Chapter 01 – Security Governance Through Principles and Policies

Security 101

- What is IT?
- Is it different or the same as security?
- What is the overall goal of security?

Security 101

- IT is the hardware/software that support the operations or functions of a business
- Security is very different
- Select security controls that provide the most significant protections for the lowest resource cost
- Security is a journey, not a finish line

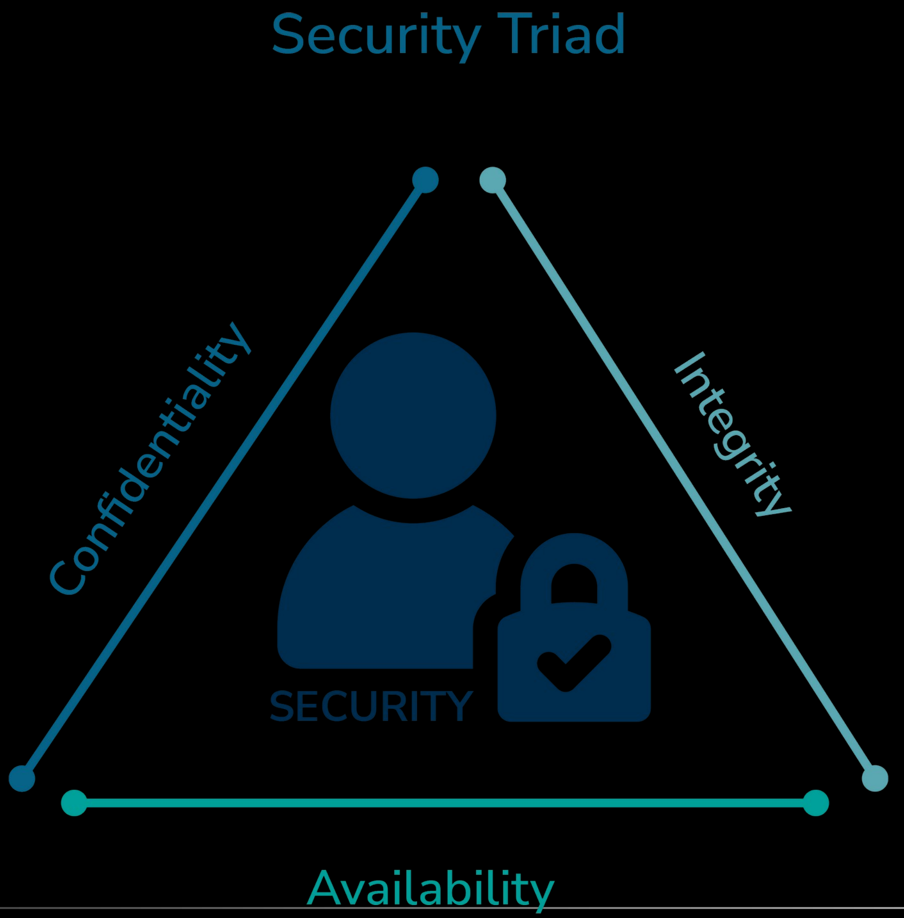
Pillars of Information Security

- Confidentiality
- Integrity
- Availability
- Authenticity
- Nonrepudiation

CIA Triad

- What is the CIA triad?

CIA Triad


Security Triad
Confidentiality
Integrity
SECURITY
Availability

Confidentiality

- What is it?
- What is the goal?
- Any Violations?
- Countermeasures?

Confidentiality

- The concept of the measures used to ensure the protection of the secrecy of data, objects, or resources
- The goal is to prevent or minimize unauthorized access to data

Confidentiality

- Violations
  - Human error
  - End user
  - System Administrator
  - Security Policy
  - Misconfigured Security Controls

Confidentiality

- Countermeasures
  - Encryption
  - Network Traffic Padding
  - Strict ACLs
  - Data Classification
  - Rigorous Authentication Procedures
  - Extensive Personnel Training

Confidentiality Vocabulary (Quizable)

- Sensitivity
- Discretion
- Criticality
- Concealment
- Secrecy
- Privacy
- Seclusion
- Isolation

Integrity

- What is it?
- What is the goal?
- Any Violations?
- Countermeasures?

