PressAcademia
www.pressacademia.org/journals/rjbm

RJBM
ISSN 2148-6689

Research Journal of Business and Management YEAR 2023 VOLUME 10 ISSUE 2

CRITICAL SUCCESS FACTORS FOR CYBERSECURITY JUST TECHNICAL? EXPLORING THE ROLE OF HUMAN FACTORS IN CYBERSECURITY MANAGEMENT

DOI: 10.17261/Pressacademia.2023.1735
RJBM- V.10-ISS.2-2023(2)-p.51-57

Cenk Aksoy
McGill University, School of Continuing Studies, Montreal, Canada.
drcenkaksoy@gmail.com, ORCID: 0000-0002-7481-0837

Date Received: March 5, 2022 **Date Accepted:** June 21, 2023

To cite this document
Aksoy, C., (2023). Are critical success factors for cybersecurity just technical issues? Cybersecurity management and the human factor. Research Journal of Business and Management (RJBM), 10(2), 51-57.
Permanent link to this document: http://doi.org/10.17261/Pressacademia.20223.1735

ABSTRACT

Purpose- With the rapid advancement of information and communication technologies, businesses are facing growing security risks. The prevalence, intensity, and complexity of cyber attacks worsen these vulnerabilities, leading to a rising focus on cybersecurity. Enterprises exposed to such cyberattacks might not only face considerable financial losses but also experience data breaches, operational interruptions, harm to their reputation, regulatory penalties, legal expenses, reduced competitive standing, and increased insurance premiums. In this concept study discusses the importance of human factors in cybersecurity management. While organizations spend billions on information technology systems and software to detect and prevent cyber threats, individuals play a critical role in managing these risks.

Methodology- Through a review of literature and statistical data, study examines the factors contributing to cybersecurity breaches, the allocation of resources to address them, and proposes potential solutions.

Findings- In the workplace, most research on cybersecurity focuses on employees as the most important source of vulnerability. In the literature review, it is understood that an employee's carelessness and lack of awareness pose the greatest risk to cybersecurity. However, businesses often fail to show sufficient attention to human behavior in their efforts to keep organizational data secure and to plan security strategies. It is important to note that effective cybersecurity management requires not only technical controls but also the management of human factors. Meanwhile, security expenditures in enterprises are often disproportionately allocated to technology investments, with 97% being spent on technology investments, despite the fact that over 85% of breaches are attributable to human factors.

Conclusion- In the literature review, it is understood that cybersecurity management is not only related to technical controls, but also the management of human factors is of critical importance. The management of individuals is also an essential cybersecurity responsibility. It is important to adopt a holistic approach to cybersecurity management includes both technical and human perspectives. Cybersecurity awareness has significant benefits for businesses to effectively manage cybersecurity which can be achieved by developing appropriate training programs and foster a cybersecurity culture.

Keywords: Cybersecurity, cybersecurity management, cybersecurity awareness, technology investments, human factor
JEL Codes: M12, M15, L86

1. INTRODUCTION

With the rapid development of information and communication technologies, the security risks faced by enterprises are increasing. The frequency, severity, and sophistication of cyber attacks make businesses even more vulnerable, and the interest in cybersecurity is growing every day. Cybersecurity vulnerabilities have become immediate threats to government agencies and businesses, leading to public and private organizations investing billions of dollars in information technology systems and software to detect these threats.

Research indicates that executives and cybersecurity professionals heavily rely on technology to prevent cybersecurity incidents. While new technologies may have unintended consequences, executives continue to view technology as the key to improving security defenses. However, managing complex cybersecurity operations with increasing human factor challenges exceeds the expertise of most information security professionals. Nevertheless, managers seem hesitant to seek the assistance of human resources specialists and behavioral scientists to implement effective strategies and objectives to reduce human error in information security (Nobles, 2018). The management of individuals is also an essential cybersecurity responsibility. Considering human factors in cybersecurity leadership is one of the factors that can affect the success of an organization and aims to reduce errors by focusing on human behavior (Pollini et al., 2021).

