International Journal of Scientific Research and Engineering Development-– Volume 7 Issue 5, Sep-Oct 2024
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Quantifying Social Engineering Impact: Development and Application of the SEIS Model

Dr. Saim Atalay Kelestemur[1], Ali Okan Yuksel[2], Oguzhan Akkaya[3], Utku Ayan[4]
[1]Email: sakelestemur@gmail.com, ORCID NO: 0000-0002-3718-3424
[2]Email: aliokan.yuksel@siyahsapka.org, ORCID NO: 0009-0000-3490-1307
[3]Email: oakkaya@ymail.com, ORCID NO: 0009-0006-7613-8171
[4]Email: utku.ayan@outlook.com, ORCID NO: 0009-0000-1394-149X

----------**********----------

Abstract:

Social engineering exploits human psychology rather than technical vulnerabilities, making it a strong threat in cybersecurity. By leveraging cognitive biases and social dynamics, attackers use methods like phishing, pretexting, and baiting to deceive individuals into compromising sensitive information. This study introduces the Social Engineering Impact Scoring (SEIS), a quantitative model designed to assess the impact of social engineering attacks on organizations. The SEIS model provides a structured, data-driven approach to evaluate key metrics, each weighted based on its empirical impact on overall risk. The study also highlights the importance of SEIS in offering a balanced assessment of technical and behavioral vulnerabilities, thereby enhancing the organization's capacity to foster a security-aware culture and mitigate the impact of social engineering threats.

Keywords — **Social Engineering, Cybersecurity, Penetration Testing, Ethical Hacking**

----------**********----------

I. INTRODUCTION

Social engineering in the scope of cybersecurity refers to the manipulation of people into divulging private information or tricking them into taking actions that compromise security. Unlike conventional cyber-attacks based on exploiting technical vulnerabilities, social engineering targets human behavior and psychological weaknesses. It exploits cognitive biases, fear-driven responses, and social dynamics to mislead its victims; hence, it poses a monumental challenge to any safeguards that one can establish in the field of cybersecurity.

Phishing, pretexting, and baiting are common tactics that leverage psychological principles to manipulate victims into unknowingly breaching security. An example of such an attack is the timely phishing attack, which creates a rush. With the belief that there may not be enough time to think it over, one may divulge sensitive information [1]. Although not merely based on chance, it is rather a carefully planned incursion taking advantage of cognitive biases and emotional responses, warranting that cybersecurity actively works against human factors and vulnerabilities involved [2].

Social engineering attacks are enabled by the psychological subtlety of human interaction. For instance, attackers often use common psychological principles like authority, urgency, and fear. Phishing attacks make false claims that emergencies are pressing, causing people to react hastily without exercising caution, thus enhancing the chances of sensitive information leaking out or users clicking on malicious links [3].

The rise of social media and digital communication platforms has aggravated the threat landscape, providing cybercriminals with unprecedented access to personal information that

can be used to tailor their attacks. The vast amount of public information available online enables attackers to craft convincing narratives that resonate with their targets, making social engineering tactics more effective than ever [4].

Consequently, understanding the psychological mechanisms that underpin these attacks is crucial for developing effective countermeasures and enhancing overall cybersecurity resilience.

II. SOCIAL ENGINEERING

In the area of penetration testing, the use of social engineering techniques provides an organization with clues regarding its security posture. The penetration testers impersonate real-world attacks to find vulnerabilities in human behavior and measure how effective each of the existing security protocols turns out to be [5].

This incorporation of social engineering into penetration testing seeks to evaluate not only an organization's technical infrastructures but also the human aspect of its defenses. Traditional penetration testing primarily seeks to identify some technical weaknesses such as unpatched systems or vulnerabilities related to networks, while social engineering tests expose insights into how manipulable the employees are. Phishing simulations, pretexting, baiting scenarios, and the like are used to examine how employees respond under supposed attack situations. Such data allows a security team to identify its critical behavioral weaknesses and further enhance targeted security training, making for a more resilient organizational security posture.

The advancements in technology and an increase in the availability of personal information on the Internet have further complicated the penetration testing work-realm landscape by getting evermore proliferated with social engineering attacks. Attackers becoming more and more tailored in crafting believable narratives, integrating them with social media platforms, resists the tactics used by penetration testers to stay one step ahead of these current practices while still maintaining good code of ethics [6].

