The Major Factors That Influence The Development Of Risk Management Plans

Zyron James Sumulong

zsumu001@odu.edu

Old Dominion University

IDS 300W: Interdisciplinary Theory and Concepts

Dr. Kat LaFever

June 18, 2023

Abstract

This interdisciplinary research paper investigates the major factors that influence cybersecurity auditors when developing a risk management plan, drawing insights from the disciplines of cybersecurity, psychology, and law. This paper aims to provide a comprehensive understanding of the major factors that influence cybersecurity auditors when developing a risk management plan. The research reveals that effective risk management plans are influenced by technical vulnerabilities; significantly, how to identify, define, manage, and mitigate these risks by utilizing penetration testing. Gaining insights into the nature of cyber-attack processes helps cybersecurity auditors create risk management plans that are tailored to specific vulnerabilities. Studying human behavior helps cybersecurity auditors understand user behavior within cyber technology, which helps cybersecurity auditors develop effective security training programs. The European data protection law, General Data Protection Regulation has been shown to influence cybersecurity auditors when creating risk management plans. Cybersecurity auditors must navigate the legal landscape and ensure legal compliance with risk management plans to protect sensitive data. The research found common ground among the three disciplinary findings, this allowed for interdisciplinary collaboration to gain a more comprehensive understanding of the underlying factors of the development of a risk management plan. This research paper also discusses the conflict of technical controls versus a human-centered approach, a conflicting insight between the disciplines of psychology and cybersecurity. Cybersecurity auditors can develop an effective risk management plan by utilizing their technical knowledge, understanding user behavior, and complying with legal implications.

Keywords: cybersecurity, risk, psychology, law

Introduction

In today's digital landscape, where cyber threats continue to increase, effective risk management is paramount for organizations. The primary role of cybersecurity auditors is to evaluate security controls, policies, and procedures in place to protect information systems and critical infrastructures. Cybersecurity auditors play a critical role in developing risk management plans that safeguard sensitive data and critical infrastructures. This poses the question, what are the major factors that influence cybersecurity auditors when developing risk management plans? Understanding the factors that influence auditors when developing risk management plans requires drawing insights from the disciplines of cybersecurity, psychology, and law. Auditors must possess the technical knowledge of cybersecurity to be able to form the technical foundation of a risk management plan. Insights from psychology contribute insights to the understanding of how individuals perceive and respond to risk. Law provides the framework for governing cybersecurity practices and ensuring legal compliance. An interdisciplinary approach was necessary for this research because the factors that influence the development of risk management plans extend beyond a single discipline. The research is relevant to students who are interested in the cybersecurity field, specifically cybersecurity auditors. By analyzing the research, students will have a more comprehensive understanding of the interdisciplinary aspects involved in developing a risk management plan.

Key Terms

Penetration testing, confidentiality, integrity, and *availability* are among the key terms that encompass the fundamental principles that guide the overall security of systems and data. Osamah Al-Matari from Cairo University (2018) defines *penetration testing* as an information assurance activity that uses the same tools and techniques as hackers but in a controlled way to

decide if the information is secured. Romuald Hoffman, a computer and information systems professor from the Military University of Technology (2020), defines these words as follows: *confidentiality* refers to the situation in which data is only accessed by those authorized, *integrity* ensures that data remains accurate and trustworthy during its lifecycle, and *availability* ensures that information is accessible when needed.

Disciplinary Findings

Cybersecurity

Hoffman et al., (2020) states that "the main requirements of cybersecurity are *confidentiality, integrity*, and *availability* of information and data" (p.656). Unfortunately, due to the development of new tools and techniques, cyber-attacks that compromise the *confidentiality*, *integrity*, and *availability* of information have increased (Bendovschi, 2015, p.24). Cybersecurity auditors must draw insights from the discipline of cybersecurity to create effective risk management plans that address technical vulnerabilities within systems. *Penetration testing* is a technique used in cybersecurity that involves simulating real-world attacks to identify vulnerabilities and weaknesses that exist within a system (Al-Matari et al., 2020). By being able to identify vulnerabilities, cybersecurity auditors will be able to assess the severity and impact of different vulnerabilities. The findings from *penetration testing* serve as a foundation for cybersecurity auditors to make informed decisions and prioritize risk mitigation strategies within their risk management plan. To develop an effective risk management plan, Hoffman et al., (2020) suggest that "it is crucial to know cyber actors, threats, vulnerabilities and to understand the nature of cyber-attack processes" (p.657). By recognizing the several types of cyber actors, cybersecurity auditors gain insights into the motives, tactics, and capabilities of potential attackers. This knowledge allows them to assess the likelihood of specific threats and anticipate