The question of whether the critical success factors of cybersecurity are limited to technical factors or if the human factor is also significant remains a subject of debate. To clarify this debate, the study examines cybersecurity management from both technical and human perspectives. Study contributes to the existing literature by providing a comprehensive analysis of the role of both technical and human factors in managing cybersecurity. By examining the ongoing debate and synthesizing research findings, it offers a valuable overview of the current understanding of cybersecurity success factors. Furthermore, by identifying common causes of cybersecurity breaches and suggesting potential solutions, provides practical guidance for businesses to improve their cybersecurity practices.

2. CYBERSECURITY

Cybersecurity is an important concept that emerged with the widespread use of computers, information technologies and the internet. The first computers were very large devices in a large room and were used by only a few people. However, with the development of technology, computers have become smaller and cheaper and are used in homes, businesses and even cell phones. These developments resulted in the greater prevalence of computers and the Internet. However, with these developments, cyber threats such as cyber crimes and cyber attacks have also started to increase. The concept of cybersecurity also emerged to combat these threats (Jones, 2015).

The concept of cybersecurity refers to the measures taken to ensure the security of computer systems, networks, software and other digital environments. The concept of cybersecurity is used to combat threats such as cyber crimes, cyber attacks, cyber terrorism and cyber espionage (Johnson, 2019).

Cybersecurity threats are increasing day by day and many large companies are exposed to cyber attacks. Some major cybersecurity breaches in recent years include:

- In 2013, the retail store chain Target suffered a cyberattack in which the personal information of 110 million customers was stolen (Goldman, 2017).
- As a result of the cyber attack in 2013, the information of 3 billion users was stolen (Hill, 2017).
- In 2017, credit reporting company Equifax suffered a cyberattack in which the personal information of 143 million people was stolen (Brown, 2017).

Due to this cost, loss of customers and reputation, cybersecurity has become an existential issue for businesses today. Cybersecurity threats continue to increase, and both large companies and small and medium-sized companies are affected by these threats. There are different types of attacks that threaten businesses. The types and characteristics of cyber attacks are:

1. Phishing attacks: In this type of attack, attackers try to capture users' personal information or identities by using tools such as fake websites or e-mails (Smith, 2021).

2. Data Breaches: In such attacks, attackers attempt to steal or disclose sensitive data by gaining unauthorized access to target systems (Baker, 2020).

3. DDoS attacks: In such attacks, attackers try to crash or render systems unusable by sending excessive traffic to target systems (Gupta, 2019).

4. Malware attacks: In such attacks, attackers try to control the system or steal data by infecting target systems with malware (Kumar, 2018).

In order to be protected from these attacks, companies need to take precautions about cybersecurity and ensure their security. In order to achieve this, businesses should focus on the causes of cybersecurity breaches and analyze and monitor how these breaches are distributed in percentage terms of technical and human factors. Some of these reasons for violations are:

- Weak or guessable passwords can allow attackers to easily access target systems (Patel, 2020).
- Out-of-date systems allow attackers to infiltrate systems and carry out their attacks (Kim, 2021).
- The fact that companies do not have enough security personnel, insufficient training of unconscious personnel, deliberate or unintentional personnel negligence and mistakes cause cybersecurity vulnerabilities (Ramakrishnan, 2019).

When these reasons are examined, it is important for businesses to pay attention to personal information security in order to be cautious against cyber attacks. In this context, the evaluation of cybersecurity together with the human factor comes to the fore.

3. CYBERSECURITY AND THE HUMAN FACTOR

Human knowledge, beliefs, values, behaviors, and expectations are critical to all aspects of businesses (Carpenter & Roer, 2022, p.21):

- People make decisions about which technologies to purchase.
- People review, adjust, design and develop business technologies.
- People prioritize, make visible and assess risks.
- People are responsible for operating and maintaining security technologies.
- People determine how to respond to suspicious activity.
- People consciously and unconsciously decide how they will interact with systems, networks and information.
- Every individual who is hired, contracted, interacted with, or sold to is a human being.
- Everything that is designed, sold, or developed by businesses ultimately serves people.

This illustrates that people's decisions, behaviors, and expectations have a significant impact on all assets and resources within businesses. However, research shows that business managers tend to focus their investments on technical infrastructure and expenditures, neglecting the human element. For instance, Carpenter and Roer's (2022) study found that less than 3% of security expenditures in enterprises are allocated to the human factor, while 97% is spent on technology investments, despite over 85% of breaches being attributable to human factors. Other studies supporting this have shown that humans are the weakest link in transmitting secure data, and certain unintentional behaviors stemming from employee ignorance (Triplett, 2022). Therefore, the fact that most security vulnerabilities are caused by human factors demonstrates that cybersecurity management is not solely a technological issue (Corradini, 2020). People's carelessness and lack of awareness pose the greatest risk to the security of digital tools (Metalidou et al., 2014). Thus, senior managers must prioritize human factors in their cybersecurity policies. Cybersecurity efforts should not solely focus on information technology systems, but also consider how people use information systems and the actions that lead to vulnerabilities.

Cybersecurity can be considered as a common combination of technology and human factors. Although technical controls have an important role in combating cyber attacks, the human factor is also a critical factor influencing cybersecurity success. Humans must also play a critical role in managing cybersecurity, as technical controls have limits in ensuring security. Therefore, it is important to adopt a holistic approach to cybersecurity management (KPMG Turkey, 2019; Solove, 2013).

4. CYBERSECURITY MANAGEMENT

Cybersecurity management is defined as directing cybersecurity activities in the most general sense. This management should have the capacity to direct the needs of a society or organization that carries out the technical, managerial, corporate and governance activities of cybersecurity (Kuusisto & Kuusisto, 2013).

Employees are frequently addressed as the most important source of vulnerability in the workplace (Ani, He & Tiwari, 2019). However, according to Klimoski (2016), cybersecurity problems belong not only to careless employees, but also to cybersecurity senior management who are inadequate in guiding individual performance in the digital environment. Therefore, cybersecurity management includes setting goals based on the protection of the digital business system, coordinating action plans, and managing comprehensive disruptions (Lehto & Limnell, 2020).

The scope of cybersecurity management in businesses can be summarized as follows:

- It includes the assessment of the cybersecurity risks of businesses, the development and implementation of cybersecurity strategies. However, cybersecurity management is not only about technological solutions, but also the management of human factors is important. Therefore, businesses should adopt a holistic approach to cybersecurity management. It should include elements such as developing and implementing cybersecurity strategies, preparing and implementing business continuity plans, preparing and testing cyber incident response plans, developing and implementing cybersecurity policies, implementing cybersecurity training and awareness programs, and developing a culture of internal communication and collaboration (CISA, 2021; Haynes & Klass, 2019; NIST, 2018).

- It includes the development and implementation of businesses' cybersecurity policies. Cybersecurity policies determine the cybersecurity goals and rules of businesses. These policies create the information security culture of enterprises and ensure that employees are trained and informed about cybersecurity issues. Cybersecurity policies enable businesses to determine their cybersecurity strategies and manage cybersecurity risks (Antonakakis et al., 2017; Williams, 2019; ISACA, 2019).
- It involves businesses preparing and testing cyber incident response plans. Cyber incident response plans define the processes of detection, analysis, prevention, response and remediation of cyber attacks. Businesses should form emergency teams and train these teams regularly to prepare response plans for cyber incidents. In addition, businesses are required to regularly test and update their cyber incident response plans (NIST, 2018; Ackerman & Volkman, 2019; SANS Institute, 2021).
- It involves businesses constantly monitoring and assessing their cybersecurity risks. Businesses must continually monitor and evaluate cybersecurity risks and stay up-to-date on new threats and defense mechanisms related to those risks. In addition, businesses are required to regularly report and assess their cybersecurity risks. This helps businesses continually improve their cybersecurity management (Solms & Solms, 2016; Khan & Khan, 2017).

As a summary, the scope of cybersecurity management in businesses encompasses various aspects. It involves assessing and managing cybersecurity risks, implementing strategies, and considering human factors. To ensure effective cybersecurity management, businesses should take a holistic approach, which includes developing and implementing strategies, continuity plans, and incident response plans. It also entails establishing cybersecurity policies, conducting training programs, fostering internal communication, and collaboration. Additionally, businesses need to regularly monitor, assess, and report on their cybersecurity risks to improve their overall security posture.