III. LITERATURE REVIEW

A. Phishing

Phishing is a form of cybercrime that involves the fraudulent attempt to obtain sensitive information from individuals by masquerading as a trustworthy entity in electronic communications. Social engineering methods during penetration testing provide organizations with insights into their internal posture against external threats. The penetration testers mimic real tactics with the aim to identify the vulnerabilities posed by humans and to assess the broad effectiveness of each of the existing security protocols [7].

The mechanisms of phishing attacks are diverse, encompassing various techniques such as deceptive phishing, spear phishing, and malware-based phishing. Deceptive phishing typically involves creating a replica of a legitimate website to trick users into entering their credentials, while spear phishing targets specific individuals or organizations with personalized messages [8].

Phishing attacks can be categorized into several types based on their methods and objectives. For instance, "pharming" redirects users from legitimate websites to fraudulent ones without their knowledge, while "keyloggers" capture keystrokes to gather sensitive information.

Furthermore, phishing can also occur through social media platforms and instant messaging, expanding the scope of potential attacks beyond traditional email [9]. The sophistication of these attacks has evolved, with attackers employing advanced techniques such as URL obfuscation to disguise malicious links, making detection increasingly challenging.

B. Pretexting

Pretexting is a specific kind of the social engineering process whereby an attacker develops a fictitious scenario or pretext that leads a target into sharing classified information. This technique is nearly based upon deception, typically where an attacker assumes a false identity or role credible enough to have the victim comply with their requests. The power of pretexting lies in its utilization of human predispositions, notably trust and authority,

rendering it a viable strategy within the social engineer's arsenal.

In most cases of pretexting, the attacker builds a credible and believable narrative that is applicable to the situation at hand. For instance, an attacker would present themselves as an IT support personnel of a certain company, expressing that they need the account details verified for some security reasons. This methodological approach aims to lower the defences and have the target divulge sensitive information like passwords or PINs. Studies indicate that pretexting is often used together with other social engineering techniques such as phishing in order to increase the success rate [10].

The prevalence of pretexting in various sectors-from e-government systems to corporate environments-indicates that it remains an important security issue. Attackers routinely exploit organizational vulnerabilities that include the lack of adequate security training and awareness among employees, to conduct pretexting attacks successfully. In a study, it was noted that attacks based on social engineering, including pretexting, find fertile ground particularly in environments in which employees are poorly trained to detect and respond to such threats [11].

C. Baiting

Baiting is a form of social engineering that offers a fictitious gift or reward to someone in order to get them to compromise their security or share private information with the attacker. This technique takes advantage of basic human traits like greed or curiosity, and usually shows some form of a bait that looks delicious or fruitful to the target. The bait can be free things, such as apps, or attractive offers, and can even include objects that people find in public places which are meant to draw in victims.

Baiting commonly takes the form of malware presented as innocent/harmless applications or files. For instance, an offender may carry static 'USB thumb drives' already infected with malware, and drop them in strategic locations where unwitting users will be likely to pick up the drives and plugin into their computers. When the bait is set, its software could infect the user's machine, letting the aggressor to breach sensitive information or systems that they are not entitled to [12]. Such a method works especially well as it takes advantage of the fact that people have an innate compulsion to pick up and use things they find or come across without regard to any danger therein.

Baiting can also be found in cyberspace, where criminals promise rewards in the form of gifts, bonuses, and services after users provide certain details. This includes fake contests or prize-draws that require participants to submit information that can be used by fraudsters. Herein, the element of psychology in baiting is extremely important, as it exploits the victim's greed which, more often than not, muffles their wariness and reasoning.

Baiting is a tactic used mostly in Red Teaming but not in penetration testing because it targets the human aspect instead of targets actual systems. Red Teaming methods are designed to replicate actual human threats focused on both technological and human defenses, not just the scope of penetration testing. In the case of baiting, curious employees gullibly take such risks by using infected USBs or responding to imaginary offers. This technique is not forever possible and productive as it needs to be ethical, organized, and needs more time to get a result, in contrast to penetration testing.

IV. MATERIALS AND METHODS

This study investigates the effectiveness of social engineering tactics and the ethical considerations involved in penetration testing. We conducted controlled social engineering simulations, focusing on phishing and pretexting attacks, within a real-world organizational setting. The following section outlines the study's participants, design, procedures, and ethical safeguards.