the potential impact of an attack on organizations. Understanding the vulnerabilities within systems helps auditors identify weaknesses that could be exploited. By having this knowledge cybersecurity auditors can create risk management plans that are tailored to the specific threats and vulnerabilities faced by an organization.

Psychology

Moustafa et al., (2021) states that 95% of cyber and network attacks are due to human error, proposing that humans are the weakest link in ensuring system security. Cybersecurity auditors play a crucial role in identifying technical vulnerabilities and risks within a system. However, it is significant that cybersecurity auditors draw insights from the discipline of psychology to create an effective risk management plan. The discipline of psychology provides insights into how humans behave and interact with cyber technology. Users can introduce vulnerabilities through their actions and lack of cyber awareness, undermining the effectiveness of security controls. However, Gratian et al., (2018) states that by analyzing how humans behave with cyber technology, cybersecurity auditors can design security training programs to raise cyber awareness (p.352). By analyzing user behavior, cybersecurity auditors can identify potential vulnerabilities and develop targeted training initiatives to address them. An effective security training program will result in users exhibiting strong device security practices and an increase in cyber awareness. Security training programs play a crucial role in risk management plans as they are designed to equip individuals with the necessary knowledge to identify, assess, manage, and respond to risks effectively. The success of a risk management plan heavily relies on aligning security measures with psychological insights.

Law

The discipline of law provides the legal framework within which cybersecurity auditors must operate. Cybersecurity auditors must collaborate with organizations to ensure that their risk management plan adheres to industry standards and legal requirements. “While regulatory effectiveness and necessity are arguable, it is better to have protections in place to safeguard consumers than to be vulnerable to cyber-attacks” (Mohammed et al., 2015, p.62). They must know relevant laws, such as the General Data Protection Regulation, and must comply with the specific requirements and principles within the law. Li et al., (2019) states that “those who can adapt to meet General Data Protection Regulation (GDPR) requirements will succeed in the future and those who cannot will eventually fail” (p. 3). The General Data Protection Regulation is a European data protection law that focuses on the rules for processing, storing, and managing data. The General Data Protection Regulation places a strong emphasis on protecting personal data and ensuring its *confidentiality, integrity,* and *availability.* Li et al., (2019) states that “the General Data Protection Regulation requires timely notification of data breaches to supervisory authorities, no later than 72 hours after being aware of it” (p. 3). Cybersecurity auditors must ensure that within their risk management plan, data breach response protocols comply with the General Data Protection Regulation notification and reporting requirements. Therefore, cybersecurity auditors must align their risk management plans to ensure compliance and mitigate potential data breaches.

Common Ground

There are three major findings disclosed by this interdisciplinary research. First, common ground is found within the discipline of psychology and cybersecurity. It highlights that cybersecurity training should be tailored to a target population (Reegård et al., 2019). This

explores how studying human behavior can benefit training programs within risk management. Second, “less than 50% of security breaches are due to criminal intended attacks, the causes being split between the intended attack, the human error, and system vulnerabilities” (Bendovschi, 2015, p. 26). This common ground is found within the discipline of cybersecurity and psychology as human error and system vulnerabilities can be the cause of security breaches. Lastly, “a lack of complying with security policies can significantly undermine information security” (Moustafa et al., 2021). This common ground is found within the discipline of law and collaborates with cybersecurity. Without complying with legal requirements this can result in a downfall of cybersecurity. Without interdisciplinary research, the insights might not otherwise have been disclosed. Interdisciplinary research was essential to gain a more comprehensive understanding of the underlying factors and their interactions within the development of a risk management plan. Each discipline brings its own perspective and expertise, and when combined, can enlighten the insights within the research.

