Journal Entry 2: The Role of Engineers in Managing Cyber Risk

Name: Leah Drew

Date: 9/22/2019

Details

According to the National Institute of Standards and Technology's Introduction to Information Security (2017), System Security Engineers are among the main roles within an organization. According to NIST, "Systems security engineering provides an elementary approach for building dependable systems" (p. 39) meaning that these engineers design and maintain the security system itself. This is a job that requires constant innovation and coordination with people who hold other roles within the organization in order for the system to run smoothly. Engineers may use encryption, intrusion detection, and other methods in their design to keep the system secure (Bourgeois, 2014).

Security is always evolving, and so are the best practices for maintaining it, so engineers have to adapt to keep up with the changes. This means that engineers will always be needed to maintain security systems. A good way of making sure a system is secure is by building it to be based on security from the start. Another word for this is "security-by-design," an approach that can be used by engineers to make it easier to keep technology secure. This design will be built on by other cybersecurity experts, so it's important to have a good basis for the system (van Ommeren, 2014, p. 35-39).

In electric grid security, physical and cyber security are very closely intertwined, as attacks against physical infrastructure can affect cyber systems and vice versa. It's even more important in these situations to have sound engineering supporting these systems. They will never be completely impermeable, but engineers can reduce the risk of an electric grid suffering a security event by creating stronger systems that are harder to penetrate. Electric grids are very important to protect because breaches impact people across wide areas. Issues with system design can leave holes open for possible security events but by creating systems that have as

few issues as possible, engineers can reduce the effects of cybersecurity events on the public (ICF International, 2016, p. 27).

References

Bourgeois, D. (2014). *Information Systems for Business and Beyond.* Retrieved September 22, 2019, from https://drive.google.com/file/d/1DxwGumLqWmoqjYT0XFekMu6dFg3ev4Eh/view

ICF International. (2016). *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats.* Retrieved September 22, 2019, from https://www.energy.gov/sites/prod/files/2017/01/f34/Electric Grid Security and Resilience--Establishing a Baseline for Adversarial Threats.pdf

National Institute of Standards and Technology (U.S.). (2017). *An Introduction to Information Security.* Retrieved September 22, 2019, from https://drive.google.com/file/d/1F4UD29y91CF47MvnSKAI1OHmj60YqB3V/view

van Ommeren, E., Borrett, M., & Kuivenhoven, M. (2014). *Staying ahead in the Cyber Security game: What Matters Now.* Retrieved September 22, 2019, from https://drive.google.com/file/d/138J6FOI3XLjz87rb0t73v4xoZIcmGp9z/view