The study was divided into two main phases: Phishing Simulation and Pretexting Simulation. Each phase tested specific social engineering techniques. The social engineering campaigns were conducted in collaboration with different medium-sized organizations, with participants from various departments including IT, HR, finance, and general administration. In total, 1000 employees were selected to participate anonymously, ensuring a diverse mix of roles and access levels to sensitive information. Participants were aware of general

cybersecurity testing in the organization, though specific details of the simulated social engineering scenarios were withheld to avoid influencing their responses.

A. Phishing Simulation

A series of phishing emails were crafted to mimic common malicious tactics, including emails from authority figures, emails conveying urgency, and emails with a sense of opportunity (e.g., prizes or benefits). These emails were designed to simulate real phishing attempts while being securely monitored. Phishing success was measured by click-through rates, credential submission rates, and time taken for participants to detect or report the email.

B. Pretexting Simulation

This phase involved telephone-based pretexting attacks, where penetration testers posed as trusted roles (e.g., IT support or HR) to request sensitive information. Calls were conducted with pre-written scripts that included specific cues to measure compliance with requests and the likelihood of disclosure. The success rate was determined by the amount and sensitivity of information disclosed during calls.

Phishing e-mails were sent via GoPhish, which is an open-source phishing simulation tool that enables the user to craft, and then to monitor the responses to e-mails. The scripts for the pretexting calls were developed in cooperation with the IT and HR departments of the companies to target some common cognitive biases, like trust in the authority and urgency. The scenarios were standardized to be consistent and ethical.

Participants were aware they were involved in cybersecurity assessments and had consented to generalized security testing per their organization's security policies. Details of specific social engineering tests were intentionally withheld to elicit natural responses, with clear consent procedures strictly observed throughout. No personal data were collected during the phishing simulations.

The social engineering tests were followed by an extensive briefing for each participant. This briefing session described the purpose of the study, the tactics used, and provided training on how to recognize and respond to social engineering attempts. This approach was aimed at reducing any potential stress and fostering positive perceptions of the security testing process.

This quantified-qualitative study measured some aspects of quantification, which helped determine the effectiveness of the attack vectors in social engineering and their relationships with ethical perceptions. Quantitative metrics were used during the social engineering tests:

- Click-Through Rate (CTR) and Credential Compromise Rate (CCR) for phishing emails.
- Disclosure Rate (DR) for pretexting calls, defined as the percentage of calls where participants disclosed sensitive information.
- Average time taken for participants to detect or report phishing emails.

Social Engineering Impact Scoring (SEIS) is a quantitative model developed to assess the overall impact of social engineering attacks on an organization based on key metrics from controlled social engineering tests. This method combines metrics from phishing and pretexting simulations to produce a composite impact score that reflects both technical and human vulnerabilities. SEIS provides organizations with a standardized approach to quantify the effects of these attacks, enabling informed decision-making for targeted interventions.

The SEIS formula integrates four primary factors: Click-Through Rate (CTR), Credential Compromise Rate (CCR), Disclosure Rate (DR), and Detection Time (DT). Each factor is weighted according to its specific contribution to social engineering risk, providing a comprehensive and balanced measure of impact on organizational security. CTR reflects the initial susceptibility of participants to phishing attempts; CCR indicates the severity of credential exposure, DR measures information disclosure risks, and DT accounts for the speed of detection, enhancing overall insight into human and technical vulnerabilities. Together, these factors enable targeted risk mitigation strategies.

Click-Through Rate (CTR): Measures the percentage of participants who clicked on phishing links, indicating initial susceptibility to the attack.

$$\frac{Number\ of\ Clicks}{Total\ Emails\ Sent} \times 100$$

Credential Compromise Rate (CCR): Measures the percentage of participants who entered credentials on a phishing page, directly affecting security by granting potential access.

$$\frac{Credentials\ Compromised}{Total\ Emails\ Sent} \times 100$$

Disclosure Rate (DR): Measures the percentage of participants who disclosed sensitive information during pretexting attacks.

$$\frac{Number\ of\ Disclosures}{Total\ Pretexting\ Calls} \times 100$$

Detection Time (DT): The average time taken for participants to report a phishing attempt, where a lower DT reduces overall impact.

$$\frac{Total\ Time\ (minutes)}{Number\ of\ Reports}$$

Each factor in the SEIS model is assigned a coefficient based on its contribution to social engineering risk and ethical impact.

