fraud focus

- COBIT came from COSO
- Used for Corporate Governance (whereas COBIT is IT governance)
- SOX (2002) is based on COSO, thus following COSO can ensure compliance with SOX

### 1.2.4 Process Management Development:

#### 1. ITIL - IT processes - UK origin

- IT service management
- Focused on internal SLAs between IT and the Business

#### 2. Six Sigma

- Based on Total Quality Management (TQM)
- All about operation efficiency, reducing variation, defects, waste (very manufacturing oriented)

#### 3. Capability Maturity Model Integration (CMMI)

- Carnegie Mellon
- Started the idea of processes maturity levels (that are now starting to fade in popularity)
- This model is still heavily influential (FFIEC and NIST assessment tools both have resemblances to it)
- Also, it mimics how infosec is slowly improved each year

### **1.2.5 Security Program Lifecycle**

1. Plan and Organized
  2. Implement
  3. Operate and Maintain
  4. Monitor and Evaluate
- Notice Figure 1-8 is closely aligned with our model

### **1.2.6 Functionality vs. Security**

## **1.3 Crime Laws**

### **1.3.1 Computer-assisted - crime could take place even without a computer**

### **1.3.2 Computer-targeted - crime could not take place**

### **1.3.3 Computer is incidental - computer just happened to be involved**

## **1.4 Complexities:**

- Hard to ID attackers
- Lack of reporting

### **1.4.1 Evolution of attacks**

- Today is much more profit driven
- See Verizon Breach report for 2016
- Types:
  - Script Kiddies
  - APT - nation state

### 1.4.2 International issues

1. Council of Europe Convention on CyberCrime – First attempt to create an international response standards
2. OECD - Guidelines on the Protection of Privacy and Transborder Flows of Personal Data The are very similar to privacy principles
  - Collection Limitation
  - Data Quality
  - Purpose Specification
  - Use Limitation
  - Openness
  - Individual Participation
  - Accountability
3. EU Data Protection Directive - strict EU rules on privacy
  - US-based companies used to use Safe Harbor Privacy Principles
  - This has since been renegotiated
  - Safe Harbor Principles:
    - Notice
    - Choice
    - Onward Transfer
    - Security
    - Data Integrity
    - Access
    - Enforcement
  - Privacy shield Replaces Safe Harbor <https://www.privacyshield.gov/Program-Overview>
4. Import Export Requirements
  - Wassenaar Arrangement - export controls restricting arms and dual-use goods exporting to certain controls
    - Cryptography can fall into a controlled export
  - China, Russia, Iran, Iraq, etc. have crypto import controls to prevent citizen use

\*

### 1.4.3 Types of Legal Systems

#### 1. Civil (Code) Law System

- France, Spain
- Rule based, non precedent based
- Most common around world and in Europe
- Lower courts not compelled to following decisions made by higher courts

#### 2. Common Law System

- Developed in England, US uses
- Uses precedent
- Criminal, civil/tortured, administrative
- Civil - wrongs against individual or company resulting in damage or loss. Jury decides "liability", not innocence or guilt. Typically derived from common law, case law.
- Criminal - conduct violates government laws. Jail, fines. Derived from statutes.
- Administrative/regulatory law - deals with regulatory standards.

#### 3. Customary Law Systems

- Personal conduct and behavior
- Based on traditions and customs
- Used in mixed legal systems (China, India)

#### 4. Religious Law Systems

### 1.5 Intellectual Property

- Companies must implement safeguards to protect IP, show that it exercised due care.
- Trade Secret
  - Resource must provide the company with some type of competitive value or advantage
  - Proprietary

- NDA - promise not to share trade secrets. This gives company right to fire, and bring charges.
- Copyright
  - Gives right to control distribution, reproduction display and adaptation of original work.
  - It protects the expression of a resource, not the resource itself
  - Copyright is weaker than a patent
  - Copyright is much longer (life plus 50 years)
- Trademark
  - Used to protect a word, name, symbol, sound, shape, color, or combination.
  - Used to protect Brand.
  - International trademark law overseen by World Intellectual Property Organization (WIPO), part of the UN
- Patent
  - Grants legal ownership and ability to exclude others from using or copying an invention
  - Invention must be novel, useful and not obvious
  - Usually a 20 year period
  - Strongest form of protection
  - Large amount of patent litigation - main reason is Nonpracticing Entities (NPEs) or patent trolls.

### **1.5.1 International Protection of Intellectual Property**

- Resources protected by law should be part of data classification scheme, and properly protected with access controls
- Failure to protect could mean the data is not protected by law because it failed to practice due care.

### 1.5.2 Software Piracy

1. Types of licencing
  - Freeware
  - Shareware
  - Commercial
  - Academic
2. EULA more granular than Master
3. Master Agreement
4. International
  - Not a crime everywhere
  - Federation Against Software Theft (FAST) and the Business Software Alliance promote enforcement of proprietary rights of software
5. Security Implications
  - Common offense is to reverse engineer code. But this is necessary for discover security flaws.
  - Can be prosecuted for reverse engineering code under Digital Millennium Copyright Act (DMCA)
  - DMCA - criminalizes production and dissemination of technology that circumvents access control measures.
  - EU has similar law called Copyright Directive

## 1.6 Privacy

### 1.6.1 Definitions

**Personally Identifiable Information** data that can be used to uniquely identify, contact or locate a single person or can be used with other sources to uniquely identify a single individual. Commonly used in identity theft, financial crimes.

- This commonly includes:
  - Full Name

- National Identification Number
- IP address (in some cases)
- Vehicle registration plate number
- Driver’s license number
- Face, fingerprints, or handwriting
- Credit card numbers
- Digital identity
- Birthday
- Birthplace
- Genetic Information
- Less common - but can be PII as well
  - First or Last name, if common
  - Country, state, or city of residence
  - Age, especially if non-specific
  - Gender or race
  - Name of school, workplace
  - Grades, salary, job position
  - Criminal record

### **1.6.2 Increasing Need for Privacy Laws**

- Data aggregation and retrieval technologies
- Loss of borders / business globalization
- Convergent technologies advancements

### **1.6.3 Laws, Directives and Regulations**

1. Federal Privacy Act of 1974 Restrictions on government maintenance and use of private records (relevant and necessary)
2. Federal Information Security Management Act of 2002 (FISMA)
  - Federal agencies must implement a risk-based program to secure agency data and systems
  - Requires annual reviews and reports to Office of Management and Budget (OMB)
  - Requirements of FISMA:

- Inventory of assets
  - Categorize by risk
  - Security controls
  - Risk assessment
  - System security plan
  - Certification and accreditation
  - Continuous Monitoring
3. Department of Veterans Affairs Information Security Protection Act
    - Only applies to the VA
    - Was already required to comply with FISMA
    - Required additional controls plus report compliance to Congress
  4. Health Insurance Portability and Accountability Act (HIPAA)
    - Storage, use and transmission of medical information
  5. Health Information Technology for Economic and Clinical Health (HITECH) Act
    - 2009
    - Promotes adoption of healthcare technology
    - Strengthen civil and criminal enforcement of HIPAA rules
  6. USA Patriot Act
    - Reduces restrictions on law enforcement searching records - big area for privacy debate here
    - Eases restrictions on foreign intelligence gathering within US
    - Expand ability to regulate financial transactions
    - Expands ability to detain and deport immigrants
    - Expands definition of terrorism
  7. Gramm-Leach-Bliley Act (GLBA)
    - Aka Financial Services Modernization Act (1999)
    - Requires financial institutions to develop privacy notices, right to prohibit sharing, security responsibilities



- Board of Directors responsible, risk management required, employee training, testing, written security policy
- Financial Privacy Rule - customer privacy rights, requires a privacy notice, restrictions on sharing and protecting data
- Safeguards Rule - written security plan
- Pretexting Protection - social engineering safeguards

#### 8. Personal Information Protection and Electronic Documents Act

- PIPEDA
- Canadian Law
- Protection of personal information
- Ensures business protect privacy data
- Standard privacy requirements (Consent, collection, notice, etc.)

#### 9. Payment Card Industry Data Security Standard (PCI DSS)

- All credit cards companys came together to develop
- Applies to any entity that processes, transmits, stores or accepts credit card data
- Minnesota actually enforces PCI via law

#### **1.6.4 Employee Privacy Issues**

- Must make employees aware of monitoring
- Monitoring must be work related and consistent
- Notice typically needs to be signed: Waiver of reasonable expectation of privacy (REP)
- Typically cannot fire an employee if they did not violate written policy

#### **1.6.5 Additional Material**

- Great resource for Privacy background: [https://my.iapp.org/NC\\_Product?id=a191a00000Pa8iAAC](https://my.iapp.org/NC_Product?id=a191a00000Pa8iAAC)

## 1.7 Data Breaches

### 1.7.1 Verizon Data Breach Report: <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/>

### 1.7.2 Reporting

- Each state has breach reporting laws - in library
- So does FISMA

### 1.7.3 US Laws pertaining to data breaches

- HIPAA - no reporting requirements (but corrected by HITECH)
- HITECH - HHS must publish annual guidance, companies that comply are not required to report. Otherwise a 60 day reporting requirement
- GLBA - only if misuse has occurred or reasonably likely to occur
- Economic Espionage Act of 1996 - Enables the FBI to investigate industrial and corporate espionage cases. This act focuses on IP.
- State Laws -
  - PII definition: First and Last name with any of the following: SSN, DL Num, Credit/Debit Card Number with security code or PIN
  - Significant variation - some just access requires notification, others use the misuse language of GLBA

### 1.7.4 Other Nation's Laws

#### 1. EU

- EU Data Protection Regulation - standardizes data breach laws
- Privacy very top down directed in EU
- 24 hour notification requirement

#### 2. Other

- 12 countries have no notification requirements: Argentina, Brazil, Chile, China, Colombia, Hong Kong, India, Israel, Malaysia, Peru, Russia, Singapore

## **1.8 Policies, Standards, Baselines, Guidelines and Procedures**

### **1.8.1 Policy - high level of requirement - typically should have a 3-5 year life**

- Advisory and Informative policies are rare - typically called Guidelines not Policy.
- Strategic
- Example: Confidential Information Must be Protected

### **1.8.2 Standards**

- mandatory
- tactical
- lower level - typically revised yearly
- also typically approved at a lower level
- See Figure 1-13
- Example: Customer PII must be encrypted with AES while stored, IPSec with transmitted

### **1.8.3 Baselines**

- NIST and ISO typically define Baseline as system configuration standards (eg. Windows 10 desktop baseline)
- Be aware is can have a broader meaning to measure progress in an organization

### **1.8.4 Guidelines**

- non mandatory

### **1.8.5 Procedures**

- The Step-by-Step tasks (eg. How to install a desktop image for a new user)
- may or may not be mandatory
- Example: How to implement AES and IPSec Technologies

### **1.8.6 Implementation**

- To be effective they must follow a life cycle
- Communicated and Trained, Tested, Reviewed and Updated

## **1.9 Risk Management**

### **1.9.1 InfoSec risk types**


- Physical damage
- Human interaction
- Equipment malfunction
- Inside and outside attacks
- Misuse of data
- Loss of data
- Application error

### **1.9.2 Risk Assessment Additional Readings:**

- FFIEC Risk Assessment Approach (<http://ithandbook.ffiec.gov/it-booklets/management/iii-it-risk-management.aspx>)
- NIST Risk Assessment Approach (<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>)
- FAIR ([https://en.wikipedia.org/wiki/Factor\\_analysis\\_of\\_information\\_risk](https://en.wikipedia.org/wiki/Factor_analysis_of_information_risk))
- Octave Allegro ([http://resources.sei.cmu.edu/asset\\_files/TechnicalReport/2007\\_005\\_001\\_14885.pdf](http://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf))

### 1.9.3 Holistic

- Integrated Risk Management looks at all risk
1. Integrated Risk Management The Gartner reframe of Governance, Risk and Compliance
    - Operational Risk Management (ORM)
    - IT Risk Management (ITRM)
    - IT Vendor Risk Management (VRM)
    - Business Continuity Management Planning (BCMP)
    - Audit Management (AM)
    - Corporate Compliance and Oversight (CCO)
    - Enterprise Legal Management (ELM)
  2. From High Risk, Low Risk to Good Risk, Bad Risk



images/From High Risk, Low Risk to Good Risk, Bad Risk/Screen Shot 2017-01-13

### 3. Gartner Articles

Note: those topics are typically too low detail to actually go in a policy.

#### **1.9.4 Process**

- NIST 800-39
- (a) Frame risk - define the context
- (b) Assess risk - set the likelihood and impact scales for each risk identified
- (c) Respond to risk - accept, mitigate, transfer - explicit decision required
- (d) Monitor risk - monitor control effectiveness

#### **1.9.5 Threat Modeling**

- See threat modeling spreadsheet as a simple approach

#### **1.9.6 Vulnerabilities**

#### **1.9.7 Information**

- Data at rest
- Data in motion
- Data in use - race conditions

#### **1.9.8 Processes**

#### **1.9.9 People**

- Social Engineering
- Social networks
- Passwords!