5. CYBERSECURITY AWARENESS IN BUSINESSES

Cybersecurity awareness enables employees to be informed about cybersecurity threats and develop their skills to deal with these threats. Cybersecurity awareness includes employees' understanding of cybersecurity concepts, threats, risks, attacks, protection methods and reporting procedures (Usta & Kurtuldu, 2020; Oktavianto & Prabowo, 2018).

Increasing cybersecurity awareness has significant benefits for businesses to effectively manage cybersecurity. These benefits can be listed as follows:

- Business employees to be better prepared against cyber attacks. As cybersecurity awareness increases, so does the ability of employees to detect and report cyber attacks. Therefore, raising cybersecurity awareness of businesses is an important step in cybersecurity management (Lambrinoudakis et al., 2020; González, 2018).
- It ensures the effective implementation of cybersecurity policies of enterprises. Cybersecurity policies of businesses include training and informing employees about cybersecurity. For this reason, employees' cybersecurity awareness should be increased in order to effectively implement cybersecurity policies of enterprises. Thus, businesses can implement cybersecurity policies more effectively (NIST, 2018; Solms & Solms, 2016).
- It reduces the cybersecurity risks of businesses. Employees' cybersecurity awareness helps businesses reduce their cybersecurity risks. While the carelessness or misbehavior of the employees increase the cybersecurity risks of the enterprises, conscious employees act in accordance with the cybersecurity policies of the enterprises to ensure cybersecurity. Therefore, it helps businesses to increase their employees' cybersecurity awareness and reduce cybersecurity risks (SANS Institute, 2021; KPMG Turkey, 2019).
- It allows businesses to trust their employees about cybersecurity. When employees are conscious about the cybersecurity of their businesses, they feel more confident about cybersecurity. For this reason, businesses increase employees' cybersecurity awareness, enable employees to spend more effort to ensure cybersecurity and learn more about the cybersecurity of their businesses (Blyth & Kovacich, 2013).
- Protects the reputation of businesses. When businesses are exposed to cyber attacks, they can lose the trust of their customers and business partners. For this reason, businesses increase cybersecurity awareness, enable them to be better prepared against cyber attacks and be less affected by attacks. In addition, raising cybersecurity awareness of businesses creates a reliable impression for customers and business partners about the cybersecurity of the business (Haynes & Klass, 2019).

As a summary, increasing cybersecurity awareness brings significant benefits to businesses. It helps employees detect and report cyber attacks, ensures the effective implementation of cybersecurity policies, reduces cybersecurity risks, fosters trust among employees, and protects the business's reputation.

5.1. CYBERSECURITY AWARENESS TRAINING PROGRAMS

Businesses need to train their employees on cybersecurity, as many cyber attacks occur due to employee carelessness or ignorance. Increasing cybersecurity awareness depends on businesses developing appropriate cybersecurity awareness training programs. Businesses' cybersecurity training programs are designed to make employees aware of cybersecurity. These programs enable employees to understand cybersecurity concepts, threats, risks, attacks, protection methods, and reporting procedures. In addition, training programs should be regularly renewed and updated by businesses. These programs enable employees to consciously prevent current cybersecurity threats and to be informed about methods of protection against attacks (ISACA, 2019).

5.2. A CULTURAL PERSPECTIVE ON CYBERSECURITY AWARENESS

Cybersecurity management aims to detect and prevent cyber attacks by adopting the strengthening of information security awareness of employees through training. However, in order to achieve this goal, it is not enough for the employees to be educated, at the same time, safe behaviors of the employees should be encouraged and spread throughout the organization. This occurs when businesses adopt a safety culture (Hashizume et al., 2013).

Adopting a security culture in businesses, increasing the awareness of employees on cybersecurity, providing training and information on cybersecurity, determining and implementing cybersecurity policies, constantly monitoring and evaluating the cybersecurity of information systems, preparing and implementing business continuity plans and response plans to cyber incidents, cybersecurity It is possible to integrate activities such as cooperating with all stakeholders on the issue and constantly monitoring cybersecurity risks into the organizational culture with the participation of all employees, especially the management (Khan & Khan, 2017; NIST, 2018).

