Literature Review

Addressing the Human Element in Advanced Persistent Threat Defense: A Literature Review of Social Engineering Mitigation Strategies

Mohamed Yusuf Mohamed Javid

A report submitted in part fulfilment of the degree of

BSc (Hons) in Computer Science

Department of Computer Science
Royal Holloway, University of London

May 21, 2024

1 Introduction

Advanced Persistent Threats (APTs) have emerged as a significant concern for organisations worldwide, particularly those responsible for safeguarding critical infrastructures. APTs are highly targeted, sophisticated attacks that persistently pursue specific objectives, often focusing on stealing sensitive data or establishing long-term access to critical systems. Notably, social engineering tactics play a pivotal role in the success of many APT campaigns targeting critical infrastructures, exploiting human vulnerabilities to gain initial access and facilitate lateral movement within target networks. (Allsopp, 2017)

This literature review examines the crucial intersection of APTs, social engineering, and critical infrastructures, analysing organisations' challenges in defending against these blended attacks. By focusing on the human element as the weakest link in cybersecurity, we argue that while training and awareness programs are essential, they alone are insufficient to mitigate the risks posed by social engineering in APTs. Instead, we propose that organisations implement stringent security policies and automated systems to effectively limit exposure to social engineering practices.

To support this argument, we draw upon several key research papers that provide valuable insights into the psychological factors contributing to individuals' susceptibility to social engineering (Bere et al., 2015), the importance of understanding the human aspect of cybersecurity (Krombholz et al., 2014), and the unique challenges faced by critical infrastructure organisations in securing their systems (Hadziosmanovic et al., 2012).

Furthermore, we explore the limitations of current organisational defences against social engineering in APTs, focusing on the inadequacies of existing training and awareness programs (Aldawood and Skinner, 2019). We argue that organisations must go beyond generic, compliance-focused training and adopt a more holistic approach that encompasses continuous, tailored education, the integration of gamification techniques, and the cultivation of a strong cybersecurity culture.

Through this literature review, the hope is to contribute to the growing body of knowledge on social engineering defences, and critical infrastructure security. Our findings aim to underscore the urgent need for organisations to prioritise the human element in their cybersecurity strategies and adopt a multi-layered approach that combines training, policies, and advanced technologies to safeguard against the ever-evolving threat of APTs.

2 Background

One of the most notable examples of an APT attack on critical infrastructure is the Stuxnet worm, discovered in 2010. This sophisticated malware targeted industrial control systems in Iran's nuclear facilities, causing significant damage and highlighting the vulnerability of critical infrastructure to cyber threats (Baezner and Robin, 2017). In recent years, similar attacks have been observed in the energy, healthcare, and transportation sectors, underlining the need for robust defences against APTs.

Looking at the data specifically shown in the book "Advanced Penetration Testing — Hacking The World's Most Secure Networks" by Allsopp (2017) it is very evident that the success of APT campaigns often relies heavily on social engineering tactics, which exploit human vulnerabilities to gain initial access to target networks. A prime example is the 2015 attack on the Ukrainian power grid, where attackers used spear-phishing emails to trick employees

into downloading malware, ultimately leading to the shutdown of multiple power distribution centres and leaving approximately 225,000 people without electricity (Case, 2016).

To combat the growing threat of APTs, organisations are investing in various defensive measures, According to a 2023 report by Gartner, global spending on information security and risk management technology and services was forecasted to reach $215 billion which is $26 billion more than the previous year (Gartner, 2023). A significant portion of these investments is directed towards "Infrastructure Protection", "Network Security Equipment" and "Security Services". However ambiguous that may seem, no specific number for "Security Training" was displayed.

Hence, despite these investments, the human factor remains a critical vulnerability in APT defence. A study by the Ponemon Institute found that 53% of successful breaches involved the use of social engineering techniques and that social engineering was the number one attack faced (Institute and Cisco, 2023). This highlights the need for effective awareness training and strict security policies to mitigate this risk. According to Krombholz et al. (2015) technical methods to mitigating the risks of social engineering attacks are usually ineffective. Furthermore, Qin and Burgoon (2007) ascertain that individuals often struggle with accurately identifying deception and lies, "People apply cognitive heuristics or have strong preconceived expectations for truthfulness". Looking at this information, and looking at the investment forecasts in the domain of attack prevention, the question "Are the investments enough?" is viable.

3 Problem Areas

One of the primary issues in addressing social engineering in APT attacks is the lack of understanding of the extent to which these techniques contribute to successful breaches. "Social engineering attacks are considered one of the most powerful and dangerous attack vectors because they directly target the human element, which is the weakest link in any security system" (Salahdine and Kaabouch, 2019). Furthermore, Aronovich (2018) suggests that up to 95% of all data breaches are a result of "Human Error". Despite this, many organisations focus their efforts and budgets primarily on technical defences, neglecting the importance of addressing human vulnerabilities (Sloan and Warner, 2019).

The effectiveness of social engineering techniques can be attributed to the psychological principles they exploit. Krombholz et al. (2015) discuss how attackers leverage principles such as authority, scarcity, and social proof to manipulate individuals into divulging sensitive information or granting access to restricted systems. The authors argue that technical defences alone are insufficient to mitigate these risks, emphasising the need for a multi-layered approach that includes employee training and awareness programs.

However, the current state of awareness training programs in many organisations is inadequate. A study by Aldawood and Skinner (2019) found that most training programs are generic, infrequent, and fail to address the specific risks faced by different roles within the organisation. The authors suggest that training should be tailored to the **individual** and the relationship between the **individual and the organisation**, **frequent**, and based on **real-world scenarios** to be effective. Moreover, Proofpoint (2024) report reveals that 78% of German organisations experienced phishing attacks in the method of TOAD (Telephone-Oriented Attack Delivery) but only 21% of those trained to defend those types of attacks. This shows the inherent inadequacies in cybersecurity training when it comes to exposure to a wide range of attacks.

Furthermore, integrating social engineering awareness into existing cybersecurity frameworks and risk management processes can be challenging. Rohleder (2023) identify several barriers, including a lack of standardisation, difficulty in measuring the effectiveness of training, and resistance to change within organisations. The authors recommend that organisations adopt a continuous improvement approach, regularly assessing and updating their training programs based on the latest threats and best practices. Additionally, according to Alshaikh (2020) the following practices have been shown to positively influence the behaviour of employees within organisations:

- "Transformation from compliance to building a culture around cybersecurity".
- "Identifying key behavioural themes from policy".
- "Developing a unique brand for the cybersecurity team".
- "Establishing a cybersecurity champion network".
- "Building a cybersecurity hub".
- "Aligning security awareness with internal and external campaigns".

Looking to the future, organisations must be proactive in addressing the evolving threat of social engineering in APT campaigns. Mashtalyar et al. (2021) discuss the potential impact of emerging technologies, such as artificial intelligence and machine learning, on social engineering tactics. The authors recommend that organisations invest in research and development to stay ahead of these threats and prioritise the creation of a strong security culture that emphasises the importance of human factors in cybersecurity.

Table 1 provides an overview of the main ideas presented in each research paper, emphasising the shortcomings of existing defence approaches and the crucial need to recognise that training programs alone do not constitute a comprehensive defence strategy. Instead, these programs often serve as a means to achieve compliance for the sake of compliance, which, in the long term, can pose significant risks to all stakeholders involved.

Research Paper	**Key Points**
Salahdine and Kaabouch (2019)	Social engineering attacks are powerful and dangerous because they target the human element, which is the weakest link in any security system.
Aronovich (2018)	Up to 95% of all data breaches are a result of "Human Error".
Sloan and Warner (2019)	Many organisations focus their efforts and budgets primarily on technical defences, neglecting the importance of addressing human vulnerabilities.
Krombholz et al. (2015)	Attackers leverage psychological principles such as authority, scarcity, and social proof to manipulate individuals. Technical defences alone are insufficient to mitigate these risks.
Aldawood and Skinner (2019)	Most training programs are generic, infrequent, and fail to address specific risks faced by different roles within the organisation. Training should be tailored to the individual, continuous, and based on real-world scenarios.
Proofpoint (2024)	78% of German organisations experienced TOAD phishing attacks, but only 21% trained to defend against them, highlighting inadequacies in cybersecurity training.
Rohleder (2023)	Integrating social engineering awareness into existing cybersecurity frameworks and risk management processes can be challenging due to lack of standardisation, difficulty measuring training effectiveness, and resistance to change.
Alshaikh (2020)	Practices such as building a cybersecurity culture, identifying key behavioural themes, and establishing a cybersecurity champion network can positively influence employee behaviour.
Mashtalyar et al. (2021)	Organisations must be proactive in addressing the evolving threat of social engineering in APT campaigns, considering the potential impact of emerging technologies like AI and machine learning.

Table 1: Summary of key points from research papers

4 Discussion and Analysis

The problem areas section highlights the critical role of social engineering in the success of APT attacks, with human error being a significant contributor to data breaches. After examining the evidence and arguments presented in the literature, it is clear that organisations are not doing enough to address the human element of cybersecurity, particularly in the context of mitigating social engineering risks in APTs.

