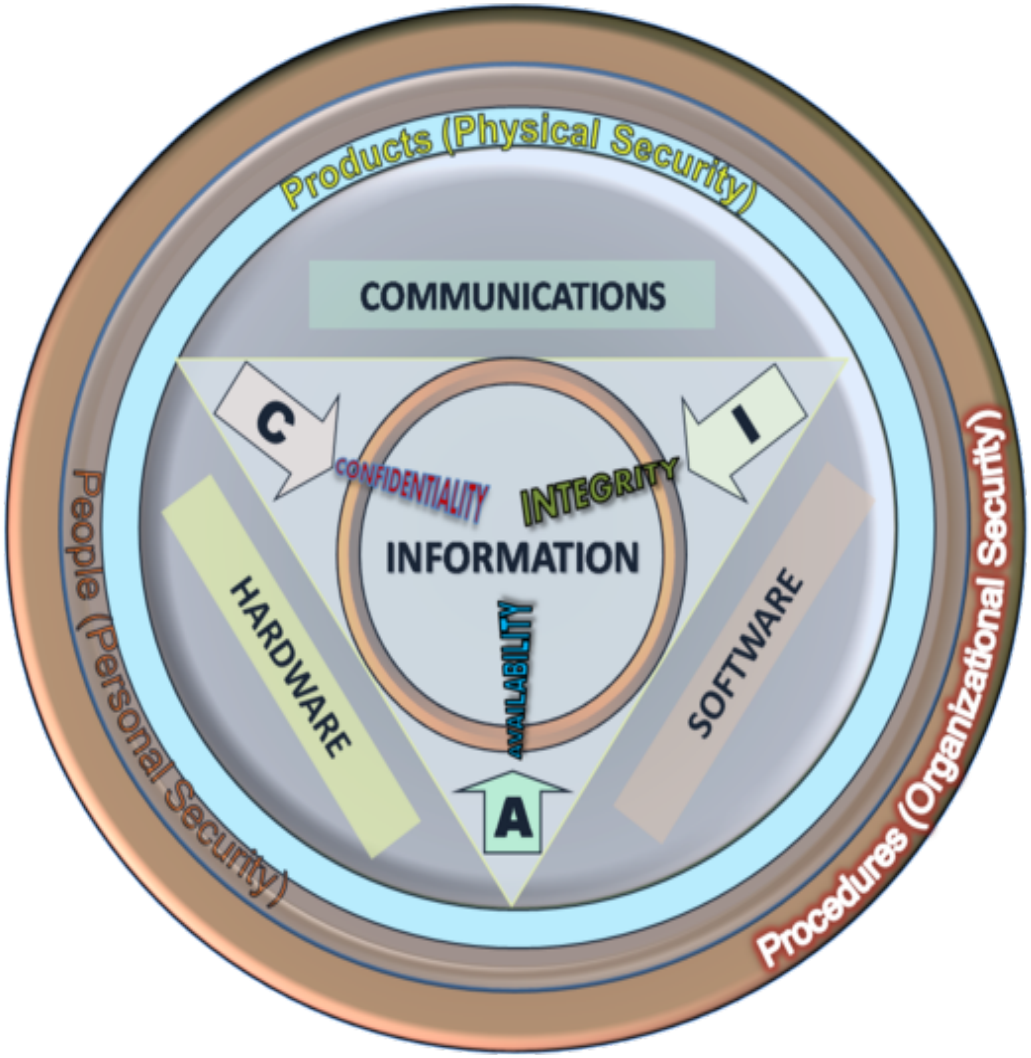
NSS

Security


Products (Physical Security)
COMMUNICATIONS
C
I
CONFIDENTIALITY
INTEGRITY
INFORMATION
AVAILABILITY
HARDWARE
SOFTWARE
A
People (Personal Security)
Procedures (Organizational Security)

Information Security Domains

Access Control

Telecommunications

Governance

Software Development

Architecture

Operations Security

Disaster Recover

Legal

Physical

Cryptography

Confidentiality

Confidentiality refers to preventing the disclosure of information to unauthorized individuals or systems.

Integrity

In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle.

Availability

For any information system to serve its purpose, the information must be available when it is needed.

Authenticity

In computing, e-Business, and information security, it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine.

Non-Repudiation

In law, non-repudiation implies one's intention to fulfill their obligations to a contract.

Controls

Administrative

Logical

Physical

Access

Preventative

Detective

Corrective

Compensating

Administrative Controls

Policies and Procedures put into place to define and guide employee actions in dealing with the organization’s sensitive information.

Technical

Devices, Processes, & Protocols to protect sensitive information

Examples include logical access systems, encryptions systems, antivirus systems, firewalls, and intrusion detection systems.

Physical Controls

Physical security controls are devices and means to control physical access to sensitive information and to protect the availability of the information.

Examples are physical access systems (fences, mantraps, guards), physical intrusion detection systems (motion detector, alarm system), and physical protection systems (sprinklers, backup generator).

Access Control

Access control is the selective restriction of access to a place or other resource.

