Cybersecurity Professional Career Paper: Information System Security Engineer

Student Name: Mario Martinez

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 11/16/2025

Introduction

The field of cybersecurity is the unique confluence of the technical and the social, building secure systems and methods that involve interactions between systems and humans. There is no methodology by which you need only consider the security needs of one side; you could for example invest in a million dollar security suite, but it may not matter if key personnel with access to the system are themselves sloppy or compromised. There is perhaps no better example of the dual-disciplinary nature of the field than that of the Information System Security Engineer (known by most simply as an ISSE). They are technical professionals responsible for designing digital and physical security mechanisms and measures for information systems, which requires both technical skill and insight into human behavior in relation to the design.

Social Science Principles in the Role of an ISSE

The primary function of an ISSE is to design security mechanisms and processes for systems. All of these mechanisms and processes, whether highly technical in nature or simple best practices and policies, are designed by them with social science principles in mind to counter or encourage certain human behaviors. Perhaps the most central principle for an ISSE to consider is Determinism, which argues that behavior is influenced by preceding events. In the paper *The Role of Human Factors Engineering in Cybersecurity (Bhaskar 2023),* it's stated that "Fifty-two percent of organizations surveyed…said employees were their greatest weakness in IT security, with their actions putting business and organizational information security strategies at risk." This is where the ISSE has to consider Determinism; i.e. why were the employees the weak point, what caused them to practice poor cyber hygiene or to disregard company policies and procedures that would've safeguarded the system? The ISSE is ultimately designing their

system security with questions like these in mind, because one of their primary duties is to consider how to best defeat (or sometimes leverage) the human factor.

ISSE Application of Cybersecurity Concepts

In their quest to design cybersecurity systems that consider the human factor, ISSEs employ and apply knowledge of a multitude of cybersecurity concepts. Primarily, it is important for them to know and understand potential threat vectors such as Social Engineering and Malware attacks. Social Engineering very much relates back to the human behavioral anticipation mentioned previously, while Malware would be the more strictly technical side of the problem. To counter social engineering, an ISSE might recommend things like compartmentalizing access of employees to different parts of the system to limit exposure if one employee's credentials were stolen or compromised. Malware on the other hand, would require an ISSE to recommend and design constant anti-virus and vulnerability assessments into the build process of the system; they might recommend evaluation against specific 'security-hardening' frameworks such as DISA STIGS or CIS Benchmarks.

Additionally, ISSE's are responsible for integrating common cybersecurity frameworks into concepts such as Human Computer Interaction (HCI) and Human Centered Design (HCD). These are great developmental frameworks that do have some level of thought toward security, however they often fail to incorporate industry standard models such as NIST, STIGS, or CIS which are designed to counter specific threats.In the article *Towards an integrative approach for designing for cybersecurity in systems engineering (Toh 2025)*, it's called out that ISSE's often have to advocate for tools such as MFA which the design frameworks like HCI and HCD would consider 'unhelpful for users' but are vital security tools explicitly called for by frameworks like CIS. The ISSE is most often the advocate for these higher level security tactics.

Marginalized Groups and Society

While the foremost concern of an ISSE is the security of a system, it's also true they have to take into consideration certain marginalized groups in the construction of their policies and systems. For example, in the article *Effects of socioeconomic and digital inequalities on cybersecurity in a developing country (Khan 2023)*, it is pointed out that for certain socioeconomic groups security tools such as mobile authenticators or text-message verification may be unreasonable due to a lack of reliable access to mobile devices. Unfortunately, this also creates a secondary problem in that those same users may be more exposed to victimization by bad actors due to a more lax security posture. The challenge of an ISSE here would be to strike a balance between system security and the ability of users to access that security, and its likely that alternative methods and schemes would need to be devised. Finally, due to their lack of general access these groups are unlikely to have the same level of cyber literacy, so alternative more-comprehensive trainings could be called for to focus on areas of what is considered 'common cyber knowledge' for other users.

How ISSE's Function in Society Today

ISSE's today are a fundamental and critical part of the security components of most companies, governments, and organizations today as they are essentially the architects of the cybersecurity scheme of the systems under their purview. In the government for example, an ISSE might be charged with designing the cybersecurity scheme of an application that works with taxpayer financial data; this data is critically sensitive and a breach could have negative financial side effects on millions of people. As another example, an ISSE working for a healthcare provider might be responsible for the security of a database storing patient health data. Not only is this critical data, but it is subject to specialty medical regulations such as HIPPA and

thus has special security requirements of its own that must be factored in as part of the design. HIPPA Laws for example, mandates the use of certain encryption standards known as FIPS for internal and external transit of data, and so an ISSE would need to design their system to that specification.

Conclusion

ISSE's are the central key to the failure or success of cybersecurity systems in the organization in which they reside; the applications and systems they serve are only as secure or insecure as they design them to be. They are primarily designers, and it is their role to balance technical requirements, company and governmental regulation, and the behavioral tendencies of the humans that interact with their systems. It is as much a role about understanding and anticipation people as it is a technical one, and an imbalance of any factor might inadvertently introduce vulnerabilities into a system that appears secure

References

1. Bhaskar, R. (2023, August 23). *The role of human factors engineering in cybersecurity*. *ISACA Journal, 2023*(4). ISACA. https://www.isaca.org/resources/isaca-journal/issues/2023/volume-4/the-role-of-human-factors-engineering-in-cybersecurity
2. Harris, M. A., Hale, M. L., & Toh, C. A. (2025). Towards an integrative approach for designing for cybersecurity in systems engineering. *Proceedings of the Design Society*, *1*(1), 1–12. Cambridge University Press. https://www.cambridge.org/core/journals/proceedings-of-the-design-society/article/towards-an-integrative-approach-for-designing-for-cybersecurity-in-systems-engineering/55462ABBA7EDC2A08B49130EA670DB1E
3. Khan, N. F., Ikram, N., & Saleem, S. (2023). Effects of socioeconomic and digital inequalities on cybersecurity in a developing country. *Security Journal*. Advance online publication. https://doi.org/10.1057/s41284-023-00375-4