International Journal of Multidisciplinary Research and Growth Evaluation.

Cyber security culture in an IT company: An empirical study

C Antony Justin Arul Selvan [1*], Dr. Clayton Michael Fonceca [2]
[1] Research Scholar, P.G & Research Department of Social Work, Sacred Heart College (Autonomous), Tirupattur, Tamil Nadu, India
[2] Assistant Professor, P.G & Research Department of Social Work, Sacred Heart College (Autonomous), Tirupattur, Tamil Nadu, India

* Corresponding Author: **C Antony Justin Arul Selvan**

Article Info

ISSN (online): 2582-7138
Volume: 04
Issue: 02
March-April 2023
Received: 02-03-2023;
Accepted: 19-03-2023
Page No: 351-354

Abstract
The collective attitudes, values, and beliefs that a company has about the protection of its digital assets and data are referred to as its cybersecurity culture. It entails cultivating a culture where the preservation of data confidentiality, integrity, and availability is given top priority. The current inquiry was observed and examined using the descriptive design. To underline the merits and significance of various study criteria, the researcher used a descriptive research technique. There are 110 employees in the organization's employees of the company. The division of software, hardware, and shared services, which had 93 people, was chosen by the researcher. A simple random sampling technique was used. As a consequence, 93 workers were chosen as a sample. The main findings include mostly employees lack on cyber security culture because it is a startup company they currently recruit for employees based on the project domain. The training needs to be given based on cyber security culture in a company.

Keywords: Policy, Behavioral, Consciousness, Preventive, Technology, Effective, Culture

Introduction

The collection of attitudes, convictions, and practices that a company or individual adopts to maintain the safety of digital assets against online attacks is referred to as cybersecurity culture. A strong cybersecurity culture encourages everyone in a company to take ownership of preserving the security of digital assets and advocates a proactive rather than reactive approach to cybersecurity.

A holistic strategy is needed to develop a strong cybersecurity culture, one that includes educating people about online dangers, offering frequent training on cybersecurity best practices, and encouraging a spirit of cooperation and open communication. Establishing rules and processes that support cybersecurity is crucial, as is making sure that every employee is aware of their duties in upholding the security of digital assets.

The International Telecommunications Union (ITU) defines cyber security as “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets” within the cyber security foci of confidentiality, availability, and integrity (CIA) objectives

Even though these definitions express the need to protect assets, they are hardware and software- focused and do not take into account the human element of cyber security. Moreover, a multidisciplinary and multisensory system impacts cyber security and the risk associated with it.

Cyber researchers and risk analysts cannot holistically assess the risk posed to systems, networks, and users in a cyber domain since the physical environment and human/social interactions are omitted from these definitions. In turn, this results in ineffective communication among cyber security experts, whether they are academic researchers or practitioners.

Security professionals are continuously challenged by the increasing threat of cyber-attacks. Researchers continue to demonstrate that online users are a weak link in information security. Studying the relationship between cyber security and cultural, personality, and demographic variables is the purpose of this research. The study was conducted in four different countries and demonstrates a multicultural perspective on cyber-security. Particularly, the study investigates how behavior, self-efficacy, and privacy attitude are influenced by culture in comparison with other psychological variables and demographics (such as gender and computer expertise).

Review of Literature

Minhaj Ahmad Khan, and Khaled Salah (2018), a study conducted in "IoT security: Review, blockchain solutions, and open challenges" In this paper, we present and survey major security issues for IoT. We review and categorize popular security issues with regard to the IoT layered architecture, in addition to protocols used for networking, communication, and management. We outline security requirements for IoT along with the existing attacks, threats, and state-of-the-art solutions. Furthermore, we tabulate and map IoT security problems against existing solutions found in the literature. More importantly, we discuss, how blockchain, which is the underlying technology for bitcoin, can be a key enabler to solve many IoT security problems. The paper also identifies open research problems and challenges for IoT security.

Dejan Kosutic & Federico Pigni (2020), conducted a study on "Cybersecurity: investing for competitive outcomes". This paper explains the connection between cybersecurity and competitive advantage in order to assist businesses in addressing the issue of growing cybersecurity spending that does not result in measurable commercial value. Design/methodology/approach Through a qualitative research study, the authors examined a large body of literature and performed two rounds of semi-structured interviews with executives and security specialists from businesses in four different countries in the financial, IT, and security sectors. Findings The development of the Cybersecurity Competitive Advantage Model, which describes how to develop cybersecurity dynamic capabilities to gain long-term competitive advantage, was made possible by the analysis of the data.

Research limitations/implications the research offers the model's theorization based on a thorough assessment of the relevant literature, information acquired, opinions from knowledgeable respondents, and the authors' professional expertise. Although we thoroughly gathered and evaluated the data and adjusted for saturation, the results may not be as generalizable as they may be due to the inductive methodology we used. Practical implications Security experts may use the model to manage cybersecurity and interact with superiors more effectively. The suggested model explains to executives how to differentiate their organization in a creative way and how to maintain that competitive advantage. Originality/Value The provided model offers a way to prevent technical bias and to gain a competitive edge, which sets it apart from previous research, cybersecurity frameworks, and industry standards.

Xianghao Nan (2021), conducted a study on "Exploration of Core Technologies of Cyber Security". This study focuses on investigating the primary duties and fundamental technology of cyber security. The analysis of the PKI certification system's proof logic and the DSA digital signature standard led to the clarification of the signature's components and the discovery that the CPK public key could satisfy them all. As a result, the evidence-based truth logic of authentication was developed, leading to the creation of the new concepts of "identity authentication" and "proof- before-event." An autonomous self-assured network was built, a generic one-step protocol was developed, a workable technological path for cyber security was produced, and the practical relevance of identification was examined. All of these developments were based on identity authentication technology.

Prashant Chauhan & Gagandeep Kaur (2022), conducted a study on "Secure Digital India: Role of Artificial Intelligence in Cyber Security". This paper will look at how artificial intelligence may help the Indian government's Digital India initiative. The approach is to identify the areas that are relevant and appropriate in the field of cyberspace where artificial intelligence can be implemented. The method of implementation is doctrinal, by which the current trend related to the application of artificial intelligence in the field of cyberspace is examined. The study report comes to the conclusion that using artificial intelligence for cybersecurity in cyberspace will be a ground- breaking move in establishing a secure digital India.

Significance of the Study

With many security concerns and cyberattacks, cybersecurity is crucial in today's environment. Many businesses create software for data protection. The data is shielded by this program. Cybersecurity is crucial since it protects not only our systems from virus attacks but also helps to safeguard information. India has the most internet users after the United States and China.

Cybersecurity is crucial since it guards against the theft and destruction of many types of data. This covers delicate information, personally identifiable information (PII), protected health information (PHI), personal data, data pertaining to intellectual property, and information systems used by the government and businesses. Your company cannot protect itself against data breach operations without a cybersecurity program, making it an unavoidable target for cybercriminals.

Due to increased worldwide connection and the use of cloud services like Amazon Web Services to hold private and sensitive data, both inherent risk and residual risk are rising. The probability that your firm may experience a successful cyber-attack or data breach is rising as a result of the widespread bad setup of cloud services and increasingly savvy cybercriminals.

AIM

To study the Cybersecurity Culture in an IT industry.

Objectives

The present study undertaken with the following objectives in mind

1. To highlight the policy factors of Cybersecurity Culture.
2. To understand the behavioral concern of the IT employees.
3. To study the consciousness factor of Cybersecurity among IT employees.
4. To know about the preventive measure provided in an IT company.

5. To study the effective measures to enhance the cyber security culture in an IT company.
6. To find out the various factor of a cybersecurity culture framework.

