CYBERSECURITY AWARENESS

Mohammed Mustafa Khan

***Abstract** - Technology is advancing at a very high speed, becoming more sophisticated and complex. Similarly, due to the vastness of the digital world, cyber threats have also increased in complexity and frequency. The rapid advancement of technology has brought unprecedented conveniences but also significant risks. Therefore, security awareness is essential for every individual and organization. Cyber threats such as phishing attacks, malware attacks, social engineering, Denial of service attacks, and insider threats have become sophisticated, proving to be a challenge to individuals and organizations. This paper evaluates security awareness in the organization with a keen interest in why the program is essential, the components of the program, challenges that might be faced while implementing the program, and what role the organization and employees have to play to ensure the environment is secure. The paper provides a comprehensive analysis highlighting the importance of security awareness in an organization's current sophisticated digital world.*

***Keywords** - Security Awareness, Cyber Threats, Phishing, Malware, Social Engineering, Information Security, Cybersecurity Training, Risk Mitigation, and Continuous Education.*

1.0 Introduction

Security awareness is the knowledge and attitude that members of an organization have concerning protecting the organization's physical and electronic information assets. Organizations are now evolving to digital platforms that expose most of their data and activities on the digital landscape, from financial transactions to personal communications [2]. Security awareness essentially means that the organization realizes the potential of people deliberately or accidentally stealing, abusing, or damaging the protected data stored on the organizational computer systems [1]. With the increase in digital breakthroughs, cyber threats have significantly increased, hence the need for security awareness in the organization to keep the workforce and business safe.

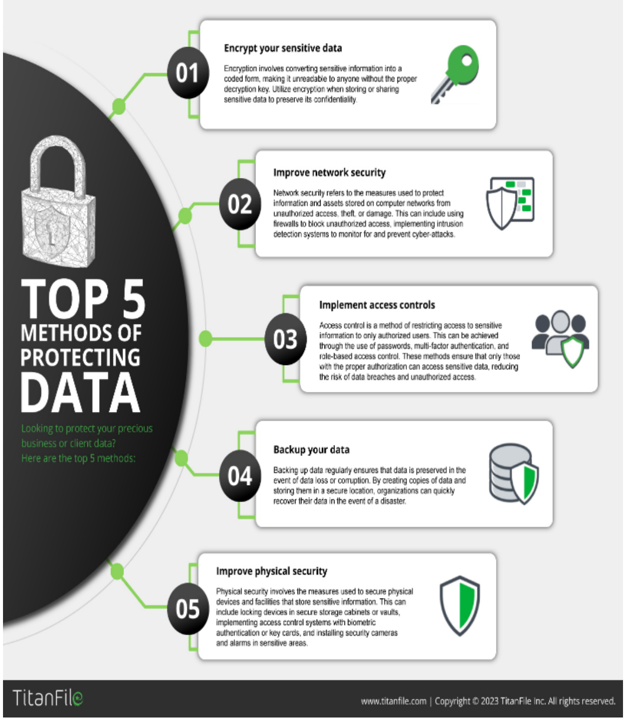
Security awareness is an ongoing process that involves educating and training employees about the threats in cyberspace. Security awareness is the long-term goal of every organization, ensuring that the environment is safe and conducive to the safety of its employees and customers [5]. A security awareness program operates best when a reasonable plan is implemented with procedures and policies that support a comprehensive team concept. The team tasked with the responsibility is crucial for sustaining a healthy corporate environment, and it should include everyone connected to corporate functions [3]. To formulate an effective team, the management should develop a team that requires each employee to form partnerships with external associates and build a diverse team. The plan should help the teams forge an effective security awareness team with various entities to achieve basic protective practices that help prevent security threats to the organization [3]. However, despite everyone possessing different essential roles, knowledge, and skills, they should understand that they are vital to protecting the organization's assets. By formulating this, the organization prevents liability risk and losses. Through this, in case of an accident, each team member will know the necessary steps to prevent the situation from escalating.

2.0 Importance of security awareness

Traditional security used to be straightforward, only using a strong password. However, with the increase in sophistication in cyber-attacks, there is a need to increase the levels of security implemented in organizations [2]. Several end users are not aware of the rampant security threats. Security awareness and training help employees become aware of threats. Security awareness is the process of promoting security in the organization. However, security awareness training is the implementation of mechanisms that remind the organization to take information security seriously [5].