### **1.9.10 Threats**

### **1.9.11 Attacks**

- Attackers think in graphs, security personnel think in checklists
- Figure 1-14 - an attack tree
- Attack kill chain: [https://en.wikipedia.org/wiki/Kill\\_chain](https://en.wikipedia.org/wiki/Kill_chain)

### **1.9.12 Reduction Analysis**

- Vulnerability - Threat - Attack triad can be risk assessed
- Ideally have a control for each node in the attack tree
- Controls at the root of the tree will defend against a broader array of attack triads
- 

## **1.10 Risk Assessment and Analysis**

### **1.10.1 Identifying risks**

- simple approach: Asset at Risk X Threat Community X Threat Type X Effect

### **1.10.2 Generic process (NIST)**

- (a) Prepare for the assessment
- (b) Conduct the assessment
  - i. Identify threat sources and events
  - ii. Identify vulnerabilities and predisposing conditions
  - iii. Determine likelihood of occurrence
  - iv. Determine magnitude of impact
  - v. Determine risk
- (c) Communicate results
- (d) Maintain assessment

### **1.10.3 Facilitated Risk Analysis Process (FRAP)**

- Qualitative, member experience driven
- No annual loss expectancy values or probability numbers
- Small scope - single system

### **1.10.4 OCTAVE**

- use facilitated workshops
- self-directed team approach
- Much wider scope of FRAP

### **1.10.5 AS/NZS 4360**

- Australia and New Zealand
- Very broad risk approach

### **1.10.6 ISO/IEC 27005**

- International risk management standard
- Deals with IT and softer security issues (documentation, personnel security, training, etc)

### **1.10.7 Failure Modes and Effect Analysis (FMEA)**

- product development
- Failure of products or software

### **1.10.8 Fault tree analysis**

- Figure 1-15

### **1.10.9 Central Computing and Telecommunications Agency Risk Analysis and Management Method (CRAMM)**

- UK
- basic risk methodology in an automated tools



#### **1.10.10 Difference:**

- Organization wide: ISO/IEC 27005 or Octave
- IT Risk: NIST SP 800-30
- Limited budget/focused assessment: FRAP
- Software engineering: FMEA, Fault Tree
- Business perspective: AS/NZS 4360

#### **1.10.11 Approaches**

- Qualitative
- Quantitative

#### **1.10.12 Quantitative**

- Asset Value X Exposure Factor (EF) = Single Loss Expectancy
- Annual Loss Expectancy (ALE) = SLE x Annualized Rate of Occurrence (ARO)

#### **1.10.13 Qualitative**

- use the High Medium Low Matrices

#### **1.10.14 Control Selection**

- Risk analysis allows a cost-benefit analysis
- ROSI:  $((\text{Risk Exposure} * \% \text{Mitigate}) - \text{Solution Cost}) / \text{Solution Cost}$
- ALE before controls - ALE after controls - annual cost = value of control

#### **1.10.15 Risk terms:**

- Inherent risk - beginning risk
- Residual risk - remaining risk

#### **1.10.16 Handling Risk:**

- Avoid
- Accept
- Transfer
- Mitigate

#### **1.10.17 Outsourcing**

- You can't outsource risk responsibility

### **1.11 Risk Management Frameworks**

- "a structured process that allows an organization to identify and assess risk, reduces it to an acceptable level, and ensure that it remains at that level."
- Commonly accepted Frameworks:
  - NIST RMF (SP 800-37r1) - Required for federal government agencies - focused on information systems.
  - ISO 31000:2009 - international standard - not focused on Information systems, can be applied broadly in an organization.
  - ISACA Risk IT - aims to bridge gap between generic framework like ISO 31000, and IT-centric ones like NIST. Integrated with COBIT.
  - COSO Enterprise Risk Management - Integrated Framework - 2004 - generic, top-down approach, can be thought of as a superset of the COSO Internal Control framework

#### **1.11.1 Categorize Information Systems**

- Identify systems, subsystems, and boundaries
- Related Business processes
- Integration with Enterprise architecture
- Types of information, it's criticality
- Regulatory and legal requirements applicable
- System interconnections

### **1.11.2 Select Security Controls**

- Assumes that you have performed a risk assessment and have identified a number of common controls across the organization
- For new systems, must determine if there any risks specific to the systems
- Can then either modify common controls (hybrid controls) or develop brand newer ones (system-specific controls)
- Baseline controls = common controls, Actual controls are the hybrid and systems-specific controls

### **1.11.3 Implement Security Controls**

- Implement the control
- Document the control

### **1.11.4 Assess Security Controls**

- Assessor must be competent and independent
- Asses whether controls are effective
- If not effective, document findings and remediation actions

### **1.11.5 Authorize Information Systems**

- Person must determine whether the risk exposure is acceptable to the organization. For a new system this will authorize connecting it to the network. For an inplace system, this is accepting risk or the mitigation plans.

### **1.11.6 Monitor Security Controls**

- Ongoing monitoring and continuous improvement
- Look for new tactics, techniques and procedures of adversary, new vulnerabilities, system changes

## **1.12 Business Continuity and Disaster Recovery**

Goal: minimize effects of a disaster or disruption Continuity planning  
- focused on the longer term procedures for dealing with outages and disasters, typically focused on Senior Management and Business Lines

Disaster Recovery Plan - short-term, typically very IT focused,  
typically focused on Business Lines and Application Availability  
Business Continuity Management - the holistic process that covers  
both of the above terms, considers Availability, Reliability, and  
Recoverability Common issue is security not being considered:

- servers in backup data center not physically secured
- emergency remote access services with insufficient encryption

Or - it's too secure and emergency actions cannot take place:

- admins cannot access servers because PAM system is inoperable, or manager approval cannot take place due to networking issues
- the term "break glass account" typically refer to providing the ability to bypass controls in case of an emergency situation

Business Continuity Planning:

- Protect lives, safety
- Reduce business impact
- Resume critical functions
- Work with outside vendors and partners
- Reduce confusion
- Ensure suitability of business
- Get "up and running"

### **1.12.1 Standards and Best Practices**

NIST SP 800-34 R1 "Continuity Planning Guide for Federal  
Information Systems"

- (a) Develop the continuity planning policy statement Provides guidance and authority
- (b) Conduct the business impact analysis (BIA)

- Identify critical functions
- Identify vulnerabilities, threats, calculate risks
- (c) Identify preventive controls
  - Identify and implement controls to reduce risk
- (d) Create contingency strategies
  - Methods to bring systems online quickly
- (e) Develop an information system contingency plan
  - How to stay functional in a crippled state
- (f) Ensure plan testing, training, and exercises
- (g) Ensure plan maintenance

Others:

- ISO/IEC 27031:2011 - information and communication technology readiness
- ISO 22301:2012 - Business continuity management systems. Can be certified against this document.
- Business Continuity Institute's Good Practice Guidelines (GPG)
  - Management Practices
  - Technical Practices
- DRI International Institute's Professional Practices for Business Continuity Planners

### **1.12.2 Making BCM Part of the Enterprise Security Program**

- Zachman Business Enterprise Framework - used to understand a company's architecture and all the pieces and parts that make it up, looks at various requirements of business processes. Looks at: data, function, network, people, time and motivation components.
- Ideally, BCM should be part of the security program and business decisions and not carved off by itself
- Ideally report to a senior executive with strong management support
- Should understand the Why of the business. For most companies, it is to make money. Not so for government, non-profit.

