The human element remains a significant challenge to cybersecurity resilience, and despite technological advancements, this area is still heavily neglected

Examining the hidden risk in cyber conflict: human behaviour as the critical blind spot

by Christopher Weir and Ally Zlatar

Introduction

Despite significant advancements in cybersecurity technology and defensive strategies, human errors continue to be a major vulnerability. This is often due to negligence or a lack of education and awareness, making the human element a persistent blind spot for organizations around the world. This paper examines the role of human behaviour in cybersecurity breaches by utilising case-study analysis to highlight how several key human-caused cyber-attacks, such as social engineering, poor security measures, and insider threats, continue to undermine even the most heightened security infrastructures. In conjunction, it will also cross-compare the real-world events with theoretical cyber scholars such as Kevin Mitnick and Bruce Schneier to illustrate the necessity for a holistic approach that prioritises human-centric cybersecurity strategies to ensure the preservation of cyber resilience.

Human errors

Cybersecurity is often perceived as a technological domain. However, as it governs and operates with people at the forefront, understanding the interplay between human psychology and cybersecurity vulnerabilities can lead to more effective risk mitigation strategies. Bruce Schneier (2018) argues that security is a process, not a product. In this regard, there is a need to emphasise that human behaviour and employee education must be continuously managed alongside technological advancements. Drawing on this

was the case study of the Equifax cybersecurity incident in September 2017, which occupies the top 10 charts of the largest data breaches in history with 148 million people affected (Kabanov, Ilya and Madnick, Stuart E., 2020). The case study reveals that the breach occurred due to an expired certificate on the Secure Sockets Layer (SSL) visibility appliance responsible for monitoring encrypted network traffic. The certificate expired in November 2016 and went unnoticed by the security team until August 2017. This oversight allowed an attack to commence in May 2017, resulting in the extraction of consumer personal identifiable information (PII) that went undetected for 78 days. The study highlights that while companies can integrate security technologies and develop high-fidelity detections, these measures are only effective if properly maintained and if poor or negligent human oversight is eliminated. In Verizon's 2024 Data Breach Investigations Report (2024), the company reported that approximately 68% of breaches involved a non-malicious human element, such as falling victim to social engineering or making an error. Remarkably, this was the same level as reported in 2020, indicating that in four years, no progress had been made to reduce the human element in security breaches.

Human psychology

Often attackers exploit human psychology rather than technical flaws to gain access to secure systems. The 2020 Twitter hack involved hackers using social engineering to manipulate employees into granting access to internal administrative tools (Witman & Mackelprang, 2022). This allowed them to take over high-profile accounts, including those of Barack Obama and Joe Biden, to promote a cryptocurrency scam. While this incident is not necessarily novel in its approach, it underscores the importance of addressing the risks posed by human psychology and the need for stronger internal security policies, such as multi-factor authentication and preventive education programmes to help reduce the likelihood of employees being exploited.

Despite significant advancements in cybersecurity technology and defensive strategies, human errors continue to be a major vulnerability

Former hacker and security consultant Kevin Mitnick illustrated how social engineering remains one of the most effective hacking techniques, exploiting emotions and the idea of trust - far easier and more effective than technical attacks - since human psychology can be fickle and not always equipped to handle situations in which individuals become 'hooked' (Mitnick in: Whiteman, 2017). This consideration highlights that, especially in this blind spot, organizations do not offer enough support to help their employees avoid emotional responses to attackers, leading many to act irrationally. Thus, the implementation of training programmes that heighten awareness of cyber-attacks can provide employees with more tools to stay vigilant (Stacey et al., 2021). A new model also focuses on using behavioural analysis to be monitored and trained with AI to detect anomalies in human behaviour and flag potential insider threats before they escalate (Verma, 2024). A comprehensive and multifaceted approach is required when addressing the complexity of human psychology. Enhancing security awareness training that incorporates phishing simulations and social engineering awareness techniques, alongside support to help employees manage their emotions during these simulations, will help strengthen this

blind spot by providing a more holistic combination of awareness and educational tools.