2.1 Protect Sensitive Data

One of the reasons why security awareness is critical is to protect company-sensitive data. Cybercriminals highly target companies' sensitive data, such as trade secrets, financial information, and customer data [5]. Employees need to be aware of how to protect sensitive data through several mechanisms, such as using passwords that are changed often, detecting phishing attempts, and securely storing sensitive information in the organization [3].



TOP 5 METHODS OF PROTECTING DATA

Looking to protect your precious business or client data? Here are the top 5 methods:

01 Encrypt your sensitive data

Encryption involves converting sensitive information into a coded form, making it unreadable to anyone without the proper decryption key. Utilize encryption when storing or sharing sensitive data to preserve its confidentiality.

02 Improve network security

Network security refers to the measures used to protect information and assets stored on computer networks from unauthorized access, theft, or damage. This can include using firewalls to block unauthorized access, implementing intrusion detection systems to monitor for and prevent cyber-attacks.

03 Implement access controls

Access control is a method of restricting access to sensitive information to only authorized users. This can be achieved through the use of passwords, multi-factor authentication, and role-based access control. These methods ensure that only those with the proper authorization can access sensitive data, reducing the risk of data breaches and unauthorized access.

04 Backup your data

Backing up data regularly ensures that data is preserved in the event of data loss or corruption. By creating copies of data and storing them in a secure location, organizations can quickly recover their data in the event of a disaster.

05 Improve physical security

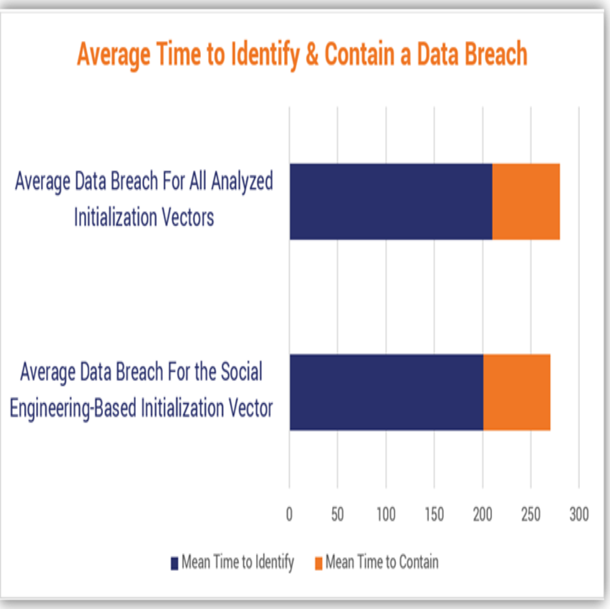
Physical security involves the measures used to secure physical devices and facilities that store sensitive information. This can include locking devices in secure storage cabinets or vaults, implementing access control systems with biometric authentication or key cards, and installing security cameras and alarms in sensitive areas.

TitanFile www.titanfile.com | Copyright © 2023 TitanFile Inc. All rights reserved.

Source: https://www.titanfile.com/blog/5-methods-of-protecting-data/

2.2 Educates Employees on Security Threats

Security awareness helps employees know about various security threats the organization faces daily. Security awareness is the first line of defense, and when employees are aware of threats, they can identify them and make crucial decisions [5]. For instance, if employees receive phishing emails, the trained ones may recover from the damage if they accidentally open them. However, the ones who have not been trained may be victims and potentially lose company data [1]. Additionally, this helps to create a culture of security in the organization. The program allows employees to know their roles and responsibilities, shifting their mindset from "someone else's problem" to "my problem," making them proactive in protecting sensitive data and reporting anything unusual [6].



Source: https://www.thesslstore.com/blog/wp-content/uploads/2023/01/time-to-id-contain-breach-shadow.png

2.3 Helps Meet Compliance Regulations

The authorities require Every organization to comply with various security policies regarding sensitive data. Failure to comply with these regulations could lead to severe repercussions for the organization [3]. The organization must educate employees about industry rules and data protection policies. Additionally, it is essential to evolve the training to ensure the organization keeps up with the changing regulations. For instance, companies associated with GDPR are trained to comply with the protection of personal data, strengthen their commitment to data privacy, and reduce legal risks [2].