Research Design

The descriptive design was used to observe and analyze the current investigation. The researcher employed a descriptive research strategy to emphasize the qualities and importance of several study criteria. The objective of this approach is to methodically gather data to characterize a phenomenon and comprehend the population designated in the research.

Universe & Sampling

The total population of the company consists of 110 employees. The researcher selected the software, hardware & shared services division which constituted 93 employees. A simple random sampling technique was adopted. This resulted in 93 employees being selected as a sample.

Tool for Data Collection

To conduct the study, the researcher used a Likert scale. This scale is utilized as a rating system to assess respondents' ideas, attitudes, and perceptions about cyber security culture.

1. Policy factor of Cyber Security
2. Behavioral factor of Cyber Security
3. Consciousness factor of Cyber Security
4. Preventive factor of Cyber Security
5. Technology factor of Cyber Security
6. Effective measures of Cyber Security

The reliability test was conducted Cronbach's Alpha value is 0.695. In this study Cronbach's Alpha as a measure was used to assess the reliability of a set of attributes or test items. The general rule of thumb is that a Cronbach's alpha of .60 and above is good, .70 and above is better, and .90 and above is best.

Analysis & Interpretation

Table 1: Distribution of respondents based on policy factor

Policy Factors on Cyber Security	Frequency	Percentage
Low	54	58.1
High	39	41.9
Total	93	100

The presented table shows that majority (58.1%) of the respondents have a low level of policy factor and more than two-fifth (41.9%) of the respondents have a high level of policy factor. This clearly shows that majority of the respondents have a low level of policy factor because they don't have a clear knowledge on policy factor.

Table 2: Distribution of respondents based on Behavioral Factors

Behavioral Factor on Cyber Security	Frequency	Percentage
Low	47	50.5
High	46	49.5
Total	93	100

The presented table shows that more than half (50.5%) of the respondents have a low level of behavioral factor and less than half (49.5%) of the respondents have a high level of behavioral factor. This clearly shows that the majority of the respondents have a low level of behavioral factors because of low behavior on the job.

Table 3: Distribution of respondents based on Consciousness Factor

Consciousness Factor on Cyber Security	Frequency	Percentage
Low	50	53.8
High	43	46.2
Total	93	100

The presented table shows that more than half (53.8%) of the respondents have a low level of consciousness factor. and less than half (46.2%) of the respondents have a high level of consciousness factor. This clearly states that most of the respondents have a low level of consciousness of cyber security.

Table 4: Distribution of respondents based on Preventive Factor

Preventive Factor on Cyber Security	Frequency	Percentage
Low	63	67.7
High	30	32.3
Total	93	100

The presented table shows that little more than the majority (67.7%) of the respondents have low level of preventive factor and less than one -third (32.3%) of the respondents have high level of preventive factor. This clearly shows that most of the respondents have low level of preventive factor because the company focus on the working domain of the employees.

Table 5: Distribution of respondents based on the Technology Factor

Technology Factor on Cyber Security	Frequency	Percentage
Low	62	66.7
High	31	33.3
Total	93	100

The presented table shows that little more than the majority (66.7%) of the respondents have a low level of technology factor and less than one-third (32.3%) of the respondents have a high level of technology factor. This clearly states that most of the respondents have a low level of technology factor because they have not aware of preventive tools.

Table 6: Distribution of respondents based on Effective Factor

Effective Factor on Cyber Security	Frequency	Percentage
Low	51	54.8
High	42	45.2
Total	93	100

The present table shows that more than half (54.8%) of the respondents have a low level of effective factor and more than two-fifth (45.2%) have of the respondent's high level of the effective factor. This shows that the majority of the respondents have a low level of respondents because of the improper measures taken on effective measures.

