CompTIA

Security+

SY0 - 601

19- Summarizing Risk Management Concepts

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Outlines

19.1- Explain Risk Management Processes and Concepts

19.2- Explain Business Impact Analysis (BIA) Concepts

19.1- Explain Risk Management Processes and Concepts

19.2- Explain Business Impact Analysis (BIA) Concepts

RISK MANAGEMENT PROCESSES

- Risk management is a process for identifying, assessing, and mitigating vulnerabilities and threats to the essential functions that a business must perform to serve its customers.
- You can think of this process as being performed over **five** phases:
  1. Identify mission essential functions—mitigating risk can involve a large amount of expenditure so it is important to focus efforts, Effective risk management must focus on mission essential functions that could cause the whole business to fail if they are not performed.
  2. Identify vulnerabilities—for each function or workflow (starting with the most critical), analyze systems and assets to discover and list any vulnerabilities or weaknesses to which they may be susceptible.

RISK MANAGEMENT PROCESSES (cont.)

3. Identify threats—for each function or workflow, identify the threat sources and actors that may take advantage of or exploit or accidentally trigger vulnerabilities.
4. Analyze business impacts—the likelihood of a vulnerability being activated as a security incident by a threat and the impact of that incident on critical systems are the factors used to assess risk.
5. Identify risk response—for each risk, identify possible countermeasures and assess the cost of deploying additional security controls, Most risks require some sort of mitigation, but other types of response might be more appropriate for certain types and level of risks.

RISK TYPES

- External
  - ✓ External threat actors are one highly visible source of risk.
  - ✓ You must also consider wider threats than those of cyberattack.
  - ✓ Natural disasters, such as the COVID-19 pandemic, illustrate the need to have IT systems and workflows that are resilient to widespread dislocation.
  - ✓ The most critical type of impact is one that could lead to loss of life or critical injury. The most obvious risks to life and safety come from natural disasters, person-made disasters, and accidents, such as fire.

- Internal
  - Internal risks come from assets and workflows that are owned and managed by your organization.
  - Internal threats can include contractors who were granted temporary access.

RISK TYPES (cont.)

- Multiparty
  - ✓ Multiparty risk is where an adverse event impacts multiple organizations.
  - ✓ Multiparty risk usually arises from supplier relationships.

- Intellectual Property (IP) Theft
  - ✓ Intellectual property (IP) is data of commercial value that is owned by the organization.
  - ✓ This can mean copyrighted material for retail (software, written work, video, and music) and product designs and patents.
  - ✓ If IP data is exfiltrated it will lose much of its commercial value.

RISK TYPES (cont.)

- Software Compliance/Licensing
  - ✓ Breaking the terms of the **end user licensing agreement (EULA)** that imposes conditions on installation of the software can expose the computer owner to substantial fines.

- Legacy Systems
  - ✓ Legacy systems are a source of risk because they no longer receive security updates and because the expertise to maintain and troubleshoot them is a scarce resource.

QUANTITATIVE RISK ASSESSMENT

- There are **quantitative** and **qualitative** methods of performing risk analysis to evaluate likelihood and impact.
- **Quantitative** risk assessment aims to assign concrete values to each risk factor.
    - ✓ Single Loss Expectancy (SLE)— the amount that would be lost in a single occurrence of the risk factor, This is determined by multiplying the value of the asset by an Exposure Factor (EF), EF is the percentage of the asset value that would be lost.
    - ✓ Annualized Rate of Occurrence (ARO)— how many times of occurrence in a year.
    - ✓ Annualized Loss Expectancy (ALE)— the amount that would be lost over the course of a year. This is determined by multiplying the **SLE** by the **ARO**.

QUALITATIVE RISK ASSESSMENT

- **Qualitative** risk assessment avoids the complexity of the quantitative approach and is focused on identifying significant risk factors.
- The qualitative approach seeks out people's opinions of which risk factors are significant.
- Assets and risks may be placed in simple categories.
- For example, Assets could be categorized as **Irreplaceable**, **High Value**, **Medium Value**, and **Low Value**.
- Risks could be categorized as **one-off** or **recurring** and as **Critical**, **High**, **Medium**, and **Low probability**.

RISK AVOIDANCE

- Avoidance
  - ✓ Means that you stop doing the activity that is risk-bearing.
  - ✓ **For Example:** a company may develop an in-house application for managing inventory and then try to sell it.
  - ✓ If while selling it, the application is discovered to have numerous security vulnerabilities that generate complaints and threats of legal action, the company may make the decision that the cost of maintaining the security of the software is not worth the revenue and withdraw it from sale.
  - ✓ Obviously this would generate considerable bad feeling among existing customers.
  - ✓ Avoidance is not often a credible option.