### **1.12.3 BCP Project Components**

- Identify a Business Continuity Coordinator - leader of the team, typically must be strong at horizontal leadership
- BCP Committee - must be familiar with each department (business units, senior management, IT, Security, Communications, Legal)
- Setting up budget and staff
- Assigning duties and responsibilities
- Senior management kick-off
- Awareness-raising activities
- Training
- Data collection to support continuity options
- Quick-wins

### **1.12.4 Scope of the Project**

- Typically scoped to larger threats with smaller threats covered by independent departmental contingency plans

### **1.12.5 BCP Policy**

- supplies the framework for and governance of designing and building the BCP effort
- Contents: Scope, mission statement, principles, guidelines and standards
- Steps to create:
  - Identify and document the components of the policy
  - Identify and define policies of the organization that the BCP might affect
  - Identify pertinent legislation, laws, regulations and standards
  - Identify "good industry practice" guidelines
  - Perform a gap analysis
  - Compose a draft
  - Review draft

- Incorporate feedback
- Get approval
- Publish

#### **1.12.6 Project Management**

- Basically - execute a BCP project like any other good project
- SWOT - strengths, weaknesses, opportunities, threats
- Project Plan:
  - Objective-to-task mapping
  - Resource to task mapping
  - Workflows
  - Milestones
  - Deliverance - Budget Estimates
  - Success Factors
  - Deadlines

#### **1.12.7 BCP Requirements**

- Need management support to get necessary resources
- Executives must provide due diligence: doing everything within one's power to prevent a bad thing from happening
- Due care: taking the precautions that a reasonable and competent person would take in the same situation
- Regulations require customer data be protected even during a disaster

#### **1.12.8 Business Impact Analysis**

- a functional analysis - what are the functions of the business and what is their criticality. Point is to identify the areas that would suffer the greatest financial or operational loss.
- Must identify:
  - Max tolerable downtime
  - Operational disruption and productivity

- Financial considerations
  - Regulatory responsibilities
  - Reputation
- This is gather through SME interviews, develop process flow diagrams

#### BIA Steps:

- Select individuals to interview
  - Create data-gathering techniques (surveys)
  - Identify critical business functions
  - Identify dependent resources
  - Calculate how long functions can survive without the resources
  - Identify vulnerabilities and threats to these functions
  - Calculate risk for each function
  - Document findings
- (a) Risk Assessment
- A BCP focused assessment should be conducted
- (b) Risk Assessment Evaluation and Process
- Set the Likelihood and Impact for disruption threats
- (c) Assigning Values to Assets
- Cost of a loss (impact)
  - Maximum tolerable Downtime (MTD), Maximum Period Time of Disruption (MPTD). Examples:
    - Non-essential functions: 30 days
    - Normal: 7 days
    - Important: 72 hours
    - Urgent: 24 hours
    - Critical: Minutes to hours

### 1.12.9 Interdependencies

## 1.13 Personnel Security

Separation of Duties :: make sure that one individual cannot complete a critical task by his/herself. Two variations: Split



knowledge :: No one person knows all the details Dual control :: Two individuals are required to complete the task Rotation of duties :: used to uncover fraudulent activities, mandatory vacations

#### **1.13.1 Hiring Practices**

Nondisclosure Agreements (NDAs) :: should be required References should be checked

#### **1.13.2 Termination**

Companies should have a set procedure Procedure should be connected to disabling account access

#### **1.13.3 Security-Awareness Training**

Should be comprehensive, tailored and organization-wide Typically three audiences: Management, Staff, technical employees Typically should require employees to sign stating understanding of their security responsibilities

#### **1.13.4 Degree or Certification?**

Awareness :: provide information, goal is recognition and retention Training :: provide knowledge, goal is providing a skill Education :: provide Insight, goal is Understanding

### **1.14 Security Governance**

Security Governance :: A framework that allows for the security goals of an organization to be set and expressed by senior management Goal is to implement security throughout the organization

#### **1.14.1 Metrics**

The means to facilitate decision making, performance improvement and accountability Must be quantitative, repeatable, reliable and meaningful Balanced score card - a standard business metrics framework (not too common within security though)

- Financial, Internal Business, Learning and Growth, Customer

Note: Getting the right metrics is hard. Too common for business to default to measuring the data they have (# of IDS alerts) rather than those that express progress towards their security objectives.

Industry best practices:

- ISO/IEC 27004:2009 - base measures, derived measures, indicator values
- NIST SP 800-55 R1 - implementation, effectiveness/efficiency, impact values

Metrics must mature as the program matures

Time Entry -> Compromise Time Compromise -> Detection Time  
Detection -> Recovery

## 1.15 Ethics

Overview:

- Protect society, the common good, necessary public trust and confidence and the infrastructure
- Act honorably, honestly, justly, responsibly, and legally
- Provide diligent and competent service to principals
- Advance and protect the profession

### 1.15.1 The Computer Ethics Institute

Ten Commandments:

- Do no harm (with a computer)
- Don't interfere with other's work
- Don't snoop
- Don't steal
- Don't bear false witness
- Don't steal software or violate copyright
- Use computers with authorization

- Don't steal IP
- Think about social consequences of programs
- Ensure consideration and respect for fellow humans

### **1.15.2 The Internet Architecture Board**

Considers the following as unethical:

- Purposely seeking to gain unauthorized access
- Disrupting the Internet
- Wasting resources
- Destroying integrity of information
- Compromising privacy
- Conducting Internet-wide experiments negligently

### **1.15.3 Corporate Ethics Programs**

Most companies have an ethical statement

## **2 Chapter 2 - Asset Security**

### **2.1 Information Life Cycle**

#### **2.1.1 Acquisition**

- Information is added to systems, metadata attached, business process metadata attached, information is indexed. Must meet policy controls such as encryption of PII

#### **2.1.2 Used**

- Must maintain Integrity of data across replicated stores, resolving inconsistencies, applying classification rules

### **2.1.3 Archival**

- Business and legal requirements. Risks for discarding too soon, and for holding too long.

