Information Technology Engineering

Mohammad Hossein Manshaei

manshaei@gmail.com

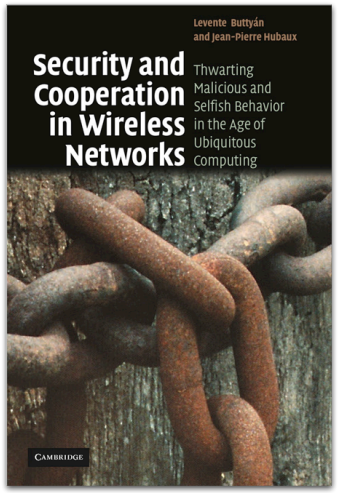
1401

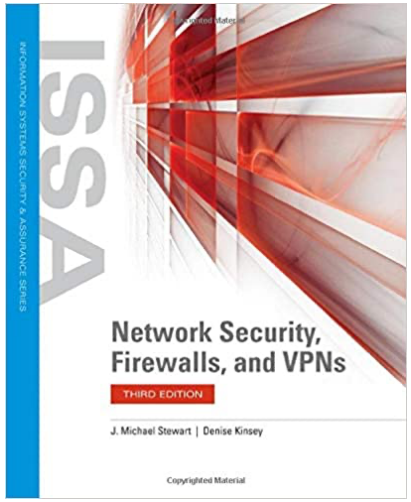
Module B.2

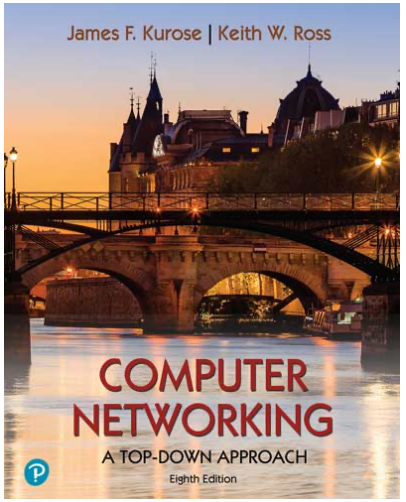
Implementing Trustworthy Computing

Reference:


SIXTH EDITION
ETHICS IN
INFORMATION
TECHNOLOGY
GEORGE W. REYNOLDS


Levente Buttyán
and Jean-Pierre Hubaux
Security and Cooperation in Wireless Networks
Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing
CAMBRIDGE


ISSA
INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES
Network Security, Firewalls, and VPNs
THIRD EDITION
J. Michael Stewart | Denise Kinsey
Copyrighted Material


James F. Kurose | Keith W. Ross
COMPUTER NETWORKING
A TOP-DOWN APPROACH
Eighth Edition