RISK TRANSFERENCE AND RISK ACCEPTANCE

- Transference (or sharing)
  - ✓ Means assigning risk to a third party, such as an insurance company or a contract with a supplier that defines liabilities.
  - ✓ **For Example:** a company could stop in-house maintenance of an e-commerce site and contract the services to a third party, who would be liable for any fraud or data theft.

- Risk Acceptance
  - ✓ Risk acceptance (or tolerance) means that no countermeasures are put in place either because the level of risk does not justify the cost or because there will be unavoidable delay before the countermeasures are deployed.
  - ✓ In this case, you should continue to monitor the risk (as opposed to ignoring it).

19.1- Explain Risk Management Processes and Concepts

19.2- Explain Business Impact Analysis (BIA) Concepts

BUSINESS IMPACT ANALYSIS

- Business impact analysis (BIA)
  - ✓ Is the process of assessing what losses might occur for a range of threat scenarios.
  - ✓ For instance, if a DDoS attack suspends an e-commerce portal for five hours, the business impact analysis will be able to quantify the losses from orders not made and customers moving permanently to other suppliers based on historic data.
  - ✓ The likelihood of a DoS attack can be assessed on an annualized basis to determine annualized impact, in terms of costs.
  - ✓ You then have the information required to assess whether a security control, such as load balancing or managed DDoS mitigation, is worth the investment.

MISSION ESSENTIAL FUNCTIONS

- Maximum tolerable downtime (MTD)
  - ✓ Is the longest period of time that a business function outage may occur for without causing irrecoverable business failure.
  - ✓ Each business process can have its own MTD, such as a range of minutes to hours for critical functions, 24 hours for urgent functions, seven days for normal functions, and so on.
  - ✓ MTDs vary by company and event.
  - ✓ **For Example:** an organization specializing in medical equipment may be able to exist without incoming manufacturing supplies for three months because it has stockpiled a sizable inventory, After three months, the organization will not have sufficient supplies and may not be able to manufacture additional products, therefore leading to failure, In this case, the **MTD** is **three months**.

MISSION ESSENTIAL FUNCTIONS (cont.)

- Recovery time objective (RTO)
  - ✓ Is the period following a disaster that an individual IT system may remain offline.
  - ✓ This represents the amount of time it takes to identify that there is a problem and then perform recovery (restore from backup or switch in an alternative system, for instance).

- Work Recovery Time (WRT)
  - ✓ Following systems recovery, there may be additional work to reintegrate different systems, test overall functionality, and brief system users on any changes or different working practices so that the business function is again fully supported.

SINGLE POINTS OF FAILURE

- Each IT system will be supported by hardware assets, such as servers, disk arrays, switches, routers, and so on.
- Reducing dependencies means the system design can more easily eliminate the sort of weakness that comes from these devices becoming single points of failure (SPoF).
- A SPoF is an asset that causes the entire workflow to fail if it is damaged or otherwise not available.
- SPoFs can be mitigated by provisioning redundant components.

SINGLE POINTS OF FAILURE (cont.)

- Mean time to failure (MTTF) and Mean time between failures (MTBF) represent the expected lifetime of a product.
- MTTF should be used for non-repairable assets.
- **For Example:** a hard drive may be described with an **MTTF**, while a server (which could be repaired by replacing the hard drive) would be described with an **MTBF**.
- The calculation for MTBF is the total time divided by the number of failures.
- **For Example:** if you have **10** devices that run for **50** hours and two of them fail, the MTBF is **250** hours (10*50)/2.
- The calculation for MTTF for the same test is the total time divided by the number of devices, so (10*50)/10, with the result being **50** hours.

SINGLE POINTS OF FAILURE (cont.)

- Mean time to repair (MTTR)
  - ✓ Is a measure of the time taken to correct a fault so that the system is restored to full operation.
  - ✓ This can also be described as mean time to "replace" or "recover".
  - ✓ This metric is important in determining the overall recovery time objective (RTO).

DISASTERS

- a disaster is an event that could threaten mission essential functions.
- For example, a privacy breach is a critical incident, but it is probably not a direct threat to business functions.
- An earthquake that destroys a data center is a disaster-level event.
- Disaster response involves many of the same principles and procedures as incident response, but at a larger scale.
  - ✓ Internal or External
  - ✓ Person-Made
  - ✓ Environmental

DISASTER RECOVERY PLANS

- Disaster recovery plans (DRPs) describe the specific procedures to follow to recover a system or site to a working state following a disaster-level event.
- The DRP should accomplish the following:
    1. Identify scenarios for natural and non-natural disaster and options for protecting systems.
    2. Identify tasks, resources, and responsibilities for responding to a disaster.
    3. Train staff in the disaster planning procedures and how to react well to change.