Student Name: Michael Everett

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Yalpi, Diwakar

Cybersecurity Analyst: Applying Social Science to Enhance Cybersecurity

Introduction

A Cybersecurity Analyst, also known as a Security Operations Center (SOC) analyst, is a very important person within any organization that aims to safeguard that organization against cyber threats. Although the analyst's job is considered very technical, the truth is that professionals within the field of information security rely greatly upon the research and theory of the social sciences. The bottom line up front is that information security cybersecurity, really is not merely a computer and networking issue but is also a people issue, a behavior issue, and a matter of social trends. The analyst's job involves tracking the behavior of the network, detecting and analyzing "suspicious behavior," and acting against "attacks" launched against the network. "Most cybersecurity incidents are not the result of a failure of a specific system, but because people get fooled, coerced, or misled into doing things that lead to cybersecurity incidents," says the Verizon Data Breach Investigations Report (2024), and over eighty percent of all incidents are the result of people's mistakes and actions. This view makes the knowledge of psychology and communication and of behavior and trends within society necessary knowledge not only of the firewalls and software used but also of the motivations and actions of the attackers and the attacked. The analyst has at his/her ready commands a security operations center and "other analytic and enforcement tools such as security information and event management systems and security incident response management software, but the analyst needs to have a good understanding of the attackers and defenders' behavior and motivations because the analyst's

work involves not only tracking and analyzing data but also explaining security risks to employees, training staff on security best practices, and implementing security processes that are practical for nontechnical and even lay staff to follow."

Social Science Principles Applied to the Career

Social science theories affect every aspect of a cybersecurity analyst's work. The first important theory of psychology that a cybersecurity analyst could apply is the theory of cognitive biases. Attackers often write phishing and scam emails that are developed to launch emotional attacks such as fear, excitement, and urgency. The analyst applying knowledge of the theory of cognitive biases such as the "Authority Bias", this is a call from your CEO act immediately, and "Scarcity Bias", in 24 hours, your account will be deleted, could understand the manipulation of the attackers and develop trainings that lead people to think before acting (Flores & Ekstedt, 2019). Another important connection to the field of social science is the theory of Social Engineering, a theory derived from Social Psychology. The analyst instead of cracking into the system through code works with manipulating people using a masquerade of a trustworthy person. The analyst needs to understand the importance of trust and influence and the reasons behind people complying with the person with the power of influence. The analyst also practices the theory of ethics; a theory taught in the field of Social Science. The analyst tries to understand a balance between security and privacy to avoid invading people's privacy while monitoring the employees' accounts and viewing confidential information. This theory of ethics provides guidance for analysts concerning matters such as the intensity of surveillance and the reasons behind the information sharing of threats.

Effects of Misinformed Discourses

The role of a security analyst is also linked to the concern of marginalized groups. The vulnerable groups such as low-income people, minorities, and immigrant communities, the elderly, and people with little access to cyberspace experience cyber threats differently. Studies indicate that people with low resources have low information and training on the internet and are also prone to cyber-attacks (Dodel & Mesch, 2018). The cyber attackers also target these groups because these people are easier targets. The vulnerable groups may also be using outdated equipment and might not be exposed to cyber security training. The other factors that could be a barrier could be language and a lack of confidence in using cyberspace. The analyst will have to prepare training programs that are clear and easily understandable. According to Jarrett and Roberts (2023), the security measures and technologies are also ignoring vulnerable groups and thus widening the cyber gap. An aware cyber security analyst also recognizes these issues and encourages organizations to take into consideration the vulnerable groups when establishing security policies. The analyst uses the research of the social sciences to influence the training program to involve various languages and cultural examples.

Career Interaction with Society

This career is also closely tied with society. Cybersecurity analysts safeguard large organizations such as schools, hospitals, banks, and government bodies, and through these actions, analysts safeguard citizens and individuals. Yet society also influences the analyst's profession. As the population of people storing private information online increases, so does the occurrence of cyberattacks and the complexity of these cyberattacks. The advent of social networking sites also increases the private data that cyber attackers steal and misuse. Cybersecurity analysts are not merely responding to the trends of cybersecurity but are also contributing towards creating a safer online environment. The analyst's profession not only deals

with the issue of cybersecurity and implementing technologies that safeguard online security but also deals with educating people and making them aware of staying online safely.

Conclusion

The Cybersecurity Analyst is a specialist whose task is to safeguard computer systems through the understanding of both technologies and people's behavior. Social science theory and knowledge of persuasion, influence of people, and making ethical decisions influence the actions of the analyst every day. The analyst understands that people are differently affected by the issue of cybersecurity and thus has the responsibility of ensuring that training and safeguarding reach all people. The issue of cybersecurity is the task of safeguarding people, and the best analysts are those using knowledge of people's behavior and actions through social sciences.

References

Jain, Samvit, Edward Felten, and Steven Goldfeder. “Determining an Optimal Threshold on the Online Reserves of a Bitcoin Exchange.” *Journal of Cybersecurity*, vol. 4, no. 1, 2018, Article tyy003, Oxford University Press, https://academic.oup.com/cybersecurity/article/4/1/tyy003/5066370

Flores, W., & Ekstedt, M. (2019) https://doi.org/ Jarrett, K., & Roberts, E. (202

Verizon. (2024). Data Breach Investigations Report (DBIR). Verizon Enterprise. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf