DOI: http://dx.doi.org/10.26483/ijarcs.v13i5.6909

Volume 13, No. 5, September-October 2022

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

REINFORCEMENT AND CONSOLIDATION OF THE WEAKEST RING IN INFORMATION SECURITY WITHIN ESTABLISHMENTS

Khalid Mohammed Osman Saeed*
Faculty of Computer Science and Information Technology
Omdurman Islamic University
Sudan

Waleed Abdelrahman Yousif Mohammed
Computer Studies and Information Technology Faculty
Nile University
Sudan

EimanAlsiddigAltyeb Ibrahim
Faculty of Computer Science and Information Technology
Omdurman Islamic University
Sudan

Abstract:Information security used to be primarily a problem for governmental organizations or organizations whose operations need a high level of security to safeguard data and infrastructure. The fact that most information is now broadcast over the air and business is conducted through communication channels means that this way of life has an impact on the security of these assets. Therefore, information security issues should be treated equally to other security issues, and both of them need to be resolved simultaneously. The elements that positively or negatively affect information security awareness are then discussed in this study, with a focus on the role of organizations, senior management, and employees as well as technological and administrative security measures. As a result of this work, information security awareness has risen to the top of the security strategy and assumed paramount importance. As a result, classification of establishments and strategy planning must be done in the future while considering information security awareness.

Keywords: Information Security, Security Awareness, Security Management

I.INTRODUCTION

In order to be safe from harm or sabotage, one must possess the quality of security [1]. Therefore, this paper demonstrates how security issues may arise in governmental and non-governmental organizations, as well as within the managerial and non-managerial workforce, how the environment of the organization affects employees' security behavior, and how the absence of information security awareness initiatives may pose a risk to those organizations. In order to change an employee's behavior, which may be outlined using the following rule, behavior is equal to employees plus environment, security needs to be improved, according to William E. Perry.

Behavior = employees + environment

Therefore, changing one of these two characteristics will change the behavior of the employee. Although Perry referred to this dogma or theory as the "hammer theory," his main worry with it is that it is changing employees' perceptions of security by emphasizing its significance to them, particularly when new ideas are implemented in the workplace and they are eager to use it [2]. The study's findings support the importance of security awareness for staff, management, andorganizations. Additionally, digital data have evolved into the foundation of any firm and a crucially important resource that supports their corporate goals.

However, according to Robert L. Braun and Harold E. Davis, all personnel should be responsible for their overall information security understanding [3]. Additionally, information security awareness includes initiatives to improve security, foster responsibility, and update staff on security-related news. Additionally, awareness searches focus the worker's attention on a particular issue or set of issues. As a result, awareness campaigns are utilized to get personnel interested in security, aware of its issues, and prepared to respond appropriately when transmitting information inside or outside of their establishments [4].

II. INFORMATIONSECURITYAWARENESSNOWADAYS

Management should monitor and control employee conduct. The management needs to take a number of factors relating to employee behavior in information security into account. This information security awareness matter urges the necessity of changing employee perception and workplace culture in accordance with information security requirements, such as

establishment security policy awareness, password sharing, sharing computers and devices, connecting employee-owned devices to establishment's network, downloading items, and using personal email accounts while on the clock. Any security system may be subject to a number of vulnerabilities as a result of these acts. Summary: In order to influence the culture and behavior of its employees, institutions must take into account topics like:

A. Password Policy

Employees must keep it secure as the first line of defense in order to protect the privacy of the data. It stops illegal access where it is needed. Instead, security issues arise regardless of how strong a security system is because employees sometimes misuse their passwords. Because of this, it's important to keep your passwords private and to not share them with anyone else, not even your colleges.

According to a study by Frank D. Appunn [5], employees seldom change their passwords, and 70% of them use weak passwords like family names, catchphrases, or establishment slogans that are fewer than eight characters long and don't contain any symbols, numbers, or letters. Even people who have strong passwords have 30% of them saved on a piece of paper or computer file. Last but not least, if an employee chooses to use a simple password to remember, he or she exposes the data to multiple threats. Dealing with passwords becomes a big problem because of this.

B. Password Sharing

As is common knowledge, accounts are created and passwords assigned to employees for their use and are not typically to be shared, unless absolutely necessary to complete a mission for a predetermined amount of time. As a result, if a password needs to be shared, it must be changed or disabled when the task is completed, as leaving it available for an extended period of time compromises security [6].

C. Sharing Work Computers and Devices

Undoubtedly, one of the top concerns for businesses is preventing or minimizing security violations. Furthermore, 21% of employees admitted to allowing others to use their company's mobile devices [7], so sharing a mobile device with an outsider could lead to security breaches.

However, some employees allow outsiders to use their mobile devices for personal purposes more frequently than they do for business-related ones. Although employees are aware that visitors have no obligation to abide by the establishment's security policies and are not bound by them, a significant number of staff members nonetheless share their workplace's portable devices with visitors [8], according to a Robert Held article. On the other hand, staff members who bring their own devices to work and connect to the establishment'snetwork pose a severe security concern. The majorities of these portable outdoor devices lack antivirus software, do not adhere to the security regulations of the organization, and are not under the authority of IT staff.

In his essay "Security Actions during Reduction in Workforce Efforts: What to Do When Downsizing," Thomas J. Bray argues that when significant changes like a decrease in the employee population occur, enterprises become prone to security infractions.

However, the study suggests a program of information security awareness training that covers social engineering, talking to the press, password safety, convincing commissioners to be watchful when reviewing security logs, and fusing computer and security awareness with physical security alertness [9] in order to circumvent and avoid security violations during establishment changes.

D. Open an E-mail

Most employees read their own emails and occasionally click links from unidentified senders. Because viruses, Trojan horses, ransomware, and other forms of malicious software are widely used, a seemingly insignificant action can result in a chain reaction that causes enormous harm or losses.

It is important to note that 10% to 20% of employees admitted to opening emails from unknown senders and their attachments or hyperlinks, which can wreak havoc on a business. In contrast, 38% of employees said they open emails from unknown senders but do not open the attachments or hyperlinks, which makes this behavior appear less risky but still poses a security risk [10].In light of this, although the challenges raised here seem technical at first glance, you are correct that they depend on human behavior in the digital environment because either intentional or unintentional errors could result in significant security risks or losses.

III.SECURITY AWARENESS IMPEDIMENTS INDIGITALENVIRONMENTS

Implementing information security awareness efforts is fraught with difficulties, particularly in a digital environment. The following issues are the most significant obstacles from the perspective of the researcher:

A. Employees Culture

Employees in any company make up the majority of the population and can help to reduce unintentional or accidental mistakes, whereas security systems are vulnerable to attacks and can be penetrated by finding their flaws and vulnerabilities. However, many businesses treat security as a secondary responsibility or a work for the IT department, so security is rarely specified as a primary responsibility of any employee's job right away. Additionally, it causes employees to develop undesirable habits. The information security awareness training, on the other hand, should be used to familiarize new employees with the establishment's security policies and set expectations before granting them access to the establishment's resources. Every employee should obtain and accept job-related awareness training within regular updates on the establishment's information security policies. Additionally, ongoing training should cover the importance of security, legal obligations and tasks, how to properly use establishment

facilities, and the disciplinary procedure for staff members who breach security [11].

B. Security is an Issue for All

Many workers share the opinion that the computer department, not them, is ultimately responsible for security. Saving property belonging to establishments is a team effort. Many scientists [12] contend that implementing security awareness as part of the establishments' asset protection mission is necessary. However, their strategy aims to raise employee awareness of the necessary asset protection procedures, what acts are forbidden in terms of an establishment's asset protection, and the proper reporting of violations.

C. New Technologies Risks

When a new technology emerges, it carries its own dangers, thus staff must swiftly refresh their expertise to identify any problems that may arise with the new technology. Establishments must therefore identify the need for training, create a training plan, secure financial support for the program, select training topics, find sources for those topics, use a variety of methods to implement those topics, assess the program's effectiveness, and update and improve the program's focus [13].

D. Establishments Deficiency

Numerous awareness campaigns have failed to alter employees' behavior and provide a reliable method and plan for delivering the messages to employees. It is difficult for the employees to communicate with the program or even know what to expect without consistency in the awareness program itself.

Therefore, maintaining consistency in your security awareness program will help to forge a bond between it and the staff.

