Brandon Creech

Professor Kirkpatrick

CYSE 200T

19 April 2023

Cybercrime, Bad Ethics, and Our War Against Them

Introduction

(1) Advancements in cyber technology have allowed companies to be able to use unethical practices that have resulted in workplace deviance. The more creative functions developed within cyber technology have allowed more opportunities for it. One opportunity would be how companies use computers with algorithms to unethically compete against humans in the open market. It's unfair competition as computers are quicker to action that a normal human would be and allows for easier workload. Another example is how an employee within a company can hack into the servers or DDOS it to take vital information. Throughout the time of an employee working at a company, they can gain more knowledge into the weak points and how to penetrate the defenses of a company. They might use their own knowledge deviously against the company for their own personal gain. Cyberbullying is another great example as it still continues to be a major issue in the online world, in which people in the same workplace who might have a disliking for each other can turn to the internet to threaten and bully them through messages and attacks such as DDOSs. Companies will continue to find more ways to inappropriately use cyber technology as it is constantly developing.

(2) Approaching the development of cyber-policy and infrastructure based on short arm predictive knowledge, **the advancement of technology has introduced a society of actions where consequences and objects can no longer be supported by ethics.** Ethics like justice, charity, and honesty are being overshadowed by a world of ineffective doer, deed, and effect. As a result, ethics bring about a new responsibility that changes the development of cyber-policy. Predictive knowledge is now falling behind technical knowledge and the recognition of ignorance needs to be part of what governs self-policing. As far as infrastructures, natural intelligence in humans is being consumed by artificial intelligence. Humans have to be able to adapt to this new sense of technological development where the works of man are felt less. We must understand that too much cumulation of technology in the form of artificial intelligence can affect how we learn and our experience towards creating infrastructure. Because of this, more natural intelligence by man needs to be developed because it is the foothold of how technological advancement has existed. (Jonas 38-39)

Importance of Training

(4) In order to battle unethical practices and cybercrime, training is important for employees because it teaches the vital defensive measures to protecting valued data and keeping the company's infrastructure secure. Employees' themselves serve as a defense against crucial infrastructure in which they are expected to be able to execute actions that quarantine the imminent threat online. They are expected to learn case-by-case scenarios in which they are to act quickly without hesitation through which training teaches them. They are also supposed to monitor the company network for malicious activity if the technology itself isn't able to detect it (Rijmenam 2022). This is why training is important because it helps employees gain insight into hackers because they have to be able to keep up with the knowledge them.

Importance of Improving Cybersecurity Technology

(5) In addition to educating employees through training, **improving the technology within the company plays an important role in cyber defense because it is the first line of defense that detects against malicious activity before the employee.** Improving technology involves ensuring all security systems have up-to-date hardware and software that will mitigate the chance of a cyberattack from happening. If a cyberattack does happen, having an up-to-date security system will be able to respond quicker to the threat and quarantine it. AI is also becoming a more growing trend in society so it could become incorporated into security systems to do the tasks of both technology and employees (Rijmenam 2022).

(7) Next, **algorithms and tasks can be incorporated into the technology so it can match the skills of the employees and the training they receive.** A CISO's landscape is constantly evolving with advancements in technology that I have to be able to match the sophisticated efforts of cyber criminals (Hay 2023). Giving Take AI for example, it is becoming so advanced that it could be the main driving line of companies, not employees. AI the knowledge of employees and their training balances out the tradeoff of having lesser funds in training the employees. Now before incorporating AI into being part of the defense system, I would test its mechanisms through means of monitoring or activity from white hats. This is how I could see the weaknesses the AI present and how I can actively improve on it before it's implemented. AI still isn't perfect so employees will still be able to play a contribution in protecting infrastructure against cyber threats until it has mitigated its issues. It's a foreseeable future that in some minds might be unnerving, but in others it's the realistic way of life for companies who seek to perform at a higher level with more profits.

Allocating Funds as a CISO (Chief Information Security Officer)

(6) Considering the factors in the importance of training and cybersecurity technology to protecting the company and its infrastructure, **being a CISO involves making the tough decision on what areas of infrastructure security should be prioritized in optimizing against a limited budget.** Whether that be physically through educating employees or cyber through improving the technology, allocating funds becomes a challenge against the ultimate objective of preventing cyberattacks.

(3) Because of this, **both training and additional cybersecurity technology are vital components to making a secure defense system against cybercrime.** Training helps educate employees on being more aware of malicious activity and helps them understand how to act in certain scenarios. Improving and adding cybersecurity technology is also important because having up-to-date hardware and software helps the security system as a whole to respond quicker to incoming threats. With advancements in technology, AI is also an option to be able to incorporate into company infrastructures. Becoming CISO carries a big responsibility of monitoring over all operations with managing a budget that crucially adheres to the company's framework. Everyone, including the CISO, ultimately share the same objective which is to protect their company's important data.

In conclusion, technology has introduced a world filled with cybercrime and bad ethics that is ever increasing. Cybercrime and unethical practices are becoming more dangerous, especially cybercrime where crimes like DDOSes and cyberbullying. Although proper training and improving cybersecurity technology is effective against these issues, companies are capable of developing other ways to fight it. These other tactics might be more budget-friendly or easier to implement for the companies involved. However, because cybercrime and unethical practices remain a significant issue in companies, perhaps in the future we can answer these important questions of if we will ever have a safe online and social world.

References

Dr Mark van Rijmenam, C. S. P. (2022, August 25). *How Cybersecurity is Changing Technology Today*. Dr Mark van Rijmenam, CSP | Strategic Futurist Speaker. Retrieved March 31, 2023, from https://www.thedigitalspeaker.com/cybersecurity-changing-technology/

Hay, A. (2023, January 5). *The Evolving Role of the CISO in 2023*. Forbes. Retrieved March 31, 2023, from https://www.forbes.com/sites/andrewhayeurope/2023/01/04/the-evolving-role-of-the-ciso-in-2023/?sh=13123c76663f

Jonas, H. (1973). Technology and Responsibility: Reflections on the New Tasks of Ethics. *Social Research*, *40*(1), 31–54. http://www.jstor.org/stable/40970125