International Journal of Electrical, Electronics and Computers
Vol-8, Issue-6 | Nov-Dec, 2023
Available: https://aipublications.com/ijeec/
Peer-Reviewed Journal

Cultivating Proactive Cybersecurity Culture among IT Professional to Combat Evolving Threats

Dr Sivaraju Kuraku[1], Dinesh Kalla[2], Fnu Samaah[3] and Nathan Smith[4]

[1]School of Computer and Information Sciences, University of the Cumberlands, Williamsburg, KY, USA
Email: skuraku5286@ucumberlands.edu
[2]Department of Computer Science, Colorado Technical University, Colorado Springs, CO, USA
Email : dinesh.kalla@student.ctuonline.edu
[3]Department of Computer Science, Harrisburg University of Science and Technology, Harrisburg, PA, USA
Email : fsamaah@alumni.harrisburgu.edu
[4]Department of Computer Science, Colorado Technical University, Colorado Springs, CO, USA
Email : nathan.smith246@student.ctuonline.edu

Received: 18 Oct 2023; Accepted: 20 Nov 2023; Date of Publication: 02 Dec 2023

Abstract— *In the current digital landscape, cybercriminals continually evolve their techniques to execute successful attacks on businesses, thus posing a great challenge to information technology (IT) professionals. While traditional cybersecurity approaches like layered defense and reactive security have helped IT professionals cope with traditional threats, they are ineffective in dealing with evolving cyberattacks. This paper focuses on the need for a proactive cybersecurity culture among IT professionals to enable them combat evolving threats. The paper emphasis that building a proactive security approach and culture can help among IT professionals anticipate, identify, and mitigate latent threats prior to them exploiting existing vulnerabilities. This paper also points out that as IT professionals use reactive security when dealing with traditional attacks, they can use it collaboratively with proactive security to effectively protect their networks, data, and systems and avoid heavy costs of dealing with cyberattack's aftermaths and business recovery.*

Keywords— ***Digital landscape, cybercriminals, information technology (IT) professionals, cybersecurity, layered defense, reactive security, traditional threats, cyberattacks, proactive cybersecurity culture, reactive security, and proactive security.***

I. INTRODUCTION

There is increased need for IT professionals to adopt robust security solutions as the rate at which successful cyberattacks keep increasing. Cybercrime is expected to cost an increasing amount approximated at 10.5 trillion dollars annually by 2025, regarding it to have third-largest economy when taken in the context of a nation's GDP [1]. Hence, IT profesionals need to shift from traditional cybersecurity to proactive security as part of their wide-ranging cybersecurity infrastructure. This entails taking measures to prevent cyberattacks from occurring, instead of responding after occurrence of a security incident. Proactive cybersecurity refers to strategic measures of safeguarding computer networks and systems from cyber threats [2]. This entails IT professionals identifying possible susceptibilities prior to cybercriminal exploiting them and implementing means of preventing these susceptibilities being taken advantage in future. It is worth noting that proactive cybersecurity approach is opposite of reactive cybersecurity. Fundamentally, rather than the reactive cybersecurity endeavoring in preventing cyberattacks, it concentrates on responding as well as recovering from cyberattacks after they happen.

Components of a proactive cybersecurity culture

1. **Having visibility of corporate assets**: IT professionals should have a platform for monitoring, recognizing, and seeing the networks and devices that employees use in order to better understand the way users access corporate assets and recognize suspicious activity.

ISSN: 2456-2319
https://dx.doi.org/10.22161/eec.86.1

2. **Leverage intelligent and modern technology**: IT professionals should adopt latest tools in machine learning and artificial intelligence and move from legacy security solutions so as to combat latent cyber threats [3].
3. **Adopt consistent and comprehensive training methods**. As cybersecurity training is an essential constituent of security, organizations should provide IT professionals with numerous training resources to their workforce, such as security tests and videos, and ensure education about cybersecurity is comprehended. This should be effectively assessed by IT professionals through testing staffs using tactics like sending them test phishing emails that helps to increase cybersecurity awareness as well as promote security best practices.
4. **Implementing risk response procedures**: IT professionals should develop identifiable and deployable procedures, platforms, and tools for intelligently and quickly responding to cyberattacks. This helps to minimize the impact caused by breaches that can occur.