One of the most compelling arguments supporting this conclusion is the disproportionate allocation of resources between technical defences and human-focused initiatives. While global spending on cybersecurity has been increasing (Gartner, 2023), the majority of these investments are directed towards infrastructure protection, network security equipment, and security services. In contrast, the percentage of cybersecurity budgets allocated to human-focused defences, such as awareness training and education, remains relatively low (Proofpoint, 2024). This imbalance suggests that organisations are prioritising technical solutions over addressing human vulnerabilities, which is a flawed approach considering the significant role of human error in successful breaches (Salahdine and Kaabouch, 2019; Aronovich, 2018).

Moreover, the effectiveness of current awareness training programs is questionable. The high percentage of organisations falling victim to social engineering attacks, despite providing training, indicates that these programs are not achieving their intended purpose (Proofpoint, 2024). This ineffectiveness can be attributed to several factors, including the generic nature of training content, infrequent delivery, and the lack of tailoring to address specific risks faced by different roles within an organisation (Aldawood and Skinner, 2019). Consequently, employees remain ill-equipped to identify and respond to evolving social engineering threats, undermining the overall security posture of their organisations.

Furthermore, it is obvious that compliance-driven training programs are insufficient and may even be counterproductive. By focusing on achieving compliance for the sake of compliance, these programs fail to address the underlying purpose of cybersecurity regulations and can create a false sense of security (Watson, 2023). Instead, organisations should prioritise training that emphasises the development of critical thinking skills, situational awareness, and the ability to adapt to evolving threats (Islam et al., 2019).

One innovative approach to addressing this challenge is the use of gamification techniques, as demonstrated by companies like KnowBe4. KnowBe4 employs methods such as simulated phishing emails to create an engaging and interactive learning experience for employees (Malik, 2020). By exposing employees to realistic scenarios in a safe, controlled environment, this approach helps them develop the skills and awareness necessary to identify and respond to real-world social engineering threats.

The effectiveness of gamification in cybersecurity training is supported by research. A study conducted by Tchakounté et al. (2020) found that participants who underwent gamified phishing awareness training demonstrated a significant improvement in their ability to recognise and report phishing attempts compared to those who received traditional, lecture-based training. The interactive nature of gamified training, coupled with immediate feedback and rewards, engages employees and motivates them to actively participate in the learning process. However, it is crucial to acknowledge the potential limitations of gamification-based training systems like KnowBe4, particularly when organisations require highly customised, bespoke training that reflects their unique security landscape and social engineering threats. In such cases, the effectiveness of gamification may be compromised, as the resources and funding necessary to develop and maintain hyper-frequent, organisation-specific, and high-quality social engineering simulation campaigns could prove economically infeasible.

One potentially novel solution warranting further research incorporates the principles outlined by Alshaikh (2020) to create a strong cybersecurity culture within organisations. This approach involves the creation of a company-wide "phishing challenge" where randomly selected employees act as "adversaries" and attempt to phish their colleagues using various methods, such as emails or voice phishing. Points are awarded to both successful adversaries and vigilant employees who identify and report phishing attempts. By providing targeted training to the adversaries and all employees. This approach not only educates staff on how to recognise and defend against phishing but also encourages them to think like attackers. This innovative method leverages human competitiveness to drive engagement, reinforce company-specific policies, and ultimately strengthen the organisation's overall cybersecurity posture.

4.1 Conclusion

In conclusion, this literature review highlights the critical role of social engineering in the success of Advanced Persistent Threat attacks targeting critical infrastructures. Despite the growing investments in cybersecurity, organisations continue to prioritise technical defences over addressing human vulnerabilities. The ineffectiveness of current awareness training programs, coupled with the challenges of integrating social engineering awareness into existing cybersecurity frameworks, underscores the need for a paradigm shift in APT defence strategies.

To effectively mitigate the risk of social engineering in APTs, organisations must adopt a holistic approach that combines continuous, tailored training, strong security policies, and innovative solutions such as gamification and company-wide phishing challenges. By prioritising the human element and fostering a strong cybersecurity culture, organisations can significantly enhance their resilience against evolving social engineering tactics.

However, further research is necessary to evaluate the effectiveness and feasibility of these proposed solutions, particularly in the context of organisations requiring highly customised training. As APT actors continue to exploit human vulnerabilities, it is imperative that organisations remain proactive, adaptable, and committed to addressing the human factor in their cybersecurity strategies.

Bibliography

Hussain Aldawood and Geoffrey Skinner. Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues. *Future Internet*, 11(3), 2019. ISSN 1999-5903. doi: 10.3390/fi11030073. URL https://www.mdpi.com/1999-5903/11/3/73.