2.4 Reduces Human Error

One of the leading causes of security breaches is human error. Whether intentional or unintentional, these errors significantly contribute to organizational security incidents [6]. The errors can range from clicking malicious emails to mishandling sensitive data. Nevertheless, employees with the proper training are less likely to make costly mistakes, saving the organization a lot of money and reducing security breaches [5].

2.5 Increases Customer Confidence

Customers are very confident when they know that an organization prioritizes their information, increasing their confidence in doing business with it. When companies don't prioritize their customers' information safety, they can lose even their loyal customers [6]. Similarly, a data breach can cost the company a lot of money regarding legal actions from complaints. According to IBM's Cost of a Data Breach Report 2022, a company may lose an average of $1.42 million in a data breach. Through a security awareness program, the company establishes a proactive barrier that separates cybercriminals from potential victims.

3.0 What Should Be Included in Security Awareness?

Security awareness has evolved from being reserved mainly for security professionals to incorporating IT administrators and employees. The mode and scope of the program may vary for different organizations based on the number of employees, the budget, and how the organization is positioned [6]. Nevertheless, some core components should be considered when implementing the program in an organization.

3.1 Email Security

Email serves as one of the core modes of communication in every organization. However, it is the easiest way for attackers to access the organization using ransomware, phishing, BEC, and malware. According to statistics, about 94% of dangerous malware and ransomware enter an organization using emails [6]. Therefore, training employees to protect themselves and the organization by securing their emails is essential.

3.2 Phishing and Social Engineering

Human attack surfaces another weak point that attackers usually exploit. Social engineering attackers are aware of this loophole, and they are very ready to exploit it [7]. They exploit human behavior and emotions to influence their decisions and take the desired actions [1]. For instance, users can be duped to provide their credentials, transfer funds to unknown people, grant system access, and disclose sensitive information. According to the 2021 Data Breach Investigation Report on Verizon, over 35% of data breaches originated from phishing attacks [2]. However, through proper training, users are less likely to fall for these traps easily.

3.3 Ransomware and Malware

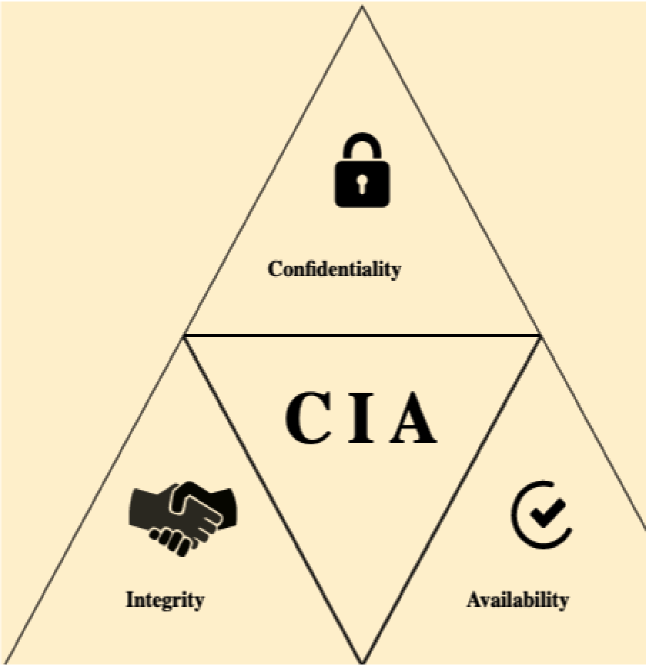
Ransomware and malware are software aimed at tampering with the normal functioning of computer systems and affecting the organizational business. These software are believed to enter the organization through phishing emails. According to research, 300,000 new malware pieces are being created daily [1]. In 2020, the SonicWall Cyber Threat Report indicated an increase in ransomware attacks by 48% [7].

3.4 Browser Security

Browsers are gateways to the internet and hold large amounts of sensitive data, such as personal information, which makes them an easy target for attackers [8]. Most website users' access is unsafe and contains links that might carry malware affecting the systems [2]. Therefore, training employees on the best practices when handling browsers, browser security tips, internet and social media policies, and browser threats is crucial.

