Security +
Risk Management

Author: Joseph Lee
Email: joseph@ripplesoftware.ca
Mobile: 778-725-3206

The Risk Formula

Risk = Probability x Vulnerability x Threat

Risk = Probability x Impact

Confidentiality
- Protecting the data from being accessed by unauthorized people

Integrity
- Data loss, destruction, non-repudiation, authenticity

Availability
- Timely reliable access to and use of information

Key Vocabulary

Risk
- The probability of a threat actor causing damage to an asset
- A combination of likelihood and impact
- As an equation **risk = probability * impact**

Risk Management
- The **science** of identifying, assessing, and categorizing risks
- Balancing resources in the best way as to mitigate risk
- Minimize the probability of **negative impact** on an organization

Probability
- Likelihood - over a period of time - of someone or something damaging assets

Reference Architecture
- Standardized vocabulary for IT security to help structure communications

Infrastructure
- Aspects of an organization including:
  - Computers
  - Networks
  - Employees

    - Departments
    - Organizational hierarchy
    - Physical security
    - Third-party access
    - Legal staff
    - Contracts
    - Policies

Threat Actor

- Anything or anyone that can cause damage such as:
    - Malicious person
    - Untrained person
    - Natural disaster

Vulnerability

- A weakness in an asset that leaves it open to a threat

Asset

- Part of an organization's infrastructure that has value such as:
    - Servers
    - Workstations
    - Other IT infrastructure
    - Physical infrastructure
    - Software applications
    - Data
    - Personnel
    - Services to customers

Vulnerability Reporting

- A communication channel for exchanging information about vulnerabilities and threats

Attack

- An attempt to take advantage of a vulnerability

Incident

- When the target recognizes an attack

Laws

- Many laws affect the design and implementation of security controls such as:
- **Health Insurance Portability and Accountability Act (HIPPA)**
    - (1996) which safeguards privacy of medical records
- **Sarbanes Oxley (SOX)**
    - (2002) Requires that companies retain critical financial records for specific periods of time

Standards

- Often required for participation in industry such as:
- **PCI-DSS Payment Card Industry Data Security Standard**
  - Which provides several highly detailed security controls to mitigate credit card fraud
  - See: https://www.pcisecuritystandards.org/
  - See: https://www.youtube.com/channel/UC7cPVL_HdnX4ZEGdYJMjOew

Best Practices
- Ruleset provided by a manufacturer on how their product should be used
- Software vendors also provided detailed best practices

Security Policies
- Documented rules determine what actions and attitudes an organization will take for certain critical aspects of their infrastructure

Acceptable Use Policy
- Create policy in the organization which outlines what employees may or may not do with resources
- Create user policy that stipulate the limitations of service for clients / users

Security Controls
- Directed actions to protect part of the infrastructure
- For example, policies such as password complexity or scheduled password changes

Baseline reporting
- Assessment of all parts of the network such as:
  - Software installed
  - Open ports and services
  - Network schematic
  - Hardware, OS, software

Code review
- A type of security assessment of examining software source code to determine how secure it is

Architecture description
- Design and organization of the information systems being used by the organization

Organizational inputs
- The sources of security controls such as laws, standards, best practices, and security policies

RMF Risk Management Concepts And Framework

- **NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle**

Approach is the de facto RMF in the IT security industry

Steps in the Risk Management Framework

Step 1: Categorize the Information Systems
- List assists and determine vulnerabilities / probabilities / impacts of loss

Step 2: Select Security Controls
- Select an initial set of baseline security controls for the information system based on security categorization

Step 3: Implement the Security Controls
- Apply the security controls

Step 4: Assess the Security Controls
- Test / assess the security controls to verify effectiveness

Step 5: Authorize Information System
- Improve and authorize the improved information system to operate

Step 6: Monitor the Security Control
- Monitor the information system on an ongoing basis checking for new vulnerabilities assessing overall performance

Security Controls

- Security controls are actions to mitigate risk of vulnerabilities being attacked
- **NIST SP 800-53** includes detailed descriptions of security controls
- Many security controls span across multiple categories

Phase Controls
- Phase controls describe in which phase of an attack a control is aimed at penetrating
- These activity phase control types are:
  - **Deterrent**
  - **Preventative**
  - **Detective**
  - **Corrective**
  - **Compensating / alternative controls**
- Some security controls can cross phases
- For example, a security camera can be classified as a deterrent and detective control

Phase Control Types
- **Deterrent Controls**
  - Used to deter a potential attacker from attempting an attack
  - Good lighting around a building, security cameras, security guards, barbed-wire
  - Also applies preventative measure such as not building a critical infrastructure on a fault-line, or flood plane

- **Preventative Control**
  - Used to prevent a successful attack and can sometimes predict attacks making them able to prevent
  - Password policies such as requiring strong passwords and enforcing periodical password changes
  - Having locks on the doors to important areas, security guards
  - Doing background checks on potential employees, and monitoring current employees with access to sensitive data
  - Some police precincts have a policy of requiring more than one officer to enter an evidence room at a time
  - Training can reduce the potential of employees doing things that they shouldn't
  - Intrusion Prevention systems IPS, OS hardening,
  - Security guards can prevent people from entering / tailgating
  - Off-boarding policies such as account disablement and inventory logging
- **Detective Control**
  - Used to detect an attack and notify appropriate people and/or take action
  - For example: an intrusion detection system, CCTV with motion detection, honeypot/honeynet, SIEM, auditing, intrusion detection systems: IDS, heuristics, security auditing
- **Corrective / Recovery Control**
  - Used to fix the problems caused by an attack
  - Used to recover from an incident or security issue (instructions and policy of what to do when a server fails due to hard-drive failure for example)
  - For example restoring backups is a common corrective control, fire suppression system, self-healing servers, quarantine for virus, APS (alternate power source) ready for critical infrastructure in case of power outage, backups and restores, fault tolerant drive systems, server clustering, antivirus software
- **Compensating / Alternate Control**
  - Used to provide temporary solution until restoration can take place
  - Attempt to fill in the gaps when other controls are not feasible or not currently available
  - For example, having a segregation of duties, alternate sites: hot/warm/cold sites

Control Types

- **Technical Controls**
  - Security controls that use technology to prevent or reduce impact of a vulnerability or attack
  - For example encryption, antivirus, firewalls, IDS/IPS, backups, requiring a minimal level of SSL/TLS, HPKP, file permissions
- **Administrative Controls**
  - Are applied to people and are built from organizational policies, guidelines, contracts, laws, etc.
  - For example, requiring testing and assessments, user-training,

certification requirements, conducting risk and vulnerability assessments, penetration testing, incident response and other planning, requiring employees to log off anytime they leave their office
    - Some administrative controls are related to software development such as SDLC, Secure DevOps, change management
    - Administrative controls are also known as **operational controls** or **management controls**
- **Physical Controls**
    - Are applied to protect physical areas and are also physical things
    - Fences, door locks, key-cards, elevator floor blockers, biometric retina scanners, signage, HVAC, fire-suppression
    - Physical controls are often closely related to technical controls since they may employ technology such as alarms

Defence In Depth / Layered Security
- Having various layers to a security system
- Physically, you may have a perimeter fence, door locks, security cameras, and finally biometrics for most sensitive areas
- For an IT network you may have **perimeter firewall**, (DMZ), application firewalls, internal firewall / NAT, host firewalls, IDS, and virus scanners

Vendor Diversity / Supply Chain Assessment
- Used to prevent single point of failure created by using a single vendor
- Using a single vendor can cause problems if a vulnerability is found in the vendors products, or if the vendor goes out of business

Control Diversity
- Using combined types of controls together to provide better security
- Do not only rely on deterrent controls, you should also use some level of detection controls

User Training
- Ensure users have received information about critical issues in order to prevent problems caused by lack of knowledge or awareness
- This may relate to any area of the organization such as:
    - Do not allow unauthorized people to tailgate
    - Do not open malicious attachments
    - Do not use your username as your password

