Security Architecture Career

Deshanta Kearney

Old Dominion University

Cyse 201S: Cyber Security & Social Science

April 10, 2023

Security Architecture Career

Cybersecurity has become crucial to contemporary society as the world relies increasingly on technology. The field of Security Architect is one of the most significant in cybersecurity. Security architects must develop and execute security solutions to safeguard a company's applications, systems, and networks from cyber threats. This paper will review how security architects use social science theories and research to carry out their job and how this career path relates to underrepresented groups and society.

Security architects are employed in various sectors, including government, banking, healthcare, and technology. Their primary responsibility is to plan and supervise the execution of security solutions that protect an organization's data, assets, and customers from cyber-attacks. They evaluate the organization's security requirements, pinpoint weaknesses, and create security plans that complement corporate goals. Security architects must stay informed about new threats and technological advancements to ensure their solutions continue working.

Security architecture highly depends on social science research and principles, including risk management, legislation, regulation, human behavior, and decision-making.

*Human Behavior and Decision-Making*

Designing security solutions that are both powerful and easy to use is one of the biggest challenges confronting security architects. Security architects must comprehend how users engage with technology and how their actions impact the organization's security posture. They must balance security requirements while considering customer experience, convenience, and usability. To make sure security solutions are accessible and user-friendly, security architects might, for instance, perform user surveys and usability testing.

Designing security systems can benefit from research into human decision-making and behavior. According to a study, users frequently reuse passwords across multiple accounts, which makes them more vulnerable to cyber-attacks (Charoen, 2014). By implementing password strength meters and offering password management tools, security architects can create security solutions that motivate users to create strong passwords that are unique to them.

*Risk Management*

In a security architecture, risk management is crucial. Developing methods to mitigate threats requires security architects to evaluate the organization's risk posture. They employ risk management models like the NIST Cybersecurity Framework to identify, evaluate, and manage risks. Social science research on risk perception and decision-making influences the risk management method.

According to studies on risk perception, people frequently overestimate the risk of unlikely occurrences like airplane crashes while underestimating more frequent risks like automobile accidents. Using this information, security architects can effectively distribute resources by explaining the risks posed by cyber threats to decision-makers and stakeholders. Additionally, a study on decision-making in uncertain situations can help design security solutions that work well in these situations (Garg & Camp, 2012).

*Policy and Regulation*

Policies and statutes, such as those governing data privacy and cybersecurity, must be kept current by security architects. These laws and guidelines must be followed when designing security solutions. The adoption and diffusion of policies are topics of social science research, and security architects can use this knowledge to encourage policy compliance within the company.

Research on the adoption and diffusion of policies has revealed that encouraging policy compliance requires strong communication and instruction (Lee, 2021). Security architects can use these insights to create security solutions that adhere to rules and laws and are simple for all parties to understand.

*Marginalized Society and Groups*

Marginalized groups, as well as society at large, are significantly impacted by security design. Security solutions must take accessibility, variety, and inclusion into account. Security engineers must ensure that security solutions do not obstruct access to technology or prevent users with disabilities from using them. Various groups of individuals, including those with various cultural or linguistic backgrounds, must be considered when developing security solutions.

Security architects also play a crucial part in safeguarding sensitive medical and financial data, which may disproportionately impact marginalized groups. For instance, people from poorer socioeconomic backgrounds might be more susceptible to financial fraud and identity theft (Finklea, 2010). Security architects must ensure that their solutions efficiently secure confidential data and do not erect further obstacles for these people.

In conclusion, security architects are essential in defending businesses against online threats. A thorough grasp of social science theory and research is essential for the position, which also calls for understanding risk management, policy, regulation, human behavior, and decision-making. Security engineers must also ensure that their solutions are usable by everyone, including all users, and do not negatively affect underrepresented groups. Security architects will be crucial in maintaining the security of our data and networks as the world becomes increasingly dependent on technology.

References

Charoen, D. (2014). Password security. *International Journal of Security (IJS)*, *8*(1), 1.

Garg, V., & Camp, J. (2012, January). End user perception of online risk under uncertainty. In *2012 45th Hawaii International Conference on System Sciences* (pp. 3278–3287). IEEE.

Finklea, K. M. (2010). *Identity theft: Trends and issues*. DIANE Publishing.

Lee, J. W. (2021). Diffusion of innovations. In *Encyclopedia of Sport Management* (pp. 137–138). Edward Elgar Publishing.