Fig.1: Proactive Security Practices

Having a proactive cybersecurity culture can enable IT professionals improve their security compliance through rooting out all threats to business and corporate data and that of their clients and as a result meeting data compliance requirements. Through utilizing both reactive and proactive cybersecurity approaches, IT professionals can effectively protect corporate networks, data, and systems and avoid heavy costs of dealing with cyberattack' s aftermaths and business recovery. A proactive cybersecurity culture can also help IT professionals boost their organization's reputations through demonstrating to customers that the organization have procedures to protect their personal data and information, thus showing their commitment to maintaining data security [4]. This paper focuses on the need for a proactive cybersecurity culture among IT professionals to enable them combat evolving threats.

II. BACKGROUND

Traditionally, information technology (IT) professionals relied on cybersecurity strategies like reactive security and layered defense approach [5]. These approaches consist of implementing a mixture of corrective, detective, and preventive measures to mitigate business risks and safeguard their organizations from cyber threats. Corrective measures consist of procedure for system recovery, vulnerability patching, and incident response to deal with security breaches and recover from them. Detective measures encompass monitoring as well as analyzing logs, security events, and network traffic to detect possible vulnerabilities and threats. Preventive measures involve access controls, intrusion detection systems, and firewalls that focuses on minimizing or blocking unauthorized access to organizational resources, such as network, data, and systems. Equally, traditional security practices focus on conducting regular audits and risk assess to detect security threats, prioritize security measures, and react to them, while reactive security takes action of responding to attacks after they have been launched, and investigating their sources, assessing the caused damage, and them embarking on recovery [6]. These approaches become costly for businesses and information technology professionals because protective actions are deployed once attacks begin to cause significant or visible harm. Equally, considering that some attacks can remain undiscovered even with the first successful defense penetration, they can drain the network handling sensitive information for months until they cause significant harm and be discovered. The IT professionals are more prone to cyber attacks or phishing threats due to spending habits and increase in browsing hours [7]. Below diagrams show significant increase in phishing attack from year 2022 to first quarter 2023 and it clearly shows the need of proactive cybersecurity culture among IT Professionals.

ISSN: 2456-2319
https://dx.doi.org/10.22161/eec.86.1

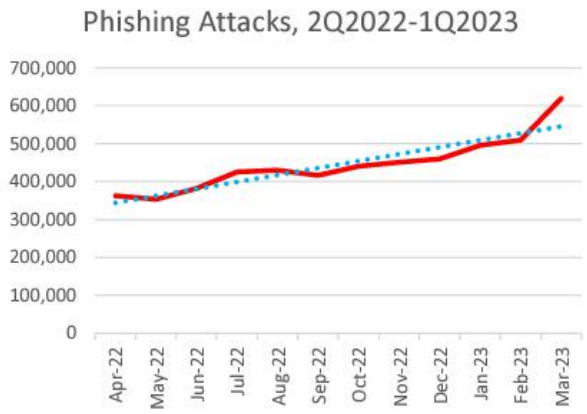

Fig.2: Phishing Attacks 2022-2023 (APWG Report)

III. PROBLEM STATEMENT

As the technology and networks keep on evolving at a rapid rate, information technology professionals in the e-commerce sector face challenges of increasing their business's attack surface. With increasing cybercrime activities, information technology professionals face challenges of securing their systems and data, improving means of reacting to cybercrimes and threats, and means to prepare instead of waiting for attacks to strike [8]. These circumstances necessitate them to utilize multiple protection layers on corporate networks, data, devices, and people. While such traditional security approaches have helped information technology professionals deal with traditional threats, they fall short of dealing with evolving cyber threats. Adding more challenges to the security issues originating from the sprawl growth of security and technology, malicious actors keep on inventing new methods, tools, and techniques to execute cyberattacks on organizations. IT professionals cannot effectively address both common vulnerabilities, exposures, and unknown threats using the reactive security since it only helps them to handle traditional attacks after identifying intrusion signs and indicators of compromise [9]. Therefore, it is important for IT professionals to enhance their security culture by shifting to proactive security, which identify and correct vulnerabilities prior to cybercriminals exploiting them, to deal with evolving threats.