6. CONCLUSION

Cybersecurity is a critical aspect of both societal and corporate security, and it plays an essential role in achieving an organization's strategic goals in an increasingly digital society. Cybersecurity management involves enabling businesses to operate on reliable and secure information networks, with the primary goal of ensuring the involvement of all stakeholders in establishing a robust cybersecurity system (Lehto & Limnell, 2016).

In the literature review, it is understood that cybersecurity management is not only related to technical controls, but also the management of human factors is of critical importance. In addition to ensuring the security of technical control systems, people must also play a critical role in cybersecurity management. Therefore, it is recommended to adopt a holistic approach to cybersecurity management (CISA, 2021; NIST, 2018; Haynes & Klass, 2019).

To ensure cybersecurity, it is imperative for businesses to increase their cybersecurity awareness. Cybersecurity awareness empowers employees to stay informed about potential cyber threats and develop their skills to deal with such risks. This, in turn, enhances their ability to detect and report cyber attacks. To increase the cybersecurity awareness of businesses, it is essential to develop appropriate training programs and foster a cybersecurity culture.

Therefore, cybersecurity management goes beyond technology and is closely intertwined with the management of individuals, organizational behavior, continuous learning, organizational culture, and change. It is not only about how people perceive cybersecurity but also about their priorities and actions, influenced by their beliefs, values, and attitudes, from the board of directors to every corner of the organization.

REFERENCES

Ackerman, G., Volkman, D. (2019). Cybersecurity culture and training: A practitioner's perspective. Journal of Business Continuity & Emergency Planning, 12(1), 10-17.

Ani, U.D. He, H., Tiwari, A. (2019). Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. J. Sys. Info. Technol., 21, 2–35.

Antonakakis, N., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J. A., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Lever, C., Ma, J., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., Zhou, Y., & Paxson, V. (2017). Understanding the Mirai botnet. In Proceedings of the 26th USENIX Security Symposium (pp. 1093-1110).

Baker, A. (2020). Cybersecurity: The Most Important Tech Skill of the Future. Forbes. https://www.forbes.com/sites/abdullahimuhammed/2020/01/08/cybersecurity-the-most-important-tech-skill-of-the-future/?sh=54d5db5b5

Blyth, M., Kovacich, G. (2013). The Routledge Handbook of Computer Security. Routledge.

Brown, J. (2017). Equifax hack hit 143 million people, and it's just the first disaster to come. The Guardian. https://www.theguardian.com/commentisfree/2017/sep/08/equifax-hack-hit-143-million-people-disaster-waiting-to-happen

Carpenter, P., Roer, K. (2022). The Security Culture Playbook: An Executive Guide To Reducing Risk and Developing Your Human Defense Layer, Wiley, NJ, USA.

CISA. (2021). Cybersecurity and Infrastructure Security Agency Strategic Plan 2021-2025. CISA. https://www.cisa.gov/sites/default/files/publications/2021-03/CISA-Strategic-Plan-2021-2025-Public-Final-508.pdf

Corradini, I. (2020). Building a Cybersecurity Culture in Organizations: How to Bridge the Gap between People and Digital Technology, Springer Nature, Berlin/Heidelberg, Germany.

Goldman, D. (2017). Target data breach: 7 lessons learned. CIO. https://www.cio.com/article/3242597/target-data-breach-7-lessons-learned.html

González, L. M. (2018). The role of employee awareness and training in cybersecurity. Journal of International Management Studies, 18(1), 55-60.

Gupta, A. (2019). DDoS Attack Types and Tools: All You Need to Know. Cloudflare. https://www.cloudflare.com/learning/ddos/ddos-attack-tools/

Hashizume, K., Rosado, D. G., Fernandez-Medina, E. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1), 5. https://doi.org/10.1186/1869-0238-4-5

Haynes, J. W., Klass, B. R. (2019). Managing cybersecurity risk: A governance approach. Journal of Business Continuity & Emergency Planning, 13(1), 30-42.

Hill, K. (2017). Yahoo says all 3 billion user accounts were hacked in 2013 data theft. Reuters. https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-3-billion-user-accounts-were-hacked-in-2013-data-theft-idUSKBN1C9188

ISACA. (2019). Cybersecurity: Understanding Cybersecurity Risk Management. ISACA.