Integrity

- The concept of protecting the reliability and correctness of data
- Integrity goal is to prevent unauthorized alterations of data

Integrity From 3 Perspectives

- Preventing unauthorized subjects from making modifications
- Preventing authorized subjects from making unauthorized modifications
- Maintaining the internal external consistency of objects so that their data is correct

Integrity

- Violations
  - Numerous attacks (viruses, logic bombs, unauthorized access, errors in code/applications, malicious modifications, intentional replacements, system backdoors, etc.)
  - Human error

Integrity

- Countermeasures
  - Strict ACLs
  - Rigorous authentication procedures
  - IDS
  - Object/data encryption
  - Hash verfications
  - Interface restrictions
  - Input/function checks
  - Extensive personnel training

Integrity Vocabulary (Quizable)

- Accuracy
- Truthfulness
- Validity
- Accountability
- Responsibility
- Completeness
- Comprehensiveness

Availability

- What is it?
- What is the goal?
- Any Violations?
- Countermeasures?

Availability

- The concept of authorized subjects are granted timely and uninterrupted access to objects
- Supporting infrastructure, including but limited to network, communications, access control mechanisms, and is functional while allowing authorized users to gain access

Availability

- Violations
  - Device failure
  - Software issues
  - Environmental issues
  - DoS attacks
  - Object destruction
  - Communication interruptions

Availability

- Countermeasures
  - Monitoring performance/networks
  - Firewalls
  - Redundancy
  - Backups
  - Business Continuity Planning (BCP)
  - Eliminating single point of failure

Availability Vocabulary (Quizable)

- Usability
- Accessibility
- Timeliness

DAD Triad

- What is it?

DAD Triad

- Disclosure
  - Sensitive or confidential material is accessed by unauthorized entities
- Alteration
  - Data is either maliciously or accidently changed
- Destruction
  - A resource is damaged or made inaccessible to authorized users

Overprotecting

- Is this an issue?

Overprotecting

- Yes!
- Confidentiality
  - Restriction of availability
- Integrity
  - Restriction of availability
- Availability
  - Loss of confidentiality and integrity

Authenticity

- Security concept
  - Authentic
  - Genuine
  - Originates from its alleged source

Nonrepudiation

- Security concept
  - Logs
  - Who caused what
  - Accounting

AAA Services

- Identification
- Authentication
- Authorization
- Auditing
- Accounting

Identification

- Claiming to be an identity when attempting to access a secured area or system
- This is before starting the AAA process
- Username, swiping smart card, proximity device, phrases, face, fingerprint, scanning device, etc.

Authentication

- Proving you are that claimed identity
- Providing additional information that is in line with identification
- Identification and authentication usually work in a single two-step process
- Passwords, MFA, PIN, ID code, etc.

Authorization

- Permission level of a resource and object access for a specific identity or subject
- Allow, deny aka need to know basis
- Identification and authentication are all or nothing
- Authorization is a lot of gray

Auditing

- Recording a log of the events and activities related to systems and subjects
- Audit trail to recreate
  - Events
  - IDS/IPS
  - System failure

Accounting

- Reviewing log files to check for compliance and violations in order to hold subjects accountable for their actions, especially violations of organizational security policy
- Support security decisions with legal backing

Protection Mechanisms

- Defense in Depth
- Abstraction
- Data Hiding
- Encryption

Defense in Depth

- Why is this used?
- You can think of it as layering

Abstraction

- Why is this used?
- You can think of it as not knowing all the details but still being able to use the security controls in place
- Think of it like driving a car, do you need to know all the internal parts to be able to drive the car?

