Information Assurance/Risk Management

An analysis by Kristof Marsolais

Information security risk identification

The process of risk identification requires several steps before moving on to the acceptance stage.

- When it comes to assets, we should categorize, classify, identify, inventory, prioritize, and value them.
- We need to identify and prioritize threats
- Most importantly, clarify the asset vulnerabilities

We also must understand the definition of risk governance.

- "Risk governance is the way that societies make collective decisions about technologies, about activities that have uncertain consequences" (ESSPmsu, 2012)

Within these societies are four groups. There are government

Information security risk identification

Risk appetite defines the quantity and nature of risk that organizations are willing to accept as they evaluate the trade-offs between perfect security and unlimited accessibility (Whitman & Mattord, 2018, p. 259).

There are a variety of threats that can threaten a business. Here ar some examples:

- Natural disasters
- Theft
- Human error
- Compromised intellectual property

Information security risk identification

- A hypothetical risk scenario I can make is using an unofficial video editing software at a cheaper price vs a renowned video editing software at an expensive price for my streaming business:
  - Professional Video editing software
    - Pro: Reliable software with a backup file for media software
    - Con: Expensive
  - Unofficial video editing software
    - Pro: Cost effective and relatively easy to access
    - Con: Unsafe network, possibly vulnerable
  - Conclusion: The Professional Video software would be costly but it would relieve the viewers if the content was guaranteed rather than halted by a hacker with nothing better to do

Information security risk assessment

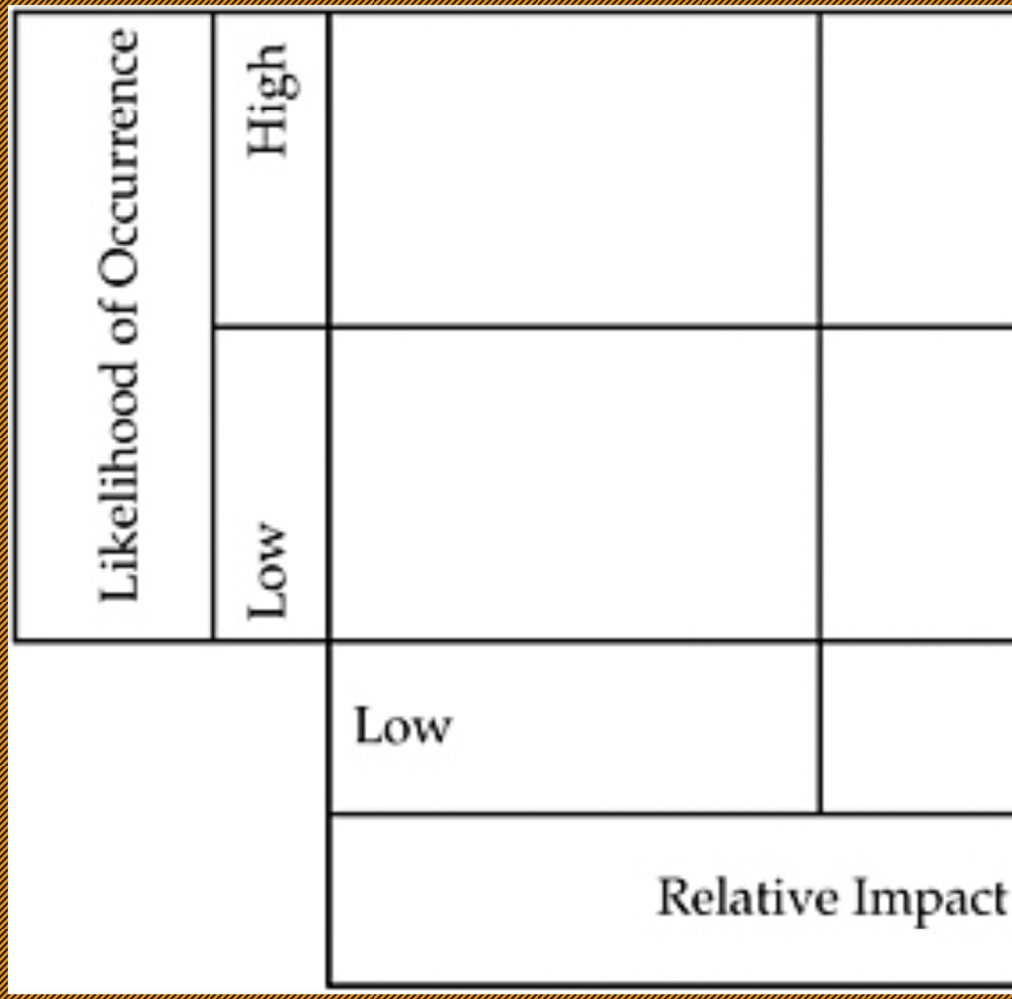
- The formula of risk is the probability of a successful attack on the organization (Loss Frequency = Likelihood * Attack Success Probability) * the Expected Loss from a Successful Attack (Loss Magnitude = Asset Value * Probable Loss) + The Uncertainty of Estimates of All Stated Values (Whitman & Mattord, 2018, p. 283).
- Quantitative analysis usually focuses on mathematical and probability formulas to calculate time and loss that risks often cos in the business environment.

