The Implications of Cyber Technology and an Approach to Cyber-policy and Infrastructure

Introduction

(1) It is evident cyber technology has rapidly advanced and is now integrated in all aspects of our lives. It is safe to say advancements and developments in cyber technology will continue in the future. Although cyber technology has greatly helped society, it also poses new risks and issues to all individuals. Hans Jonas in "Technology and Responsibility: Reflections on the New Tasks of Ethics", brings forth the issue that there is a "short arm" in predictive knowledge regarding cyber technology and its long-term impact on society. There are a myriad of possibilities regarding the future and impact of cyber technology thus, the future is unpredictable. With that "short arm" of predictive knowledge, how can we approach developing cyber-policy and infrastructure? In my point of view, the best approach to developing cyber-policy and infrastructure is one that has adaptability, flexibility, and the best interest of society in mind. Policy and infrastructure must be adaptable and flexible to time and situations as well as keeping future implications in mind. Cyber technology is a tool meant to make our lives easier. By having the best interest of society in mind when developing cyber policy and infrastructure negative implications can be prevented.

An Approach to Developing Cyber-policy and Infrastructure

Given the "short arm" of predictive knowledge when developing cyber-policy and infrastructure we must keep the future in mind. Cyber-policy and infrastructure must be developed to be broad enough that it can almost be considered universal without losing its purpose. A balance between broadness and purpose must be achieved in order for the cyber-policy or infrastructure to become universal.

Cyber technology has become widespread and prevalent not just in our daily lives but also in our occupations. Cyber technology has become prevalent in almost every field of occupation. Cyber-policies and infrastructures must be able to accommodate and address the various fields and uses of cyber technology. The development of cyber-policy and infrastructure must be a collaborative project in order to attain that universality. The opinions and suggestions of experts from various fields should be taken into consideration in the development of cyber-policy and infrastructure.

Due to the unpredictability of the future, it is important that policies and infrastructures can be changed as new situations arise. Policies and infrastructures must be developed to be able to include additions in the future that will accommodate any changes in the cyber technology landscape. For example, the simplest way to accommodate any changes is to create a policy that allows for developing addendums to the policy based on certain rules and constraints.

Given the rapid advancements of technology, policies and infrastructures can quickly become outdated and deemed useless if it has not been updated to match present times. Changes and updates to policy and infrastructure cannot be made without a team dedicated to that specific purpose. The creation of a team dedicated to the constant and consistent review and update of policies and infrastructures is necessary. The team must also research and study changes in the cyber technology world and develop appropriate changes according to the current times.

In order to account for the "short arm" of predictive knowledge and the unpredictability of the future when developing cyber-policy and infrastructure it must always have these three characteristics of being adaptable, universal, and constantly improving. Cyber-policy and infrastructure must be able to change through time and given any situation. Although thinking about the possibilities of the future is a good approach, we must also not forget to address the implications of cyber technology that we've already witnessed. Issues within our control must be resolved first prior to thinking of future implications.

The Implications of Cyber Technology

(7) Although developing cyber-policy and infrastructure to be able to handle future implications is important, it is as important or even more so to solve the current issues today. There are many implications we've already witnessed due to cyber technology such as the blurring of lines between reality and fiction with the use of artificial intelligence to the increasing need to protect personal information. The workplace is one aspect of our lives that has been impacted by the emergence of cyber technology. This impact is one that we have witnessed and must resolve first prior to thinking about the future. The emergence of cyber technology in the workplace has created opportunities for workplace deviance by providing another form for employees to harm both each other and the company.

With the use of technology, workers have another method to partake in workplace bullying and harassment as well as providing anonymity to its perpetrators. Employees have the potential to be subjected to cyberbullying and harassment through cyber technology. While this behavior is not new to the workplace, cyber technology allows another way for this to occur rather than the typical workplace bullying and harassment that is done face to face. Additionally, cyber technology has made it easier for disgruntled employees and ex-employees to gather corporate information and reveal it as an anonymous source. If a company does not have strict data protocols it is easy for disgruntled and dissatisfied employees to transfer that data using devices such as hard drives. The increase in reliance of cyber technology also allows the opportunity for employees to introduce malware, viruses and other cyber threats into the system thus, affecting the entire workplace. In almost every workplace, every employee has access to the organization's systems via their private workplace computer, an application on their phone, a personal computer with access to the company, or a computer accessed by everyone in the company that only requires a code. There are more places now that an employee can insert malicious code into. Without proper authentication and authorization protocols, a company may not be able to determine the identity of a perpetrator. Workplace deviance also includes the possibility of employees not completing their work and using their work devices for other means. An employee may slack off and decide to watch videos or play games using their workplace computer. Cyber technology is heavily relied on and more prevalent in the workplace now. Companies must have proper systems in place in order to prevent harm between employees and between employees and the company.

Issues such as workplace deviance is an example of the impact of rapid advancement of cyber technology that we have already witnessed. Workplace deviance is an issue that can hinder society and must be resolved when developing cyber-policy and infrastructure. The rise of workplace deviance due to cyber technology can be considered unprecedented. This is an example of an issue that newly developed cyber-policy and infrastructure must address but also what current cyber-policy and infrastructure must adapt to. Policies and infrastructures must be

able to change to account for these types of situations. Given workplace deviance can occur in various fields of occupation, developing cyber-policy and infrastructures must be adaptable and flexible to any given situation.

The Threat to Society: Humans and Cyber Technology

(8) The biggest threat to society in regards to cyber technology and society is society itself. Cyber technology is a tool that humans can use to their advantage. Humans have been using cyber technology to advance their own self-interests and harm others. Humans contribute to cyber threats in various ways including human error, insider threats, white-collar crimes and cybercrimes. In order to mitigate against cyber threats a Chief Information Security Officer will have to allocate and balance their limited cybersecurity budget between training and additional cybersecurity technology. Although training and additional technology are both equally important, one must not forget maintenance of current technology.

Employee training is an integral part of cybersecurity measures and must always have funds allocated towards it. Cyber threats that are a result of or facilitated by human error is an unnecessary risk to take. Training is the easiest and best preventable measure against human error and therefore, against cyber threats. Consistent, constant and quality training is the needed approach to minimizing human error as well as ensuring the preparedness of employees. In order for training to be consistent and constant, it needs a high amount of funds allocated for it. Furthermore, the quality of training is directly linked to its budget. A higher amount of funds allocated for training would result to a higher quality of training. A characteristic of quality training is being interactive as well as incorporating live exercises that will improve the employees' experience and better equip them to handle situations as they arise. Training should not just be going through presentation slides.

Training and cyber technology are both of equal importance in preventing cyber threats. The continuous rapid development of cyber technology has resulted in new and emerging cyber threats. According to Brian Payne's "White-Collar Cybercrime: White-Collar Crime, Cybercrime, or Both?", due to the routine use of computers in the workplace there are new opportunities for that technology to be used for white-collar crimes. This indicates a potential for insider threats that cannot be eliminated through training alone. Thus, companies should invest in cyber technology to defend against these types of threats. Additionally, due to the development of cyber threats if an organization or company falls behind in regards to cyber technology, even consistent, constant, and quality training will not be enough to defend against cyber threats.

While employee training and cyber technology are important cybersecurity measures, we must not forget to maintain the currently used system. Training employees is useless if the system itself does not work. Funds must be allocated to mitigate and prevent machine errors, faulty equipment, hardware degradation and potential loss of availability to equipment due to poor facilities. Maintenance is not limited to just the cyber devices. It would be undesirable to put the company at risk for things that are preventable such as a broken outlet or a water pipe that has burst. Not only does equipment failures prevent employees from doing their work but it also contributes to low morale and the disgruntlement of the workers. A disgruntled worker has the potential to be an insider threat.

When developing cyber-policy and infrastructure, the best interest of society is one where aspects of cybersecurity measures such as those listed above are taken into consideration and

regulated to have the most benefit to society. With the emergence of cybercrime, white-collar crime and workplace deviance, cyber-policies and infrastructures must have the best interest of people in mind. Cybersecurity measures can greatly prevent or mitigate any future negative impacts of cyber technology. Again, cyber technology is a tool that we must ensure benefits us instead of disadvantaging us.

Conclusion

(11) The rapid developments in cyber technology has resulted in both positive and negative impacts to society. We don't know the future implications however, we have already witnessed some of those implications such as the emergence and rise of workplace deviance as well as cybercrime and white-collar crime. In order to prevent against those implications, cybersecurity measures in an organization such as training, cyber technology and maintenance must be taken. Many approaches to developing cyber-policy and infrastructure can be taken however, I believe an approach that prioritizes adaptability, flexibility, and benefits to society is the easiest approach that will have great results. Adaptability and flexibility allows it to be applied regardless of time and any situation while having the best interest of society in mind ensures that cyber technology is used as a tool to help us rather than hinder us. It is true that adaptability and flexibility can result in cyber-policy and infrastructure to be too broad that it has no benefit therefore, it is important for there to be a balance when achieving that adaptability and flexibility. Additionally, developing new cyber-policies and infrastructures as new problems arise is possible but requires more time and effort to do so. Only time will tell what other implications cyber technology has on society. One thing that is certain is that we must develop cyber-policy and infrastructure to deal with these implications.

References

Payne B. (2018). White-Collar Cybercrime: White-Collar Crime, Cybercrime, or Both?. *Criminal Justice, Law & Society, 19*(3), 16-32.

Collins J., Sainato V., Khey D. (2011). Organizational Data Breaches 2005-2010: Applying SCP to The Healthcare and Education Sectors. *International Journal of Cyber Criminology*, *5*(1), 794-810.

Jonas H., (1973). Technology and Responsibility: Reflections on the New Tasks of Ethics. *Social Research*, *40*(1), 31-54.