W. Allsopp. *Advanced Penetration Testing: Hacking the World's Most Secure Networks*. Wiley, 2017. ISBN 9781119367680. URL https://books.google.co.uk/books?id=xukgDgAAQBAJ.

Moneer Alshaikh. Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers Security*, 98:102003, 2020. ISSN 0167-4048. doi: https://doi.org/10.1016/j.cose.2020.102003. URL https://www.sciencedirect.com/science/article/pii/S0167404820302765.

A Aronovich. Why educating your employees on cyber intelligence and security will reduce risk, 2018.

Marie Baezner and Patrice Robin. Stuxnet. Technical report, ETH Zurich, 2017.

Mercy Bere, Fungai Bhunu Shava, Attlee Gamundani, and Isaac Nhamu. How advanced persistent threats exploit humans. *IJCSI*, 11 2015.

Defense Use Case. Analysis of the cyber attack on the ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*, 388(1-29):3, 2016.

Gartner. Gartner forecasts global security and risk management spending to grow 14% in 2024. https://www.gartner.com/en/newsroom/press-releases/2023-09-28-gartner-forecasts-global-security-and-risk-management-spending-to-grow-14-p September 2023. Accessed: 2024-04-06.

Dina Hadziosmanovic, Damiano Bolzoni, Sandro Etalle, and Pieter Hartel. Challenges and opportunities in securing industrial control systems. *2012 IEEE Workshop on Complexity in Engineering, COMPENG 2012 - Proceedings*, 06 2012. doi: 10.1109/CompEng.2012.6242970.

Ponemon Institute and Cisco. Exclusive research report. Technical report, Poneman Institute LLC, 2023. URL https://www.cisco.com/c/dam/en/us/products/collateral/security/ponemon-report-smb.pdf. Accessed: 2024-04-06.

Tasmina Islam, Ingolf Becker, Rebecca Posner, Paul Ekblom, Michael McGuire, Hervé Borrion, and Shujun Li. A socio-technical and co-evolutionary framework for reducing human-related risks in cyber security and cybercrime ecosystems. In *International Conference on Dependability in Sensor, Cloud, and Big Data Systems and Applications*, pages 277–293. Springer, 2019.

Katharina Krombholz, Heidelinde Hobel, Markus Donko-Huber, and Edgar Weippl. Advanced social engineering attacks. *Journal of Information Security and Applications*, 22, 10 2014. doi: 10.1016/j.jisa.2014.09.005.

Katharina Krombholz, Heidelinde Hobel, Markus Huber, and Edgar Weippl. Advanced social engineering attacks. *Journal of Information Security and Applications*, 22:113–122, 2015. ISSN 2214-2126. doi: https://doi.org/10.1016/j.jisa.2014.09.005. URL https://www.sciencedirect.com/science/article/pii/S2214212614001343. Special Issue on Security of Information and Networks.

Javvad Malik. Making sense of human threats and errors. *Computer Fraud & Security*, 2020 (3):6–10, 2020.

Nikol Mashtalyar, Uwera Nina Ntaganzwa, Thales Santos, Saqib Hakak, and Suprio Ray. Social engineering attacks: Recent advances and challenges. In *International Conference on Human-Computer Interaction*, pages 417–431. Springer, 2021.

Proofpoint. The state of the phish 2024. `https://www.proofpoint.com/uk/resources/threat-reports/state-of-phish`, 2024.

Tiantian Qin and Judee K Burgoon. An investigation of heuristics of human judgment in detecting deception and potential implications in countering social engineering. In *2007 IEEE Intelligence and Security Informatics*, pages 152–159. IEEE, 2007.

N. Krinken Rohleder. Why cybersecurity awareness training programs fail. *LinkedIn*, September 2023. URL `https://www.linkedin.com/pulse/why-cybersecurity-awareness-training-programs-fail-krinken-rohleder/`. Accessed: 2024-04-08.

Fatima Salahdine and Naima Kaabouch. Social engineering attacks: A survey. *Future Internet*, 11(4):89, 2019.

Robert Sloan and Richard Warner. *Why Don't We Defend Better?: Data Breaches, Risk Management, and Public Policy*. CRC Press, 2019.

Franklin Tchakounté, Leonel Kanmogne Wabo, and Marcellin Atemkeng. A review of gamification applied to phishing. 2020.

Hayley Watson. Security think tank: Training can no longer be a compliance exercise. *Computer Weekly*, Feb 2023. URL `https://www.computerweekly.com/opinion/Security-Think-Tank-Training-can-no-longer-be-a-compliance-exercise`. Accessed: 2024-04-06.