Data Hiding

- Why is this used?
- You can think of it as security through obscurity

Encryption

- Why is this used?
- You can think of it as I don’t want anyone to be able to access my data

Security Boundaries

- Divisions between secure areas
- Think LANs, Internet, public/private, open areas vs closed areas etc.
- Classifications depending on the subject and what that subject can do in certain areas

Applying Security Governance

- Supporting, evaluating, defining, and directing an organization’s security efforts
- Closely related to or intertwined with corporate or IT governance
- Security is never just an IT issue
- NIST SP 800-53, NIST SP 800-100, etc. focused on military/gov but can be followed

3rd Party Governance

- External entity oversight that law, regulation, industry standards, contractual obligation, or licensing requirements mandate
- Outsource creates problems e.g. McDonalds, MGM, etc.
- Document exchange = standards meet

Documentation Review

- Process of reading the exchanged materials and verifying them against standards and expectations
- Documents not met = loss or void of ATO (Authorization to Operate)
- Managing, assessing, and addressing risk

Security Function

- Operating a business that focuses on the task of evaluating the improving security over time
- Security MUST be measurable
- Align security functions to business strategy, goals, mission, and objectives

Security Function

- Security policy
- Business case
- Top-down approach (effective)
- Bottom-up approach (rarely used)
- CIO, CISO, ISO, CSO, CTO, etc.

Security Management

- How will security be managed?
- Who will be responsible for security?
- How security will be tested?
- Who will be developing security policies?
- Who will be performing risk analysis?
- How will security education be implemented?

Security Management

- All of the previous questions is guided through a <u>management plan</u>
- The best security plan is useless without one key factor
  - Approval by senior management

Sample Three Type Plan

- Strategic Plan
- Tactical Plan
- Operational Plan

Strategic Plan

- Long-term plan that is fairly stable
- Purpose, goals, mission, and objectives of the organization
- ~ 5 year road map updated annually
- Include an annual, bi-annual, or quarterly risk assessment