Backup :: a copy of data currently in use, typically becomes less useful as it gets older  
Archive :: Copy of data that is no longer in use

### **2.1.4 Disposal**

Usually this means data destruction, needs to be destroyed correctly  
Physically devices can be wiped, degaussed or shredded

## **2.2 Information Classification**

- Sensitivity of data should be commensurate with the impact to the organization upon loss of confidentiality (PII is sensitive)
- Criticality of data is an indicator of impact to the fundamental business processes (Product research could be critical)
- Be sure to consider: Confidentiality, Availability and Integrity
- Each classification should have associated rules/controls

### **2.2.1 Classifications Levels**

Common ones:

- Public
- Sensitive - financial information, details of projects
- Private - PII, personal related
- Confidential - trade secrets, company related

Government:

- Unclassified
- Sensitive but Unclassified
- Confidential
- Secret
- Top Secret

### **2.2.2 Classifications Controls**

Some controls to consider:

- Fine-grained access controls
- Encryption at rest and in transmission
- Auditing and monitoring (logging)
- Separation of duties
- Periodic reviews
- Backup and recovery
- Change control procedures
- Physical security
- Information flow channels
- Proper disposal actions (shredding, degaussing)
- Marking, labeling and handling procedures

## **2.3 Layers of Responsibility**

### **2.3.1 Executive Management**

C-Suite ultimately responsible CEO CFO CIO CPO CSO (Chief Security Officer)

CISO vs. CSO - CISO usually technology focused, CSO is broader to include Physical. Privacy - related to the amount of control an individual should have to their personal data

### **2.3.2 Data Owner**

- member of management is charge of a business unit, ultimately responsible for a subset of information
- Decides data classification, responsible for security of data

### **2.3.3 Data Custodian**

- Maintains and protects data, usually IT
- Maintaining security controls, backing up data, validating integrity

#### **2.3.4 System Owner**

- Owner of a system which may process data owned by different data owners
- Typically the business

#### **2.3.5 Security Administrator**

- implementing and maintaining specific security devices

#### **2.3.6 Supervisor**

- user manager, responsible for user activity

#### **2.3.7 Change Control Analyst**

- approving or rejecting change requests

#### **2.3.8 Data Analyst**

- ensuring that data is stored in a way that makes sense

#### **2.3.9 User**

- uses the data

#### **2.3.10 Auditor**

- conducts checks to ensure policy and regulatory compliance

#### **2.3.11 Why so many roles?**

### **2.4 Retention Policies**

#### **2.4.1 Developing a Retention Policy**

These can vary a lot between types of information, need to identify and document Taxonomy :: scheme to classify data types

Classification :: sensitivity Normalization :: Large data sets must be normalized to allow searching Indexing :: Common approach to allow searching e-discovery :: Process of producing for a court or external attorney all electronically stored information (ESI) pertinent to a legal proceeding

#### Electronic Discovery Reference Model (EDRM)

- (a) Identification of data required under order
- (b) Preservation - prevent from deletion, destruction
- (c) Collection - from various stores
- (d) Processing - put in correct format
- (e) Review - ensure it is relevant
- (f) Analysis - for proper context
- (g) Production - give to those requesting it
- (h) Presentation - show to external audiences to prove or disprove a claim

## **2.5 Protecting Privacy**

### **2.5.1 Data Owners**

- Decide who gets access to data

### **2.5.2 Data Processors**

- Those that handle the data

### **2.5.3 Data Remanence**

- What remains after a simple delete of data
- NIST 800-88 R1 - Guidelines for Media Sensitization
- Solutions: "secure delete", encryption, destruction

#### **2.5.4 Limits on Collection**

- Collection limitation - only collect the minimal PII necessary to perform job

Privacy Policy:

- What is collected
- Why and how do we use
- With whom do we share
- Who owns
- What are the rights of the data subject
- When do we destroy
- Pertinent laws

### **2.6 Protecting Assets**

Threats: theft, service interruptions, physical damage, compromised system and environment integrity, unauthorized access

#### **2.6.1 Data Security Controls**

Data States: In Motion, In Use, At Rest

At Rest:

- encryption (NIST 800-111, "Guide to Storage Encryption Technologies for End User Devices")
- Geographic boundaries - some countries require providing access to encrypted data

In Motion:

- Encryption TLS, IPSec
- VPN

Data in Use:

- Side-channel attacks
- Memory attacks



### **2.6.2 Media Controls**

- Physically secure backup tapes
- Media libraries
- Managing media (such as backup tapes) - track inventory, track against retention, testing, destroying

## **2.7 Data Leakage**

- Employee mishandling is the most common form of mis-use

Technical controls:

- USB or external media controls
- email screening (DLP)

### **2.7.1 Data Leakage Prevention**

Prevent leakage to external parties Should be considered a program, not a technology (processes, policy, culture, people)

Data Inventories: know where sensitive data lies Data Flows: should be mapped - there may be more locations to put sensors than just at the perimeter (ie. between dev and qa teams) Data Protection Strategy - Steganography - hiding data in other data Areas to consider:

- Backup and recovery
- Data life cycle - security of data as it transitions life cycles - such as going to an archival facility
- Physical security
- Security culture
- Privacy
- Organizational change

Implementation, Testing, Tuning:

- Sensitive data awareness
- Policy engine

- Interoperability
- Accuracy

Network DLP - sit on perimeter of network Endpoint DLP - software running on each endpoint Hybrid DLP - Both the above

## **2.8 Protecting Other Assets**

### **2.8.1 Protecting Mobile Devices**

- Theft is main threat

Controls:

- Inventory
- Harden configurations
- Password protect BIOS on laptops
- Maintain in personal possession
- Encrypt
- Backup
- Remote wiping
- Tracing

### **2.8.2 Paper Records**

- easily overlooked
- lock away when not in use
- Label with classification
- Destroy with a crosscut shredder

### **2.8.3 Safes**

- Inventory - know where they are
- Ensure they are fit for purpose

## 3 Chapter 3 - Security Engineering

### 3.1 System Architecture

**Architecture** tool used to conceptually understand the structure and behavior of a complex entity through different views.

**Architecture description** formal description and representation of a system, the components that make it up, the interactions and interdependencies between those components, and the relationship to the environment.

**System Architecture** describes the major components of the system and how they interact with each other, with the users, and with other systems. Answers: "How is it going to be used?" "What environment?" "What type of security and protection?" "Communication needs?"

