ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 4| April 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

A STUDY OF CYBERSECURITY AWARENESS PROGRAM IN ORGANISATION

Mr.S. Muruganantham[1], R.E. Silviya[2]
[1]*Assistant Professor, Department of B.com IT, Dr.N.G.P Arts and Science College*
[2]*Student, Department of B.com IT, Dr.N.G.P Arts and Science College*

ABSTRACT
In the digital age, organizations face increasing threats from cyberattacks, often exacerbated by human error and lack of cybersecurity awareness among employees. This study investigates the effectiveness of cybersecurity awareness programs within organizational environments, focusing on their impact on employee behavior, threat recognition, and overall organizational security posture. Using a case study approach, data were collected through surveys, interviews, and security incident reports from a mid-sized enterprise over a 12-month period. The results indicate a significant improvement in employees' understanding of cybersecurity best practices and a measurable reduction in phishing incidents post-training. The study underscores the importance of continuous education, management support, and an adaptive training model tailored to organizational needs. Findings contribute to best practices for implementing and refining cybersecurity awareness programs in similar organizational contexts.

KEYWORDS: *Cybersecurity Awareness, Organizational Security, Security Culture, Employee Behavior.*

INTRODUCTION

Cybersecurity awareness is essential for recognizing potential threats and implementing strategies to protect both individuals and organizations from malicious attacks. It involves understanding how to identify phishing attempts, the importance of strong passwords, and safe online practices. As cyber threats continue to evolve, awareness programs play a critical role in educating employees about the risks they face daily and how to mitigate those risks. These programs help foster a culture of vigilance, where individuals are empowered to recognize and respond to threats promptly.

The goal of cybersecurity is to safeguard systems, networks, devices, and data from cyber-attacks. By applying technologies, processes, and controls, organizations reduce the risk of unauthorized exploitation and damage to their IT infrastructure. The digital landscape is increasingly targeted by hackers and cybercriminals, aiming to steal sensitive data or disrupt services. Cybersecurity measures are crucial for protecting various types of data, including sensitive personal information, intellectual property, and confidential business data. Understanding these threats and adopting appropriate security measures is key to maintaining organizational integrity and reputation.

Cybersecurity awareness involves educating individuals about the nature of cyber threats and promoting good security hygiene. Employees, regardless of their role in the organization, must understand basic security practices such as safe browsing, email verification, and cautious online interactions. High-profile cases, such as the ransomware attack on Ireland's Health Service Executive, highlight the devastating consequences of a lack of cybersecurity awareness. In this case, a single employee opening a phishing email led to a $100 million loss. This underscores the need for regular cybersecurity training, ideally at least once a year, to ensure employees remain vigilant and informed.

When cybersecurity awareness becomes ingrained within an organization, it evolves into a security culture. In such an environment, cybersecurity practices are not only understood by individuals but are collectively embraced and consistently applied across departments. In a security-conscious culture, potential threats are addressed proactively, breaches are swiftly reported, and security risks are minimized. The result is a stronger, more resilient organization that can better withstand the challenges of an ever-evolving cyber threat landscape.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 4| April 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

STATEMENT OF THE PROBLEM

As organizations continue to integrate digital technologies into their daily operations, the risk of cyber threats has risen exponentially. Despite investing in sophisticated cybersecurity tools and systems, many organizations still face significant vulnerabilities due to inadequate human awareness and behavior. Employees, who often serve as the first line of defense, are frequently unaware of basic cybersecurity practices, making them susceptible to phishing, malware, social engineering attacks, and other cyber risks. The lack of a formal cybersecurity awareness program exacerbates these vulnerabilities, as employees are not equipped with the necessary knowledge or skills to recognize and prevent potential threats. This gap in understanding often leads to negligent actions, such as weak password practices, unsafe browsing habits, or inadvertently disclosing sensitive information, which can compromise the organization's security and lead to costly data breaches, financial losses, and reputational damage. This project aims to address this critical gap by developing and implementing a cybersecurity awareness program tailored to the needs of the organization, focusing on educating employees about best practices, common threats, and the importance of maintaining robust cybersecurity hygiene. By fostering a culture of security awareness, organizations can significantly reduce their exposure to cyber risks and enhance their overall security posture.

ABOUT OF THE STUDY

The scope of this study on cybersecurity awareness programs in organizations involves a comprehensive exploration of the design, implementation, evaluation, and continuous improvement of such programs. It focuses on identifying the defects and challenges within these programs and offers solutions to make them more effective in mitigating cyber risks and enhancing organizational security. This study will address various aspects of cybersecurity awareness, including training content, employee engagement, measurement of effectiveness, and organizational culture.

