Tammy Rizo

October 11, 2026

Cybersecurity Curriculum Development: The Need for Awareness

Introduction

Cybersecurity is an interdisciplinary field that requires more than technical knowledge. According to the National Institute of Standards and Technology (NIST, n.d.), Cybersecurity Curriculum Development professionals develop, coordinate, and evaluate cybersecurity education and training. Understanding human behavior and society is essential in this career because social science research helps professionals develop effective training programs.

Social Science Research and Principles

Cybersecurity Curriculum Development professionals must understand why people make the choices they do. Psychological, sociological, and workplace influences all play a role in these decisions. Research helps these professionals in two ways. First, existing social science research teaches them about human factors, cognitive biases, and social influences. Singh (2025) shows how emotions influence our cybersecurity decisions. Cybercriminals exploit these emotions through social engineering. Another thing they consider is cognitive bias, such as overconfidence and affect bias, which can also cause people to overlook threats (Singh, 2025). Curriculum developers apply these concepts when creating training materials that teach people to recognize manipulation and take steps to protect themselves and their data.

Secondly, research helps developers identify weaknesses and improve training. Curriculum developers may use surveys, interviews, observations, and assessments to help evaluate their programs. Prümmer et al. (2024) found that many cybersecurity training studies measured knowledge or intentions rather than actual behavior.

Cybersecurity and Marginalized Groups

Examination and support for marginalized groups are vital in cybersecurity awareness and education. In a study, Aly et al. (2025) found that younger adults preferred video instruction and older adults preferred text-based materials. Digital literacy and resource limitations in rural communities were also looked at in this study. The challenges these groups face can increase cybersecurity risks for individuals and their communities. Limited digital literacy, fewer educational resources, and training availability are things that need to be considered when educating communities. Curriculum developers can help address these challenges through accessible materials, varied learning formats, and instruction tailored to different experience levels.

Cybersecurity and Society

Cybersecurity Curriculum Development professionals are influenced by society and influence it as well. As technology changes, professionals must adapt training to new threats and the ways people use technology. For example, remote work creates a need for education about home networks and protecting organizational information. In return, effective training can influence people's behavior and help protect individuals and organizations. Research helps professionals determine whether these changes actually improve security practices (Prümmer et al., 2024).

Conclusion

Cybersecurity Curriculum Development professionals help improve cybersecurity practices and protect society by considering influences and challenges that extend beyond technology. This career depends on social science research to understand human behavior, address different learning needs, and evaluate training effectiveness.

References

Aly, H., Liu, Y., Khan, S., Anaraky, R. G., Byrne, K., & Knijnenburg, B. (2025). Digital privacy education: Customized interventions for U.S. older and younger adults in rural and urban settings. *Technology in Society, 81*, Article 102805. https://doi.org/10.1016/j.techsoc.2024.102805

National Institute of Standards and Technology. (n.d.). *NICE framework work role videos*. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-work-role-videos

Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security, 136*, Article 103585. https://doi.org/10.1016/j.cose.2023.103585

Singh, T. (2025). *Cybersecurity, psychology and people hacking*. Palgrave Macmillan. https://doi.org/10.1007/978-3-031-85994-6