**Development** The entire life cycle of a system, including the planning, analysis, design, building testing, deployment, maintenance, and retirement phases.

**System** can be an individual computer, an application, a select set of subsystems, a set of computers, or a set of networks

#### 3.1.1 ISO/IEC 42010:2011 - System Architecture Standard. Establishes a shared vocabulary

- Architecture
- Architecture description

**Stakeholder** Individual, team or organization with an interest in the system

**View** Representation of a whole system from a perspective of a related set of concerns

**Viewpoint** Specification of the conventions for constructing and using a view

- Security goals must be defined before the architecture of a system is created. Need a security view.

### 3.2 Computer Architecture

**Computer Architecture** all the parts of a computer system that are necessary for it to function, including the central processing unit,

memory chips, logic circuits, storage devices, input and output devices, security components, buses, and networking interfaces.

### 3.2.1 The Central Processing Unit

**CPU** brain of the computer

**register** temporary storage within CPU

**arithmetic logic unit** actual execution of instructions

**control unit** manages and synchronizes the system while different applications' code and OS instructions are being executed

**General registers** holds variables and temporary results as ALU works through execution steps

**special registers** special information such as program counters, stack pointer, program status word (PSW)

**program counter** memory address of the next instruction to be fetched

**program status word** holds different condition bits - user mode, privileged mode. Privileged mode has access to more functions.

memory has specific memory addresses.

Memory bus - can be 8, 16, 32 or 64 bits wide. Most today are 64.  
 $2^{64}$  address space.

### 3.2.2 Multiprocessing

- More than one processor
- symmetric mode - like load-balancing
- asymmetric mode - processor dedicated to a task

### 3.2.3 Memory Types

**Random Access Memory (RAM)** temporary storage. DRAM - must be refreshed, slower. Static RAM (SRAM) - does not require refresh, require more transistors, faster than DRAM

**Synchronous DRAM (SDRAM)** synchronizes with the system's CPU clock - increases speed

**Extended data out DRAM (EDO DRAM)** faster than DRAM  
can capture next block while first block is being sent to CPU  
(look ahead)

**Burst EDO DRAM (BEDO DRAM)** Can send more data  
at once

**Double data rate SDRAM (DDR SDRAM)** Carries out two  
operations per clock cycle, twice the throughput

**Hardware segmentation** physically segregating hardware be-  
tween processes instead of just logically

**Read-Only Memory** non-volatile memory

**Programmable read-only memory (PROM)** can be modi-  
fied after manufacture

**Erasable programmable read-only memory (EPROM)**  
can be erased, modified and upgraded.

**Electrically erasable programmable read-only memory (EEPROM)**  
can be erased and modified electrically (no UV light wand)

**Flash memory** was special type of memory used in digital  
cameras, BIOS chips, memory cards, video game con-  
soles. Solid state. Now in computer hard drives.

**Cache Memory** used for high speed writing and reading activities -  
for caching data for easy access

**Memory mapping** software uses logical addresses, CPU uses phys-  
ical addresses (absolute addresses). A security feature. Relative  
addresses: known address with an offset.

**Buffer Overflows :: when too much data is accepted as input to a specific process.** E  
allocated segment of memory.

### 3.2.4 Buffer Overflow Resources

- [http:// opensecuritytraining.info/ IntroX86. html](http://opensecuritytraining.info/IntroX86.html)
- [http:// www.reddit.com/ r/ hacking/ comments/ 1wy610/ exploit\\_tutorialbufferoverflow/](http://www.reddit.com/r/hacking/comments/1wy610/exploit_tutorial_buffer_overflow/)
- [https:// www.corelan.be/ index.php/ 2009/ 07/ 19/ exploit-  
writing-tutorial-part-1-stack-based-overflows/](https://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/)
- [http:// www.lethalsecurity.com/ wiki](http://www.lethalsecurity.com/wiki)
- [http:// opensecuritytraining.info/ Exploits1. html](http://opensecuritytraining.info/Exploits1.html)
- [https:// exploit-exercises.com/ protostar/](https://exploit-exercises.com/protostar/)

Narnia Setup ([http:// overthewire.org/ wargames/ narnia/](http://overthewire.org/wargames/narnia/))

### 3.2.5 Memory Protection Techniques

- Address space layout randomization (ASLR) - changes address layout randomly
- Data Execution Prevention (DEP) - executable code does not function within memory segments that could be dangerous

### 3.2.6 Memory Leaks

- When applications do not correctly release memory. Can open the door to a DoS attack.

## 3.3 Operating Systems

### 3.3.1 Process Management

**Process** set of instructions that is actually running. A program loaded into memory. A process has computer resources (CPU, memory) assigned to it.

**Multiprogramming** More than one program can be loaded into memory at the same time. Legacy term.

**Multitasking** more than one application and the OS can handle requests from these applications simultaneously

**Cooperative multitasking** required the process to voluntarily release resources

**preemptive multitasking** all modern OSes, the OS controls how long a process can use resources

**spawning** when a process creates a child process

**running state** CPU is executing its instructions

**blocked state** on hold

**process table** one entry per process - process state, stack pointer, memory allocation, program counter, status of open files

**interrupts** request for CPU time. Uses process priority levels.

**maskable interrupt** low priority

**nonmaskable interrupt** cannot be overridden by an application

**stack** each process has its own memory stack (Last in First Out LIFO)

**thread** a sub-process effectively. Executed in parallel.

**process scheduling :: can be exploited to starve system of memory (DOS).** Software processes are waiting on each other.

**Process Activity** ensuring only one process is access resources (memory/files) at a time. Process isolation. Means to enforce: encapsulation of objects, time multiplexing of shared resources, naming distinctions, virtual memory mapping. Encapsulation provides data hiding, processes communicate through an API. Time multiplexing, means of sharing the CPU. Naming distinctions - unique PID values. Virtual address memory mapping - logical vs. physical. Each application usually starts with 0.

### 3.3.2 Memory Management

**Abstraction** details are hidden to the applications.

**Memory manager** allocate and deallocate different memory segments.

- Relocation - swap hard drive / RAM, provide pointers to applications
- Protection - limit processes to only access the memory assigned to them, provide access control to memory segments
- Sharing - provide integrity and confidentiality when processes share memory segments, allow users to share an application
- Logical organization - provide an abstracted addressing scheme, allow for sharing of software modules such as DLLs
- Physical organization - segment physical memory space

**Base register** beginning address assigned to a process

**Limit register** ending address - describes the bounds of the process.

**Virtual Memory** uses secondary storage. Swap space. Security issue is that data on disk could potentially be captured, especially if swap space is not appropriately wiped. Consider: an encrypted file is opened, and hence decrypted. The unencrypted file in memory is then written to swap space. An attacker could then find means to access the file within the swap space.