Disciplinary Conflicts

A conflicting insight within the disciplines of psychology and cybersecurity is that “different approaches to reducing cyber-attacks can be related to implementing technical controls or to focus on empowering employees to contribute to an organization's security.” (Reegård et al., 2019). This raises the conflict of technical controls versus a human-centered approach. This refers to implementing technical controls to protect sensitive data, while the discipline of psychology advocates for improving user behavior. To bridge the gap between these two insights, it is important to foster collaboration. Discussing how each insight can complement one another. This creates a layered defense strategy that addresses technical vulnerabilities and human factors.

Conclusion

By combining the technical expertise of cybersecurity, the understanding of human behavior from psychology, and the legal frameworks provided by law, a more holistic understanding can be achieved. The technical knowledge of cybersecurity involves identifying and assessing threats and vulnerabilities within organizations. Human behavior analyzes how individuals interact with cyber technology. Law influences the development of risk management plans by providing regulations and guidelines on handling sensitive data and compliance with legal requirements. By combining these different propositions this causes cybersecurity auditors to ensure risk management plans are updated to align with human factors, address new cyber threats, and are within legal compliance.

Reflecting on the insights from the disciplines of cybersecurity, psychology, and law, there are opportunities to further build on this research by incorporating the discipline of economics. Economics offers valuable insights into the cost-benefit analysis of cybersecurity investments that influence decision-making in organizations. By integrating economic perspectives, researchers can examine the financial implications of risk management planning, such as the costs associated with implementing security measures versus the potential losses from cyber-attacks. This interdisciplinary approach would contribute to a more comprehensive understanding of the factors influencing cybersecurity auditors and provide additional insights for developing effective risk management plans. Future research could explore the intersection of economics with cybersecurity, psychology, law, and policy to enhance the knowledge of what really influences cybersecurity auditors when creating a risk management plan.

In conclusion, cybersecurity auditors develop risk management plans with the goal of safeguarding sensitive data and critical infrastructures. Interdisciplinary research on the factors

that influence cybersecurity auditors when developing a risk management plan has highlighted the significance of drawing insights from cybersecurity, psychology, and law. Cybersecurity auditors possess the technical knowledge to identify risks and review current security measures. By understanding how users behave with cyber technology, cybersecurity auditors create risk management plans and security awareness training that address human factors. Insights from law have shown that cybersecurity auditors must consider and comply with the legal implications when developing a risk management plan. This research has demonstrated that a comprehensive understanding of the development process of risk management plans requires considering technical expertise, human behavior, and legal compliance. Overall, interdisciplinary research on this topic is crucial for ensuring risk management plans are effective.

References

Al-Matari, O. M. M., Helal, I. M. A., Mazen, S. A., & Elhennawy, S. (2018). Cybersecurity tools for IS auditing. In *2018 Sixth International Conference On Enterprise System*. https://doi.org/10.1109/es.2018.00040

Bendovschi, A. C. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia. Economics and Finance*, *28*, 24–31. https://doi.org/10.1016/s2212-5671(15)01077-1

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. M. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, *73*, 345–358. https://doi.org/10.1016/j.cose.2017.11.015

Hoffmann, R., Napiórkowski, J., Protasowicki, T., & Stanik, J. (2020). Risk based approach in scope of cybersecurity threats and requirements. *Procedia Manufacturing*, *44*, 655–662. https://doi.org/10.1016/j.promfg.2020.02.243

Li, H., Yu, L., & He, W. (2019). The impact of GDPR on global technology development. *Journal of Global Information Technology Management*, *22*(1), 1–6. https://doi.org/10.1080/1097198x.2019.1569186

Mohammed, D., Mariani, R., & Mohammed, S. (2015). Cybersecurity challenges and compliance issues within the U.S. healthcare sector. *International Journal of Business and Social Research*, *5*(2), 55–66. https://doi.org/10.18533/ijbsr.v5i2.714

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving cyber security management. *Frontiers in Psychology*, *12*. https://doi.org/10.3389/fpsyg.2021.561011

References

Reegård, K., Blackett, C., & Katta, V. (2019). The concept of cybersecurity culture. In *Proceedings of the 29th European Safety and Reliability Conference (ESREL)*. https://doi.org/10.3850/978-981-11-2724-3_0761-cd