The Human Factor in Cybersecurity

Lauren S. Ferro
lsferro@diag.uniroma1.it
Sapeinza University of Rome
Rome, Italy

ABSTRACT

Cybersecurity strategies could be greatly improved by identifying *when* errors are more likely to occur, therefore being able to anticipate, mitigate, and resolve issues more efficiently. At their core, most cybersecurity issues all have one thing in common - the human user. As a result, an emerging and important area of considerations is the study of Human Factors. This paper presents an initial review that situates Human Factors within the context of cybersecurity.

CCS CONCEPTS

• **Security and privacy → Systems security**; **Human and societal aspects of security and privacy**; • **Human-centered computing**;

KEYWORDS

human factors, cybersecurity

1 INTRODUCTION

The ubiquity of internet access has provided us with the opportunity to exist in both physical and digital spaces in parallel - meaning that we are always connected. As a result it is easy to forget that the responsibility of our online security begins and end with us. However, there are several factors that impact our abilities to protect ourselves from threats and ultimately, maintain the integrity of data. One area that encapsulates such considerations is Human Factors. Until recently, it has not been an area automatically associated with improving the cybersecurity awareness of users. But given its potential, this paper presents a more concentrated approach to considering it within the context of cybersecurity and not their original context - aviation maintenance.

1.1 Human Factors in Cybersecurity

A main issue of human factors within cybersecurity is the current state that it is actively used within cybersecurity. Moreover, of the research that does exist, its scope is often limited [4] or ambiguous and varied, or only acknowledges the concept of human factors in passing [3].

Cybersecurity encompasses both the practice of safe online behaviour (e.g. scanning downloaded files) and the use of tools and resources to achieve it (e.g. anti virus, firewalls). Therefore, at its core, all behaviour related to addressing or causing cybersecurity issues require some level of human input. For example, it is possible that a user's awareness of phishing scams and their impact can vary based on a variety of things such as not knowing what a phishing scam is or not scanning files before opening them. To illustrate this, this paper presents an adapted contextual approach to the "Dirty Dozen" [1], which considers the list of 12 human factors within the context of cybersecurity. The Dirty Dozen consists of the following: Lack of Communication, Complacency, Lack of Knowledge, Distraction, Lack of Teamwork, Fatigue, Lack of Resources, Pressure, Lack of Assertiveness, Stress, Lack of Awareness, and Norms. Within the context of cybersecurity, it is easy to describe situations where any of the 12 Human Factors play a part. For example, a *Lack of Knowledge* can result in an employee revealing sensitive information to a scammer. *A Lack of Teamwork* could compromise a system where each person plays a particular role, therefore resulting in additional *Stress and Pressure*, which results in additional errors.

1.2 Conclusion

Lastly, research within this area also presents a prime opportunity within the field of threat modelling, as suggested by [2], which could help to identify precursors for behaviour that will compromise the security of data. For example, if we can identify stress, workplace norms, lack of knowledge, and so on, we can then use this information to implement strategies to reduce them, and predict the likelihood of when human factors may impact a systems security. As a result, future work needs to aim towards refining and developing the relationship along with the considerations for anticipating, mitigating, and resolving issues related to human factors.

2 CITATIONS AND BIBLIOGRAPHIES

REFERENCES

[1] Gordon Dupont. 1997. The dirty dozen errors in maintenance. In *The 11th Symposium on Human Factors in Maintenance and Inspection: Human Error in Aviation Maintenance.*

[2] Adam Shostack. 2014. *Threat Modeling: Designing for Security.* John Wiley Sons. Google-Books-ID: YiHcAgAAQBAJ.

[3] Alex Vieane, Gregory Funke, Robert Gutzwiller, Vincent Mancuso, Ben Sawyer, and Christopher Wickens. 2016. Addressing human factors gaps in cyber defense. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 60. SAGE Publications Sage CA: Los Angeles, CA, 770–773.

[4] Heather Young, Tony van Vliet, Josine van de Ven, Steven Jol, and Carlijn Broekman. 2017. Understanding Human Factors in Cyber Security as a Dynamic System. In *International Conference on Applied Human Factors and Ergonomics.* Springer, 244–254.

womENcourage '19, September 16–18, 2019, Rome, Italy
2019. ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn