Alex Bonhomme

12/2/2021

CYSE201S

Career Professional Paper

Security Architect

Security architects are management-level workers who supervise the security of an organization's network. This includes the design, implementation, and operation, as well as the entire life of the network. These certain architects assess their organization's Information Technology as well as the organization's computer systems. This occurs to identify strengths and weaknesses. Some of these assessments include penetration testing, risk analysis, and ethical hacks. These ethical hacks can be performed on local area networks, wide area networks, and virtual private networks. Knowing what must be done, one could say that security architects think like hackers. The previously mentioned assessments are in place to identify and work on vulnerabilities and improve on the strong points of the network as well. Another task held to security architects is to respond to security breaches. Whenever vulnerabilities are exploited, the incident is assessed in terms of causes, the damage done, and figuring out how to recover lost data. Appropriate changes will then be exacted.

Security architects use social science research and social science principles more than one may think. Regarding the research portion, they participate in experiments all the time when assessing the vulnerabilities and strengths of their assigned network(s). Now although it may not be a 'classic' experiment as one would do in chemistry class, they are done in the field of cyberspace. These architects may also use archival research as assistance in their assessments, whether it is help on conducting it, or just trying to find out what risks certain vulnerabilities may impose on the network. As for the social science principles, I believe that security architects indulge in most, if not every principle, even if they do not know it themselves. Objectivity may be the most obvious principle in how these professionals only need to complete their designated tasks in designing, cultivating, and maintaining their network and its security. For tasks that may raise questions, the main focus is to not let those opinions shape their performance. They also use parsimony when explaining a factor of design or maintenance of the network to an organization or to a team. It is up to them and their communication / speech-delivery skills to bring everyone together and give an explanation easy enough for even people who aren't in the field to understand the problem(s) and what needs to be done. Almost every career in cybersecurity is going to include a bit of skepticism as well. This regards the questioning and requestioning of research, encouraging research toward newer and stronger methods of security, and combating malware.

When looking at security architects, and careers in cybersecurity, it is more inclusive than it has ever been before. Hoping that this trend continues, I personally have seen many women, minorities, and people who identify as other genders and things of that nature included in the cybersecurity role. This is amazing regarding how many people this brings into the field. This is an improvement for society in how more backgrounds and knowledge can be included in research and improving security systems.

Works Cited

Failed Architecture. “How More Security Makes Women and Queer People Feel Less Safe.” *Failed Architecture*, https://failedarchitecture.com/how-more-security-makes-women-and-queer-people-feel-less-safe/.

“How to Become a Security Architect: Requirements for Security Architect Jobs.” *Cybersecurity Degrees | Cybersecurity Degrees Online*, 15 Nov. 2021, https://www.cyberdegrees.org/jobs/security-architect/.

A Hybrid Cloud Architecture for a ... - Projects at Harvard. https://projects.iq.harvard.edu/files/lwisniewski/files/iqss_rce_cloud_04.15.2014.pdf