3.5 Information Security

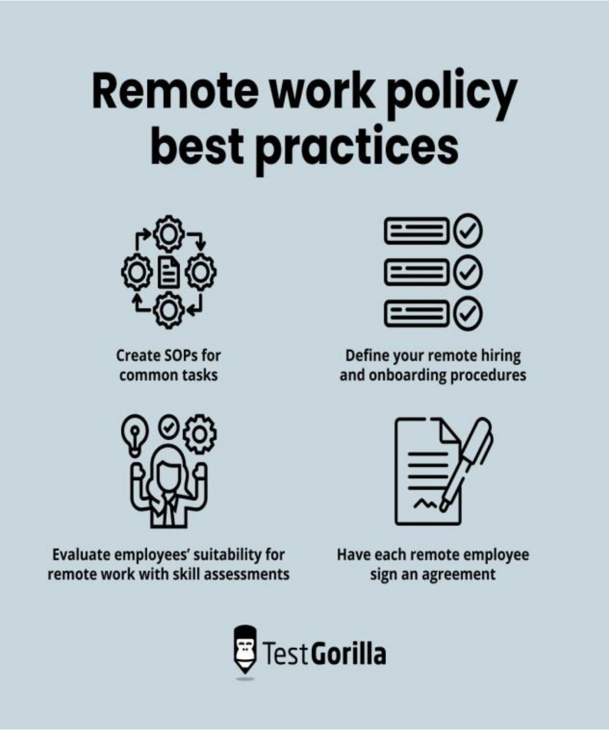
Information is the most prized asset in the organization. That is why it is crucial to maintain its integrity, confidentiality, and availability. The program should incorporate courses that emphasize the criticality of the data and how everyone should strive to protect it. Consequently, teach employees how to store, share, handle, and dispose of sensitive information to prevent it from leaking to attackers [8]. Similarly, they should be trained on the legal and regulatory obligations and what might happen to the organization if any data breach occurs [7]. Employees should also be trained on incident reporting to handle issues and prevent massive destruction quickly.



Source: https://www.hackerone.com/sites/default/files/infograph.png

3.6 Remote Work Protocol

With the advent of technology, organizations are now evolving to remote work and implementing a hybrid model. This creates a new security threat to the organization's infrastructure because now employees are required to ensure there is robust security in their home systems, too [7]. However, the additional security risks can be reduced using the proper knowledge and tools provided for employees. In the program, employers should include the dangers of connecting to the company resources using public WIFI networks, the use of personal devices and authorized software, and the importance of using VPNs for additional security layers [7].


Remote work policy best practices
Create SOPs for common tasks
Define your remote hiring and onboarding procedures
Evaluate employees' suitability for remote work with skill assessments
Have each remote employee sign an agreement
TestGorilla

Source: https://www.testgorilla.com/blog/remote-work-best-practices/

3.7 Password Security

According to the Federal Trade Commission's (FTC) Consumer Sentinel Network, over 5.7 million cybercrime reports were filed by consumers in 2021, with identity theft accounting for 25% of these incidents [1]. In today's environment, where threats are pervasive, a strong password is essential. Security awareness programs should emphasize the importance of effective password management and include best practices for creating and maintaining strong passwords. Additionally, employees should be encouraged to use multifactor authentication (MFA) whenever possible to safeguard accounts from potential compromises further.

PASSWORD SECURITY TIPS
Include numbers and characters
Use a password manager software
Lie when answering security questions
Change your password regularly
Use 8-word phrase to generate a coded password
***
LE VPN
INTERNET BY YOUR OWN RULES

Source: https://www.le-vpn.com/password-security/

4.0 Components of an Effective Security Awareness Program

An effective security awareness program is comprehensive, engaging, and tailored to an organization's or individual's specific needs. The program should cover a wide range of topics, from basic cybersecurity hygiene to more advanced concepts like recognizing sophisticated phishing attempts or understanding the implications of a data breach [3].

4.1 Training and Education

The first critical component of any security awareness program is training and education. as such, employees should also be trained on what risks or threats they might face in the working environment [8]. This includes identifying a phishing email, comprehending the significance of the password, and even reporting suspicious activity [2]. Training should be done so that it is repetitive to update the employees with the trends in cybersecurity.