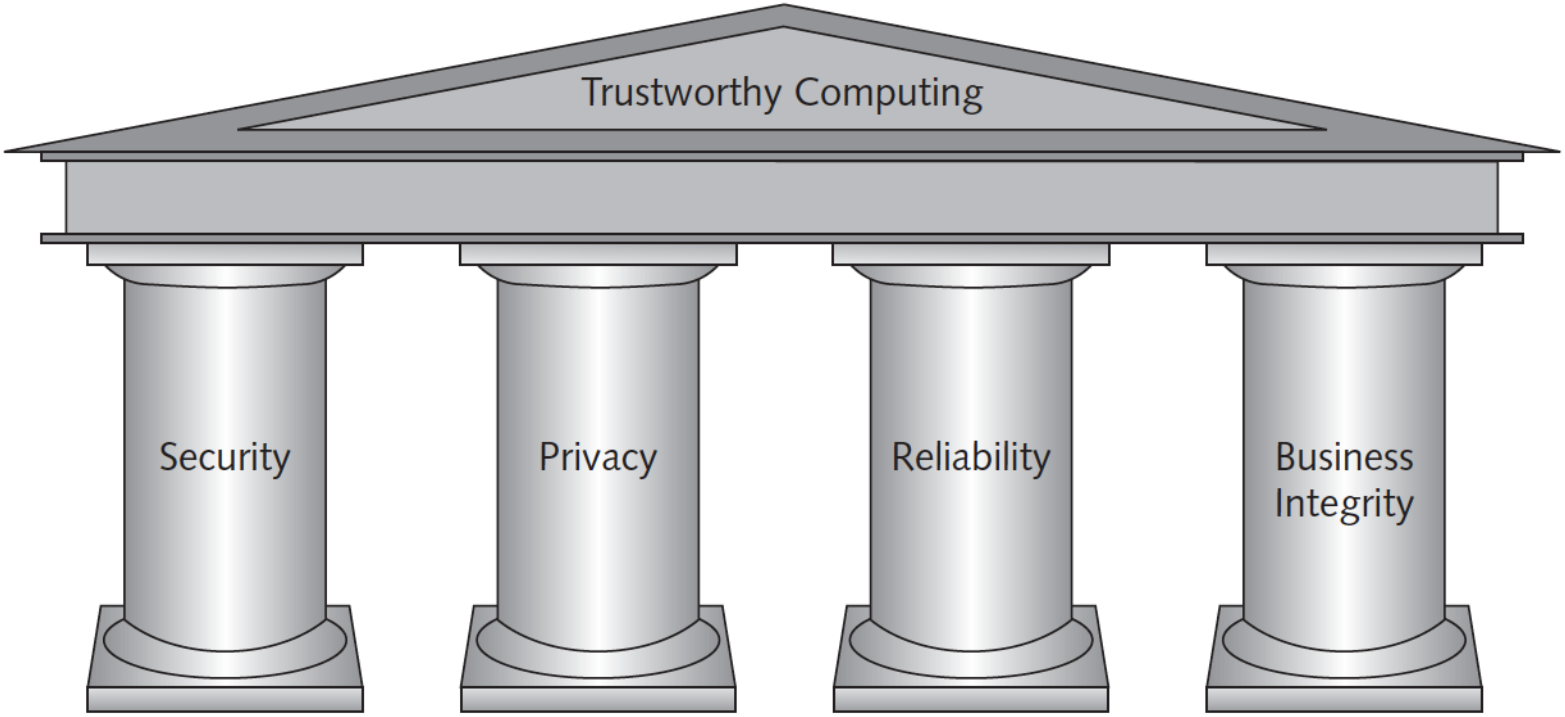
Contents

- ➢ Implementing Trustworthy Computing
  - ◇ CIA Security Triad
  - ◇ Implementing CIA at the Organization Level
    - ✦ Risk Assessment, Disaster Recovery, Security Policy, Security Audit, Regulatory Standards Compliance, Security Dashboard
  - ◇ Implementing CIA at the Network Level
    - ✦ Authentication Methods, Firewall, Routers, Encryption, VPN, IDS
  - ◇ Implementing CIA at the Application Level
    - ✦ User Roles and Accounts, Data Encryption
  - ◇ Implementing CIA at the End-User Level
    - ✦ Security Education, Authentication Methods, Antivirus Software
  - ◇ Response to CyberAttack

Trustworthy Computing

A method of computing that delivers
secure, **private**, and **reliable**
computing experiences
based on sound business practices

Microsoft's Four Pillars of Trustworthy Computing



Microsoft's Actions to Support Trustworthy Computing

Pillar	Actions taken by Microsoft to support trustworthy computing
Security	Invest in the expertise and technology required to create a trustworthy environment. Work with law enforcement agencies, industry experts, academia, and private sectors to create and enforce secure computing. Develop trust by educating consumers on secure computing.
Privacy	Make privacy a priority in the design, development, and testing of products. Contribute to standards and policies created by industry organizations and government. Provide users with a sense of control over their personal information.
Reliability	Build systems so that (1) they continue to provide service in the face of internal or external disruptions; (2) in the event of a disruption, they can be easily restored to a previously known state with no data loss; (3) they provide accurate and timely service whenever needed; (4) required changes and upgrades do not disrupt them; (5) on release, they contain minimal software bugs; and (6) they work as expected or promised.
Business integrity	Be responsive—take responsibility for problems and take action to correct them. Be transparent—be open in dealings with customers, keep motives clear, keep promises, and make sure customers know where they stand in dealing with the company.