Preventive Controls

Preventive security controls are put into place to prevent intentional or unintentional disclosure, alteration, or destruction (D.A.D.) of sensitive information.

Policy – Unauthorized network connections are prohibited.

Firewall – Blocks unauthorized network connections.

Locked wiring closet – Prevents unauthorized equipment from being physically plugged into a network switch.

Detective Security Controls

Detective security controls are like a burglar alarm. They detect and report an unauthorized or undesired event (or an attempted undesired event).

Corrective Controls

Corrective security controls are used to respond to and fix a security incident.

- Procedure to clean a virus from an infected system
- A guard checking and locking a door left unlocked by a careless employee
- Updating firewall rules to block an attacking IP address

Deterrent Controls

Deterrent security controls are controls that discourage security violations.

Compensating Controls

Compensating security controls are controls that provide an alternative to normal controls that cannot be used for some reason.

For instance, a certain server cannot have antivirus software installed because it interferes with a critical application. A compensating control would be to increase monitoring of that server or isolate that server on its own network segment.

NIST Security Controls

Management	Certification, Accreditation and Security Assessments
	Planning
	Risk Assessment
	System and Services Acquisition

NIST Security Controls

Operational	Awareness and Training
	Configuration Management
	Contingency Planning
	Incident Response
	Maintenance
	Media Protection
	Physical and Environmental Protection
	System & Information Integrity

NIST Security Controls

Technical	Access Control
	Audit and Accountability
	Identification and Authentication
	System and Communications Protections

Identification

Identification is an assertion of who someone is or what something is. If a person makes the statement "Hello, my name is John Doe" they are making a claim of who they are.

Authentication

Authentication is the act of verifying a claim of identity. When John Doe goes into a bank to make a withdrawal, he tells the bank teller he is John Doe—a claim of identity.

Authorization

After a person, program or computer has successfully been identified and authenticated then it must be determined what informational resources they are permitted to access and what actions they will be allowed to perform (run, view, create, delete, or change).

Cryptography

Information security uses cryptography to transform usable information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption.

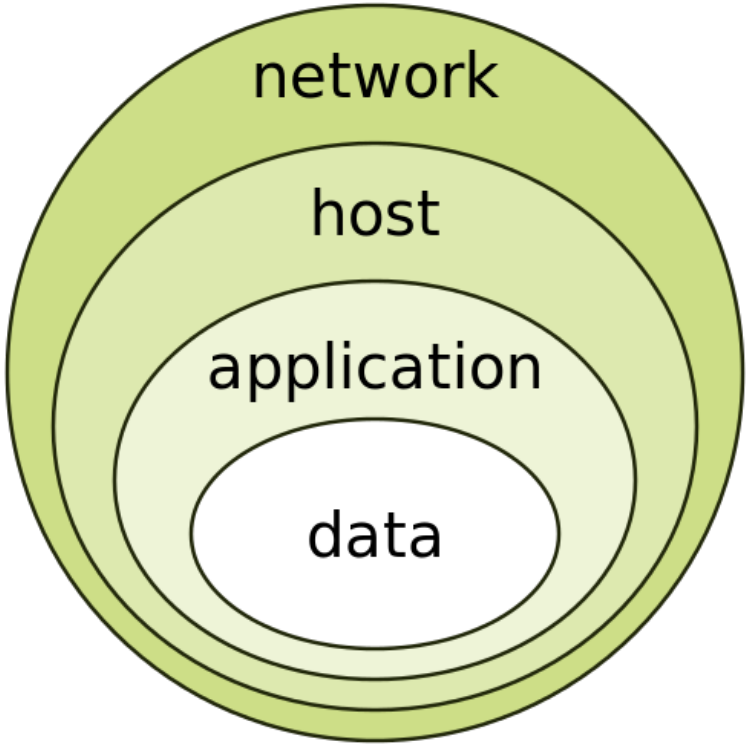
Disaster Recovery Planning

While a business continuity plan (BCP) takes a broad approach to dealing with organizational-wide effects of a disaster, a disaster recovery plan (DRP), which is a subset of the business continuity plan, is instead focused on taking the necessary steps to resume normal business operations as quickly as possible.

Incident Management

Incident management aims to restore normal service operation as quickly as possible and minimise the adverse effect on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

Defense in Depth



Common Vulnerabilities Types

Common Vulnerabilities

Memory Safety Violations

Input Validation Errors

Race Conditions

Privilege-Confusion

Privilege Escalation

User Interface Failures

Memory Safety Violations

Buffer Overflow is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory

Dangling Pointers and wild pointers in computer programming are pointers that do not point to a valid object of the appropriate type.

Input Validation Errors

Format string attacks - stems from the use of unchecked user input as the format string parameter in certain functions that perform formatting

SQL injection - malicious SQL statements are inserted into an entry field for execution

Code injection - is the exploitation of a computer bug that is caused by processing invalid data.

E-mail injection - is a security vulnerability that can occur in Internet applications that are used to send email messages.

Input Validation Errors

Directory traversal - consists in exploiting insufficient security validation / sanitization of user-supplied input file names, so that characters representing "traverse to parent directory" are passed through to the file APIs.

