Brittany Cowdrey

CYSE 201S

03 December 2023

Cyber Security Risk Analyst

In the modern world, the thought of doing anything not on a computer or phone of some kind is a strange thought to most. Technology has taken over the lives of billions worldwide and has brought forth with it the desperation for improved cyber security. That need for cyber security is why there are so many career paths a person can take while pursuing a career in a cyber field. A cyber security risk analyst is one of the many careers one could choose among these career fields.

Cyber security risk analysts have become vital in the fight against cybercrimes and vulnerabilities. A cyber analyst requires many technical skills and can fortify a network. They should be able to prevent exploits through vulnerabilities, monitor possible breaches, fix security issues, and train the organization on best security practices. According to Matzelle, “In addition to these technical skills, a cyber risk analyst should also be able to see the big picture and apply their analytical and problem-solving skills to determine which potential threats deserve attention.” (Matzelle). On top of these skills, an analyst must understand the current threat landscape and trends in the cyber world. This requires them to do possible archival research to find information of cyber-attacks and current trending attacks that are taking place. This research could help them determine currently known vulnerabilities by the adversaries. Overall, the risk analyst is the front line that should point out any possible security threat they can think of that could happen to a system.

A cyber security risk analyst should be more than capable of including human factors into their risk management. The analysts must be able to go further than their own thinking when it comes to these risks. They should be able to think like a simple everyday user as well as like a cybercriminal. This means that they must understand the social science behind cybersecurity. The analyst should think of the possibility of a worker that travels to malicious websites and base their assessment off that possibility. They cannot only rely on knowing what they would do or would not do on a network. According to Telefonica Tech, "Human error is the leading cause of cybersecurity breaches. In 2021, found to be responsible for 95% of these breaches according to the 'IBM Cyber Security Intelligence Index Report'. This means that, if the human factors were mitigated, only 1 out of 20 security breaches would take place." (Telefonica Tech). With human error being such a big risk factor for cybersecurity, understanding the everyday user becomes a vital to a secure network. This understanding helps to build proper policies and training for the organization. With proper training even the everyday user could be the one who protects against a breach because of their proper use of security practices.

Understanding a person's mindset while operating on a computer might help in predicting certain risks as well. According to Moustafa, "Non-compliance with a security policy can go beyond mere ignoring warnings, choosing poor passwords or failing to adopt recommended security measures." (Moustafa, et al.). They go on to say that the real motive behind it is possible psychological factors such as narcissism. Understanding this would allow the analyst to plan for it as a possibility of a security threat. The analyst must sometimes look at why a person does something to try and figure out the way they may attack a system. Sometimes understanding the motive behind a cyber-attack could even lead a risk analyst to what they are after on a network and could better understand how to protect the data. For example, if their motive is money, they may go after data that is valuable and can be held for ransom. This information could help an analyst to choose better encryption for such data to better protect it. On top of understanding the perpetrator, understanding the victim is important as well. This is where victimization can help with risk assessment as well. If the analyst understands the idea of how an individual increases their chances of becoming a victim through their online activities, they may be able to protect against users that partake in such online behaviors. They could train the users on how to not victimize themselves further online as it could potential be a risk for the company as well.

Cyber security is a necessity that is never going to disappear unless all the technology in the world was wiped out. Thanks to this societal need, a career like cyber security risk analyst exists. This career is not only needed by organizations that use technology but by those individuals who use the technology that is run by these organizations. The analysts exist to help protect organization’s data which can include normal user’s data that may be customers of the company. This career not only focuses on technical understanding but also social understanding that helps them fight against cyber risks and properly train personnel. Cyber security risk analysts benefit billions worldwide by securing networks everywhere.

Works Cited

Matzelle, Emily. *Your Next Move: Cyber Risk Analyst*. 20 September 2023. Accessed 29 November 20023. https://www.comptia.org/blog/your-next-move-cyber-risk-analyst#:~:text=The%20cyber%20risk%20analyst%20role,in%20a%20computer%2Drelated%20field.

Moustafa, Ahmed A. et al. *The Role of User Behaviour in Improving Cyber Security Management.* 18 June 2021. Accessed 01 December 2023. https://www.frontiersin.org/articles/10.3389/fpsyg.2021.561011/full

Telefonica Tech. *Human Factors in Cybersecurity: Protect Yourself.* 10 November 2022. Accessed 01 December 2023. https://telefonicatech.com/en/blog/human-factors-in-cybersecurity.