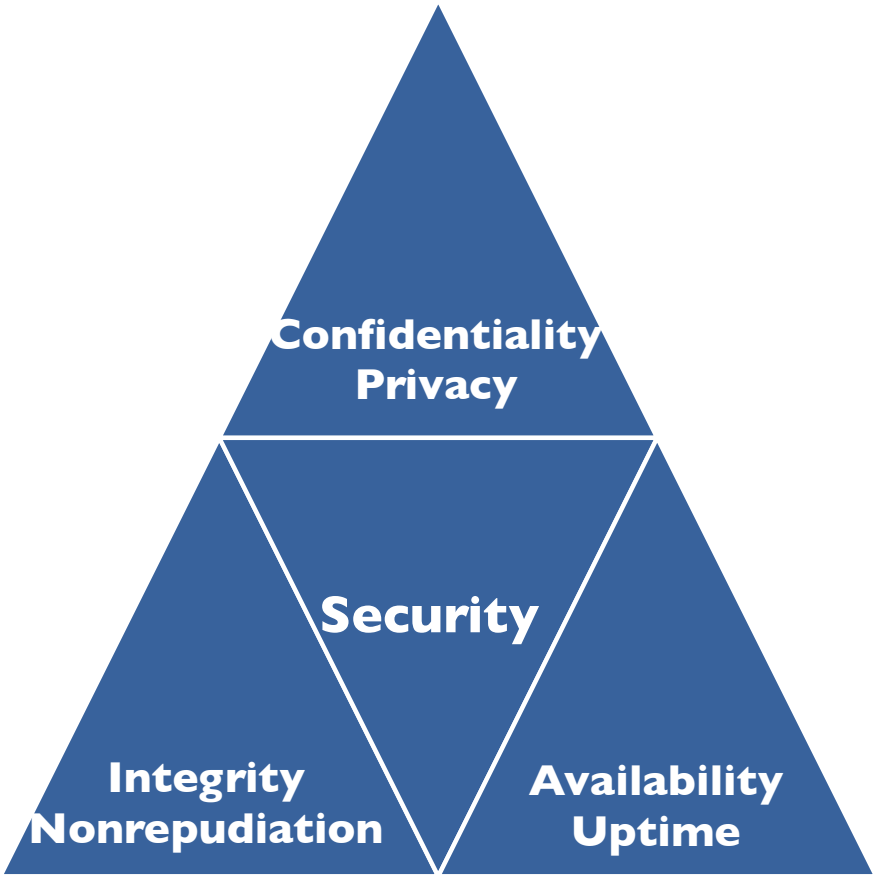
The Need for Information Security

- **Risk**: Likelihood that a threat will exploit a vulnerability and the impact it will have on an organization
- **Threat**: The possibility of an vulnerability being exploited
- **Vulnerability**: Weakness in a process or system that has the potential to adversely impact confidentiality, availability, or integrity