Lack of adaptation and investment

The current scope of cyber resilience primarily focuses on automation to account for the sheer volume and variety of threats. However, as examined above, most threats are human-correlated. Cavelty (2024) further contributes to this discourse by discussing the importance of investment within the economics of cybersecurity to address this primarily through financing improved security awareness and training programmes. When the healthcare sector became a prime target for cyber threats during the COVID-19 pandemic, phishing scams led to several breaches, such as the attack against the European Medicines Agency (EMA). The incidents often exploited pandemic-related anxieties, yet institutions like EMA, hospitals, and research institutions were not well trained to handle this new type of threat alongside the high emotional stakes of the pandemic situation (Awaludin et al., 2023). Psychological stressors such as these can lead to increased human susceptibility to phishing threats, and the lack of adaptation in cybersecurity training programmes during this time allowed attackers to gain access to vaccine-related data through compromised emails and accounts (Awaludin et al., 2023). While brief, the analysis of attacks and cybersecurity in the health sector during the COVID-19 pandemic reaffirms the importance of organizations to adopt a multi-layered approach to mitigate human-related cybersecurity risks, combining both technological and psychological training.

> **“Often attackers exploit human psychology rather than technical flaws to gain access to secure systems**

Conclusion

The human element remains a significant challenge to cybersecurity resilience, and despite technological advancements, this area is still heavily neglected. As outlined in the case studies, such as the Equifax breach, Twitter Bitcoin scam, and EMA COVID-19 healthcare phishing attacks, major blind spots within the last five years are primarily social engineering and psychological vulnerabilities. Accordingly, the best methods to address this blind spot require further emphasis on education and training to improve awareness of social manipulation and psychological factors. Cybersecurity requires a holistic approach that prioritises education and human-centred strategies to reduce the current and evolving security risks.

References

Awaludin, A., Sulistyadi, W., & Chandra, A. F. (2023). Analysis of Attacks and Cybersecurity in the Health Sector During a Pandemic COVID-19: Scoping Review. Journal of Social Science, 4(1), 62-70.

Kabanov, Ilya and Madnick, Stuart E., A Systematic Study of the Control Failures in the Equifax Cybersecurity Incident (2020). MIT Sloan Research Paper No. 2020-19.

Cavelty, M. D. (2024). The Politics of Cyber-Security. Taylor & Francis.

Schneier, B. (2018). Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. WW Norton & Company.

Stacey, P., Taylor, R., Olowosule, O., & Spanaki, K. (2021). Emotional Reactions and Coping Responses of Employees to a Cyber-attack: A Case Study. International Journal of Information Management, 58, 102298.

Verizon. (2020). 2020 Data Breach Investigations Report. Verizon Business.

Verizon. (2024). 2024 Data Breach Investigations Report. Verizon Business.

Verma, D. (2024). Enhancing Cybersecurity Through Adaptive Anomaly Detection Using Modern AI Techniques (Master's thesis).

Whiteman III, J. R. (2017). Social engineering: Humans Are the Prominent Reason for the Continuance of These Types of Attacks (Master's thesis, Utica College).

Witman, P. D., & Mackelprang, S. (2022). The 2020 Twitter Hack--So Many Lessons to Be Learned. Journal of Cybersecurity Education, Research and Practice, 2021(2).

ABOUT THE AUTHORS

Christopher Weir is a Technical Security Manager at Lloyds Banking Group with over seven years of experience in cybersecurity. Specializing in process automation, internal audits, and risk management, he leads initiatives to enhance the organization's security posture. Previously a Cyber Security Analyst, Christopher played a key role in identifying vulnerabilities and implementing solutions. His expertise in security policies, process automation, and auditing ensures the bank's systems remain secure and compliant with industry standards.

Dr Ally Zlatar is an artist, scholar, and activist. She is the founder of The Starving Artist, an artist initiative that utilises creative voices as a way to create advocacy and systemic reform since 2017. She has received numerous accolades for her humanitarian work, such as the Commonwealth Innovation Award (2023), UN Women 30 for 2030 (2024), the Princess Diana Legacy Award (2021), and the King Hamad Award for Youth Empowerment (2022).

Download UNICRI publications