E. Resources and Management Support Deficiency

For any security awareness program to be effective and efficient, the organization's leaders must support it and give it top priority. This support must include establishment resources that are included in the budget and ensure that the establishment has enough adequately trained employees to protect its assets [4]. The most important requirement for security awareness campaigns is management top-down support. Unfortunately, it's also one of the most difficult [8], since a lack of resources will limit what the security awareness campaign can accomplish. Although top management consistently expresses a desire to support security measures, the reality is somewhat different, as they prioritize their economic interests over security.

F. Job Performance and Security

According to Donn B. Parker, the primary motivation for information security must come from rewards and penalties that are directly related to work output. Donn B. Parker asserts that by incorporating security requirements into job performance, conflicts and inconsistencies between job performance and security restrictions must be avoided [14].

G. Communication Deficiency

Since educating managerial staff would not result in a meaningful improvement, educating employees is noticeably expensive in terms of budget. Simply put, top management doesn't consistently communicate with their staff to let them know how important information security knowledge is. To combat employees' ignorance of information security and reluctance to take accountability for security issues, information security awareness efforts have been launched. According to Nicholas Gaunt [15], clear definitions of workers' duties for information security are necessary for putting an organization's information security policy into effect. The policy should also be periodically taught to all employees, and compliance with it should be required under the terms and conditions of employment.

IV.NECESSITYOF INFORMATIONSECURITY AWARENESS

Information security as a concept emerged throughout time as a result of many safeguards to secure the assets of establishments, including administrative and technical controls, which are regarded as integral parts of any information security mechanism. In the process of information security, persons, processes, and technology all play comparable roles [16]. However, even if a building has robust firewalls and intruder detection systems, security breaches can still occur if a staff member guides an intruder in through the back door [17].

Employee performance is a crucial component of any security measure because employees make up the majority of the population in any institution [18]. Therefore, staff mistakes might put firms in more danger than external attacks. Therefore, obtaining their input requires an efficient information security awareness campaign that is supported by all management levels [19].

Mikko T. Siponen has claimed that human morality plays a part in the security of establishments. In order to encourage employees' security-minded behavior, he also advises ethical education [20].

V.SECURITY AWARENESS EFFECTIVENESS

All groups of staff and employees within the organization must agree, support, and embrace the information security awareness program for it to be appropriate, valuable, and effective. More than ever, it is crucial that the management team fully adheres to the information security policy procedure; otherwise, there is a slim chance that they will not have the desired effect.
Again, Mikko T. Siponen opposes the idea that information security awareness initiatives should be based on behavioral theories and should explain to employees why adhering to security protocols is important in his study, "A Conceptual Foundation for Organizational Information Security Awareness." Achieving a situation where personnel are compliant with information security standards should be the goal of such a program [21].

However, employees must be aware of their responsibilities to safeguard the property of their employers; according to Ronald

L. Krutz and Russell Dean Vines, employees are frequently the weakest link in the security chain because they are unaware of the importance of security. Employees should be guided by management to understand how their actions can have a momentary impact on the establishment's overall security [22].

However, Telders E. [23] asserts that lack of employee motivation is the primary problem with information security. As a result, altering an employee's behavior is difficult enough and requires a detailed plan to succeed. The following are some areas that businesses should focus on to ensure the success of their information security awareness program:

- The backing of senior management.
- The assistance of human resources.
- Assessing and measuring employees' attitudes toward information security as part of job performance evaluations.
- Keeping track of security efforts and announcing awards.
- Encouraging supervisors to support information security.
- Commitment.
- Communication.

VI.CONCLUSION

Without a doubt, any new technology has advantages and disadvantages. These dangers, which include viruses, malware, worms, and vulnerabilities, keep getting worse every day or whenever a new technology is developed. Information security awareness is becoming more demanding due to these circumstances, nevertheless. Therefore, from a different vantage point, technology and attacks are not waiting either; however, it is evident that the majority of employees lack the necessary concentration of security awareness, or have a limited understanding of their security responsibilities with regard to the property of the establishments.

