ISSN 2320 - 2602
Volume 13 No. 9, September 2024
International Journal of Advances in Computer Science and Technology
Available Online at http://www.warse.org/IJACST/static/pdf/file/ijacst011392024.pdf
https://doi.org/10.30534/ijacst/2024/011392024

Cybersecurity within organizations: Who should be responsible for ensuring that the organization is protected against cybercrime?

Ainsley Robin Anesone
Victoria University of Wellington, New Zealand, a.anesone@nus.edu.ws

Received Date : July 24 , 2024 Accepted Date : August 29, 2024 Published Date : September 07, 2024

ABSTRACT

Cybersecurity within organizations: Who should be responsible for ensuring that the organization is protected against cybercrime? The aim of this research is to identify who is accountable for safeguarding organizations from cybercrime. The study focused on internal cybersecurity, particularly the roles of managers and employees. The human factor refers to managers and employees. The methodology used to collect the data was the collection of literature from Google Scholar. The findings indicate that cybersecurity is a shared responsibility between managers and employees.

Key words: Cybersecurity, Human factors, Organizational culture, Security policies, Policy compliance, Employee actions

1. INTRODUCTION

Information technology has brought numerous benefits to organizations, yet cybersecurity remains a primary concern for organizations relying on these technologies. Cybersecurity is a widely used term, and its meaning has evolved in the fields of engineering, technology, computer science, and security and defense [1]. There are multiple definitions of cybersecurity, but nine definitions have been consistent throughout; viewed by [1] which provided materials with cybersecurity perspectives. In this essay, the definition stands out to describe this phenomenon as a collection of tools, policies, and security concepts; as well as managing risk approaches that could be used to protect the cyber environment and the resources of the organization and its users [1]. Implementing effective cybersecurity measures is particularly challenging today because there are more devices available than people, and attackers are becoming more innovative. According to [2] reported, cyber threats were initially viewed as mostly technological issues, but the view has expanded to include other issues, including aspects of the user's behavior. Also, [3] generally, emphasizes the user's behavior, and it has been reported that 80% of significant cybersecurity problems can be caused by employees' poor security behavior, rather than inadequate solutions. According to [4], they also view internal actors in organizations as having caused 55% of incidents.

These findings are like those published by Ernest and Young (2003) and cited in [5], where between 50% - 75% of security incidents that originated within an organization were repeatedly committed by employees. These results raise a question as to who should be responsible for ensuring that the organization is protected against cybercrime [6], [7]. This essay argues that cybersecurity should be a shared responsibility between managers and employees within any organization, to ensure safety and security. This paper focuses on cybersecurity within organizations, emphasizing human factors. In this context, the human factor refers to managers and employees.

Next is the methodology, discussing the process I used and how data was selected from various collections of academic research papers. Thirdly, are the findings from the research papers I used for this essay. Fourth is the discussion and limitation, followed by the conclusion.

2. LITERATURE REVIEW METHODOLOGY

The Google Scholar website has been used to search for literature materials for this research. The materials collected for this work are about cybersecurity within organisations emphasizing human factors over technological issues. The collected materials were analyzed to develop the title and subtopics of this essay, which involves several systematic steps:

- Defining the research question helps to narrow down the literature search and ensures that the review is relevant to the essay's goals.

- Google Scholar was used to find relevant, comprehensive literature. Keywords related to human factors and cybersecurity were used to identify relevant studies, papers, and articles. The search results were restricted based on the publication date, peer-reviewed status, and subject area.
- Identify relevant sources by reviewing the abstracts and titles of the search results.
- The selected literature was critically reviewed to determine the study's quality and relevance, including the sample sizes, methodology, findings, conclusion, and any biases or limitations.
- Identify common themes, patterns, and gaps in the collected literature. This involves dividing the studies based on their findings regarding human issues in cybersecurity.
- Highlight key insights and views for comparison and evaluation.
- Select subtopics to build the essay's structure, providing that each subtopic addresses a specific aspect of the human factor.

3. FINDINGS

3.1 Roles and Responsibilities of Management

3.1.1 Organizational Culture

Organizational Culture is defined by Schein (1992), cited in [8], as a set of shared values, beliefs, observations, and practices that share and direct member's organizational behavior. These practices are shaped by the founders of the organization or the management; through communicating knowledge about the information risks in the organizational environment. An excellent example of this is the adoption of the SETA program, according to [5] is to provide employees with general knowledge of the information security environment along with the skills necessary to perform any required procedures. The SETA program stands for security, education, training, and awareness [5]. According to [9] the SETA program raises awareness of employee responsibilities regarding organizational information resources and daily physical security issues. The awareness program emphasizes management priorities to persuade potential abusers that the company will take serious responsibility and, therefore, will not take intentional violations lightly. These practices can strengthen the organizational culture by implying the advantages of understanding these procedures. To prevent misuse attempts, there is disclosure of information on the objective and subjective use of information systems, punishment associated with incorrect usage, and knowledge of organizational and legal actions [5].