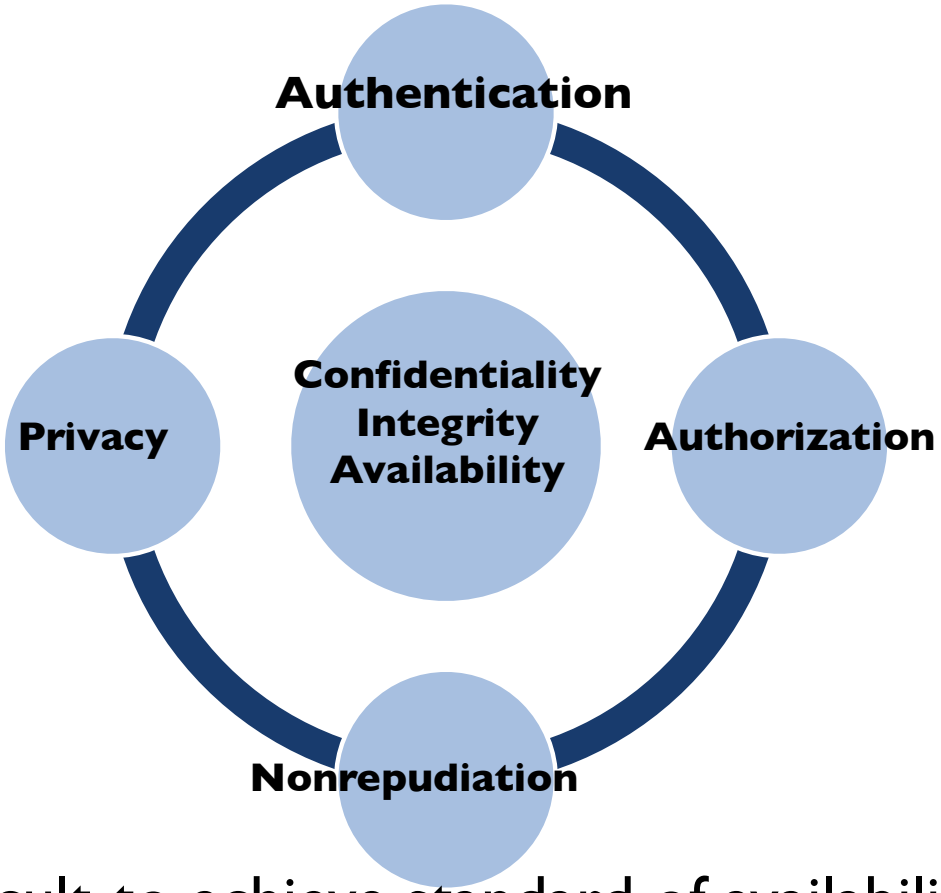
Reducing Vulnerabilities

- **Security**
  - **Combination of technology, policy, and people**
  - **Requires a wide range of activities to be effective**
- **Assess threats** to an organization's computers and network
- **Identify actions that address the most serious vulnerabilities**
- **Educate users**
- **Monitor** to detect a possible intrusion
- **Create a clear reaction plan**