4.2 Communication and Engagement

Effective communication is critical to maintaining a security-aware culture. The employees should receive frequent, meaningful information on new threats, new safety measures, and new company policies via emails, company newsletters or intranet portals [2]. Engaging employees through interactive sessions, such as workshops or simulated phishing exercises, where employees receive invitation for the employee to take the bait and click a link that poses a potential threat to the company's security, as a reminder, to stay alert for such threats.

4.3 Policy and Procedure Development

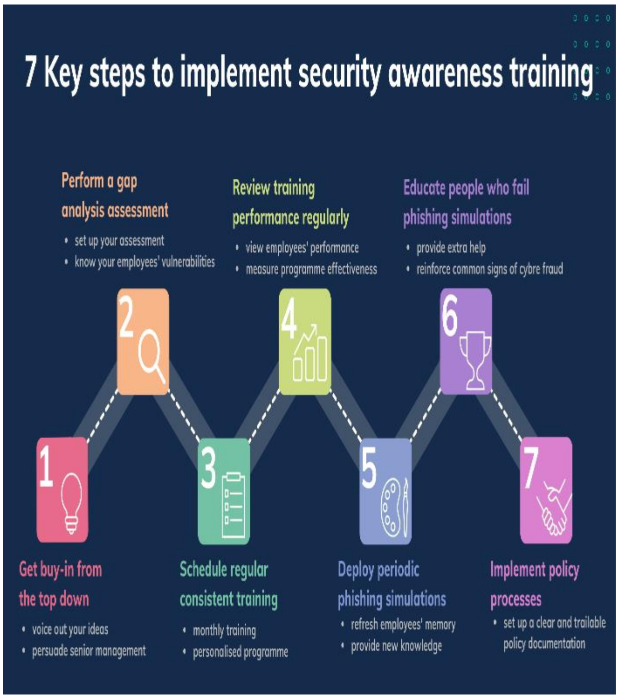
An organization must have clear policies and procedures for explaining conduct, which provides security standardization. These should be well recorded and made available to all employees [9]. It may contain acceptable use policies – computer, telecommunication resources, and data; security measures on data collection, storage, processing, and dissemination; and security procedures in the event of security breaches [4]. These policies also require being reviewed and updated frequently for new threats to be addressed and changes to the organization's environment.

4.4 Leadership and Support

Leadership support is a vital component in managing a security awareness program. Quite often, the management of an organization influences the rest of the company through its actions, and if the management is committed to cyberspace security, then others will follow [1]. Leadership support also aids in identifying the resources required to support an effective program and support in the form of time to train funding for the tools, resources, and workforce to drive the initiative [9].

4.5 Continuous Improvement

Awareness and training cannot be conducted in a 'conventional manner' where it is performed once a year or once a semester; instead, it is a process that is carried out perennially. Threats are dynamic, which means the measures used to counter them are also dynamic. Security awareness quizzes, surveys, and reinvention of security awareness programs are good interventions that can be used to determine new areas that have to be covered [9]. Other approaches that could also be applied include employee feedback, where their concerns and challenges can be gathered to enhance the program and better respond to their needs.



7 Key steps to implement security awareness training

1 Get buy-in from the top down
- voice out your ideas
- persuade senior management

2 Perform a gap analysis assessment
- set up your assessment
- know your employees' vulnerabilities

3 Schedule regular consistent training
- monthly training
- personalised programme

4 Review training performance regularly
- view employees' performance
- measure programme effectiveness

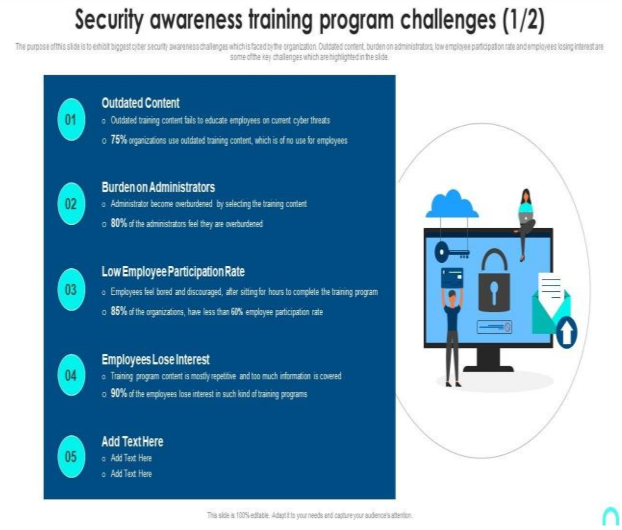
5 Deploy periodic phishing simulations
- refresh employees' memory
- provide new knowledge