Johnson, K. (2019). What Is Cybersecurity? Definition, Best Practices & More. Digital Guardian. https://digitalguardian.com/blog/what-cybersecurity-definition-best-practices-more

Jones, S. (2015). A Brief History of Cybersecurity. Huffington Post. https://www.huffpost.com/entry/a-brief-history-of-cyber_b_11229522

Khan, S., Khan, M. A. (2017). An overview of cyber security policy for organizations. International Journal of Scientific & Engineering Research, 8(11), 1815-1823.

Kim, T. (2021). The Importance of Cybersecurity Updates and Patches. Security Intelligence. https://securityintelligence.com/posts/importance-of-cybersecurity-updates-and-patches/

Klimoski, R. (2016). Critical success factors for cyber security leaders: Not just technical competence. People Strategy, 39, 14–18.

KPMG Turkey. (2019). Türkiye Siber Güvenlik Raporu. KPMG Turkey. KPMG Turkey. https://assets.kpmg/content/dam/kpmg/tr/pdf/2019/03/Siber%20Guvenlik%20Raporu%202019.pdf

Kumar, A. (2018). What is Malware? A Comprehensive Guide to Cyber Threats. Norton. https://us.norton.com/internetsecurity-malware-what-is-malware.html

Kuusisto, R., Kuusisto, T. (2013). Strategic Communication for Cyber-security Leadership. Journal of Information Warfare, 12(3), 41–48. https://www.jstor.org/stable/26486840

Lambrinoudakis, C., Kambourakis, G., Gritzalis, D. (2020). Enhancing cyber security awareness in organizations. International Journal of Information Management, 50, 280-291.

Lehto, M., Limnell, J. (2016). Cyber Security Capability and Case Finland. In Proceedings of the 15th European Conference on Cyber Warfare and Security (ECCWS) (pp. 182–190).

Lehto, M., Limnell, J. (2020). Strategic Leadership in Cyber Security, Case Finland. Information Security Journal: A Global Perspective, 30, 1-10. 10.1080/19393555.2020.1813851.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., Giannakopoulos, G. (2014). The Human Factor Of Information Security: Unintentional Damage Perspective. Procedia Soc. Behav. Sci., 147, 424–428.

National Institute of Standards and Technology (NIST) (2018). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. NIST. https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

Nobles, C. (2018). Botching Human Factors in Cybersecurity in Business Organizations. Holistica–Journal of Business and Public Administration, 9(3), 71-88.

Oktavianto, R. A., Prabowo, R. (2018). Cybersecurity awareness training using gamification approach: A literature review. Procedia Computer Science, 135, 313-320.

Patel, N. (2020). The Top 10 Cybersecurity Risks of 2020. Security Boulevard. https://securityboulevard.com/2020/02/the-top-10-cybersecurity-risks-of-2020/

Pollini, A., Callari, T.C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., Guerri, D. (2021). Leveraging Human Factors in Cybersecurity: An Integrated Methodological Approach. Cogn. Technol. Work, 24, 371–390.

Ramakrishnan, R. (2019). Why Cybersecurity is Essential for Small and Medium-Sized Businesses. Entrepreneur. https://www.entrepreneur.com/article/336329

SANS Institute. (2021). What is Cybersecurity? SANS Institute. https://www.sans.org/cybersecurity/

Smith, C. (2021). Phishing. Britannica. Retrieved from https://www.britannica.com/topic/phishing

Solms, R. V., Solms, B. (2016). Information security governance simplified: From the boardroom to the keyboard. Apress.

Solove, D. J. (2013). Privacy and the media. Harvard University Press.

Triplett, W.J. (2022). Addressing Human Factors in Cybersecurity Leadership. Journal of Cybersecurity and Privacy, 2, 573–586. https://doi.org/10.3390/jcp2030029

Usta, H., Kurtuldu, H. (2020). Evaluation of information security awareness of healthcare workers. Journal of Information Security and Applications, 55, 102580.

Williams, P. A. (2019). Cybersecurity: A comprehensive overview for directors and executives. Wiley.