Primary Objectives/Goals of Information Security

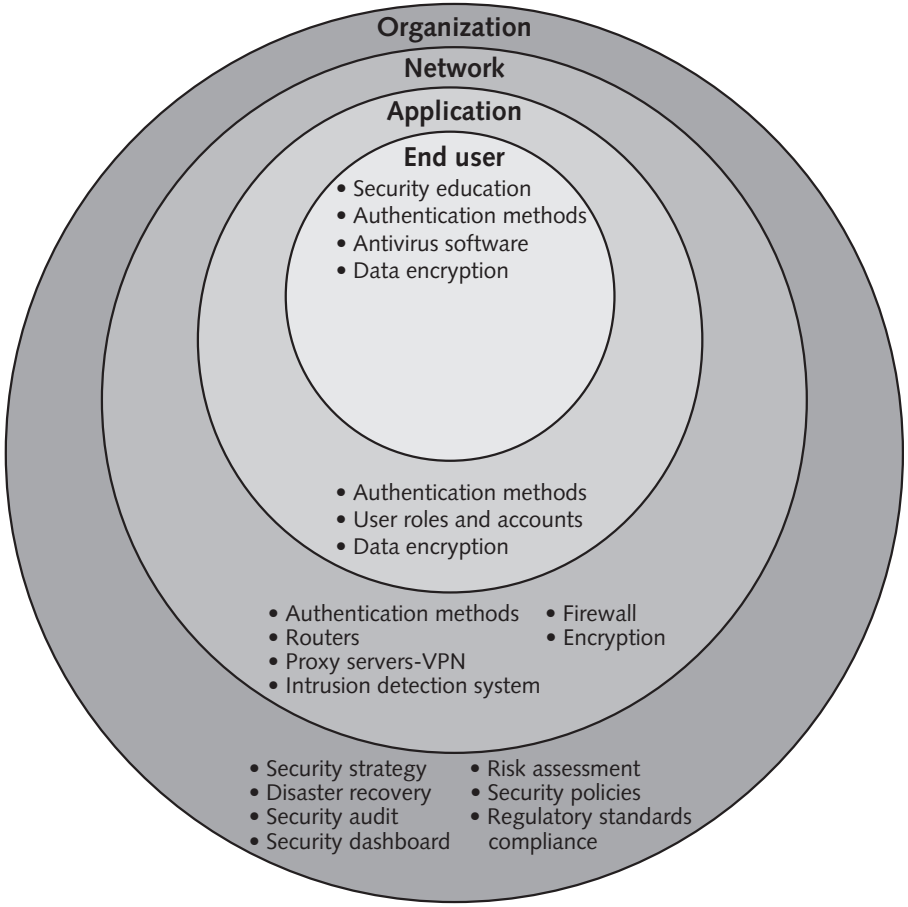


Secondary Objectives/Goals of Information Security

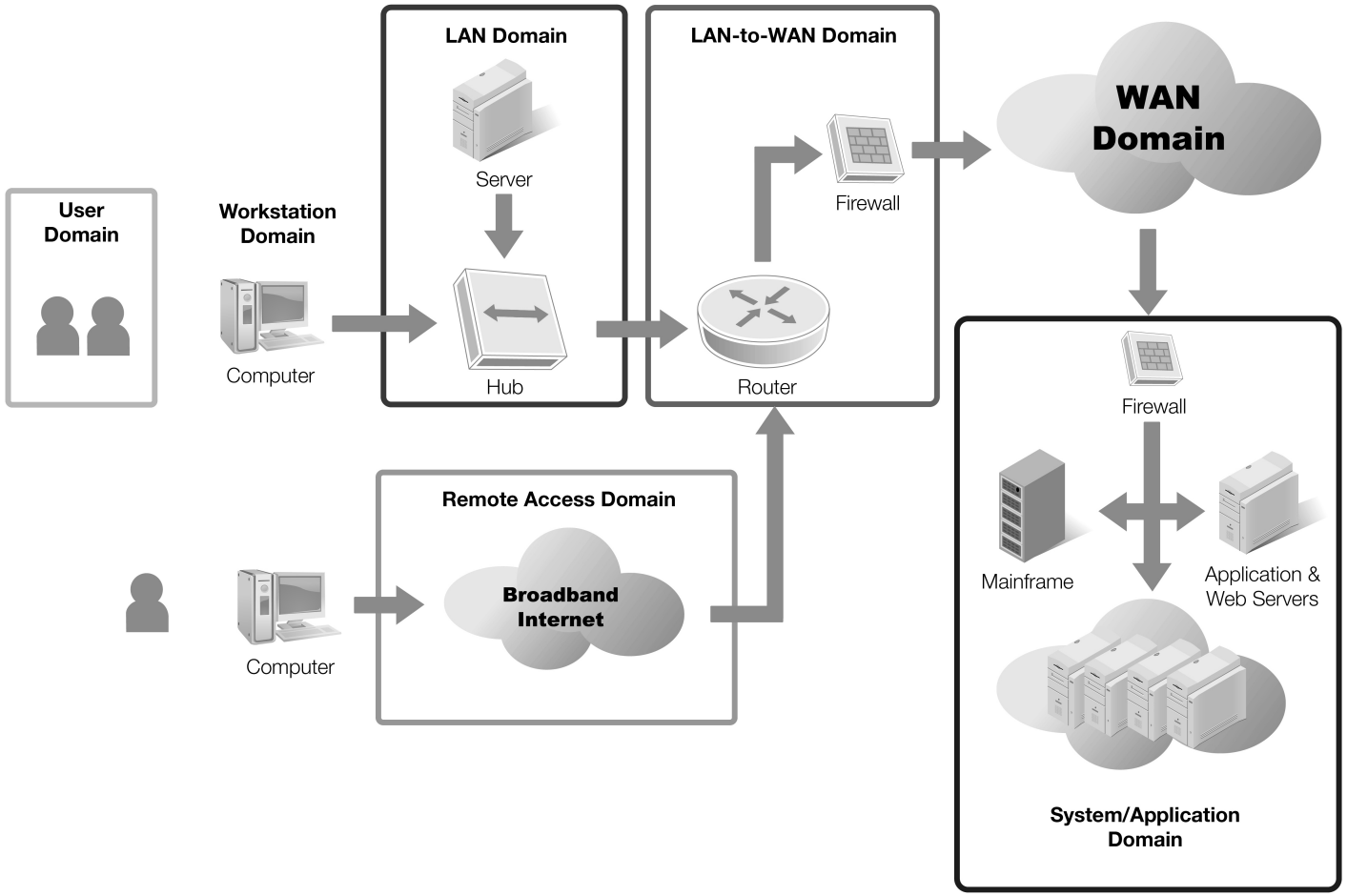


A widely held but difficult-to-achieve standard of availability for a system or product is known as "five 9s" or 99.999 percent availability.

