Brandon Wichern

April 6, 2024

Cybersecurity Consultant

Strategic Experts Advising Budget, Training, and Assessments

Prevent. Detect. Respond.

According to Forbes Advisor, consultant roles focus on prevention, detection, and response strategies to defend an organization's networks from unauthorized access (Uche, 2024).

Human error plays a critical role in security breaches. Prevention requires an understanding of how psychological factors impact individuals' interpretation and adherence to security policies. How to educate teams and positively influence safe cyber decision making behaviors requires consideration of differences in culture, language barriers, and what, if any, impact solutions have on users with disabilities

Personnel at all levels play a role in the organizational cybersecurity culture. Identifying vulnerabilities requires an understanding of both hardware and software systems, along with the staff that operates them. Human factors programs require alignment of all of these elements in effort to detect cyber threats.

Ultimately, cyberattacks are inevitable. Those most vulnerable have less financial and legal resources to respond and recover after incidents. Response plans for different scenarios are required for effective communication, damage control, and risk mitigation The National Institute of Standards and Technology (NIST) maintains the “Incident Response Recommendations and Considerations for Cybersecurity Risk Management” as a baseline for cybersecurity framework to provide organizations with guidance (Cichonski, Millar, Grance, Scarfone, 2012).

Sounds NICE, Tell Me More.

Cybersecurity consultants require a working knowledge of a variety of social engineering techniques such as phishing and tailgating, as well as circumstances in which clients could be vulnerable to these kinds of attacks.

They work to enforce good cyber hygiene standards and additional concepts addressed by the Global Commission on the Stability of Cyberspace's CyberStability Page Series (Global Commission on the Stability of Cyberspace, 2019).

Field Engineer's (FE) description is in line with the social behaviors expected of cybersecurity professionals. Communicating test findings to different audiences across a range of technical backgrounds, staying updated on the latest information to keep systems secure, and building cohesive security teams to maximize effectiveness (Field Engineer, 2024).

Cyberseek refers to the applicable NICE (National Initiative for Cybersecurity Education) cybersecurity workforce framework categories, as well as supplementary knowledge, skills, and abilities. Consultant is listed as a mid-level role with identity and access management (IAM), computer science, and project management as the top job skills requested for positions (Cyberseek, 2024).

Doing It Right.

The intricate balance between security and privacy is a complex issue for cybersecurity consultants. Both facets are important for different reasons. Different organizations will consider this challenge in a unique way as well. Determining how to best manage the fact that more users share an increasing amount of information across a larger number of connected devices and networks is required to calibrate the equilibrium between convenience and security.

The legal and ethical landscapes involving general data protections and health information evolve over time. Consultants must exercise their abilities to monitor, advise on, and implement current regulatory and social compliance. Maintaining trust and transparency regarding these issues is essential to a cybersecurity consultant’s reputation and the affected relationships between employee and employer.

Conclusion

Cybersecurity consultant is an excellent career for those with the appropriate social and technological aptitude and skills. Incident prevention through education, weakness identification, and regulation compliance are a few of their goals. They are responsible for safeguarding organizations through detection and remediation of security threats by managing audit teams and incident response policies. Good consulting provides recommendations for a safe and working configuration between personnel, networks, and telecommunication systems that is built for accessibility to better ensure acceptance by and ease of use for all members of the organization (Rao & Golden, 2019).

References

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (August 2012). *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology.* NIST Special Publication (SP) 800-61 Revision 2. https://csrc.nist.gov/pubs/sp/800/61/r2/final

Cyberseek (2024). *CYBERSECURITY CAREER PATHWAY.* https://www.cyberseek.org/pathway.html

Field Engineer (2024). *Cyber Security Consultant.* https://www.fieldengineer.com/skills/cyber-security-consultant

Global Commission on the Stability of Cyberspace (November 2019). *Advanced Cyberstability.* https://cyberstability.org/report.html

Rao, Gautam & Golden, Lori (18 November 2019). *How inclusive design uplifts equity: foundational to transformational.* EY (Ernst & Young). https://www.ey.com/en_gl/about-us/diversity-equity-inclusiveness/how-inclusive-design-uplifts-equity-foundational-to-transformational

Uche, Nneoma (January 2024). *How To Become A Cybersecurity Consultant: Salary, Education And Career Outlook.* Forbes Advisor. https://www.forbes.com/advisor/education/it-and-tech/become-a-cybersecurity-consultant/