In order to gather awareness needs, be aware of and follow the establishment's security policies and procedures, and be suitably qualified about the rules of behavior for the resources which they have the right to use and access, employees must collaborate with their management or vice versa. Managers then need to be aware of all the options available to them for lowering information security threats. Additionally, relying solely on technical safeguards to protect data and property is insufficient. The success of the security procedure is mostly due to the staff. No one is an exception, and according to the results of this study, if anyone doesn't pay attention to the importance of security awareness, they become the weakest link in the security system. For this reason, both managers and employees need to understand the importance of security awareness in order to strengthen and consolidate the weakest link.

VII.REFERENCES

[1] Dhiren R. Patel, Information Security: Theory and Practice, PHI Learning, 2008.

[2] William E. Perry, Management Strategies for Computer Security, Butterworth Publishers, 1985.

[3] Robert L. Braun and Harold E. Davis, Computer Fraud: Analyzing Perpetrators and Methods. The CPA Journal, ABI/INFORM Global database, 2004.

[4] Mark Wilson, Kevin Stine, Pauline Bowen, Information Security Training Requirements: A Role- and Performance-Based Model, National Institute of Standers and Technology, 2009.

[5] Frank D. Appunn, Computer User Security: A model Facilitating Measurement, Ph.D. thesis, Capella University, Dissertations & Theses: Full Text database, Publication No. AAT 3304130, 2008.

[6] Harold F. Tipton and Micki Krause, Information Security Management Handbook, 6th Edition, CRC Press, 2007.

[7] R. Casmir, a Dynamic and Adaptive Information Security Awareness (DAISA) Approach. Stockholm University Department of Computer and Systems Sciences, Royal Institute of Technology, 2005.

[8] Robert Held, Security Awareness – Are Your Users "clued in" or "clueless"?, http://rr.sans.org/policy/sec_aware.php., 2001.

[9] Thomas J. Bray, Security Actions during Reduction in Workforce Efforts: What to Do When Downsizing, Information system security, Vol. 11, No. 1, 2002.

[10] G. Hinson, the True Value of Information Security Awareness. IsecT Publication, http://www.noticebored.com/html/why_awareness_.html. 2009.

[11] ISO, Information Technology - Code of practice for information system security management, International Organization for Standardization/International Electrotechnical Commission (ISO\IEC), 2005.

[12] Dr. Gerald L. Kovacich, Edward Halibozek, the Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program, Butterworth- Heinemann, 2003.

[13] Mark Wilson and Joan Hash, Building an Information Technology Security Awareness and Training Program, National Institute of Standards and Technology, 2003.

[14] Donn B. Parker, Fighting Computer Crime: A New Framework for Protecting Information, Computer Security Journal, Vol. 15, No. 4, John Wiley & Sons, 1998.

[15] Nicholas Gaunt, Installing an Appropriate Information Security Policy, International Journal of Medical Informatics, Vol. 49, No. 1, 1998.

[16] InfoSec Reading Room, Security Awareness: Implementing an Effective Strategy, http://www.sans.org/reading_room/papers/47/418.pdf, Sans Institute, 2002.

[17] Richard Power, Computer Crime and Security Survey, Computer Security Issues & Trends, Vol. VIII, No.1, 2002.

[18] The European Network and Information Security Agency (ENISA), Information security awareness in financial organizations, http:// http://www.enisa.europa.eu/doc/pdf/deliverables/is_awareness_financial_organisations.pdf, 2008.

[19] T. Olzak, Strengthen Security with an Effective Security Awareness Program, http://adventuresinsecurity.com/Papers/Build_a_Security_Awareness_Program.pdf, Erudio Security LLC, 2006.

[20] Mikko T. Siponen, On the Role of Human Morality in Information System Security: The Problems of Descriptivism and Non-descriptive Foundations, Proceedings of IS Security for Global Information

Infrastructures, IFIP TC11 15th Annual Working Conference on Information System security, 2000.

[21] Mikko T. Siponen, A Conceptual Foundation for Organizational Information Security Awareness, Information Management & Computer Security, Vol. 8, No.1. MCB UP Ltd, 2000.

[22] Ronald L. Krutz and Russell Dean Vines, The CISSP Preparation Guide, John Wiley & Sons, 2002.

[23] Telders E., Security awareness programs: a proactive approach, Computer Security Journal, Vol.7, No. 2. 1991.