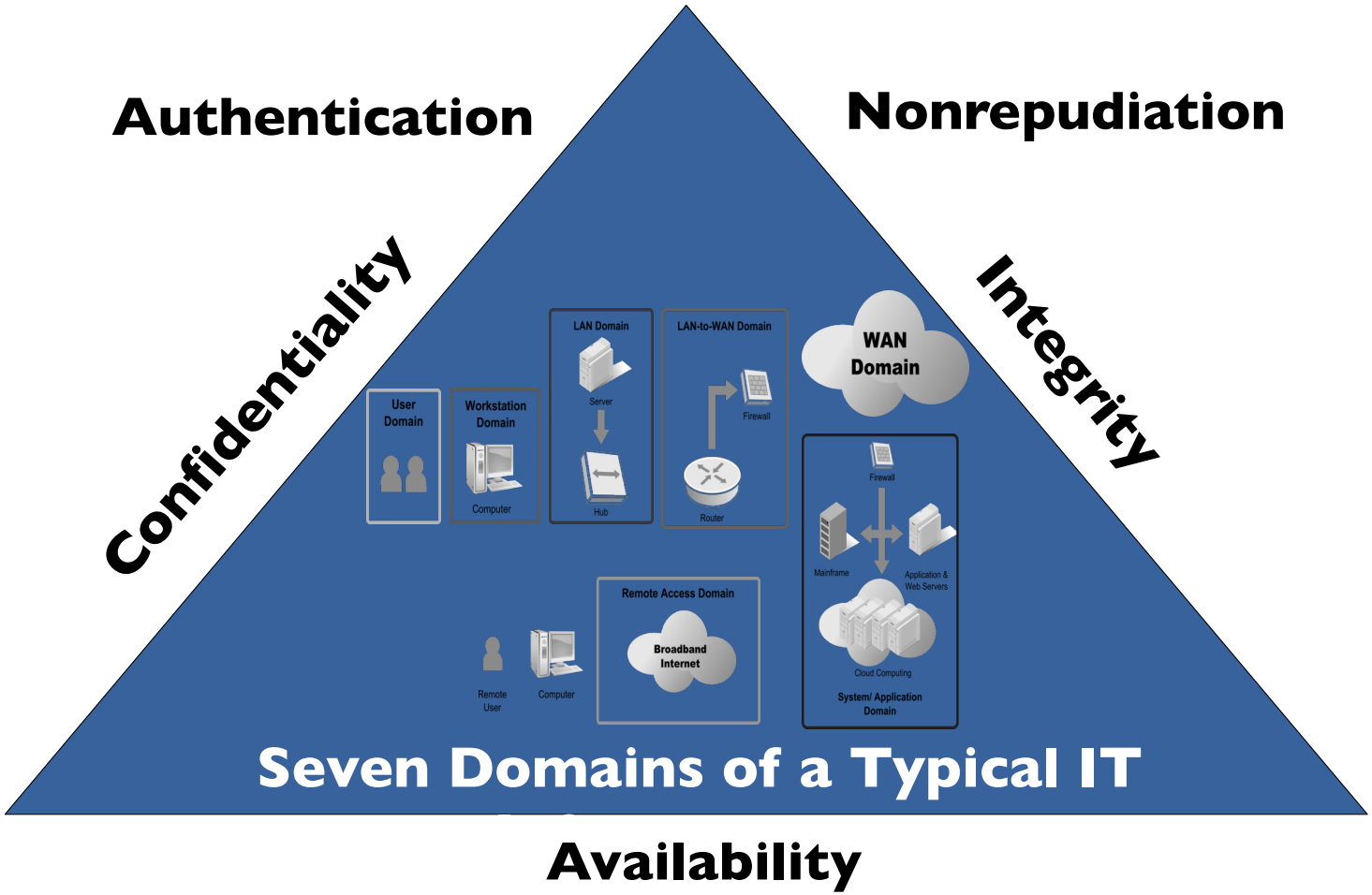
Implementing CIA Security at the Organization, Network, Application, and End-user Levels