TABLE 1 SEIS FACTORS AND COEFFICIENTS

Factor	Coefficient
Click-Through Rate (CTR)	0.20
Credential Compromise Rate (CCR)	0.35
Disclosure Rate (DR)	0.30
Detection Time (DT)	0.15

The coefficients are assigned to align with risk management principles and empirical analysis. Factors that directly lead to breaches (such as compromised credentials) carry the highest coefficient since they pose immediate risks to organizational security. Conversely, behavioral factors like detection time, while still important, are assigned a lower coefficient because they indirectly influence outcomes.

By distributing coefficients this way, the SEIS model can prioritize factors that more directly indicate vulnerability and impact, allowing for a balanced and accurate assessment of social engineering risk. The total Social Engineering Impact Score (SEIS) is calculated by summing each factor's score weighted by its respective coefficient:

$$SEIS = (CTR \times \alpha) + (CCR \times \beta) + (DR \times \gamma) + \left(\frac{1}{DT} \times 100 \times \delta\right)$$

Where, α, β, γ, and δ represent the coefficients for each respective factor.

The SEIS method allows organizations to quantify the effects of social engineering attacks while incorporating ethical considerations, offering a balanced view of technical and psychological vulnerabilities within their security framework. The SEIS value provides a quantitative score for the overall social engineering impact:

- Low Impact: 0 - 10
- Moderate Impact: 11 - 20
- High Impact: 21 - 30
- Critical Impact: >30

The analysis for this study was conducted using Python, leveraging its robust ecosystem of libraries for statistical analysis, data processing, and visualization. Python's *Pandas* and *NumPy* libraries facilitated efficient data manipulation, ensuring that the SEIS model could handle complex, large-scale datasets from the social engineering simulations with precision. *SciPy* and *Statsmodels* were utilized to perform advanced statistical tests and regression analysis, which were essential for calculating and validating the coefficients assigned to each factor in the SEIS model.

Visualizations, created using *Matplotlib* and *Seaborn*, provided clear graphical representations of patterns in click-through rates, credential compromise rates, and other factors, enabling

insights into the social engineering impact metrics. Python's flexibility also allowed for rapid model iteration and validation through *Scikit-Learn*, which enhanced the study's scientific rigor by enabling cross-validation and ensuring the model's accuracy and reliability in assessing social engineering risks.

V. STUDY RESULTS

A. Demographic Information

Among the respondents, the majority were male, accounting for 68.1% of the total participants, with 681 identifying as male. In contrast, 319 females, accounting for 31.9% of the participants, were recorded. This shows that more males contributed to the respondent pool and may serve as a factor in interpreting the responses or trends based on gender perspective. This knowledge of the distribution is very important while analyzing any pattern or bias of a particular gender which may appear in the data.

The distribution of age shows that the age group of 31-40 had the highest frequency of 257 participants, comprising 25.7% of all respondents. Close to that was the 41-50 age bracket with a total of 244 participants, accounting for 24.4% of the total. These two groups combined formed half of the total participants. It means there is a strong middle-aged group present within respondents. The emerging trend seems to be one of the predominance of the pool of participants with people in their thirties and upwards, even forties.

The share of the 20-26-year-old age group was 12.6% with 126 participants, while the 27-30-year-old group was 18.1% with 181 participants. Already from this, significant, although smaller, representation can be seen for younger professionals or early-career individuals. Finally, the age group 60 and above was the least represented, with only 14 participants or 1.4%, which underlines the very limited presence of senior participants in this survey. This might be further influenced by the fact that this distribution of age will have an effect on the general feeling given, with middle-aged and younger groups represented more than other age groups.

By departmental representation, information technology was the highest with 23.5% of the participants, being 235, followed by Sales and Marketing with 208 participants, 20.8% of the total; thus, the bulk of the people responding seem to be in mainly technological or client-serving functions. On the other hand, the Research and Development category accounted for 18.3% with 183 participants. It indicates that within this sample, there are participants who develop new software, services, products and technologies within their respective organizations. These are the topmost departments in which a pool of participants expresses their area of concentrated expertise.

The other departments represented were on a smaller scale but were significant in the overall distribution. Management accounted for 11.4% of the respondents, with 114 participants, while Human Resources followed closely at 11.3% or 113 participants. Finance and Accounting added 14.7% to the total number, at 147 persons showing that there was moderate involvement with administrative and financial roles.