Cross-site scripting in web applications - XSS enables attackers to inject client-side script into Web pages viewed by other users

HTTP header injection - is a general class of web application security vulnerability which occurs when Hypertext Transfer Protocol (HTTP)headers are dynamically generated based on user input.

HTTP response splitting - is a form of web application vulnerability, resulting from the failure of the application or its environment to properly sanitize input values.

Race Condition

A **race condition** or **race hazard** is the behavior of an electronic or software system where the output is dependent on the sequence or timing of other uncontrollable events.

Race Conditions

Time-of-Check-to-time-of-use bug - is a class of software bug caused by changes in a system between the *checking* of a condition (such as a security credential) and the *use* of the results of that check.

Symlink Races - is a kind of software security vulnerability that results from a program creating files in an insecure manner.

Privilege-Confusion Bug

Cross-site request forgery in web applications - is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts

Clickjacking - is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages

FTP bounce attack - is an exploit of the FTP protocol whereby an attacker is able to use the PORT command to request access to ports indirectly through the use of the victim machine as a middleman for the request.

Privilege Escalation

Privilege escalation - is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.

User Interface Failures

Warning fatigue or user conditioning.

Blaming the Victim - Prompting a user to make a security decision without giving the user enough information to answer it

Race Conditions

Software Best Practices (from ISC^2)

- Protect the Brand Your Customers Trust
- Know Your Business and Support it with Secure Solutions
- Understand the Technology of the Software
- Ensure Compliance to Governance, Regulations, and Privacy
- Know the Basic Tenets of Software Security
- Ensure the Protection of Sensitive Information
- Design Software with Secure Features
- Develop Software with Secure Features
- Deploy Software with Secure Feature
- Educate Yourself and Others on How to Build Secure Software

Security Development Lifecycle (Microsoft)

Training

Requirements

Design

Implementation

Verification

Release

Response

Training

Assess organizational knowledge on security and privacy –establish training program as necessary

- Establish training criteria
  - Content covering secure design, development, test and privacy
- Establish minimum training frequency
  - Employees must attend n classes per year
- Establish minimum acceptable group training thresholds
  - Organizational training targets (e.g. 80% of all technical personnel trained prior to product RTM)

Requirements

Opportunity to consider security at the outset of a project

- Development team identifies security and privacy requirements
- Development team identifies lead security and privacy contacts
- Security Advisor assigned
- Security Advisor reviews product plan, makes recommendations,may set additional requirements
- Mandate the use of a bug tracking/job assignment system
- Define and document security and privacy bug bars

Design

Define and document security architecture, identify security critical components

- Identify design techniques (layering, managed code, least privilege, attack surface minimization)
- Document attack surface and limit through default settings
- Define supplemental security ship criteria due to unique product issues
  - Cross-site scripting tests
  - Deprecation of weak crypto
- Threat Modeling
  - Systematic review of features and product architecture from a security point of view
  - Identify threats and mitigations
- Online services specific requirements

Implementation

Full spectrum review – used to determine processes, documentation and tools necessary to ensure secure deployment and operation

- Specification of approved build tools and options
- Static analysis (PREFix, /analyze (PREfast), FXCop)
- Banned APIs
- Use of operating system “defense in depth” protections(NX, ASLR and HeapTermination)
- Online services specific requirements (e.g., Cross-site scripting ,SQL Injection etc)
- Consider other recommendations (e.g., Standard Annotation Language (SAL))

Verification

Started as early as possible – conducted after “code complete” stage

- Start security response planning – including response plans for vulnerability reports
- Re-evaluate attack surface
- Fuzz testing – files, installable controls and network facing code
- Conduct “security push” (as necessary, increasingly rare)
  - Not a substitute for security work done during development
  - Code review
  - Penetration testing and other security testing
  - Review design and architecture in light of new threats
- Online services specific requirements

Release - Response Plan

Creation of a clearly defined support policy – consistentwith MS corporate policies

- Provide Software Security Incident Response Plan (SSIRP)
  - Identify contacts for MSRC and resources to respond to events
  - 24x7x365 contact information for 3-5 engineering, 3-5 marketing, and 1-2 management (PUM and higher) individuals
- Ensure ability to service all code including “out of band” releases and all licensed 3rd party code.

Release - Final Security Review

Verify SDL requirements are met and there are no known security vulnerabilities

- Provides an independent view into “security ship readiness”
- The FSR is NOT:
  - A penetration test – no “penetrate and patch” allowed
  - The first time security is reviewed
  - A signoff process
  - Key Concept: The tasks for this phase are used as a determining factor on whether or not to ship – not used as a “catchall” phase for missed work in earlier phases

Release - Archive

Security response plan complete

- Customer documentation up-to-date
- Archive RTM source code, symbols, threat models to a central location
- Complete final signoffs on Checkpoint Express – validating security, privacy and corporate compliance policies

Post-SDL Requirement: Response

“Plan the work, work the plan…”

Execution on response tasks outlined during Security Response Planning and Release Phases