The Social Significance and Effects of Technical Systems Associated with Cybersecurity

Zakiria Jordan

School of Cybersecurity, Old Dominion University

CYSE200T: Cybersecurity , Technology, and Society

Professor Chris Bowman

April 18, 2024

The Social Significance and Effects of Technical Systems Associated with Cybersecurity

As you all may know, technology tends to evolve constantly and at a rapid pace. Personally, technology is used very frequently and I'm pretty sure it is the same way for you. The technical cyber security systems are, therefore, very much necessary for protecting personal data, critical infrastructure, and cyber assets from untoward cyber incidents in modern digital times. Such systems are simply indispensable for the increasingly digital world of present times. However, with such advances come new challenges and risks that have to be met. In my opinion, the development of cyber-policy and infrastructure is crucial for ensuring that cybersecurity works effectively. It is like creating a set of rules and tools to protect us from cyber threats. That is to say, cybersecurity is, for the most part, a matter of policy and infrastructure that can be greatly compromised or sustained. This would make sure that people are able to use technology with safety and security, which is definitely an important thing to do in this modern, digitized world.

The Social Impact

These are the technical systems associated with cybersecurity that influence society's social interactions, hence making a contribution to social behaviors. On one hand, the systems have people who can reach other individuals, access information, and transact online, hence making life easy and efficient. The new times bring new risks: privacy problems, identity theft, and cyberbullying combine with a boundary of social interaction and behavior that moves closer and closer. If done, these technological systems have made it harder to distinguish between social engagement and online activity, which has both advantages and disadvantages. It is important that people, organizations, and legislators address these concerns, figure out how to safeguard privacy, and make sure that the internet is still a safe and beneficial place for social connections.

Impact on Business and Government

Marketing and advertising a small business can also be a good investment; attracting new Cybersecurity is the spine for asset protection in business and governments' ability to sustain continuous operations. Indeed, cybersecurity holds the key to the business's protection of its intellectual property, customer data, and financial information. An attack may lead to some financial loss, tarnishing of reputation, and even litigation. When you are talking about these things, cybersecurity is crucial for safeguarding sensitive data, important infrastructure, and national security from online attacks. In my opinion, there are still other protocols that could be put in place to safeguard these companies.

Even if many small businesses don't have a lot of money, the little that they do have can be put to some use.Certain aspects of the company should definitely receive investment. Doing a risk assessment would be the starting point for investment. This assessment would show the cybersecurity risks that could possibly happen to the organization. Another investment, which I feel is one of the most important,. would be investing in employee training. Making simple mistakes is often one of the most common causes of cybersecurity accidents. For example, a lot of cybercriminals try to win people over to their way in order to get sensitive data that could put the business in danger. So it is very important for employees to know these tactics in order to protect the business. There should also be money set aside for possible attacks that could occur within the company. This could be from backup plans, response plans, or cybersecurity insurance. When your company is attacked unexpectedly, with no monetary consideration, this could be horrible for the organization to be restored effectively.This can assist you in recovering from a cyberattack with the least amount of disturbance to your company. customers through marketing campaigns or on social media could have a great impact on the business, which will

lead to expansion. So even though small businesses do not start out with tons of money, if you budget correctly, they will still be able to thrive smoothly until more money is generated.

Cyber Threats

Although there are many things you can do to try to remain safe, you are bound to receive cyberthreats. The Information Systems Audit and Control Association points out many malicious cyber-related activities, but my focus would be hacking. Hacking generally means "the act of compromising digital devices and networks through unauthorized access to an account or computer system." However, when it comes to cybersecurity, this can happen when users are not using equipment properly, including computers or smartphones, to gather confidential information or steal data. There are different types of hackers, with one being "black hat hackers." The black-hat hackers "go out of their way to discover vulnerabilities in computer systems and software to exploit them for financial gain or for more malicious purposes, such as to gain reputation, carry out corporate espionage, or as part of a nation-state hacking campaign." Another type of hacker would be "white-hat hackers," who tend to hack proactively(“What Is Hacking? Types of Hacking & More | Fortinet”). There are some ways to possibly prevent getting hacked; one would be to update your software often. This is very crucial, being that hackers are always looking for problems to have easy access to your software.

Other protocols that can be followed in order to prevent being hacked are to make sure you choose a strong password. Making sure that you have a good password established can help ensure that a hacker will not be able to get into your information. Also, you should make sure that you avoid suspicious links. These links could lead to untrustworthy users having access and malware infections on your devices. So it is very important to be cautious when using the internet.

The Information Systems

I know understanding cybersecurity can be very hard, but lucky for you, there are special systems that tell you all about computer security. One important framework would be the information security triangle, which consists of three elements: availability, integrity, and secrecy. Each of these security triad members has its own definition and goal. First, secrecy ensures that only those with permission or individuals have access to conscious information. Integrity is the second component of the security trinity, which guarantees accuracy and dependability while guarding against unauthorized users altering data. The final factor is availability, which is only utilized to ensure that the resources and information are accessible to authorized users when they need them.

Another frequently used framework could be the Zero Trust Model. According to this technique, everyone attempting to access network resources must first authenticate themselves; no one is trusted by default, either inside or outside the network.By using this method, it could add another layer of security for whoever is using it (Cloudflare, n.d.).

Conclusion

In conclusion, in the current digital era, safeguarding people, companies, and governments against cyber dangers requires the establishment of cyber- policies and infrastructure. Although there are many advantages to these systems, there are also new hazards and obstacles that need to be considered. You and I can achieve the benefits of technology without increasing its risks by putting in place strong security measures and comprehending the societal impact of cybersecurity.

References

"What Is Hacking? Types of Hacking & More | Fortinet." *Fortinet*, https://www.fortinet.com/resources/cyberglossary/what-is-hacking . Accessed 19 Apr. 2024.

Cloudflare. (n.d.). Zero Trust Security | What's a Zero Trust Network? | Cloudflare. *Cloudflare*. https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/