Seven Domains of a Typical IT Infrastructure



Information Assurance



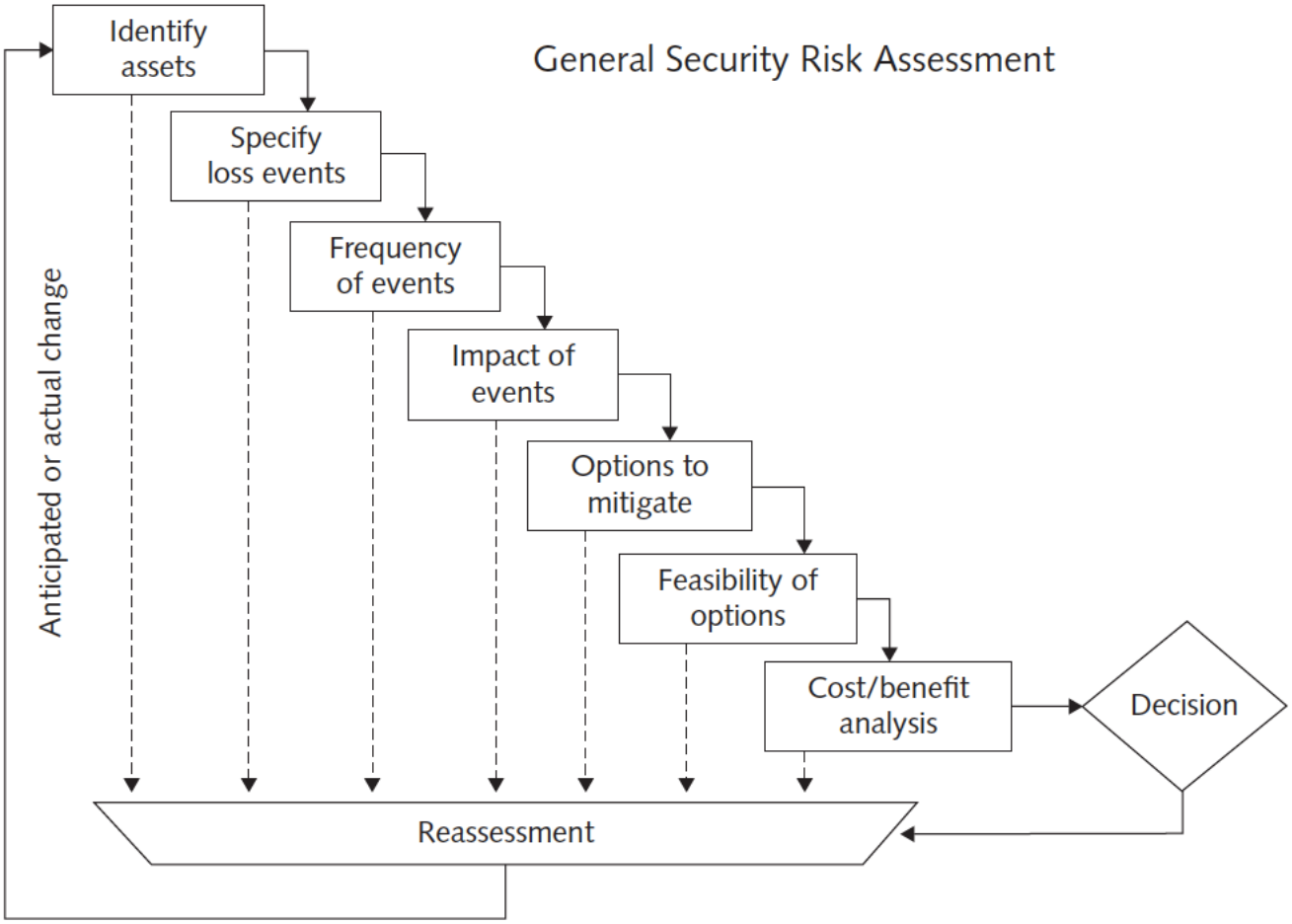
Contents

- ➢ Implementing Trustworthy Computing
  - ◇ CIA Security Triad
  - ◇ Implementing CIA at the Organization Level
    - ✦ Risk Assessment, Disaster Recovery, Security Policy, Security Audit, Regulatory Standards Compliance, Security Dashboard
  - ◇ Implementing CIA at the Network Level
    - ✦ Authentication Methods, Firewall, Routers, Encryption, VPN, IDS
  - ◇ Implementing CIA at the Application Level
    - ✦ User Roles and Accounts, Data Encryption
  - ◇ Implementing CIA at the End-User Level
    - ✦ Security Education, Authentication Methods, Antivirus Software
  - ◇ Response to CyberAttack

1. Risk Assessment

- Organization's **review** of:
  - Potential threats to computers and network
  - Probability of threats occurring
- **Identify** investments that can best protect an organization from the most likely and serious threats
- Reasonable **assurance**
- Improve security in areas with:
  - **Highest** estimated **cost**
  - **Poorest** level of **protection**

Risk Assessment



Source: General Security Risk Assessment Guideline, ASIS International, www.asisonline.org/guidelines/guidelinesgsra.pdf.

Risk Assessment for a Hypothetical Company

Adverse event	Business objective threatened	Threat (estimated frequency of event) per year	Vulnerability (likelihood of success of this threat) (%)	Estimated cost of a successful attack ($)	Risk = Threat × Vulnerability × Estimated cost ($)	Relative priority to be fixed
Data breach of customer account data	Provide a safe, secure website that consumers can trust	18	3	5,000,000	2,700,000	1
Distributed DDoS attack	24/7 operation of a retail website	3	25	500,000	375,000	2
Email attachment with harmful worm	Rapid and reliable communications among employees and suppliers	1,000	0.05	200,000	100,000	3
Harmful virus	Employees' use of personal productivity software	2,000	0.04	50,000	40,000	4
Invoice and payment fraud	Reliable cash flow	1	10	200,000	20,000	5

2. Disaster Recovery

- **Recovery Plan:** A documented process for recovering an organization's business information system assets—including hardware, software, data, networks, and facilities—in the event of a disaster
- To be considered:

1. Technologies vs People
2. Natural vs Manmade
3. Recovery time for different business process (Mission Critical Process)
4. Cloud computing: Pros vs Cons
5. Files and Database