IV. SIGNIFICANCE OF THE STUDY

This study on proactive cybersecurity culture can improve IT professional's threat detection. Through fostering a proactive cybersecurity culture that emphasis security knowledge-sharing and vigilance, IT professionals can improve their aptitude to promptly identify emerging threats while enabling staff to react to cyberattacks as corporation's first line in defense [10]. The study can enable IT professionals enhance their response to incidents as they prepare for attacks in advance through continuous monitoring, regular drills, and having effectively-defined plans to respond and minimize any impacts of cyberattacks. The study builds heightened awareness amid IT professionals about possible risks that they may face thus enabling them to be extremely security-conscious organization's stakeholders who are less vulnerable to phishing and social engineering attacks. Building a proactive security culture and IT professionals foster continuous adaptation and learning that enable them be ahead of evolving threats through staying up to date with latest trends in cybersecurity, frequent security training programs, and sharing security best practices. The study enables IT professionals to reinforce their layered defense by complementing it through ensuring alignment of all security layers, including human factors, policies, and technical controls, to safeguard against evolving threats. Through this study, IT professionals can develop preemptive risk management strategies through building a proactive security culture that emphasis on assessing inherent business risks, identifying susceptibilities on corporate systems, and implementing proactive measures to minimize potential cyber threats.

V. LITERATURE REVIEW

Organizations need to include cybersecurity in their workplace culture to change employee's and IT professional's attitude towards improved security behaviors [11]. Branley-Bell et al., (2021) further posits that a strong and proactive cybersecurity culture among IT professionals facilitates reduction of nonconformity with corporate security policies, therefore reducing the threats originating from their human behavior. Alshaikh (2020) concurs that corporations need to go a step further to not only ensure workers have regular cybersecurity awareness training, but also substantially invest on developing a proactive cybersecurity culture among IT professionals at the workplace. Such investment includes working collaboratively with external and in-house information technology professionals and service providers to find out the most common kinds of cyberattacks in the industry that their organization operates in to enable them safeguard it to maintain it running efficiently. Equally, Alshaikh (2020) advices that IT professionals should proceed to prioritize the identification of cyber threats through determining the way every identified security concern can damage numerous parts of the organization's network. IT professionals can effectively do that by listing all corporate devices connected to internet, kind of data that they handle, like low-importance, mission-critical, or regulated data, and the access they have.

ISSN: 2456-2319
https://dx.doi.org/10.22161/eec.86.1

Fig.3: Benefits of Proactive Cybersecurity Culture

Selvan et al., (2023) describes an ideal and proactive security culture among IT professionals as one where employees are knowledgeable and security-conscious and have conscientious behaviors that signifies compliance with security policies. In regard to proactive cybersecurity among IT professionals, Selvan et al., (2023) regards an ideal corporation as a proactive one to facilitating IT professionals have candid engagement with staffs on actions and cyber threats that affect organization. The study urges IT professionals to adopt a co-creative, systematic, and holistic strategy to cybersecurity to help employees become more open and engaged on cybersecurity. According to Selvan et al., (2023), adopting a co-creative, systematic, and holistic strategy to cybersecurity can be done by change IT professional's security culture to a more cautious and conscious one where they teach employees and stakeholders to take part in protecting corporate assets and guard them from cyber threats.

According to Bhuyan et al., (2020), healthcare IT professionals are not an exception from IT professionals in the e-commerce sector and hence, should take a proactive strategy to cybersecurity instead of utilizing ad hoc strategy to handling threats as they discover them case after another. Ad hoc strategy faces a significant challenge in sufficiently detecting and addressing evolving security gaps. Bhuyan et al., (2020) posits that the healthcare IT professional's proactive cybersecurity strategy should be part of an all-inclusive approach of building the business's resilience to cyber-attacks in terms of withstanding credential stealing attack's and returning back to business operations [12]. The healthcare IT professional's all-inclusive approach of building the business's resilience should be at the center of governance over every security process as well as ensuring that there is adequate cybersecurity training and financing on cybersecurity education.

