CYSE 201S

Cybersecurity Professional Career Paper

Student Name: Fallon Sullivan

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: **Diwakar Yalpi**

Date: 14APR26

INTRODUCTION

The job is more or less in the name when it comes to Cyber Risk Analysts. Risk analysis with a focus on cyber security to identify weaknesses and recommend responses to them. As the world becomes more and more digitized, the need for cyber security becomes more intertwined with previously unrelated fields. This paper will inform the reader of how cyber risk analysts utilize social science principles, theories, and implement strategies related to risk management to safeguard information.

Relation/Connection to Social Science Principles

The core principles which stand out the most in relation to Cyber risk management would be objectivity, and parsimony. There are of course other principles at play within the context of cybersecurity: ethical neutrality, for when it comes to researching new methods of defense, and relativism for explaining behaviors and gaining more understanding into why cyber events occur, and how cyber offenders think and behave.

Parsimony is particularly important in this context, because as a cyber risk analyst, your job is not limited to identifying and informing, but explaining and convincing. If the analyst can't accurately and succinctly convey their findings or

suggestions to the individuals who have to make decisions and take action, then they may fail in their job even if they've done everything else correctly. The concept of science educators comes to mind here: People such as Neil DeGrasse Tyson, Bill Nye, Carl Sagan, Milo Rossi, and Kyle Hill - a group of individuals whose job it is to bring science to the masses in a more digestible manner.

In the same way Carl Sagan brought astrophysics to entertainment, or Bill Nye brought chemistry to classrooms, we must employ the principle of parsimony to educate the average user on cyber security practices, and convince those higher up in the company chain to spend money on training, hardware, or software to achieve cyber security goals.

Application of Key Concepts

One of the most impactful key concepts I have learned throughout this course relates to the "Weakest Link" theory. The concept I speak of is the "Human Firewall". No matter how advanced your hardware, or robust your software, the most likely point of entry for an attacker is almost always going to be through human error. Whether it be a bad actor within the organization, or a bad link clicked out of mistaken belief of authenticity, it is found time and time again that the weakest point in a secure system is the lack of vigilance from a human.

Keeping this concept in mind, professionals in the field of cyber risk management, employ many types of cyber security education sessions, or employee training regimens to remind and update the average user's knowledge

base. Through education and repetition, a stronger cyber security stance can be achieved through an informed workforce. In the same way that a nation of highly educated individuals is bad for authoritarian regimes, highly educated end-users are bad for cyber criminals as they are harder targets to manipulate and crack.

Marginalization

It is no surprise that marginalized communities are at higher risk for hacking. As information technology becomes more and more pervasive in everyday tasks, it acts as either a barrier to entry, or a new vector for threats when it comes to those individuals to whom the technology is unfamiliar. Underfunded schools, hospitals, or infrastructure institutions in countries with lower budgets who are still required to keep up with modern practices and technologies in their fields, but who lack the proper education and funding to properly secure their systems from intrusion.

CISA (Cybersecurity and Infrastructure Security Agency) has programs to aid marginalized communities combat the challenges they face when it comes to cybersecurity. Some of these resources include no-, or low-cost applications and services, digital literacy courses to educate and inform, inclusivity bills such as Diverse Cybersecurity Workforce Bill[(2)].

Connection to Society

You can find cyber risk analysts among all levels of society these days. From health care institutions to banks, from public transport to Amazon. The areas in

our society that don't include some form of cyber security are shrinking by the year, and that is a trend that I do not foresee stalling any time soon. In fact, evidence points to the contrary: That as LLMs and technology continue their inexorable march forward, we will only become more and more intertwined in society.

Organizations such as NIST, GSA, and the previously mentioned CISA are constantly updating framework, implementing new policy for best practices at private and government levels, and ensuring critical infrastructure remains secure from threats.

Scholarly Journal Articles

Source 1: The journal provides a particularly clear indication of the importance of social sciences in relation to the field of Cybersecurity. This includes the career field of cyber risk management, and further reinforces the concept of the Human Firewall.

Source 2: The workforce bill from 2024 clearly promotes inclusivity and outreach for marginalized communities. That is the intended goal of the bill, and CISA has many other examples of such policies and programs with the intent of aiding marginalized communities when it comes to Cyber security.

Source 3: The article goes into the behavioral implications and psychological disconnect the cyber security community seems to have. It further provides the

idea that 'risk as potential threats'[3] logic may act as a bridge between conventional risk management, and cyber risk management.

REFERENCES

(1) Domalewska, D., Gasztold, A. & Arcos, R. (2025). Mapping the Role of Social Sciences in Cybersecurity Research. *Political Science Studies*, *77* https://www.studiapolitologiczne.pl/Mapping-the-Role-of-Social-Sciences-nin-Cybersecurity-Research,211103,0,2.html

(2) Ribeiro, Anna, New Diverse Cybersecurity Workforce bill to promote inclusivity, provide CISA with millions for outreach, Industrial Cyber, May 24,

2024

https://industrialcyber.co/training-development/new-diverse-cybersecurity-workforce-bill-to-promote-inclusivity-in-cybersecurity-provide-cisa-with-millions-for-outreach/

(3) Sarah Backman, Tim Stevens, Cyber risk logics and their implications for cybersecurity, *International Affairs*, Volume 100, Issue 6, November 2024, Pages 2441–2460, https://doi.org/10.1093/ia/iiae236