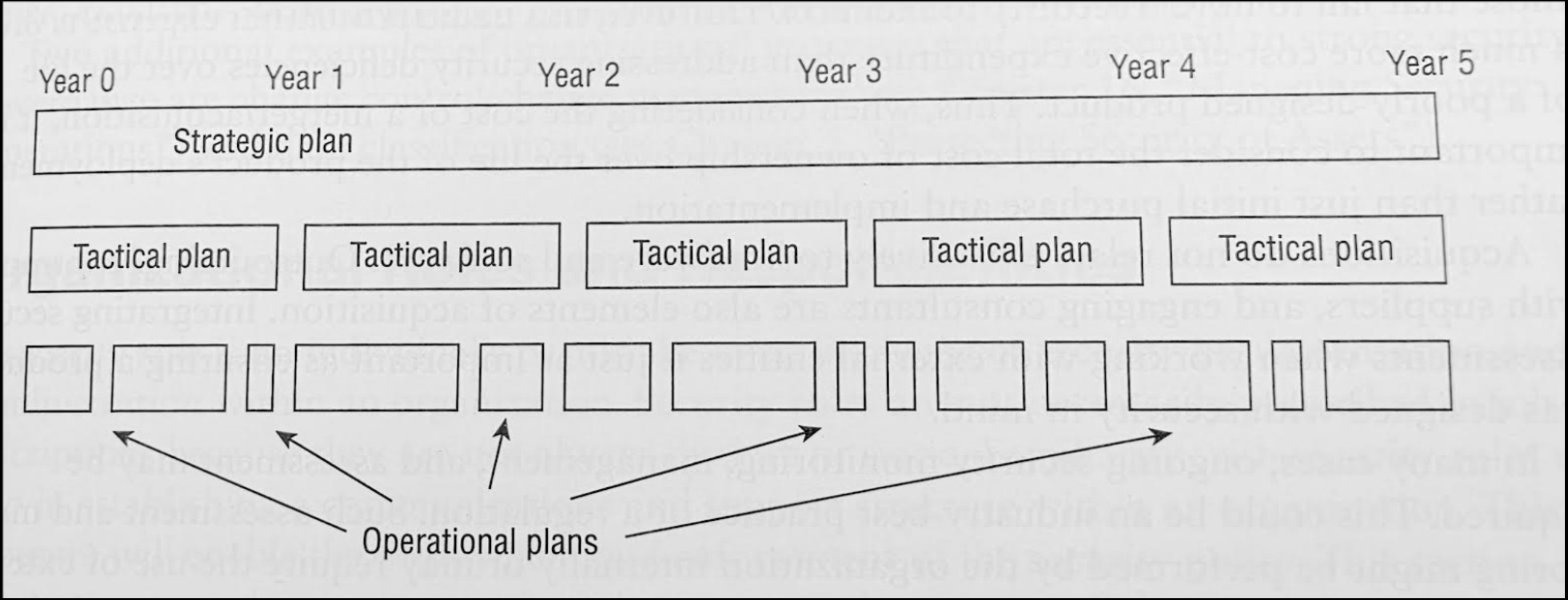
Tactical Plan

- Midterm planning with more details
- Planned or via ad hoc on events
- Good for ~1 year
- Projects, acquisitions, hiring, budget, maintenance, support, system development, etc.

Operational Plan

- Short term, highly detailed plan
- Must be updated often (monthly or quarterly)
- Retaining compliance
- Spell out how to accomplish various goals
- Training, system deployment, product design, etc.

Overall Timeline



Organizational Process

- On-Site Assessment
- Document Exchange and Review
- Process/Policy Review
- Third-Party Audit

Roles & Responsibilities

- What is a security role?
- Can you tell me how you can put that in policy and procedure?

Roles & Responsibilities

- Senior Manager
- Security Professional
- Asset Owner
- Custodian
- User
- Auditor

Security Control Frameworks

- ISO (International Organization for Standardization)
- NIST (National Institute of Standards and Technology)
- COBIT (Control Objectives for Information and Related Technologies)

Security Control Frameworks

- SABSA (Sherwood Applied Business Security Architecture)
- PCI DSS (Payment Card Industry Data Security Standard)
- FedRAMP (Federal Risk and Authorization Management Program)
- ITIL (IT Infrastructure Library)

Security Policies

- Document that defines the scope of security needed by the organization and discusses the assets that require protections and the extent to which security solutions should go to provide the necessary protection.
- Policies are broad overviews

Security Standards and Baselines

- More details and specific implementation from policies
- Standards define compulsory requirements for the homogeneous use of hardware, software, technology, and security controls
- Baseline is a minimum level of security hat every system throughout the organization must meet

Security Standards and Baselines

- Guidelines offer recommendations on how standards and baselines are implemented and serves as a operational guide for both security professionals and users
- Guidelines are flexible and should be customized

Security Procedures

- Procedures or Standard Operating Procedure (SOP) is a detailed, step by step how to document that describes the exact actions necessary to implement a specific security mechanism, control, or solution
- Final element of the formalized security policy structure

Keep Them Separate Benefits

- Not all users need to know the security standards, baselines, guidelines, and procedures for all security classification levels
- When changes occur, it is easier to update and redistribute only the affected material rather than updating a monolithic policy and redistributing it throughout the organization

Keep Them Separate Benefits

- Not all users need to know the security standards, baselines, guidelines, and procedures for all security classification levels
- When changes occur, it is easier to update and redistribute only the affected material rather than updating a monolithic policy and redistributing it throughout the organization

Threat Modeling

- Threat modeling is the security process where potential threats are identified, categorized, and analyzed
- Potential harm
- Probability of occurrence
- How to eradicate or reduce threats

Threat Modeling

- Different approaches
- Defensive approach
- Proactive approach
- Reactive approach
- IoC are involved in all cases