RESEARCH METHODOLOGY

It's a logical, systematic plan to resolve a research problem. A methodology details a researcher's approach to the research to ensure reliable, valid results that address their aims and objectives. It encompasses what data they're going to collect and where from, as well as how it's being collected and analyzed.
Example, how did the researcher go about deciding:

- What data to collect (and what data to ignore)
- Interview (which can be unstructured, semi-structured or structured)
- Focus groups and group interviews
- Surveys (online or physical surveys)
- Observations (watching and recording activities)
- Biophysical measurements (e.g., blood pressure, heart rate, etc.)
- Documents and records (e.g., financial reports, court records, etc.)

DEFINITIONS

Research into how individuals and businesses collect and analyze data. Accurate and relevant research guides key business decisions, including marketing plans, staffing decisions and expansions, and critical data, like environment impacts, health care, and social characteristics. Determining what data is most useful for your goals and finding the most effective ways to obtain it can help your company make successful long-term decisions.

RESEARCH DESIGN

Research design refers to the overall strategy utilized to carry out defines a succinct and logical plan to tackle established research questions through the collection, interpretation, analysis, and discussion of data. Research into design is research about design, with design is research about design, with design and designers as its subject. Much research into design is academic, where scholars from different disciplines-psychology, anthropology, education, history…-turn their gaze to design and creative work.

SOURCES OF DATA

The sources of data can be classified into two types: statistical, statistical and non - statistical. Statistical sources refer to data that is gathered for some official purposes, incorporate censuses, and officially administered surveys. Non-statistical sources refer to the collection of data for other administration purposes or for the private sector.

DIFFERENT SOURCES OF DATA

INTERNAL SOURCES

When data is collected from reports and records of the organization itself, they are known as internal sources.
For example, a company publishes its annual report' on profit and loss, total sales, loans, wages, etc.

EXTERNAL SOURCES

When data is collected from sources outside the organization, they are known as external sources. For example, if a tour and travel company get information on Karnataka tourism from Karnataka Transport Corporation, it would be known as an external source of data.

TYPES OF DATA

Primary Data

- Primary data means first-hand information collected by an investigator.
- It is collected for the first time.It is original and more reliable.
- For example, the population census conducted by the government of India after every ten years is primary data.

Secondary data

- Secondary data refers to second-hand information.
- It is not originally collected and rather obtained from already published or unpublished sources.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 4| April 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

- For example, the address of a person taken from the telephone directory or the phone number of a company taken from just Dial are secondary data.

STATISTICAL TOOLS USED FOR ANALYSIS

The following tools were employed in time with objective of study:

- Aerage Rank Analysis

REVIEW OF LITERATURE

Nash (2023) reviewed emerging trends in cybersecurity training, highlighting the need for adaptive, real-time training programs that evolve with the ever-changing cyber threat landscape. Nash argued that organizations should continuously update training content to address new and evolving cybersecurity challenges.

Patel, Bhatt, and Patel (2022) explored the impact of gamification and simulation-based learning in cybersecurity training, suggesting that interactive approaches significantly increase employee engagement and improve knowledge retention.

OVERVIEW OF STUDY

This study investigates the effectiveness of cybersecurity awareness programs in organizations, particularly focusing on how these programs influence employee knowledge, behaviour, and overall security outcomes. In an era where cyber threats are increasingly sophisticated, many organizations are prioritizing cybersecurity training to equip their workforce with the necessary skills to prevent and respond to cyberattacks.

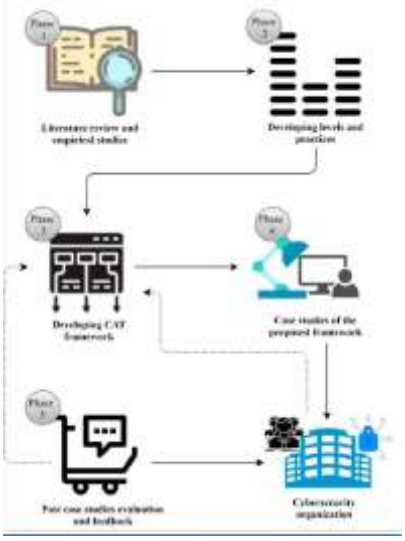
The primary objective of the study is to evaluate the impact of these programs on employee understanding of common cyber threats, such as phishing, malware, and data breaches. Additionally, the research will explore whether enhanced awareness leads to improved security practices and reduced vulnerabilities within the organization. By identifying gaps in current training methodologies, the study will offer recommendations for improving the design and delivery of cybersecurity education.