VI. METHODOLOGY

This study harnessed quantitative methodologies, drawing insights from responses obtained through surveys administered to 71 professionals in the Information Technology sector. The core focus was on discerning distinctions in phishing IQ score, attitude score, and behavior score. The ultimate goal was to pinpoint elements that might curb impulsive phishing clicks by implementing proactive culture. This research used a survey tool called "The Human Aspects of Information Security Questionnaire (HAIS-Q)," deals behaviors and attitudes of the individuals [13]. The study also got approval to use an online phishing IQ test from Phishing Box's president. You can find the test at https://www.phishingbox.com/phishing-iq-test. Below diagram represents qualitative research methodology steps conducted for the research. The steps includes development of survey, deployment of survey , reporting and data analysis based on the survey results.

Fig.4: Research Methodology Architecture

VII. RESULTS AND TESTS

This chapter presents the findings and analysis of the study. We're looking at survey results from people in the Information Technology sector, checking out how they behave, their attitudes, and their phishing IQ regarding phishing. We're using a method called ANOVA to see how different factors like demographics relate to behaviors, attitudes, and phishing IQ

ISSN: 2456-2319
https://dx.doi.org/10.22161/eec.86.1

Anova: Single Factor

SUMMARY

Groups	Count	Sum	Average	Variance
Phishing Score	71	4480	63.0985915	241.6901408
Behavior Score	71	2772	39.0422535	30.01247485
Attitude Score	71	2735	38.5211268	44.56740443

ANOVA

Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	27998.4	2	13999.1972	132.7903022	5.303E-38	3.03887691
Within Groups	22138.9	210	105.42334			
Total	50137.3	212				

Fig.5: Annova Statistical Analysis

Aforementioned statistical ANOVA model tabular results is statistically significant because the p-value (5.30E-38) is much less than the significance level of 0.05. The F-statistic (132.79) is greater than the critical F-value (3.04), further supporting the rejection of the null hypothesis which is suggesting that there are significant differences among the means of the groups (Phishing Score, Behavior Score, and Attitude Score).The between-groups variability (model effect) is significantly larger than the within-groups variability (error).Post-hoc tests have conducted to identify which specific group means are different from each other as shown in the figure (2).

	$HSD_{.05}$ = 4.0677			
Pairwise Comparisons	$HSD_{.01}$ = 5.0758	$Q_{.05}$ = 3.3382 $Q_{.01}$ = 4.1655		
	M_1 = 63.10			
Phishing Score:Behavior Score	M_2 = 39.04		24.06	Q = 19.74 (*p* = .00000)
	M_1 = 63.10			
Phishing Score: Attitude Score	M_3 = 38.52		24.58	Q = 20.17 (*p* = .00000)
	M_2 = 39.04			
Bahvior Score : Attitude Score	M_3 = 38.52		0.52	Q = 0.43 (*p* = .95084)

Fig.6 : Post Hoc Turkey HSD

In summary, the Tukey HSD pairwise comparisons reinforce the findings of the ANOVA. The Phishing Score group significantly differs from both the Behavior Score and Attitude Score groups, while there is no significant difference between the Behavior Score and Attitude Score groups. These results provide valuable information for understanding specific group dynamics and can guide targeted interventions in the context of phishing awareness and behavior. If we simplify the results further, the following interpretation was derived.

Phishing Score vs. Behavior Score:

People who scored higher in Phishing Score (63.10) had a significantly different behavior compared to those with lower scores in Behavior Score (39.04). The difference (24.06) is much bigger than what we would expect by chance.

Phishing Score vs. Attitude Score:

Again, people with higher Phishing Scores (63.10) behaved differently than those with lower Attitude Scores (38.52). The difference (24.58) is significant, meaning it's not likely due to random chance.

Behavior Score vs. Attitude Score:

Surprisingly, there's no significant difference in behavior between those with higher Behavior Scores (39.04) and those with lower Attitude Scores (38.52). The small difference (0.52) could just be random.