Risk Assessment

- Create a **map of risk in order to allocate resources** in the more effective way possible
- Effectiveness means getting the most value out of the available resources
- NIST SP 800-30 describes four main steps:
    - Prepare for assessment
    - Conduct assessment:
        1. Identify threat sources and events

2. Identify vulnerabilities and predisposing conditions
3. Determine likelihood of occurrence
4. Determine magnitude of impact
5. Determine risk

- Communicate results
- Maintain assessment

Quantitative Impact

- Numerical value assigned such as dollar value

Qualitative Impact

- Intangible and generally incalculable value such as loss of brand sentiment
- When qualitative data provides limitations such as lack of data or subjective data, or when an issue has an inherently incalculable risk such as loss of reputation
- Can be scaled into a **semi-quantitative** value

Risk Register

- Scatter plot of probability and impact used to help identify threats and sort them according to value

Categories (page 350 in landscape)
Specific risk
Likelihood of occurrence
impact
Risk score
Security controls
Contingencies
Risk score with security controls
Action assigned to
Action deadline

Asset Value

- The value of the asset can be calculated to include the replacement costs and should also include associated costs of downtime, such as loss of revenue when production is halted or reduced

Exposure Factor (EF)

- The **percentage of an asset that could be lost** during a negative event
- Usually expressed as a decimal
- 0.4 = 40%
- Exposure value can be difficult to calculate
- Expert opinions "best guess" or industry statistics are examples of what can be used to calculate EF

Single Loss Expectancy (SLE)

- SLE = AV ($ asset value) x EF (exposure factor)

Annualized Rate of Occurrence (ARO)
- ARO = How many times per year you expect a negative event to take place
- Related to probability

Annualized Loss Expectancy (ALE)
- ALE = SLE x ARO

Risk Response

- Selecting security controls depends on factors such as cost, expected effectiveness, and impact on preserving value. The cost of the security control will determine if the security control will be implemented
- **Risk Mitigation**
  - Aims to reduce expected losses by reducing likelihood, through reducing exposure or reducing potential negative impact if a negative event does occur
- **Risk Transfer**
  - Is sharing burden of risk such as by purchasing insurance. Does not reduce the likelihood
- **Risk Acceptance**
  - Is after the security control has been implemented and some residual risk still exists
- **Risk Avoidance**
  - Is to change activities to not participate in some activities that present excessive risk

Business Impact Analysis (BIA) & Contingency Planning (CP)
- A business impact analysis is designed to mitigate the effects of an incident, not to prevent an incident
- Done during the preparation stage before incident happens
- The three stages described in **NIST SP 800-34** are:
  1. Determine mission / business processes and recovery criticality
  2. Identify recovery requirements
  3. Identify recovery priorities for system resources

Types of Impact
- The types of impact caused by down time can be categorized into at least five areas as follows:
- **Financial**
  - Lost or delayed sales, increased expenses, overtime, outsourcing, and fines
- **Reputation**
  - Lost sentiment in the customer, user, or employee, or greater community (translates to financial)
- **Property**
  - Loss of any type of physical property such as security cameras, real-

estate, intellectual property (data)
- **Safety / Life**
  - Be careful, your employees and customers lives depend on you
- **Privacy**
  - Legal responsibility to secure personal data properly
  - **Privacy Impact Assessment's (PIA)**
    - Goal is to ensure the system is complying with local laws, regulations, and guidelines and **privacy threshold assessment (PTA)**
    - Locate personal data within the organization and workflow in order to identify the legal requirements and develop a control to manage the risk
  - The goal is to ensure the system is in compliance throughout it's lifecycle with the regulations with respect to any PII or PHI that the organization holds

Calculating Downtime
- **MTBF Mean time between failure**
  - Average time between failures
  - Assumes product will be repaired
- **MTTF Mean time to failure**
  - Total operation time / lifecycle
- **MTTR Mean time to recovery / repair**
  - Total amount of corrective time to recover from failure
  - Includes shipping and repair time
  - In fault-tolerant design includes the latent time before the fault is discovered
- **RTO Recovery time objective**
  - Is the maximum amount of time that a resource may remain unavailable before an unacceptable negative impact affects other business critical system resources
- **RPO Recovery point objective**
  - Is the difference between the time of the incident and the time represented by the most recent backup
  - The backups should be scheduled such that the data recovery point does not cause extra-ordinary actions (such as re-doing much work, or calling customers)
  - The lower the recovery point objective the better

Data Security and Privacy Policies
- **Organizing Data by Type**
- **Classifying Data Sensitivity Level**
  - Classify data into levels of security such as public, and various levels of classified data based sensitivity to exposure
- **Security Objectives** - Low - Moderate - High

Commercial Data Security Access Labels
- Confidential
- Private

- Proprietary
- Public
- Internal use
- Sensitive
- Restricted

Government / Military Labels
- Top Secret
- Secret
- Confidential

Roles
- **Data owner**
  - Legal ownership of the dataset, copyrights, trademarks
- **Data custodian**
  - Technical aspect of the data set are in good order
- **Data Steward**
  - Data steward creates the data schematics, makes sure data requirements are met in terms of schematics, define metadata requirements, and defined access portals
- **Privacy Officer**
  - Performs due diligence to conform to all laws and regulations

Legal and Compliance
- **Personally Identifiable Information (PII)**
  - Names, alias
  - Phone numbers, SSN, passport number, driver's licence, tax, bank accounts, credit-card number
  - Address information
  - Personal characteristics
  - Date of birth, place of birth, medical information, education information, financial information

BCP Business Continuity Plan

- **Helps an organization predict and plan for potential outages of critical services**

BIA Business Impact Analysis
- Identify critical systems / functions
- Identify dependencies related to these critical systems / functions
- What is the maximum downtime limit of these critical systems / functions
- What scenarios could impact these systems / functions (fire, attacks, power outage, flood, earthquake)

Impacts
- Loss of life
- Loss of property

- Reduction in safety for personnel or property
- Potential financial losses to the organization
- Losses to the organizations reputation

Recovery Sites

- **Hot site**
  - Available 24/7 as a backup location site, can take over full functionality quickly
- **Warm site**
  - Between hot and cold sites designed to meet the organizations specific priorities and save costs
  - Configuration of the site can vary widely between organizations
- **Cold site**
  - Power and internet connectivity
  - The organization brings all system infrastructure to the site upon activation
- **Mobile site**
  - Self-contained transportable unit with outfitted with specific systems to meet requirements of an impacted system / function
- **Mirrored site**
  - Are identical to the primary location and provide 100 percent availability
- **Order of restoration**
  - Organizations would restore the most critical functions first
- **DRP Disaster recovery plan**
  - Includes a hierarchal list of critical systems and instructions to restore functionality
  - Activate the disaster recovery plan
  - Implement contingencies
  - Recover critical systems
  - Test recovered systems
  - Test recovered systems
  - After action report

Testing Plans

- **Tabletop exercise** (desktop exercise / structured -walk-though)
  - **Meeting based approach** to reviewing the stages of the recovery
- **Functional exercise**
  - **Simulated operational environment** is used to test the continuity **BCP/DRP**

Incident Response Plan

Security Incident

- An event that can negatively affect **confidentiality, integrity, or availability** of data or systems

Incident Response Policy

- Is a policy on how to respond to security incidents

- These policies are reviewed on a routine schedule, or in response to an incident such as to include lessons learned from the incident

IRP Incident Response Plan

- Provides more details than the **incident response policy**
- A more formal coordinated plan:
  - Definitions of incident types
  - Cyber-incident response teams
  - Roles and responsibilities
  - Escalation
  - Reporting requirements
  - Exercises

Incident Response Process

- **Preparation**
  - Occurs before the incident and provides guidance
  - This can include mitigation controls
- **Identification**
  - Verification of the incident as being valid incident, **and not a false positive**
- **Containment**
  - Isolate or contain the incident by quarantining / removing from the network
- **Eradication**
  - Remove all remnants of the attack such as malware on systems, removing compromised accounts, etc.
- **Recovery**
  - Return all affected systems to normal functionality
- **Lessons learned**
  - Share the individual experience, strengths, weaknesses and note potential improvements