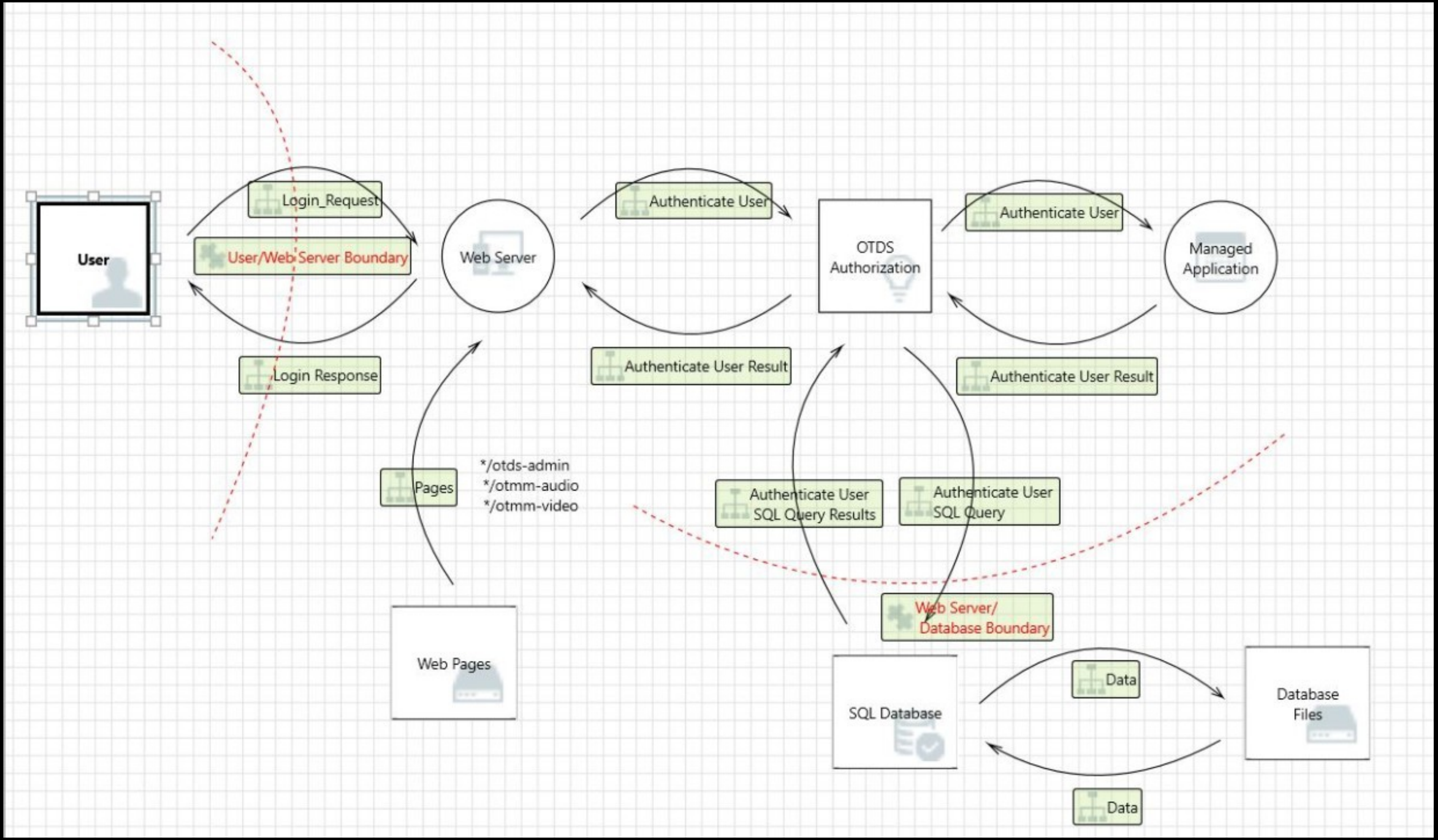
Identifying Threats

- Focused on Assets
- Focused on Attackers
- Focused on Software

Identifying Threats – STRIDE Model

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service (DoS)
- Elevation of Privilege

Diagramming Potential Attacks



Reduction Analysis

- Reduction analysis is decomposing the application, system, or environment
- Trust Boundaries – Any location where the level of trust or security changes
- Dataflow Paths – the movement of data between locations

Reduction Analysis

- Input Points – Location where external input is received
- Privileged Operations – Any activity that requires greater privileges than a standard user account or process typically required to make system changes
- Details about Security Stance and Approach – Security policy, foundation, assumptions

Prioritization and Response

- Rank/rate the threats
- Wide range of techniques
- Probability x Damage Potential
- Risk Matrix
- DREAD Rating System

Supply Chain Risk Management

- Supply Chain is the concept that most computers, devices, networks, systems, and even cloud services are not built by a single entity
- Supply Chain Risk Management (SCRM) ensure all vendors are reliable, trustworthy, reputable organization and disclose their security requirements