Table 7: Distribution of respondents based on Overall Factor

Overall Factors on Cyber Security	Frequency	Percentage
Low	51	54.8
High	42	45.2
Total	93	100

The present table shows that more than half (54.8%) of the respondents have a low level of cyber security culture and more than two-fifth (45.2%) of the respondents have a high level of cyber security culture. This shows that the majority of the respondents have a low level of respondents because the company is a startup so they have a low level of the concept of cyber security.

Suggestions

The study was conducted using a variety of aspects, including policy, behavioral, conscious, preventative, technological, and effective elements. This component in the cyber security architecture highlights the numerous facets of workers. Most of the data shows that employees' attitudes toward cyber security are low, while just a small number of employees have good attitudes toward the topic.

By providing them with skill training and raising their knowledge of cyber security, the organization should be more successful in upgrading the cyber security framework.

Conclusion

In conclusion, creating a strong cybersecurity culture is essential in the modern digital environment to safeguard people, businesses, and countries from online dangers. A cybersecurity culture entails raising awareness, defining rules and guidelines, offering resources and training, and instilling a feeling of accountability in all workers.

Recognizing that cybersecurity is not only a technical problem but also a human one is crucial. As a result, developing a cybersecurity culture calls for a comprehensive strategy that integrates people, processes, and technology. A robust cybersecurity culture may reduce the likelihood of cyberattacks, lessen the effects of security lapses, and guarantee the confidentiality, integrity, and accessibility of critical data.

In the end, creating a cybersecurity culture is a continual process that needs constant work and adaptability to emerging threats and technological advancements. Organizations and people may better defend themselves against cyberthreats and contribute to a safer and more secure digital ecosystem by prioritizing cybersecurity and encouraging a culture of awareness.

References

1. Access CS. Cybersecurity: Opportunities, Threats, and Challenges, 2016.
2. Bordoff. Cyber Attacks, Contributing Factors, and Tackling Strategies: The Current Status of the Science of Cybersecurity. International Journal of Cyber Behavior, Psychology, and Learning, 2017, 68-82.
3. Catherine AV, Fonceca CM. Employee stress and its impact on their job performance. Journal of Academia and Industrial Research (JAIR). 2022; 10(3):34-38.
4. Chauhan. Secure Digital India: Role of Artificial Intelligence in Cyber Security published in Asian Journal of Organic & Medicinal Chemistry. Asian Journal of Organic & Medicinal Chemistry, 2022, 640-649.
5. Cirani. Enforcing Security Mechanisms in the IP-Based Internet of Things. An Algorithmic Overview, 2013.
6. Elleithy. Denial of Service Attack Techniques: Analysis, Implementation and Comparison, 2000, 66-71.
7. Fehling. Cloud Computing Patterns. Fundamentals to Design, Build, and Manage Cloud Applications. Springer-Verlag Wien, 2014.
8. George KN, Fonceca CM. Job Stress and its Impact on Employees in Industries. Journal of Academia and Industrial Research (JAIR). 2022; 11(1):1-5.
9. Hogail. How is the ministry fostering public-private partnerships (PPPs) with local private developers?, 2015.
10. Khan. Cognitive-Radio-Based Internet of Things: Applications, Architectures, Spectrum Related Functionalities, and Future Research Directions. IEEE Wireless Communications, 2017, 17-25.
11. Klynveld PG. Clarity on Cybersecurity. Driving growth with confidence, 2018.
12. Kosutic. Cybersecurity: investing for competitive outcomes. Journal of Business Strategy, 2021, 28-36.
13. Kshetri N. Cybercrime and cybersecurity in India: causes, consequences and implications for the future. Crime, Law and Social Change, 2016.
14. Lin Z. Pricing Cyber Security. Journal of Mathematical Finance, 2022, 46-70.
15. Maani. Thinking, System Dynamics: Managing Change and Complexity. New Zealand: Pearson Education, 2007, 1-278.
16. Umesh Samuel Jebaseelan A, Michael Fonceca C. Transdisciplinary Research: A social work perspective. Int. J of Aquatic Science. 2021; 12(2):549-557.