3.1.2 Security Policies

Managers responsible for information security create computer security policies in organizations to confirm security. Security policies also have various definitions and interpretations, but they have been broadly defined as "guiding statements of goals to be achieved" (Gaston 1996, p.1975). Many scholars [6], [8], [10], hold the view that to avoid misinterpretation between different organizational parties, policies must be in place so that people understand what is expected of them; user unawareness can introduce further vulnerabilities. These policies are futile if employees and end-users misinterpret the significance of these practices when they are not prepared to follow them accordingly [11]. The extensive efforts of managers should be practical and transparent, so that employees and end-users recognize the importance of their behavioral patterns when performing their daily tasks. Employee and end-user responsibilities reported by [6], such as using a weak password, installing untrustworthy software, and using insecure devices and applications, are expected to minimize risks if staff members realize the policies in place. Security policies certainly provide a basis for sanctions or internal measures punishing the behavior of misuse of information security. As [12] believes that the lack of security policies can lead to poor communication about acceptable system usage and lead users to assume that misuse of the information system is not subject to enforcement and has little or no consequences. The acceptable use of such guidelines as described in security policies also suggests that punishments must be imposed if the user chooses not to comply [5].

3.2 Roles and Responsibilities of the General Staff

3.2.1 Policy Compliance

Policy definitions may be crystal clear and detailed, but there may be a lack of compliance, particularly about information security behavior [10]. According to [3], there are three factors to improve user security behaviors. These considerations are the behavior demonstrated by senior management and colleagues; the user's security common sense, the ability to make decisions, and the strength of the user's contract with the company [3]. The behavior shown by others has a

more powerful effect on the attitudes and behaviors of the employees than what they are told. In the view of [11] also supported [3] results on the effect of the behavior by others on employees. Behaviors are shaped or influenced to motivate employees to take security measures and to act immediately [11]. The behavior of peers can help staff members develop and strengthen their security common sense to reduce user security errors. The continuation of security training can develop a user's security decision-making skills [3]. These skills will encourage staff members to ensure policy compliance through their roles and responsibilities, which will benefit the organization in terms of security negligence and deliberate attacks. Policy compliance reported by [3] also points out to employees that their contracts with the company also obligate them to comply.

3.2.2 Employee Actions

Technology is often said to play a significant role in cybersecurity, but humans pose the weakest connection. However, [6] believe that people play a vital role in keeping and updating systems, to ensure that the latest defense in place can immediately detect attacks and take countermeasures. These roles are also highlighted by [13], which can lead to attacks starting at the desktop; users sharing their username and password with attackers who might use them to gain access to the network. There is some evidence [13], [14], [15], to indicate that security policies are not always working effectively for employees. Some do not focus on the cybersecurity policies of their organizations, while others tend to underestimate the danger of information security risks even though they understand the concept of security and related instructions [15]. It is not only risky but also costly to underestimate the dangers of information security. Take, for instance, the Target data breach. The negligence of employees [7] to attend to their emergency response systems could have saved time and money. An individual employee's commitment to an organization through best practices is likely to play a role in his or her engagement in security behavior to prevent human error. Employees with greater involvement in an organization are likely to believe that their actions influence the overall performance of the organization [11].

4. DISCUSSION AND LIMITATIONS

Cybersecurity is a wide-ranging topic, including computer science, engineering, political studies, phycology, security studies, management, education, and sociology [1], and it continues to evolve at every opportunity. Firstly, most of the literature covers user security awareness programs to convey knowledge to employees and end users. Secondly, the behaviors of users and how motivation factors affect their decision making in executing their roles and responsibilities. This motivation factor also ties to the behaviors of managers and how organizational cultures and norms mold employees' security policy compliance. Lastly, policies should be transparent to reduce risks. Even though there are more works of literature about cybersecurity, the majority of the fifteen that were collected for this work did not clearly emphasize human factors in terms of what and how to perform their task of reducing these risks.

The limitation of this work was looking at fifteen works of literature highlighting cybersecurity within organizations concentrating on the human factor. The comparison of the research was also from the two-research literature since 1990, and the rest was from 2000 to 2018.