6 Educate people who fail phishing simulations
- provide extra help
- reinforce common signs of cybre fraud

7 Implement policy processes
- set up a clear and trailable policy documentation

5.0 Challenges in Implementing Security Awareness Programs

While the importance of security awareness is widely recognized, implementing an effective program is not without challenges. Organizations often face several obstacles that can hinder the success of their initiatives [10].



Security awareness training program challenges (1/2)

The purpose of this slide is to exhibit biggest cyber security awareness challenges which is faced by the organization. Outdated content, burden on administrators, low employee participation rate and employees losing interest are some of the key challenges which are highlighted in the slide.

01 Outdated Content
- Outdated training content fails to educate employees on current cyber threats
- 75% organizations use outdated training content, which is of no use for employees

02 Burden on Administrators
- Administrator become overburdened by selecting the training content
- 80% of the administrators feel they are overburdened

03 Low Employee Participation Rate
- Employees feel bored and discouraged, after sitting for hours to complete the training program
- 85% of the organizations, have less than 60% employee participation rate

04 Employees Lose Interest
- Training program content is mostly repetitive and too much information is covered
- 90% of the employees lose interest in such kind of training programs

05 Add Text Here
- Add Text Here
- Add Text Here

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Source: https://www.slidegeeks.com/media/catalog/product/cache/1280x720/S/e/Security_Awareness_Training_Program_Challenges_Rules_PDF_Slide_2.jpg

5.1 Lack of Resources

One major critical issue is the absence of money, time, and staff – or rather, a severe scarcity of these commodities. Essentially, tiny organizations may be unable to dedicate the right amount of capital towards achieving and sustaining an effective security awareness program. This may result in some areas being uncovered in training, outdated materials, or inadequate employee engagement.

5.2 Employee Resistance

Another typical issue is the resistance from the organizational members, specifically the workforce. Security awareness training can sometimes be viewed as boring and inconsequential if the presented content does not meet the needs or position of the employee [10]. However, this resistance can be overcome by observing certain strategies for programmes' creation: making the participants focus not only on the training content as essential but also as crucial for their choice [3].

5.3 Measuring Effectiveness

Another of the challenges of managing security awareness is the difficulty of assessing the success of security awareness programs. Compared to restricting security targets with quantifiable measures, the outcome of the security awareness training is hard to measure [1]. To determine the effectiveness of their efforts, organizations must often use indirect signs, including the number of recorded phishing occurrences or password renewals.

5.4 Keeping Pace with Evolving Threats

The rapidly changing nature of cyber threats poses a continuous challenge for security awareness programs. The problem with security awareness content is that it has to be refreshed periodically in response to emerging threats from attackers [4]. This calls for constant learning and change, often a costly affair, although it can also involve many other costs.

6.0 The Role of Continuous Education

Security awareness must, of necessity, be an ongoing process; the element of training is intrinsic to this. With information security threats continuing to evolve, using one-off training sessions is likely only to result in short-term engagement [10]. However, security awareness requires constant updates, tuition, realistic practice, drills, and exercises.

6.1 Regular Updates

To remain relevant to the threats and security measures, constant updates are necessary to communicate the information to the employees. This can be done through short newsletters, online webinars or videos [10]. The issue is to provide information in such a way that it is quickly consumable and related to the performance of the employees on the job.

6.2 Real-World Simulations

A positive outcome of simulations is that they can be used in reminders and to check the effectiveness of security awareness programs, such as phishing tests [10]. One-way organizations can evaluate their capacity to identify threats and hazards is to mimic situations that an employee could experience [4]. These exercises also make it possible to gather helpful information to help the healthcare organization determine which aspect of further training is required.