B. Phishing & Pretexting Engagement

The engagement statistics provide a clear view of participant behavior at each stage, from emails sent to final data submission. Of the 1,000 participants who received the emails, a significant 84.8% (848 participants) opened them, indicating strong initial interest or appeal in the email content or subject line. However, engagement decreases at each stage, with 56.2% clicking the link and 24.1% ultimately submitting data. This shows a typical engagement funnel pattern, where each step sees some attrition, potentially pointing to areas where content, accessibility, or user experience might be optimized to maintain interest.

Examining gender distribution across these stages, we find that male participants were consistently a larger portion of the respondent pool, with 67% of those who opened the email being male, 65.5% clicking the link, and 64% submitting data. This slight decrease in male representation through each stage suggests that while men were more likely to open the email, they were less likely to follow through to submission compared to women. Female participants, by contrast, showed increasing representation at each engagement level, rising from 33% at email open to 36% at data submission. This

trend indicates that once engaged, female participants were more likely to complete each step, signaling potentially higher content resonance or relevance for female participants.

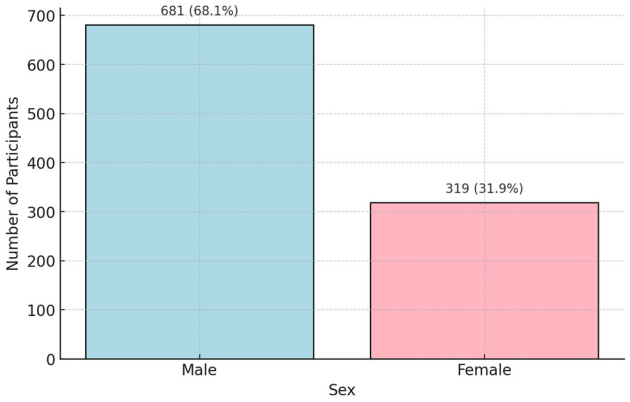

Fig. 1 Sex distribution of participants

Looking at age distribution, participants aged 31-40 were the most engaged at each stage, consistently representing a little over a quarter of each engagement metric. This group accounted for 26% of those who opened the email, increasing slightly to 27% at the data submission stage. The high engagement levels among this age group may reflect a resonance between the email content and the professional or personal interests of participants in this life stage. The 41-50 age group was the next most engaged, with a slight decline as they progressed through the engagement stages, suggesting potential barriers to full completion for some in this cohort.

Among younger participants, those aged 20-26 and 27-30 showed consistent engagement, particularly in the early stages, though it slightly decreased as they progressed to data submission. This was more pronounced among the 51-60 and 60+ age groups. Participants aged 51-60 saw a decrease in engagement from 17.8% of emails sent to 14.2% of data submissions, while the 60 and above age group had the lowest engagement across all stages, likely indicating that older participants were either less interested in, unfamiliar with, or found the process less accessible, which is common in digital engagements. This trend highlights the importance of tailoring engagement strategies to accommodate all age groups for improved inclusivity and response.

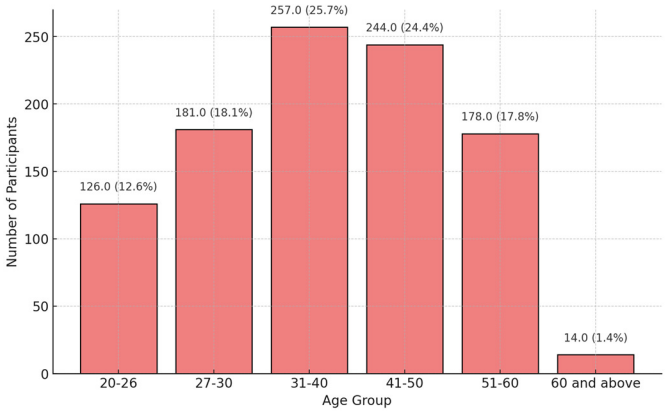

Fig. 2 Age distribution of participants

Departmental engagement shows Information Technology (IT) leading in every stage, with IT participants making up 22.8% of those who opened the email, 22.3% who clicked the link, and 21.8% who submitted data. Sales and Marketing followed closely, particularly in the later stages, with a notable increase from initial engagement to final data submission. Research and Development also showed strong engagement, but with a small drop-off by the data submission stage, indicating stable but slightly decreased follow-through. These high engagement levels in IT, Sales, and R&D may suggest that the content was more relevant or engaging for these departments.