### 3.3.3 Input/Output Device Management

**Interrupts** Request for CPU time

**Programmable I/O** sends data to I/O device and polls the device to see if it is ready to accept more data. Can waste the CPU's time.

**Interrupt-Driven I/O** Device sends an interrupt when it's ready. Have to deal with a lot of interrupts.

**I/O using DMA** Direct Memory Access - can transfer data without using the CPU. Significant speed advantages.

**Premapped I/O** CPU sends physical memory address to I/O device, I/O device must be trusted to access memory correctly.

**Fully mapped I/O** OS does not trust device, uses logical addresses

### 3.3.4 CPU Architecture Integration

**instruction set** the language of the CPU - x86 is most common in use today.

**microarchitecture** makes up the CPU - registers, logic gates, ALU, cache, etc.

**Rings** protection system of the OS - levels of trust for processes - kernel runs in Ring 0, other OS components in Ring 1, Drivers/utilities in Ring 2, Applications in Ring 3. Lower level processes can access high level processes. Windows and OS X don't use Rings 1 and 2.

**Application Programming Interface (API)** means for software to communicate with each other.

**CPU Operations Modes** Ring 0 is Kernel Mode, Ring 3 is User mode.

### 3.3.5 Operating System Architectures

**Monolithic architecture** all the OS processes work in kernel mode. MS-DOS and early OSes like this.

**Layered operating system** all still work in kernel mode, functionality was laid out into layers that called on each other. Provides data hiding. Think kernel modules or DLLs in Windows.



**Microkernel model** only a subset of critical kernel processes operating in kernel mode. Others in user mode. This introduced some performance issues.

**Hybrid microkernel** client server type architecture where applications are the clients. All of OS operates in kernel mode.

### 3.3.6 Virtual Machines

- Enables a single hardware to run multiple operating systems

Hypervisor manages the system resources between OSes

- Resource from CISSP book: [www.kernelthread.com/publications/virtualization](http://www.kernelthread.com/publications/virtualization)
- 

## 3.4 System Security Architecture

### 3.4.1 Security Policy

**Security Policy** a strategic tool that dictates how sensitive information and resources are to be managed and protected.

### 3.4.2 Security Architecture Requirements

**Trusted Computing Base (TCB)** Collection of hardware, software and firmware components that provides security and enforces policy.

**Trusted Path** communication channel between user, program and TCB

**Trusted shell** a user cannot "bust out of it"

**Security Perimeter** divides trusted from untrusted - requires an interface

**Reference Monitor** defines how access control within a system is carried out

**Security Kernel** all hardware, software and firmware that fall within the TCB, it implements and enforces the reference monitor concept. TCB contains the security kernel, which implements the reference monitor concept.

**Multilevel security policies** permit a subject to access an object only if the subject's security level is higher than or equal to the object's classification.

### 3.5 Security Models

#### 3.5.1 Bell-LaPadula Model

- First mathematical model.
- enforces confidentiality only. Its about protecting secrets. One of the first models developed in the 70s. Is a multilevel security system.

Simple security rule a subject at a given security level cannot read data that resides at a higher security level. No read up.

\*-property rule a subject in a given security level cannot write information to a lower security level. No write down.

Strong star property rule a subject with both read and write capabilities can only perform both at the same security level.

#### 3.5.2 Biba Model

- Addresses Integrity. Prevents data at any integrity level from flowing to a higher integrity level.

\*-integrity axiom a subject cannot write data to an object at a higher integrity level. No write up.

Simple integrity axiom Cannot read from a lower integrity level. No read down.

Invocation property Subject cannot request service (invoke) at a higher integrity.

- Memorization tip: "Simple" is about reading. \* is about writing.

#### 3.5.3 Clark-Wilson Model

- Developed after Biba, different approach to protecting Integrity
- Three goals: subjects can access objects only through authorized programs, separation of duties enforced, auditing is required.
- Focuses on well-formed transactions and separation of duties.

Transformation Procedures (TPs) programmed abstract operations (read, write, modify)

Constrained Data Items (CDIs) can be manipulated only by TPs

Unconstrained Data Items (UDIs) can be manipulated by users via primitive read/write operations

Integrity verification procedures (IVPs) Check the consistency of CDIs with external reality - audits the work done and validates integrity

#### **3.5.4 Noninterference Model**

- Less concerned about the flow of data than what a subject knows about the state of the system.
- A lower level entity should not be able to detect that an operation took place at a higher level of security. That would be a form of information leakage.

Covert channel a way to receive information in an unauthorized manner. Either storage or timing.

#### **3.5.5 Brew and Nash Model**

- Chinese wall model. A subject can write to an object if, and only if, the subject cannot read another object that is in a different dataset.
- Provides dynamic access control and separation of duty controls / conflicts of interests.

#### **3.5.6 Graham-Denning Model**

- Shows how subjects and objects should be created and deleted
- defines a set of basic rights in terms of commands that a specific subject can execute on an object. Eight primitive protection rights/rules.
- How to securely create/delete a object/subject
- How to securely provide read/grant/delete/transfer access rights

#### **3.5.7 Harrison-Ruzzo-Ullman Model**

- Shows how a finite set of procedures can be available to edit the access rights of a subject
- Access rights of subjects and the integrity of those rights.

## 3.6 Systems Evaluation

### 3.6.1 Common Criteria

- Only framework of global significant
- ISO standard - 1993
- ISO/IEC 15408
- Seven assurance levels (Evaluation Assurance Level (EAL))
- EAL1 - Functionally tested
- EAL2 - Structurally tested
- EAL3 - Methodically tested and checked
- EAL4 - Methodically designed, tested and reviewed
- EAL5 - Semiformally designed and tested
- EAL6 - Semiformally verified design and tested
- EAL7 - Formally verified design and tested - based on a model that can be mathematically proven

protection profiles contains the set of security requirements, their meaning and reasoning, and the corresponding EAL rating that the intended product will require

- Security problem description
- Security objectives
- Security requirements

Target of evaluation (TOE) product being tested

Security target what the product does and how it does it according to the vendor

Security functional requirements security functions that must be provided by the product

Security assurance requirements Measures taken to assure compliance with the claimed security functionality

Packages-EALs functional and assurance requirements bundled into packages for reuse.

### 3.6.2 Why Put a Product Through Evaluation?

- DoD requires rating for some products

## 3.7 Certification vs. Accreditation

### 3.7.1 Certification

**Certification** comprehensive technical evaluation of the security components and their compliance for the purpose of accreditation. Certification process is: evaluation, risk analysis, verification, testing and auditing.

