Career Paper: Red Teaming

by

Galen Cole

A Research Paper

Submitted to CYSE 201S

Old Dominion University

Career Paper

November, 2024

Introduction

Professionals in cybersecurity careers, such as red team penetration testers, depend heavily on social science research and principles to conduct their research and observations. The article by S. Paoli and J. Johnstone highlights how penetration testers use methods influenced by criminological theories, such as Routine Activity Theory (RAT), and socio-technical approaches to evaluate organizational vulnerabilities and security posture. Utilizing RAT, we can view penetration testing as a simulation of crime, where the tester is the “likely offender,” the organization vulnerabilities represent “suitable targets,” and deficiencies in security practices embody the “absence of capable guardians” (De Paoli & Johnstone, 2023). These frameworks emphasize the need to consider human behavior, organizational culture, and societal structures alongside technical vulnerabilities. Critical social science concepts, such as understanding the motivations and behaviors of individuals within an organization, play a vital role in cybersecurity. For instance, during a penetration test, technological systems and organizational practices are examined. We can explore how group structures and “Ideological Leaders” influence ideological and decision-making matters (DeNegre et al., 2019). This approach can reveal gaps, such as inadequate training or poor security practices, which increase vulnerabilities. This socio-technical perspective, rooted in social science, shows how vulnerabilities emerge from the complexities of interconnected systems and human behaviors tied to them. This approach stresses the importance of the human element in security, including cultural factors and the training of employees to mitigate risks.

Marginalized Groups & Issue Resolution

Cybersecurity professionals attempt to address issues regarding society at large. However, risks are so vast a team is needed to ensure effective mitigation. Cybersecurity is forged through teamwork and mutual understanding. Not one person will know everything. Effective security policies must account for diverse user needs and ensure inclusivity in digital spaces. For example, protecting personal data and ensuring equitable access to secure systems are critical. The goal is to safeguard vulnerable populations, such as those disproportionately affected by cybercrimes like phishing and identity theft. After the COVID-19 pandemic, these marginalized groups have only grown as typical in-person workers are forced to access company resources online and at home with minimal prior training. The legitimacy of penetration testing lies in its ethical framework, which distinguishes it from criminal hacking. By maintaining ethical boundaries and focusing on inclusivity, cybersecurity professionals can maintain the community's trust and foster a safer digital environment where individuals feel confident to engage in technology without fear of exploitation or inequity. Ethics, diverse technical expertise, and resource limitations provide challenges professionals must overcome. Policies should prioritize inclusivity, ensuring no group is disproportionately disadvantaged by gaps in cybersecurity measures or digital access.

Internal Influence

Not only is it essential to take a look at external societal influences, but it is also important to reflect on internal influences. Personal biases and blindspots regarding how tests should and are conducted can influence findings and practices exhibited by an individual. These influences often operate unconsciously, without individuals realizing it. Cognitive biases, such as confirmation bias or the halo effect, can lead researchers to favor information that supports their pre-existing beliefs while overlooking or undervaluing data that challenges their assumptions. Moreover, cultural or personal experiences may impact how particular phenomena are understood or framed, leading to skewed conclusions. The human factor in red teaming raises questions regarding how red teamers come to be selected, biases and blindspots when considering criteria in tests, and the effect of harmful content on researchers (Zhang, et al., 2024).

Conclusion

Applying social science principles in daily cybersecurity routines highlights the necessity of a holistic view of security. By integrating perspectives from the social sciences, experts can develop more robust and socially responsible solutions that account for the interplay between technical defenses and societal impacts. This interdisciplinary approach ensures that security solutions protect systems and consider broader societal implications, promoting equity, accessibility, and trust. Adopting a more comprehensive view of security leads to more resilient systems, greater public confidence, and a safer digital environment.

Works Cited

De Paoli, S., Johnstone, J. (2023, October). “A qualitative study of penetration testers and what they can tell us about information security in organisations.” Information Technology & People. https://doi.org/10.1108/ITP-11-2021-0864

Myers, K., DeNegre, A., Gallos, L., Lemanski, N., Mayberry, A., Redere, A., Schwab, S., Stringham, O., Fefferman, N. H. (2019, June). “Dynamic Ad Hoc Social Networks in Improvised Intelligence/Counter-Intelligence Exercises: A Department of Homeland Security Red-Team Blue-Team Live-Action Roleplay.” Journal of Homeland Security and Emergency Management. https://doi.org/10.1515/jhsem-2018-0027

Zhang, A. Q., Shaw, R., Anthis, J. R., Milton, A., Tseng, E., Suh, J., Ahmad, L., Kumar, R. S., Posada, J., Shestakofsky, B., Roberts, S. T., Gray, M. L. (2024, November). “The Human Factor in AI Red Teaming: Perspectives from Social and Collaborative Computing.” In Companion Publication of the 2024 Conference on Computer-Supported Cooperative Work and Social Computing (pp. 712-715). https://doi.org/10.1145/3678884.3687147