Social Engineering Attacks and Human-Centric Defense Mechanism in Corporate Network

NAGESHWAR MASAKAPALLI[1], ROHITH VODAPALLY[2]
[1]*Information Technology, Franklin University*
[2]*Information Technology, University Fairfax*

Abstract- ***The exploitation of human characteristics through social engineering has become an important network security threat which addresses mental vulnerabilities instead of system weaknesses. The phishing baits pretext attacks force users to expose secrets or let their actions endanger the security infrastructure. Most traditional security defenses which primarily depend on technical methods do not address human vulnerabilities and therefore create an important hole in cyber security systems. The research evaluates defense systems that focus on human beings as a means to reduce social engineering attack risks across different environments. A combination of literature review and case study and comparative analysis demonstrates why organizations need awareness training with reinforced behavioral practices and culture changes to improve their defenses. Organizations need to combine psychological and behavioral scientific knowledge with their cyber security plans to establish enduring security systems for their corporate facilities.***

Indexed Terms- ***Social Engineering, Human-centric Security, Corporate Network, Phishing, Cyber security Awareness, Insider Threats, Social Manipulation***

I. INTRODUCTION

Current cyber threats use psychological approaches instead of technical vulnerabilities to conduct advanced attacks against human conduct. Social engineering proves to be the most effective cyber attack method since its reliance on human psychology instead of technical weaknesses. Businesses across the world encounter significant financial losses along with reputation damage due to phishing attacks along with deceptive phone calls and insider abuse. Social engineering tactics form the initial stage of more than 90% of all cyber-attacks which end up being successful. The modern cyber security system has been built better but people continue to be the fundamental vulnerability. This research investigates social engineering attacks and the pivotal role of human-centric defense mechanisms in corporate networks. Security methods that prioritize people over hardware foundation focus on teaching staff members about potential threats and changing their inappropriate behavior patterns rather than using conventional barrier systems. The research presented in this paper establishes a connection between technological security solutions and human-operated factors to build effective organizational protection systems. Human-centric approaches need organizations to develop culture change by making cyber security the responsibility of every department rather than an isolated IT function. Employees develop enhanced vigilance and pro activity toward social engineering threats after they realize the possible risks. Security awareness programs create a culture where staff members develop skills to detect manipulation schemes and report odd behaviors and build team between technical personnel and users. The paper demonstrates why organizations need collaboration across different fields to develop successful defense systems.

II. LITERATURE REVIEW

Multiple research studies examine the effects of social engineering on business security measures. The authors at Mitnick and Simon (2002) defined social engineering through two key concepts: manipulating individuals to perform specific actions and extract confidential data from them. The target audience becomes susceptible to attack through manipulations based on trust relations and authority commands as well as urgency demands and curiosity ingrained

human behavior. Research shows that phishing together with pretexting and tailgating and baiting represent established methods in social engineering attacks. Dhamija et al. (2006) discovered that knowledgeable website users still become prey to deceptive websites which imitate genuine ones. According to Jagatic et al. (2007) spear-phishing achieves high success rates by incorporating social profile data from LinkedIn and Facebook networks. Multiple research works demonstrate the necessity of user education yet acknowledge that standard training methods need repeated encouragement to maintain crisp effectiveness. The existing research fails to adopt psychological principles sufficiently in developing defense systems. A complete security solution requires the integration of cognitive behavior with organizational psychology alongside communication strategies. The military requires both adaptive learning platforms as well as realistic training environments that enhance education.

Table 1: Summary of Social Engineering Techniques

Technique	Description	Common Targets	Success Rate (%)
Phishing	Deceptive emails mimicking legitimate sources	Employees, Executives	30-50%
Baiting	Enticing victims with free items or services	General Staff	25-35%
Pre texting	Impersonation to gain sensitive information	HR, Finance	20-30%
Tailgating	Physical intrusion by following authorized personnel	All departments	15-25%

III. METHODOLOGY

The research methodologies combine both qualitative and quantitative methods to understand social engineering effects and to study human-focused defensive actions inside corporate organizations. The research method incorporates both real-world case study analysis and survey data from threat records from different business sectors. The authors gathered information using standard questionnaires sent to 150 workers from IT, HR, finance, and management divisions within five worldwide companies. The study evaluated workers' knowledge regarding frequent social engineering techniques as well as their detection abilities for dubious communications and understanding of enterprise response frameworks. The research employed semi-structured interview methods with ten cyber security experts and risk control managers who provided organizational perspective on operational practices together with difficulties in training execution and observed human actions during security incidents. The research drew secondary information from industry white papers published research and threat intelligence reports. The study aimed to discover employee exposure patterns along with training assessment and leadership and organizational culture effect on cyber security resilience. Statistical evaluations using SPSS along with thematic coding procedures identified main patterns from both quantitative and qualitative dataset components. The extensive research design produces multiple layers of insight about employee security behavior that enables improvements of threat prevention methods through human-centric solutions.