3. Security Policy

- A security policy defines
  - Organization's security **requirements**
  - **Controls and sanctions needed** to meet the requirements
- Delineates responsibilities and expected behavior
- Outlines what needs to be done
  - Not how to do it
- Automated system policies should mirror written policies
- **NIST SP 800**: http://csrc.nist.gov

SANS Security Policy Templates

The SysAdmin, Audit, Network, Security (SANS) Institute's website (www.sans.org) offers a number of security-related policy templates

http://www.sans.org/security-resources/policies

Establishing a Security Policy

- Trade-off between
  - Ease of use
  - Increased security
- Areas of concern
  1. E-mail attachments
  2. Wireless devices
- **VPN** uses the Internet to relay communications but maintains privacy through security features
- Additional security includes encrypting originating and receiving network addresses

4. Security Audit

Federal agency	2007	2006	2005	2004
Department of Homeland Security	B+	D	F	F
Department of Justice	A+	A–	D	B–
Nuclear Regulatory Commission	F	F	D–	B+
Department of State	C	F	F	D+
Department of the Treasury	F	F	D–	D+
Department of Defense	D–	F	F	D
NASA	C	D–	B–	D–
Department of Energy	B+	C–	F	F
Government-wide grade	**C**	**C–**	**D+**	**D+**

Made by: Federal Information Security Management Act (FISMA)

Important prevention tool to evaluate whether an organization has a well-considered security policy in place and if it is being followed.

5. Regulatory Standards Compliance

Your organization may also be required to comply with one or more standards defined by external parties.

Act or standard	Who is affected?	Subject matter
Bank Secrecy Act of 190 (Public Law 91-507)—Amended several times, including by provisions in Title III of the USA PATRIOT Act (see 31 USC § 5311–5330 and Title 31 Code of Federal Regulations Chapter X)	Financial institutions	Requires financial institutions in the United States to assist U.S. government agencies in detecting and preventing money laundering
European Union—United States Privacy Shield	Organizations that do business with companies and/or individuals in the European Union	Provides companies on both sides of the Atlantic with a mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce
Federal Information Security Management Act (44 U.S.C. § 3541, et seq.)	Every federal agency	Requires each federal agency to provide information security for the data and information systems that support the agency's operations and assets, including those provided or managed by another agency, contractor, or other source
Foreign Corrupt Practices Act (15 U.S.C. § 78dd-1, et seq.)	Any person who is a citizen, national, or resident of the United States and engages in foreign corrupt practices; also applies to any act by U.S. businesses, foreign corporation's trading securities in the United States, American nationals, U.S. citizens, and U.S. residents acting in furtherance of a foreign corrupt practice whether or not they are physically present in the United States	Makes certain payments to foreign officials and other foreign persons illegal and requires companies to maintain accurate records
Gramm-Leach-Bliley Act (Public Law 106-102)	Companies that offer financial products or services to individuals, such as loans, insurance, or financial and investment advice	Governs the collection, disclosure, and protection of consumers' nonpublic personal information or personally identifiable information
Health Insurance Portability and Accountability Act (Public Law 104–191)	Healthcare clearinghouses, employer-sponsored health plans, health insurers, and medical service providers	Regulates the use and disclosure of an individual's health information
Payment Card Industry Data Security Standard (PCI DSS)	All organizations that store, process, and transmit cardholder data, most notably for debit cards and credit cards	Provides a framework of specifications, tools, measurements, and support resources to help organizations ensure the safe handling of cardholder information
Sarbanes-Oxley Act (Public Law 107–204 116 Stat. 745)	All public corporations	Protects shareholders and the general public from accounting errors and fraudulent practices in the enterprise

6. Security Dashboard

#	Key performance measure	Goal	Actual	Status
1	Number of segregation-of-duty violations	0	2	Red
2	Number of users with weak, noncompliant passwords	<5	4	Green
3	Percentage of critical IT assets that passed penetration tests	>96%	93%	Yellow
4	Backlog of software security patches and updates	<3	3	Green
5	Number of days since last internal security audit	<90	94	Yellow
6	Percentage of employees and contractors who passed security exam	>95%	87%	Red
7	Score on last disaster-recovery test	>90%	93%	Green

Red - Immediate action required
Yellow -Caution, should be monitored
Green - OK, goal has been met

Provide a comprehensive display of all key performance indicators related to an organization's security defenses, including threats, exposures, policy compliance, and incident alerts.