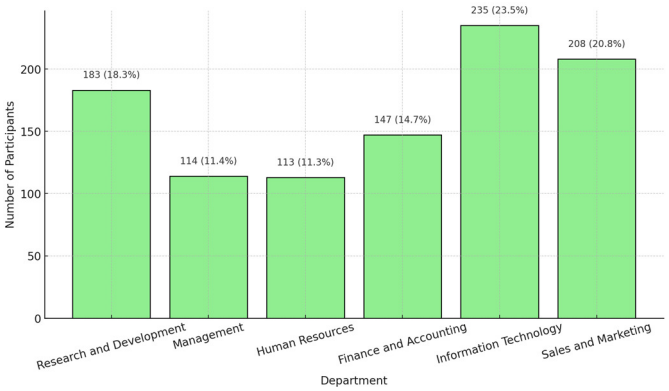

Fig. 3 Department distribution of participants

Other departments, such as Management and Human Resources, had lower engagement, especially at the data submission stage. Management, for example, started with 11.4% at the email sent

stage and increased slightly to 12.9% at data submission, while HR saw a decline to 10.2% at the final stage. Finance and Accounting, however, maintained a steady progression, increasing from 14.7% at email sent to 16.4% at data submission.

C. Application of SEIS Model

Following the completion of phishing and pretexting simulations, the next step involves applying the SEIS model to analyze the findings comprehensively. This requires a detailed review of email engagement statistics to ensure accurate input data for each metric within the SEIS framework.

TABLE 2 ENGAGEMENT STAGES AND PARTICIPANT RATES

Social Engineering Stage	**Participants**
Email Sent (Phishing)	1000/1000
Clicked Link (Phishing)	562/1000
Submitted Data (Phishing)	241/1000
Info Disclosure (Pretexting)	20/100

$$CTR = \frac{562}{1000} \times 100 = 56.2\%$$

$$CCR = \frac{241}{1000} \times 100 = 24.1\%$$

$$DR = \frac{20}{100} \times 100 = 20.0\%$$

$$DT = \frac{450}{50} = 9.0\ minutes$$

CTR weighted = 56.2×0.20=11.24

CCR weighted = 24.1×0.35=8.435

DR weighted = 20.0×0.30=6.0

DT weighted = $\frac{1}{9.0} \times 100 \times 0.15 = 1$

SEIS = 11.24 + 8.43 + 6.0 + 1.67 = **27.34**

This places the SEIS within the **High Impact** category (21-30), highlighting a significant vulnerability level.

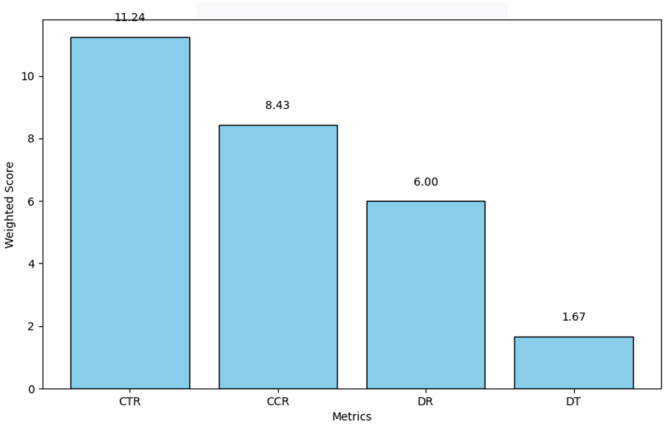

Fig. 4 Weighted contributins of each SEIS metric

This result points to a need for focused security awareness efforts and tighter response mechanisms to mitigate social engineering attacks. With nearly 84.8% of participants opening phishing emails and 56.2% clicking on embedded links, there is clear evidence of susceptibility to initial social engineering tactics. Additionally, the CCR of 24.1% highlights that users are vulnerable to share sensitive information under phishing conditions.

The weighted scoring within SEIS reveals that the CCR carries the highest influence on the final score due to its direct threat to organizational security. This factor alone contributes 8.435 to the SEIS, emphasizing the need to reduce CCR through training and reinforcing secure credential management practices. Meanwhile, the DT of 9.0 minutes, although weighted lower, still underscores the importance of rapid reporting of suspected phishing attempts.

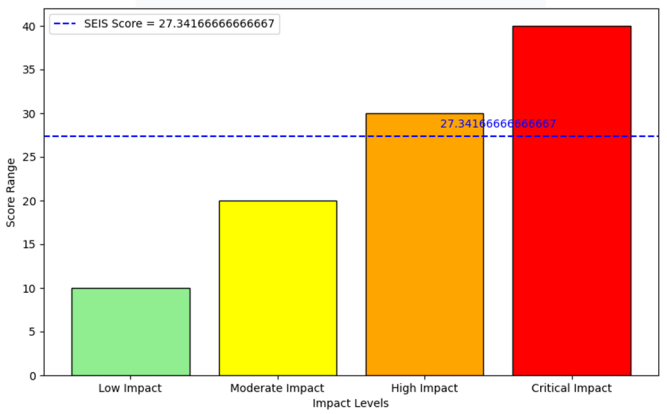

Fig. 5 SEIS Impact Level

This SEIS evaluation recommends prioritizing interventions that target both credential compromise and click-through behavior. Regular security awareness training, particularly focused on recognizing phishing cues and avoiding suspicious links, would directly address these high-risk behaviors. Furthermore, implementing simulated phishing exercises to track improvements in both CTR and CCR could allow the organization to measure progress over time.

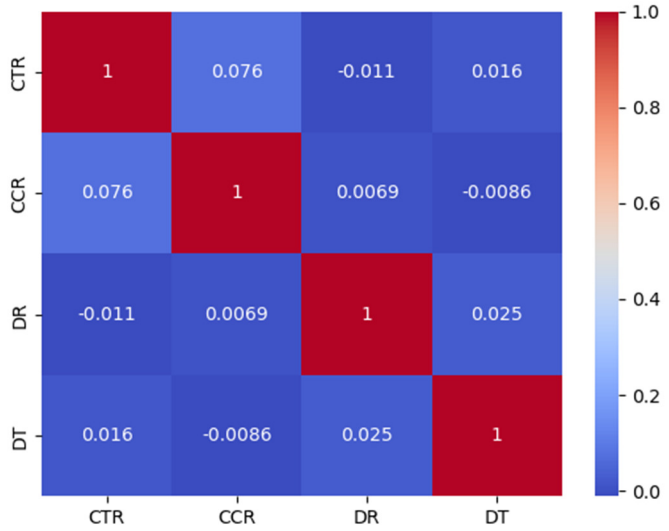

Fig. 6 Correlation matrix of SEIS metrics

VI. CONCLUSIONS

The SEIS model gives important insights into the social engineering risk profile of an organization by underlining those factors that are most influential, in particular, the Click-Through Rate and the Credential Compromise Rate. These metrics are direct representations of vulnerability: CTR describes initial vulnerabilities about the tendency to engage with a phishing attack, while the CCR shows the true risk of unauthorized access due to credentials being exposed.

Because these metrics are so closely associated with breaches in information security, certain targeted interventions should be prosecuted as a matter of priority; for example, continuous security awareness training needs to include both recognition and avoidance of social engineering tactics and longer-term resilience against evolving threat vectors. Proactive measures in those areas will surely contribute to reducing the capability of malicious attackers to exploit and compromise critical systems and data.

Analysis hereby performed is just to show that reduction in DT is very important; due to the velocity potential phishing attempts get identified and reported by users, which bears on the impact a social engineering incident may have. With a shorter DT, containment and mitigation efforts can quickly be effected to prevent an attack from escalating into a wider security breach. This can be achieved through appropriate structured reporting mechanisms and a vigilant security culture that emphasizes timely reporting principles.

As indicated by empirical evidence, training employees on the rapid recognition of suspicious communications and quick reporting can have a material impact on exposure time, thereby reducing the window of opportunity available to the attacker. The emphasis on real-time response becomes more critical, as modern attackers employ sophisticated methods in exploiting latency in human responses.

This research further establishes the SEIS model as a valid, robust quantitative model for assessing social engineering risk, which gives differentiated data-driven insight into the organizational vulnerabilities. By bringing these various measures together in weighted consideration to empirical and ethical considerations, the SEIS manages to maintain an appropriate balance between the assessment of immediate versus latent risk factors in the security posture of an organization. Weighting these factors allows prioritization of interventions at the highest risk behaviors and thus maximizes efficacy in the mitigation of risk. The ethical consideration of employee behaviors by the SEIS model in detection and reporting times considers the human factor in security resilience and respects employee privacy, cultivating a culture of supportive security rather than punitive responses.