5. CONCLUSIONS

The study revealed that effective cybersecurity within organizations hinges on a collaborative effort between managers and employees. Key findings include:

5.1 Shared Responsibility

Both managers and employees play crucial roles in maintaining cybersecurity. Managers are responsible for establishing policies, providing training and ensuring compliance. Clear policies establish clear cybersecurity policies and ensuring that all employees understand their roles and responsibilities is essential. This includes guidelines on data handling, use of personal devices and remote work protocols. Employees, on the other hand, are expected to follow these policies and remain vigilant against potential threats.

5.2 Importance of Training

Continuous training and awareness programs are essential. Employees need to be educated about the latest cyber threats and best practices for mitigating risks. Employees need regular training on the latest cyber threats and security practices. This includes recognizing phishing attempts, understanding the importances of strong passwords, and knowing how to handle sensitive information. Conducting simulated phishing attacks can help employees recognize and respond to real threats more effectively.

5.3 Communication and Reporting

Open lines of communication between managers and employees are vital. Creating an environment where employees feel comfortable in reporting suspicious activities without fear of repercussions is crucial. Fostering a culture where security is a priority can significantly reduce risks which

will encourage employees to take security seriously and integrate it into their daily routines.

5.4 Human Factor

The human element is a significant factor in cybersecurity. Mistakes or negligence by employees can lead to vulnerabilities, making it imperative for organizations to foster a culture of security awareness. Holding employees accountable for following security policies and procedures helps maintain a high standard of security. Conduct regular audits of access controls to ensure compliance and identify any potential vulnerabilities. Encourage collaboration between other departments of the organization to create a comprehensive approach to cybersecurity.

5.5 Literature Review

The data was collected through an extensive review of existing literature on Google Scholar, which provided a comprehensive understanding of the current state of cybersecurity practices and the roles of different stakeholders.

REFERENCES

[1] J. M. Bauer and M. J. Van Eeten, **"Cybersecurity: Stakeholder incentives, externalities, and policy options,"** *Telecommunications Policy,* vol. 33, no. 10-11, pp. 706-719, 2009.

[2] N. S. Safa, C. Maple, T. Watson and R. Von Solms, **"Motivation and opportunity based model to reduce information security insider threats in organisations,"** *Journal of information security and applications,* vol. 40, pp. 247-257, 2018.

[3] J. S. Lim, S. Chang, S. Maynard and A. Ahmad, **"Exploring the relationship between organizational culture and information security culture,"** *7th Australian Information Security Management Conference*, Perth, Western Australia, 2009.

[4] S. M. Furnell, M. Gennatou and P. S. Download, **"A prototype tool for information security awareness and training,"** *Logistics Information Management,* pp. 352-357, 2002.

[5] T. Herath and H. R. Rao, **"Protection Motivation and Detterrence: A framework for security policy compliance in organisations,"** *European Journal of Information Systems,* pp. 106-125, 2009.

[6] L. Dubé, **"Autopsy of a Data Breach: The Target Case.,"** *International Journal of Case Studies in Management,* vol. 14, no. 1, pp. 1-8, 2016.

[7] D. Craigen, N. Diakun-Thibault and R. Purse, **"Defining Cybersecurity,"** *Technology Innovation Management Review,* p. 4 (10), 2014.

[8] J. D'Arcy, A. Hovav and D. Galleta, **"User awareness of security countermeasures and its impact on Information Systems misuse: A Deterrence Approach.,"** *Information systems research,* vol. 20, no. 1, pp. 79-98, 2009.

[9] H. De Bruijn and M. Janssen, **"Building Cybersecurity Awareness: The need for evidence-based framing strategies,"** *Government Information Quarterly,* vol. 34, no. 1, pp. 1-7, 2017.

[10] M. Evans , L. A. Maglaras, Y. He and H. Janicke, **"Human Behaviour as an aspect of Cybersecurity Assurance,"** *Security and Communication Networks,* pp. 4667-4679, 2016.

[11] J. Leach, **"Improving User Security Behaviour,"** *Computers & Security,* vol. 8, no. 22, p. 685*692, 2003.

[12] L. Li, W. He, L. Xu, I. Ash, M. Anwar and X. Yuan, **"Investigating the impact of cybersecurity policy awarness on employees' cybersecurity behaviour,"** *ELSEVIER International Journal of Information Management,* 2019.

[13] R. V. Solms and B. V. Solms, **"From Policies to Culture,"** *Elsevier: Computer and Security,* vol. 23, no. 4, pp. 275-279, 2004.

[14] D. W. Straub, **"Effective IS Security: An Empirical Study,"** *Information Systems Research,* vol. 1, no. 3, pp. 255-276, 1990.

[15] R. Torten, C. Reaiche and S. Boyle, **"The impact of security awarness on information technology professionals' behaviour,"** *ELSEVIER Science Direct Computers & Security,* no. 79, pp. 68-79, 2018.