Module 1 Discussion Topic: Computer Security vs. Information Security

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 300 – Introduction to Cybersecurity, Professor Dr. Joseph Kovacic

August 29, 2025

Instructions:

What is the defining difference between computer security and information security? Why can we argue that information security is really an application of social science?

Computer Security vs. Information Security

What is Information Security:

It is a broad term used to describe the active protection of data and information (both digital and physical) by using a wide range of tools, including hardware and software applications, to prevent unauthorized access, modification, disruption, disclosure, and destruction (Kim & Solomon, 2021).

What is Computer Security:

Also known as 'Cybersecurity' or 'Information Systems Security,' Computer Security is a subfield of information security that focuses on protecting the systems (e.g., digital systems, computers, servers, network devices) that hold and process critical data from cyber threats.

Both Information and Computer Security follow the CIA Triad using similar security measures. Security controls categories include Technical, Managerial, Operational, and Physical. Security control types include Preventive, Deterrent, Detective, Corrective, Compensating, and Directive. Both Information and Computer Security follow the CIA Triad, but in their own unique ways. In other words, Computer Security focuses on protecting technology itself, while Information Security focuses on protecting the information itself.

Why can we argue that information security is really an application of social science?

Information security is an application of social science because a significant portion of its practice involves managing human behavior. While it has a strong technical component, the most critical vulnerabilities are often related to people (Verizon Business, 2024; Sophos, 2025). Social

science fields, such as sociology, psychology, and organizational behavior, are essential for understanding why people make security mistakes, creating effective security policies, and educating users to reduce risk (Nobles, 2018 As seen with the 2017 WannaCry attack and other prolific ransomware attacks on tens of thousands of computer users over the past decade, cybersecurity professionals agree that the human factor is the "weakest link" in security, requiring a better understanding of social dynamics, ethics, and human psychology to be adequately addressed (Kaspersky, 2020; Kumar et al., 2020; KL, 2025). Therefore, understanding the human factor and implementing information security is really an application of social science at its core.

References

Kaspersky. (n.d.). (2020, April 20). *Ransomware WannaCry: All you need to know*. Kaspersky. Retrieved July 19, 2025, from https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

Kim, D., & Solomon, M. G. (2021). Fundamentals of information systems security (4th ed.). Jones & Bartlett Learning.

Kumar, R., Ben-Othman, J., & Srinivasagan, K. G. (2020). *An investigation on WannaCry ransomware and its detection*. Electronics, 9(8), 1312. https://ieeexplore.ieee.org/document/8538354

Nobles, C. (2018). *Botching human factors in cybersecurity in business organizations*. HOLISTICA, 9(3), 71–88. https://www.researchgate.net/publication/329806166_Botching_Human_Factors_in_Cybersecurity_in_Business_Organizations

Sophos. (2025, June). *The state of ransomware 2025* [White paper]. Sophos. Retrieved August 29, 2025, from https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2025.pdf

Verizon Business. (2024, June). *2024 Data Breach Investigations Report*. Retrieved August 29, 2025, from https://www.verizon.com/business/resources/reports/dbir/#top-takeaways