While noting this, the SEIS model allows the security teams to implement continuous assessment cycles that provide effective feedback on the timelines of the security interventions. This will, therefore, enable organizations to track regularly the scores that the SEIS achieves after implementation

of new training modules or process improvements and thereby have real-time progress monitoring and refinement of their approach based on data-backed results.

This will be necessary through adaptation in a constantly changing threat environment where new social engineering techniques are developed on a regular basis and require constant adjustment in defensive strategies. This provides an organization with a dynamic and responsive security posture through periodic assessment of the metrics within the SEIS model, updating training to include current tactics utilized by attackers.

Such solutions provided by SEIS, when applied in a structured manner, will enhance the resilience of an organization to social engineering attacks. The insights from SEIS provide visibility of current vulnerabilities in addition to emphasizing behavioral factors in mitigating risks, hence enabling the derivation of a more comprehensive understanding of the organizational social engineering threat landscape.

In long-term, the SEIS model contributes to creating a security-conscious workforce that is more aware of potential threats and how to react. In addition, such a workforce is an important investment in decreasing the risk of successful attacks and strengthening the general defense posture of the organization.

ACKNOWLEDGMENT

We would like to express our gratitude to all colleagues and participants who contributed to this study. Their engagement in the controlled social engineering tests provided invaluable data, enabling a comprehensive analysis and formulation of the Social Engineering Impact Scoring (SEIS) model. We are particularly grateful for the support of our company's information security team, who facilitated this research and offered critical insights into the practical implications of social engineering tactics in real-world scenarios. Their expertise and feedback were instrumental in refining the SEIS model to ensure it accurately reflects organizational vulnerabilities.

REFERENCES

[1] Taylor, J., McAlaney, J., Hodge, S. E., Thackray, H., Richardson, C., James, S., … & Dale, J. (2017). Teaching psychological principles to cybersecurity students. 2017 IEEE Global Engineering Education Conference (EDUCON). https://doi.org/10.1109/educon.2017.7943091

[2] Nobles, C. and Mcandrew, I. (2023). The intersectionality of offensive cybersecurity and human factors: a position paper. Scientific Bulletin, 28(2), 215-233. https://doi.org/10.2478/bsaft-2023-0022

[3] Kheruddin, M. S., Zuber, M. A. E. M., & Radzai, M. M. M. (2024). Phishing attacks: unraveling tactics, threats, and defenses in the cybersecurity landscape. https://doi.org/10.22541/au.170534654.48067877/v1

[4] Almutairi, B. S. and Alghamdi, A. (2022). The role of social engineering in cybersecurity and its impact. Journal of Information Security, 13(04), 363-379. https://doi.org/10.4236/jis.2022.134020

[5] Klimburg-Witjes, N. and Wentland, A. (2021). Hacking humans? social engineering and the construction of the "deficient user" in cybersecurity discourses. Science, Technology, &Amp; Human Values, 46(6), 1316-1339. https://doi.org/10.1177/0162243921992844

[6] Montañez, R., Golob, E. J., & Xu, S. (2020). Human cognition through the lens of social engineering cyberattacks. Frontiers in Psychology, 11. https://doi.org/10.3389/fpsyg.2020.01755

[7] Jari, M. (2022). An overview of phishing victimization: human factors, training and the role of emotions. Computer Science and Information Technology. https://doi.org/10.5121/csit.2022.121319

[8] Shukla, A., Chavan, S. R., & R, S. (2023). Spear watch: a thorough examination to identify spear phishing attacks. International Journal of Innovative Technology and Exploring Engineering, 12(8), 46-51. https://doi.org/10.35940/ijitee.h9680.0712823

[9] Suleman, T. (2021). A survey on web phishing detection techniques. International Journal for Electronic Crime Investigation, 5(2), 25-36. https://doi.org/10.54692/ijeci.2021.050279

[10] Aldawood, H. and Skinner, G. (2019). A taxonomy for social engineering attacks via personal devices. International Journal of Computer Applications, 178(50), 19-26. https://doi.org/10.5120/ijca2019919411

[11] Salahdine, F. and Kaabouch, N. (2019). Social engineering attacks: a survey. Future Internet, 11(4), 89. https://doi.org/10.3390/fi11040089

[12] Bao, J., Ji, C., & Mo, G. (2010). Research on network security of defense based on honeypot. 2010 International Conference on Computer Application and System Modeling (ICCASM 2010). https://doi.org/10.1109/iccasm.2010.5622780.