Key research questions include:

- How do cybersecurity awareness programs impact employee behaviour and security practices?
- What is the correlation between training frequency and the reduction of security incidents?
- What are the challenges organizations face in implementing effective cybersecurity training?

Methodologically, the study will combine surveys and interviews with employees and cybersecurity professionals to assess changes in knowledge and security practices pre- and post training. Additionally, data on organizational security incidents will be analysed to gauge the effectiveness of the programs.

TABLE 4.2 CYBERSECURITY AWARENESS TRAINING



S.NO	Training	Total of the Respondent	Percentage
1	Yes	109	90.8%
2	No	11	9.2%
	Total	**120**	**100%**

Source: Primary data

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 4| April 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

INTERPRETATION

The above Table Reveals the Cybersecurity Awareness Training 90.8% of them above Yes, 9.2% of them above No.

INFERENCE

Here Majority 90.0% of the Respondent are between Yes.

CHART NO 4.2 CYBERSECURITY AWARENESS TRAINING

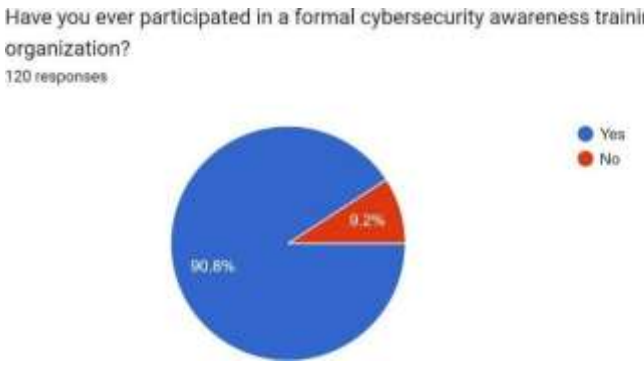


TABLE 4.3 AFTER COMPLETING THE TRAINING

S.NO	Completing Training	Total of the Respondent	Percentage
1	Very poor	7	5.8%
2	Poor	3	2.5%
3	Average	15	12.5%
4	Good	55	45.8%
5	Excellent	40	33.3%
	Total	**120**	**100%**

Source: Primary data

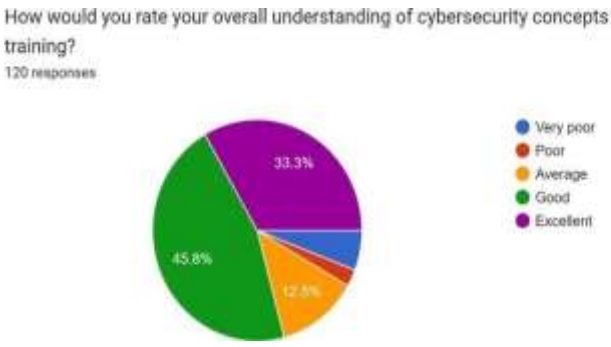
INTERPRETATION

The above Table Reveals the After Completing the Respondent is clear that 5.8 of them above Very poor, 2.5% of them above Poor, 12.5% of them above Average, 45.8% of them above Good, 33.3% of them above Excellent.

INFERENCE

Here Mostly 45.8% of the Respondent are between 55.

CHART NO 4.3 AFTER COMPLETING THE TRAINING



CONCLUSIONS

In conclusion, a study of cybersecurity awareness programs in organizations highlights the critical importance of continuous, tailored training in enhancing overall security posture. The findings typically emphasize that when employees are well-informed about cybersecurity risks and best practices, the likelihood of security breaches, such as phishing attacks or data leaks, decreases significantly. Additionally, the research often underscores the role of leadership in cultivating a security-first culture, where cybersecurity is seen as a shared responsibility rather than solely the domain of the IT department. It also reveals that interactive and engaging training methods, such as gamification or scenario-based simulations, tend to yield better results in terms of employee retention and real-world application

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 4| April 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

of security concepts. However, the study may also point out the challenges organizations face in implementing effective programs, especially in small and medium-sized enterprises (SMEs) that may lack the resources to invest in robust training infrastructure. Ultimately, the study suggests that a well-structured cybersecurity awareness program not only reduces organizational risk but also empowers employees to become proactive defenders of organizational data and systems.

BIBLIOGRAPHY

REFERENCE

1. *"Cybersecurity for Beginners" by Raef Meeuwisse.*
2. *"The Cybersecurity Survival Guide" by Paul J. DeRocco.*
3. *Cybersecurity & Infrastructure Security Agency (CISA) (www.cisa.gov).*