6.3 Continuous Feedback and Improvement

To enhance the security awareness program, employee feedback should be more frequent. From the surveys, focus group discussions and one-on-one interviews, one can find where workers are vulnerable or lack confidence [10]. This feedback should be used to filter, improve and transform the content of training programs into the most relevant and interactive.

6.4 Certification and Recognition

To ensure that the employees engage in the programs, organizations must provide certification programs or recognition of the courses taken within the scope of security awareness training. It also creates a culture of security for the employees but, at the same time, motivates employees to work harder [4]. Rewarding good behaviors is even more effective because it promotes secure workplace practices and keeps a lousy actor away.

7.0 Conclusion

In conclusion, security awareness is an essential component of modern cybersecurity strategies. The importance of informed and vigilant individuals cannot be overstated as the threat landscape continues to evolve. As seen from the preceding cases, it is clear that well-informed and observant people cannot be overemphasized, especially as the threats are abound and constantly changing. Thus, Security awareness programs are a multi-faceted social engineering endeavor involving training, communication, policy development, leadership support, and analyst improvement. Despite the challenges, the benefits of a well-implemented security awareness program are clear: The benefits of the programs are the minimized risks of security breaches, meeting regulatory requirements, and a safer organizational environment. With modern threats changing and evolving, the effectiveness of continuous training has assumed a much higher level of importance than before. Organizations should be willing to continue enhancing and evolving policies and practices of security awareness. It is thus the role of organizations to ensure they create security awareness so that employees can effectively hold their hands as they protect the organization from cyber security threats and, as a result, protect its stakeholders from the harsh impact of a security breach.

10. Reference

[1] A. Sultan, Elmabruk Laias, and A. El, “Investigating Practices of Information Security Awareness: Perspectives from Government Entities in Libya,” International Journal of Computer Applications, vol. 186, no. 1, pp. 9–15, Jan. 2024, doi: https://doi.org/10.5120/ijca2024923330.

[2]G. Lyon, “Informational inequality: the role of resources and attributes in information security awareness,” Information & computer security, Nov. 2023, doi: https://doi.org/10.1108/ics-04-2023-0063.

[3] E. Riahi and M. Sirajul Islam, “Employees’ information security awareness (ISA) in public organisations: insights from cross-cultural studies in Sweden, France, and Tunisia,” Behaviour & Information Technology, pp. 1–23, Feb. 2024, doi: https://doi.org/10.1080/0144929x.2024.2311734.

[4] Adamu Abdullahi Garba, Maheyzah Md. S, and S. othman, “Holistic Systematic Review on Methodologies of Assessing Effectiveness Cybersecurity Awareness Program,” Research Square (Research Square), May 2024, doi: https://doi.org/10.21203/rs.3.rs-4329496/v1.

[5] Concepcion, “An Assessment of Cybersecurity Awareness among Academic Employees at Quirino State University: Promoting Cyber Hygiene,” Deleted Journal, vol. 20, no. 7s, pp. 769–775, May 2024, doi: https://doi.org/10.52783/jes.3445.

[6] G. Alotibi, “A Cybersecurity Awareness Model for the Protection of Saudi Students from Social Media Attacks,” Engineering, Technology & Applied Science Research, vol. 14, no. 2, pp. 13787–13795, Apr. 2024, doi: https://doi.org/10.48084/etasr.7123.

[7] Areej Alyami, D. Sammon, K. Neville, and C. Mahony, "Critical success factors for Security Education, Training and Awareness (SETA) programme effectiveness: an empirical comparison of practitioner perspectives," Information & computer security, Aug. 2023, doi: https://doi.org/10.1108/ics-08-2022-0133.

[8] S. M. Ho and M. Gross, "Consciousness of cyber defense: A collective activity system for developing organizational cyber awareness," Computers & Security, vol. 108, p. 102357, Sep. 2021, doi: https://doi.org/10.1016/j.cose.2021.102357.

[9] K. Khando, S. Gao, S. M. Islam, and A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review," Computers & Security, vol. 106, no. 1, p. 102267, 2021, doi: https://doi.org/10.1016/j.cose.2021.102267.

[10] A. Wiley, A. McCormac, and D. Calic, "More than the individual: Examining the relationship between culture and Information Security Awareness," Computers & Security, vol. 88, p. 101640, Jan. 2020, doi: https://doi.org/10.1016/j.cose.2019.101640.