In plain terms, people who are more aware of phishing (higher Phishing Score) seem to behave differently than those who have lower scores in behavior or attitude. However, there's not much difference in behavior between those with higher behavior scores and those with lower attitude scores. These findings give us a better understanding of how different factors might influence people's responses to phishing threats.

VIII. DISCUSSION

The ANOVA results shed light on notable distinctions among the means of the Phishing Score, Behavior Score, and Attitude Score groups. The exceptionally low p-value (5.30E-38) and the substantially high F-statistic (132.79) provide robust evidence that the observed differences are not mere chance occurrences. In essence, there are genuine variations in scores across these groups. Digging into the specifics, the Phishing Score group stands out with the highest average score (63.10), implying a more cautious or knowledgeable response to phishing scenarios. Conversely, the Behavior Score and Attitude Score groups have lower averages (39.04 and 38.52, respectively), suggesting potential differences in behavioral and attitudinal aspects related to cybersecurity. It's crucial to recognize that the substantial variance within each group, especially in the Phishing Score group, suggests diverse individual responses. Unraveling the factors contributing to this diversity could unveil valuable insights into the intricacies of participants' perceptions and actions regarding phishing threats. To gain a clearer picture, post-hoc tests can be employed for pairwise comparisons. These tests will pinpoint which specific pairs of groups exhibit significant differences, providing a more nuanced understanding of the relationships between the scores.

Practical implications of these findings should not be overlooked. While statistical significance is crucial, the magnitude of these differences in real-world scenarios

ISSN: 2456-2319
https://dx.doi.org/10.22161/eec.86.1

needs consideration. Assessing the practical significance will help discern whether the observed variations have meaningful implications in the context of cybersecurity awareness and response.

Therefore, building a proactive security culture among IT professionals stretches beyond utilizing reactive security strategies and implementing technical security safeguards to creating a corporate consciousness and mindset whereby IT professionals in the organization share cybersecurity responsibility and actively involve themselves in detecting and responding to potential cyber threats and attacks [14]. This culture of cybersecurity puts emphasis on the necessity for continuous security training and education to remain updated on emerging threats. A significant benefit that IT professionals gain from a proactive security culture is improving their capability to timely detect and mitigate evolving threats. By encouraging IT professionals to be active in identifying and reporting security incidents, organizations can effectively take swift measures to reduce the impacts of cyberattacks and prevent extensive damage that can prove costly for the business. Furthermore, the culture supports systematic assessment of the present security measures and, as a result, ensures IT professionals update themselves on safeguarding the business from emerging threats. Equally, the culture promotes security accountability among IT professionals as they follow security best practices and protocols after understanding and appreciating their role in protecting sensitive information, thus further minimizing negligence and human errors that can result in security breaches.

IX. CONCLUSION

In summary, the ANOVA results unequivocally demonstrate that the Phishing Score, Behavior Score, and Attitude Score groups are not statistically equal. The rejection of the null hypothesis underscores the presence of genuine disparities among the means of these groups. Moving forward, delving into the factors influencing participants' responses will be essential for a more comprehensive understanding. Post-hoc tests will provide specific details on which pairs of groups are driving the observed differences. These insights are pivotal for tailoring interventions and educational initiatives to address specific needs related to phishing awareness and response. The practical significance of these differences should guide future actions. Understanding not just that differences exist, but also how impactful they are in practical terms, will inform the design of effective and targeted strategies to bolster cybersecurity awareness and resilience. This study lays the foundation for a more nuanced exploration of individual and group dynamics in the realm of cybersecurity behavior. Therefore, there is a greater necessity for having a proactive cybersecurity culture among IT professionals to effectively combat evolving cyberattacks in the current digital landscape. The threat of cyberattacks continues to increase as connectivity keeps on getting more pervasive and technology advances, rendering reactive measures sorely inadequate to address cybersecurity challenges. Fundamentally, proactive cybersecurity culture among IT professionals encompasses creating a mindset at the organization that prioritizes threat prevention, proactive cybersecurity measures, and continuous learning on evolving threats and mitigation approaches. It also consists of establishing strong procedures and policies in businesses, fostering security responsibility, vigilance, and resilience among IT professionals and all corporate stakeholders, and implementing advanced security technologies to prevent and combat cyber threats. A proactive security culture among IT professionals' nurtures collaboration and cybersecurity information sharing in the organization, thus further improving the entity's aptitude to identify, avoid, and respond to evolving cyber threats effectively. This also strengthens an organization's entire cybersecurity posture as IT professionals effectively disseminate security best practices, lessons learned, and threat intelligence. By adopting a proactive cybersecurity culture, IT professionals can effectively mitigate threats and risks that can originate from evolving threats as well as protect the privacy and security of data, digital assets, and the entire organization's information.