3. Human-centric Defense Mechanisms

organizations need to establish defensive systems which protect the human aspect because social engineering attacks continue to rise in frequency. These defense approaches differ from traditional firewall systems and intrusion detection because they are designed to enable users with information-based protection along with established organizational support systems.

3.1 Security Awareness Training

Education functions as the leading barrier to guard against social engineering attacks. Through structured

training programs combined with phishing tests and e-learning modules staff members can build their skills to deal with questionable activities. Traditional cyber security training programs for organizations result in a 70% decrease of social engineering attack exposure.

3.2 Behavioral Reinforcement and Gamification

Keeping employees vigilant requires a sustained effort to promote secure behaviors in their workplace practices. Reliable educational software combined with immediate performance assessment technologies and rewards mechanisms help users participate actively in training activities better. A scoring system used for reporting phishing emails provides users with the motivation to be actively involved in corporate security efforts.

3.3 Policy Development and Communication

Security policies need to be delivered to employees through understandable communication methods. Staff members must understand their duties in different workplace situations such as protecting organizational information assets and dealing with questionable email correspondence. The healthcare organization must maintain simple policies which employees can easily access and update frequently to match emerging security threats.

3.4 Organizational Culture and Leadership

Leadership functions as the primary element for developing security-first organizational culture. Security initiatives within organizational goals along with executive examples of secure practices encourage employees to adopt these practices themselves. The regular communication from leadership regarding security importance directly affects employee attitudes combined with their conduct.

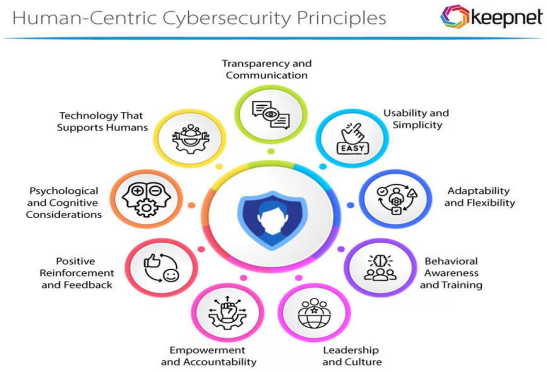

Figure 1: Layers of Human-centric Defense in Corporate Networks / source: Keepnet

IV. CASE STUDY: IMPLEMENTATION OF HUMAN-CENTRIC DEFENSES AT ALPHATECH INC.

Alpha Tech Inc. became victim to a serious phishing attack in early 2023 when criminal actors used this tactic to access employee credentials which in turn enabled them to break into internal systems. Product development sensitive information flowed into public domains when attackers breached the system because Alpha Tech operated without financial stability for two weeks and endured estimated costs of $1.2 million. Alpha Tech changed its cyber security approach to human-centric after the attack occurred. Alpha Tech established regular phishing tests as part of its strategy while redesigning its training program and including interactive learning aspects. Regular town hall meetings started under leadership supervision to build cyber security goal awareness while promoting employee involvement. Staff members demonstrated improved abilities in detecting phishing attempts to a degree of 60% while reporting a 40% increase in suspicious activities leading to successful protection against attacks. Staff members displayed increased confidence when they detected and reacted to social engineering attacks according to interviews.