### 3.7.2 Accreditation

**Accreditation** formal acceptance of the adequacy of a system's overall security and functionality by management. *Management acceptance of risk.*

C&A came into focus with the passage of FISMA in 2002 - required it for federal agencies.

## 3.8 Open vs. Closed Systems

### 3.8.1 Open Systems

- built on standards, protocols and interfaces that have published specifications. Windows, OS X and Unix are open.

### 3.8.2 Closed Systems

- Architecture does not follow industry standards. Proprietary. Potentially more secure. Don't work well with other systems.

## 3.9 Distributed System Security

### 3.9.1 Cloud Computing

- use of shared, remote computing devices for the purpose of providing improved efficiencies, performance, reliability, scalability and security.

**Software as a Service (SaaS)** web based application

**Platform as a Service (Paas)** computing platform in the cloud.  
OS instance, or something like Salesforce Platform.

**Infrastructure as a Service (IaaS)** full system in the cloud.  
Full responsibility for managing and patching.

### 3.9.2 Parallel Computing

- use of multiple computers to solve a task. Bit level, instruction level or task level. Bit level is in every device these days. Instruction - requires two or more processors. Task - multiple threads.

### 3.9.3 Databases

**Aggregation** Ability to combine separate pieces of allowed information, to infer unallowed information. Think, multiple pieces of unclassified information can add up to secret information.

**Inference** result of aggregation. When a subject deduces the full story from the pieces.

**Content-dependent access control** based on the sensitivity of data.  
More sensitive = smaller subset of subjects have access.

**Context-dependent access control** software understand state and sequence of requests. eg. If you access A, you cannot access B.  
Time based, location based, etc.

**Cell suppression** hide certain cells

**Partitioning** dividing the database into different parts

**Noise and perturbation** inserting bogus information

### 3.9.4 Web Applications

- Input sanitization - input should be assumed rogue
- Encryption to prevent interception
- Failing securely - errors that don't reveal system details
- Must be human friendly
- Web application firewalls (WAF) - inspect traffic

### 3.9.5 Mobile Devices

- Threats: malware, theft, DOS, transmission of cellular networks (may be encrypted only over cellular network, not wired).
- Solutions: centrally managed devices, remote policies pushed each device, data encryption, idle timeout locks, screen-saver lockouts, authentication, remote wipe. Lock bluetooth capabilities. Endpoint security. App whitelist. 802.1x implemented on wireless VOID clients on mobile devices.

### 3.9.6 Cyber-Physical Systems

- where computer and physical devices collaborate. Internet of Things.

Embedded systems digital thermometer. Cheap, small. Not always designed with security in mind. Hard to update.

- Internet of Things
  - Authentication - typically poor
  - Encryption - require high processing power which devices may not have
  - Updates - hard to do

Industrial Control Systems specifically designed to control physical devices in industrial processes. Conveyor belts to robots.

- NIST 800-82 - Guide to ICS Security

Programmable Logic Controller (PLC) computers that control electromechanical systems.

Distributed Control System (DCS) network of control devices. Manufacturing plants, oil refineries, power plants.

Control and Data Acquisition (SCADA) control large-scale physical processes across large distances. Power lines.

- ISC Security: increasing connectivity to traditional IT networks increases risk.
  - \* apply risk management processes
  - \* segmentation
  - \* disable unneeded ports and services
  - \* least privileged
  - \* encryption
  - \* patch management
  - \* audit trail monitoring

### **3.10 A Few Threats to Review**

#### **3.10.1 Maintenance Hooks**

- a type of back door. Allow developer to view and edit the code bypassing access controls. Should be removed prior to going to production.
- Control: code reviews, host-based intrusion detection, file system encryption, auditing/logging

#### **3.10.2 Time-of-Check/Time-of-Use Attacks**

- asynchronous attack. Switch out a file after authorization is validated. Race condition.
- Controls: atomic operations of critical tasks.

### **3.11 Cryptography in Context**

#### **3.11.1 The History of Cryptography**

- Substitution cipher ROT13
- Enigma
- Data Encryption Standard (DES) - 1976 - now Triple DES

### **3.12 Cryptography Definitions and Concepts**

#### **3.12.1 Kerckhoffs' Principle**

- Algorithm should be public, only key is secret

#### **3.12.2 The Strength of the Cryptosystem**

- amount of work necessary to break the cryptosystem



### **3.12.3 Services of Cryptosystems**

- confidentiality
- integrity
- authentication
- authorization
- nonrepudation

### **3.12.4 One-Time Pad**

- a perfect encryption scheme - unbreakable - if done properly
  - pad must be used only one time
  - pad must be as long as the message
  - pad must be securely distributed and protected at its destination
  - pad must be made up of truly random values
- They are typically impractical

### **3.12.5 Running and Concealment Ciphers**

- Running key - use every day objects such as books.
- Concealment - "every third word in a letter"

### **3.12.6 Steganography**

- method of hiding data in another media. Text hidden in a picture.

## **3.13 Types of Ciphers**

### **3.13.1 Substitution Ciphers**

- uses a key to dictate how the substitution should be carried out
- Caesar cipher.

### 3.13.2 Transposition Ciphers

- values are scrambled or put into a different order.

frequency analysis method of breaking a cipher using known non-randomness in english language

Key Derivation Functions (KDFs) used to generate keys that are made up of random values.

## 3.14 Methods of Encryption

### 3.14.1 Symmetric vs. Asymmetric Algorithms

**Symmetric** use symmetric keys (secret keys)

**Asymmetric** use public/private keys

### 3.14.2 Symmetric Cryptography

- Sender and receiver must have same key. Distributing the keys is a problem. And large # of people requires  $2^n$  keys. But they are very fast and hard to break.
- Example algorithms:
  - Data Encryption Standard (DES)
  - Triple-DES (3DES)
  - Blowfish
  - International Data Encryption Algorithm (IDEA)
  - RC4, RC5, RC6
  - Advanced Encryption Standard (AES)

### 3.14.3 Asymmetric Cryptography

- Solves the key distribution problem, better scalable, can provide authentication and nonrepudiation
- Much slower, mathematically intensive.
- Examples:
  - RSA
  - ECC
  - El Gamal
  - DSA

#### **3.14.4 Block and Stream Ciphers**

- Block cipher - message is divided into blocks
- Stream - stream of bits, operation performed on each bit individually

Initialization Vectors (IVs) random values that are used with algorithms to ensure patterns are not created during the encryption process.

#### **3.14.5 Hybrid Encryption Methods**

- Asymmetric and Symmetric - both common. Use asymmetric to distribute symmetric keys.
- Session key - a single-use symmetric key used to encrypt messages between two users.