REFERENCES

[1] Sharif, M. H. U., & Mohammed, M. A. (2022). A literature review of financial losses statistics for cyber security and future trend. *World Journal of Advanced Research and Reviews*, *15*(1), 138-156. https://doi.org/10.30574/wjarr.2022.15.1.0573

[2] Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber threat intelligence mining for proactive cybersecurity defense: A survey and new perspectives. *IEEE Communications Surveys & Tutorials*,1-1. https://doi.org/10.1109/comst.2023.3273282

[3] Dhayanidhi, G. (2022). Research on IoT Threats & Implementation of AI/ML to Address Emerging Cybersecurity Issues in IoT with Cloud Computing. file:///C:/Users/user/Downloads/1b076ecd-286f-4020-b1da-490b6f088036.pdf

[4] Kalla, D., Samaah, F., Kuraku, S. & Smith, N. Phishing Detection Implementation Using Databricks and Artificial Intelligence. SSRN Electronic Journal 185, doi: 10.2139/ssrn.4452780 (2023).

[5] Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., Kumar, S., Levy, M., Kedia, S., Dasgupta, D., & Dobalian, A. (2020). Transforming healthcare cybersecurity from reactive to proactive: Current

status and future recommendations. *Journal of Medical Systems*, *44*(5). https://doi.org/10.1007/s10916-019-1507-y

[6] Xu, S. (2020). The cybersecurity dynamics way of thinking and landscape. *Proceedings of the 7th ACM Workshop on Moving Target Defense*. https://doi.org/10.1145/3411496.3421225

[7] Kuraku, S., & Kalla, D. (2023). Impact of phishing on users with different online browsing hours and spending habits. *International Journal of Advanced Research in Computer and Communication Engineering*, *12*(10), 34–41. https://doi.org/10.17148/IJARCCE.2023.121005

[8] Lee, C., & Ahmed, G. (2021). Improving IoT privacy, data protection and security concerns. *International Journal of Technology, Innovation and Management (IJTIM)*, *1*(1),18-33. https://doi.org/10.54489/ijtim.v1i1.12

[9] Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, *63*(4), 531-540. https://doi.org/10.1016/j.bushor.2020.03.010

[10] Selvan, C. A. J. A., & Fonceca, C. M. (2023). Cyber security culture in an IT company: An empirical study. https://www.researchgate.net/profile/Clayton-Fonceca/publication/370059163_Cyber_security_culture_in_an_IT_company_An_empirical_study/links/643cc5df2eca706c8b64b5a6/Cyber-security-culture-in-an-IT-company- An-empirical-study.pdf

[11] Branley-Bell, D., Coventry, L., & Sillence, E. (2021). Promoting cybersecurity culture change in healthcare. *The 14th PErvasive Technologies Related to Assistive Environments Conference*. https://doi.org/10.1145/3453892.3461622

[12] Kuraku, S., and Kalla, D. (2020). Emotet Malware—A Banking Credentials Stealer. Iosr J. Comput. Eng, 22, 31-41. https://doi.org/10.9790/0661-2204023140

[13] McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017).Individual Differences and Information Security Awareness. Computers in HumanBehavior, 69, 151-156. *(PDF) A Reliable Measure of Information Security Awareness and the Identification of Bias in Responses*. Available from: https://www.researchgate.net/publication/321349520_A_Reliable_Measure_of_Information_Security_Awareness_and_the_Identification_of_Bias_in_Responses [accessed Nov 17 2023].

[14] Corradini, I. (2020). Building a cybersecurity culture. *Studies in Systems, Decision and Control*, 63-86. https://doi.org/10.1007/978-3-030-43999-6_4