Table 2: Alpha Tech Security Metrics Before and After Human-centric Measures

Metric	Before Implementation	After 6 Months	Improvement (%)

Phishing Detection Rate	38%	61%	+60.5%
Reported Suspicious Activities	95 per month	133 per month	+40%
Successful Social Engineering	12 incidents/month	5 incidents/month	-58.3%

V. DISCUSSION

All research evidence gathered in the survey and case study along with literature review shows that human factors stand as security's primary weakness and most effective protection against social engineering attacks. The protection capabilities of traditional cyber security systems become less effective since users can be fooled into disabling security measures with ease. Social engineering techniques along with their psychological aspect typically escape the discovery of organizations. Alpha Tech security systems prevented initial network breaches only after human security interventions enhanced security protocols following the incident. The change proves that cyber security requires development into a socio-technical domain. Effective human-centric security systems require both continuous training programs as well as high-quality engagement levels. Uninteractive training materials combined with rare sessions have an ineffective impact on shaping employees' operational choices. Continuous learning models along with interactive simulations together with scenario-based training and authentic leadership support are necessary to make security a regular part of corporate culture. Defense mechanisms within organizations achieve their best results according to cultural and hierarchical organizational dynamics. Workers follow security procedures better because they receive support from executive leadership as well as colleagues in their organization. The active involvement of different organizational entities across all levels confirms that cyber security adoption belongs to every department rather than remaining within IT silos alone. The ability of social engineering strategies to change their tactics remains a vital aspect to consider. Security measures need to match the improvements attackers make in their procedures. The key elements for adaptive defense lie in ongoing assessment together with threat modeling and cycles of feedback to ensure security adaptability. Models focusing on human behavior should adopt psychological research together with behavioral assessment data because this equips them to avoid new tactics of manipulation. The research marks the requirement to create cyber security protection systems which unite automated defenses along with humans' determination to resist cyber threats. Companies which create empowered staff and establish secure organizational cultures will succeed in fighting against social engineering attacks and reducing their consequences.

Figure 2: Post-breach Human-centric Cybersecurity Strategy at AlphaTech Inc. / source: SPRINTZEAL

VI. RECOMEDATION

A complete array of recommended security strategies should be employed by organizations to handle social engineering threats in their corporate networks through human-based approaches. Every employee needs to receive absolute security awareness training that continues without interruption. The training system needs to pass simple phishing simulations to include applications that direct employees through realistic attack scenarios plus illustrations of cognitive biases combined with attacker psychological manipulation methods. Organizations should perform periodic examinations to measure staff knowledge maintenance and change in behavior. A positive workplace security culture must exist where staff members possess the freedom to report security issues

without having to worry about negative consequences. An organization should establish anonymous communication networks which alongside positive recognition for early detection will promote staff engagement with security protocols. Security must become a permanent operational part of daily work routines because leadership demonstrates safety practices while communicating security protocols through established policies. The implementation of technology needs to function as an accessory to human security efforts. AI-based behavioral monitoring tools enable organizations to find changes in user activities that represent possible attacks or deception attempts. These systems function better with employee training data to supply tailored feedback that will help identify staff members needing assistance or intervention. The essential nature of departmental collaboration needs emphasis as the last step. The departments consisting of Human Resources, IT, and Compliance must establish policies which unite to support secure workplace behavior. ratings to security-related policies and hosting interactive workshops and implementing gamified learning activities create an enhanced and effective security environment.

CONCLUSION

A complete array of recommended security strategies should be employed by organizations to handle social engineering threats in their corporate networks through human-based approaches. Every employee needs to receive absolute security awareness training that continues without interruption. The training system needs to pass simple phishing simulations to include applications that direct employees through realistic attack scenarios plus illustrations of cognitive biases combined with attacker psychological manipulation methods. Organizations should perform periodic examinations to measure staff knowledge maintenance and change in behavior. A positive workplace security culture must exist where staff members possess the freedom to report security issues without having to worry about negative consequences. An organization should establish anonymous communication networks which alongside positive recognition for early detection will promote staff engagement with security protocols. Security must become a permanent operational part of daily work routines because leadership demonstrates safety practices while communicating security protocols through established policies. The implementation of technology needs to function as an accessory to human security efforts. AI-based behavioral monitoring tools enable organizations to find changes in user activities that represent possible attacks or deception attempts. These systems function better with employee training data to supply tailored feedback that will help identify staff members needing assistance or intervention. The essential nature of departmental collaboration needs emphasis as the last step. The departments consisting of Human Resources, IT, and Compliance must establish policies which unite to support secure workplace behavior. ratings to security-related policies and hosting interactive workshops and implementing gamified learning activities create an enhanced and effective security environment. Success in corporate network cybersecurity will require advanced technical defense systems as well as highly adaptable and watchful employees. Continued development of threat tactics by attackers demands an equal level of dynamism from organizations through material updates and risk assessments and employee training for critical thinking skills. Organizations that strategically implement security practices into their operational procedures will develop their workforce into a strategic security asset.