Information security risk assessment

- There are four methods of handling risk:
  - Acceptance
  - Mitigation
  - Termination
  - Transfer
- Depending on the severity of the risk, these controls will be applied accordingly.

Information security risk assessment (dealing with risk controls)

- Using a qualitative method of risk assessment like this, you can place certain components in charts like these.
- If the likelihood and impact of a risk are both low, it's a practice that is not detrimental to the business. If they are both high, you might want to terminate the practice (National Research Council, 2015).
- Depending on the High/Low or Low/High ranking of factors, you may choose to mitigate or accept a given practice.



Information security risk response and mitigation

- Inherent risks are risks that are natural and controls are usually not placed on the risk because of unique scenarios.
- Residual risks are risks that are still lingering despite the fact that controls have been established for the risks.

Information security risk response and mitigation

These are the risk elements with their corresponding plans (Whitman & Mattord, 2018, p. 295):

- Risk acceptance: is basically acknowledging the risks that the practice will create.
- Risk mitigation: is the attempt to reduce a risk's ability to damage an asset to a minimum or null level.
- Risk Termination: is the cancellation of a given practice because the risks were deemed too high and therefore a hinderance to continue following.
- Risk Transference: is the attempt to take the risk of one asset and switch it to another asset that would not affect it or the company.

Information security risk control monitoring

- Key risk indicators are metrics to demonstrate how damaging a specific risk can be. By determining this, you can analyze the potential of a risk before it occurs, essentially creating a warning system for that given risk (Marr, 2018).
- Key performance indicators are essentially a way to measure a company's performance through its companies, business units, projects, and employees (Marr, 2018).

Information security risk control monitoring

- Risk policy is the combination of risk action plans, guidelines for the corporation and procedures for the business to implement them (IRM, 2019).
- The Institute of Risk Management (IRM) has an excellent chart example with four different levels in the horizontal level of its IRM chart: Leadership, Senior, Management, and Support
- The vertical part of the chart shows Policy, Roles and Responsibilities – see chart on next slide.

https://www.theirm.org/about/professional-standards/strategy-and-performance/risk-management-policy-and-procedures

	Leadership level	Senior level	Management level	Support level
Policy	Develops a risk management policy that is consistent with the risk management strategy.	Implements plans and priorities to deliver risk management policy within agreed timescales and budgets.	Explains the purpose, role and benefits of embedding risk management policy and procedures into organisational policies and procedures.	Explains the purpose of risk management policy and procedures and its components.
Roles and responsibilities	Defines risk management accountabilities and methodologies that meet strategy requirements.	Implements risk management policy ensuring that ownership and responsibilities are fulfilled within authority limits.	Advises on the appropriate use of methodologies, tools and techniques within the context of the risk policy.	Explains the features of methodologies, tools and techniques and their uses.
Resources	Secures commitment and resources that will enable the implementation of the risk strategy.	Reviews the effectiveness of risk management policy and processes and the use of resources and makes recommendations.	Uses a range of resources to analyse management information to support recommendations for improvements to risk management policies and procedures.	Provides management information to support improvements to risk management policies and procedures.

References

- References
- ESSPmsu. (2012, February 27). Ortwin Renn on risk governance [Video file]. Retrieved from https://www.youtube.com/watch?time_continue=27&v=lnPbpiZ0DLw
- IRGC. (2019). What is Risk Governance? - IRGC. Retrieved from https://irgc.org/risk-governance/what-is-risk-governance/
- IRM. (2019). Risk management policy and procedures. Retrieved from https://www.theirm.org/about/professional-standards/strategy-and-performance/risk-management-policy-and