Risk and Security Planning

Cristina Laing

Cybersecurity Principles

CYSE 600

August 6, 2021

Dr. George Mikulski

Authors Note

This is my own work and has been done solely by me. This paper has been written for the Old Dominion University's CYSE-600 Cybersecurity Principles class and not used for any other purposes.

Cristina Laing

Abstract

This paper introduces the topic of risk management or risk analysis in conjunction with security planning. The paper explains why risk management/analysis is essential to organizations developing a security plan—issues and challenges of risk management and security planning. The focus of this paper is an analytical review of a peer-reviewed paper that examines risk assessment. The paper will be summarized and discussed briefly.

Risk and Security Planning

Introduction

Risk is defined as a possibility of loss or injury (Merriam-Webster, n.d.). Most of us want to avoid risks. Yet, we make quick decisions based on time, and convenience, every day. For example, most lock doors and purchase security for our homes based on the risk of theft in our personal lives. In our professional lives, we also use risk analysis to make decisions. For example, when planning a project or preparing for an event, we consider several variables such as people, location, safety, laws, policies, and possible negative scenarios. Knowing the risks helps us make the best decisions with the knowledge at hand.

Enterprises, organizations, and governments also use risk analysis to anticipate and reduce harmful results from adverse events (Rosencrance, 2021). Adverse events include natural disasters (i.e., earthquakes, hurricanes, fires, and floods), human error (i.e., fires, floods, erasure, and accident), and malicious human activity (i.e., malware, fire, flooding, and explosion). The risk analysis process helps identify the potential for harm and the likelihood of the harmful event happening. Yet, risk analysis is not only about avoiding all risks because avoiding all threats is impossible. Instead, risk analysis helps an organization understand the risk so they can prevent, if possible, share the risk with a third party (i.e., insurance company), accept risk (i.e., when risk cannot be mitigated), organize risk, and control risk.

Not everyone is on the risk analysis and security planning side. Some who argue against risk analysis give the reasons below:

- False sense of precision and confidence
- Hard to perform
- Immutability

- Lack of accuracy

The above are great points to ponder, and they are not the only challenges that the practice of risk analysis faces. The following section is research by E. Zio from the University of Paris-Saclay, exploring changes and innovations that pose challenges to risk assessment.

Literature Review

Author Zio advises that the field of risk assessment must evolve to adequately address existing and future challenges and considering new technology, systems, and networks. The author states that digitalization brings opportunities but also the complexity of cyber-physical systems (Zio, 2018). Climate change and extreme natural events are increasingly threatening our infrastructures; terrorist and malevolent threats are posing severe concerns for the security of our systems and lives (Zio, 2018). These sources of hazard are extraordinarily uncertain and, thus, difficult to describe and model quantitatively (Zio, 2018).

Nevertheless, though challenging to assign likelihoods, the author expresses that quantitative measures remain essential for rational, effective decision-making when combined with evidential knowledge and subjective beliefs (Zio, 2018). The author's findings led to a list of steps that may improve risk assessments.

- Using simulation for accident scenario identification and exploration and relying on data for condition monitoring-based, dynamic risk assessment (Zio, 2018).
- Increasing modeling and computational capabilities and data availability for mining knowledge and improving models (Zio, 2018).
- Frameworks of integration of the condition data-driven predictive models into the risk assessment model must be soundly developed and practically implemented for actual industrial benefit (Zio, 2018).

- Safety mindfulness and adaptive thinking (Zio, 2018).

Discussion

The paper, the future of risk assessment, is a well-thought-out study of the future of the risk assessment field. The author is aware that the study does not give an absolute point of view or present a solution to the problem. The value of the paper is that it offers a lookout for risk assessment, presents considerations, and incites discussion. The author warns about adverse events like climate change and terrorism as extreme and uncertain events challenging to describe and model.

The author also points out that technology such as the internet of things (IoT) and big data, the industrial internet, are changing the way we design, manufacture, supply products and services, the way we move and live in our environment (Zio, 2018). This creates a complex network of things and people that are seamlessly connected and communicating (Zio, 2018). It provides opportunities to make production systems and services more efficient, faster, and more flexible and resilient complex supply chains and distribution networks that tie the global economy (Zio, 2018). Nevertheless, these advances also create liability and create a large surface for attack.

Summary

Risk analysis is a valuable practice, and it is doubtful that enterprises and organizations will stop using the process to make better decisions or create competent security plans. So risk assessment is considered a key component of business that several government agencies provide free templates of risk assessments for companies and individuals to use as a guide. Considering risk can become overwhelming and create feelings of helplessness. Yet, it is vital to keep in mind that being informed and in the know fosters control. Knowing what an organization might be against can help prioritize mitigation and employ safety controls. The benefits of a well-

researched security plan outweigh any argument against risk analysis. Knowing what is in line can save an organization downtime and money when an adverse event takes place. An organized organization with a speedy recovery from an adverse event looks more competent to the outside world.

References

Merriam-Webster. (n.d.). Risk. In Merriam-Webster.com dictionary. Retrieved August 6, 2021, from https://www.merriam-webster.com/dictionary/risk

Rosencrance, L. (2021). What is risk analysis? Tech Target. What is Risk Analysis? - Definition from SearchSecurity.com (techtarget.com)

Zio, E. (2018). The future of risk assessment. Reliability Engineering & System Safety, 177, 176-190.