REFERENCES

[1] Aditi M Jain. (2025). The Role of Predictive Analytics in E-Commerce Conversion Rate Optimization. Journal of Computer Science and Technology Studies, 7(2), 114-121. https://doi.org/10.32996/jcsts.2023.5.4.25

[2] Akinsuli, O. (2025). The rise of Al-enhanced ransomware-as-a-service (RaaS): A new threat frontier. World Journal of Advanced Engineering Technology and Sciences, 1(2), 85-97. https://doi.org/10.30574/wjaets.2021.1.2.0019

[3] Blake, H. (2025). Al-driven ransomware-as-a-service: The next wave of cybercrime innovation. ResearchGate Preprint.

[4] Chaudhary, A. (2025). How to combat the growing threat of ransomware. New Haven Register. NEW HAVEN REGISTER

[5] Jain, A. M. (2025). Enhancing e-commerce accessibility with AI-powered chatbots:

Integrating accessibility tools and navigation assistants. Journal of Information Systems Engineering and Management, 10(15s), 797–809. https://doi.org/10.52783/jisem.v10i15s.2522

[6] Jain, A. M., & Jain, A. (2025). AI-based content creation and product recommendation applications in e-commerce: An ethical overview. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11(1). https://doi.org/10.32628/CSEIT2410414

[7] K. S. Sharif, M. M. Uddin and M. Abubakkar, "NeuroSignal Precision: A Hierarchical Approach for Enhanced Insights in Parkinson's Disease Classification," 2024 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA), Bali, Indonesia, 2024, pp. 1244-1249, https://doi.org/10.1109/ICICYTA64807.2024.10912990

[8] Liu, X., Liang, J., Yan, Q., Ye, M., Jia, J., & Xi, Z. (2025). Cyber defense reinvented: Large language models as threat intelligence copilots. arXiv Preprint. https://arxiv.org/abs/2502.20791 Mezzi, E., Massacci, F., & Tuma, K. (2025). Large language models are unreliable for cyber threat intelligence. arXiv Preprint. https://arxiv.org/abs/2503.23175

[9] Machireddy, J. R. (2024). Machine learning and automation in healthcare claims processing. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 6(1), 686-701.

[10] Machireddy, Jeshwanth,Automation in Healthcare Claims Processing: Enhancing Efficiency and Accuracy(April 16, 2023). International Journal of Science and Research Archive, 2023, 09(01), 825-834, Available at http://dx.doi.org/10.2139/ssrn.5159747

[11] Mezzi, E., Massacci, F., & Tuma, K. (2025). Large language models are unreliable for cyber threat intelligence. arXiv Preprint. https://arxiv.org/abs/2503.23175

[12] Oyekunle, S. M., Tiwo, O. J., Adesokan-Imran, T. O., Ajayi, A. J., Salako, A. O., & Olaniyi, O. O. (2025). Enhancing data resilience in cloud-based electronic health records through ransomware mitigation strategies using NIST and MITRE ATT&CK frameworks. Journal of Engineering Research and Reports, 27(3), 436-457. https://doi.org/10.9734/jerr/2025/v27131444

[13] Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. Sensors, 23(16), 7273. https://doi.org/10.3390/s23167273

[14] Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A.

[15] Sorokoletova, O., Antonioni, E., & Colò, G. (2025). Towards a scalable Al-driven framework for data-independent cyber threat intelligence information extraction. arXiv Preprint. https://arxiv.org/abs/2501.06239

[16] Sorokoletova, O., Antonioni, E., & Colò, G. (2025). Towards a scalable Al-driven framework for data-independent cyber threat intelligence information extraction. arXiv Preprint. https://arxiv.org/abs/2501.06239

[17] Threat Intelligence 1. Liu, X., Liang, J., Yan, Q., Ye, M., Jia, J., & Xi, Z. (2025). Cyber defense reinvented: Large language models as threat intelligence copilots. arXiv Preprint. https://arxiv.org/abs/2502.20791

[18] Willie, A. (2025). The evolution of ransomware-as-a-service (RaaS): Al's role in cybercrime and countermeasures. ResearchGate Preprint. 4. Dhawan, A., Foley, S., & Mollica, V. (2025). Splitting the spoils: The economics of ransomware as a service. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5110191