Risk Management - The Process

Objectives:

At the end of this episode, I will be able to:

Understand what risk management is.

Explain the different phases of the risk management process.

Identify the different steps involved in the risk management process.

Define what a risk management plan is.

External Resources:

Risk Management - The Basics

What is Risk Management?

A set of policies and procedures to identify, assess, prioritize, minimize, and control risks.

Listed below are the objectives of risk management:

```
▪ Identifying potential risks the organization faces
▪ Identify the impact of risks and help the organization develop better risk
management strategies and plans
▪ Prioritize the risks depending on the impact/severity of the risk through
the use of established risk management methods, tools, and techniques
▪ Understand and analyze the risks and report identified risk events
▪ Control the risk and mitigate the risk effect
▪ Create awareness among the security staff
▪ Develop strategies and plans for risk management
```

NOTE: Risk management is a continuous process performed by achieving goals at every phase. Applied across the ENTIRE organization in strategic and operational contexts.

The risk management process includes the following phases: (3)

1. Risk Assessment - identification of risks, estimation of impact, and determining sources to recommend proper mitigation measures.

Identification of risk is the initial step of the risk management plan.

The risk assessment process involves identifying the hazard(s), determining its impact, risk evaluation and mitigation development, documenting the results, and updating the risk assessment continuously.

2. Risk Mitigation - prepare for handling risks and reduce its impact on organizations. This phase addresses and treats the risk according to their severity level. It estimates the potentiality of each risk to prioritize them and reduce their impact.

3. Risk Management Plan Evaluation - It is important for organizations to update the risk management plan on a regular basis as risks can change due to the change in business strategies, policies, and operations.

Steps involved in the risk assessment process: (9)

1. System Characterization: Identify all the resources and infrastructure boundaries

2. Threat Identification: List all the possible threat sources applicable to the critical IT assets

3. Vulnerability Identification: List all the vulnerabilities that can be maliciously exploited by threat sources

4. Control Analysis: Identify and analyze the existing controls (The output of this step includes the list of all existing and planned security controls used to eliminate the likelihood of a threat source exploiting system vulnerabilities)

5. Likelihood Analysis: Evaluate the likelihood of attacks and consequences (The output of this step is the likelihood rating of a potential vulnerability being exploited by a threat source)

```
    Risk Likelihood and Consequence.xlsx
```

6. Impact Analysis: Analyze the financial and operational impact of a threat to the business (Qualitative vs Quantitative)

   Quantitative - measures "tangibles" | Numerical assessment

   Annualized Loss Expectancy (ALE) = Single Loss Expectancy (SLE) * Annual Rate Occurrence (ARO)

   ```
   SLE * ARO = ALE
   ```

   $ 1,000.00 * 3 = $3,000

```
Qualitative - measures "intangibles" | the product of likelihood and impact
produces the level of risk. The higher the risk level, the more immediate the
need for the organization to address the issue. (Risk Matrix)
```

7. Risk Determination: Determine the risk based on likelihood, impact, and capability of security controls

(To measure the risk, it is important to define the risk levels and risk matrix;
The output of this step is the identification of risk levels)

The risk level is an assessment of the resulted impact on the network.

To analyze risks, you need to work out the frequency or probability of an incident happening (likelihood) and the consequences it would have.

This is referred to as the level of risk.

Incident responders can represent and calculate the risk levels using the following formula:

```
Level of risk = consequence × likelihood
```

There are five risk levels:

```
1. Insignificant
2. Minor
3. Moderate
4. Major
5. Severe
```

NOTE: Remember that control measures decrease the level of risk, but do not always eliminate it.

A risk matrix is used to scale risk by considering the probability, likelihood, and consequence/impact of the risk.

How do we "TREAT" Risk? -

```
▪ Accept
▪ Avoid
▪ Transfer
▪ Mitigate (Minimize)
```

8. Control Recommendation: Recommend controls based on the likelihood, impact, and criticality of risk to/for business operations

The seven main types of control are:

```
1. Directive: specify acceptable rules of behavior within an organization

2. Deterrent: discourage people from violating security directives

3. Preventive: stop a security incident or information breach

4. Compensating: substitute for the loss of primary controls and mitigate risk
down to an acceptable level

5. Detective: signal a warning when a security control has been breached

6. Corrective: remedy circumstance, mitigate damage, or restore controls

7. Recovery: restore conditions to normal after a security incident
```

9. Risks Assessment Report: Present the results of the risk assessment formally

==========

What is the Risk Management Plan? -

Designed to identify, eliminate, or mitigate the risks that can cause damage to the organizational network and systems.

It contains predictions about various cyber risks that might affect, their impacts, and how to respond to those risks.

NOTE: Reviewing a risk management plan regularly is necessary in order to identify new risks and to monitor the efficiency of risk treatment strategies employed by the organization.