Old Dominion University

How can we Build a Safer Cyber World?

Christopher Hossele

POLS426 Cyber War

Dr. Saltuk B. Karahan

April 20th, 2024

Decades of rapid technological innovation brought the gift of a digital environment where data and information are shared every second globally and throughout the United States in all sectors which can be noted as the cyber world. The concept of the cyberworld means to exist on the internet and to participate in the sharing of information and data in many ways. Knowing this, the rapid advancement of digital technology outpaces the ability to ensure total safety within the cyber world which results in a consistent call to action to ensure better methods of safety. These concerns can impose risks on our national security, areas of critical infrastructure, and even individual personal information such as bank information and medical records. Due to the idea of cybersecurity being fairly new and still unacknowledged, the cyber world is still going to be lacking in areas of safety. This question regarding what it would take to ensure a safer cyber world at both the national and private level requires a conceptual understanding that showcases the many dynamics of solutions and approaches with cybersecurity methods. These dynamics consist of measures that would benefit the United States' cyber world substantially while addressing critical areas that lack strength and resilience capabilities. Identifying these critical areas as education and awareness, strategies and policies, physical technological methods, international cooperation with other countries, predictive knowledge, and consistent fortification across all types of systems nationally helps narrow the areas of improvement, factoring in ways to better the cyber world and its safety. There are supportive reasons as to why these concepts can create a safer cyber world and acknowledging the usefulness and benefits that these critical areas bring allows for a greater motive for prioritization. These reasons, such as protecting government entities information, medical organization information, business information, individual personal information, and overall guaranteeing the constitutional right to privacy are important factors to consider when understanding the importance of constructing a safer cyber world. A lot of these motives can impose a risk on privacy and finances across all areas within the cyber world. Through extensive research and development, these concepts of cybersecurity methodology can be used generously to develop a safer cyber world and to develop better research and understanding of the importance of securing areas of digital technology in many different ways.

Education and Awareness

One of the most important concepts to understand when it comes to ensuring a secure cyber world is understanding the importance of education and awareness. Education and awareness in this matter can be approached across all demographics of technology usage within the cyber world, such as governments, businesses, critical infrastructure, and personal information. Having an adequate amount of education regarding the concepts of cybersecurity awareness training and education helps minimize the negative impacts of cybercrimes by decreasing the risk of them occurring. The lack of education and awareness hinders the evolution of a strong and safe cyber world. The lack of education and awareness practices throughout the billions of individuals that utilize the internet daily attest to the rising inconveniences that occur with data and information insecurity and vulnerabilities (Shillair, 2022). These situations can be caused by weak passwords, outdated systems, and a lack of system implementations such as authentication devices, strong updated software systems, and firewalls. It is said that a rather small number of individuals were able to recognize examples of authentication methods and other forms of cybersecurity devices (Shillair, 2022). This lack of knowledge of authentication methods is just the first step of a domino effect of catastrophe to vulnerable systems due to lack of education and awareness even of simple concepts. Not having the education and awareness to implement and identify such methods imposes risks on information systems. Understanding the importance of authentication methods and their significance can ensure the availability of information and data and are used throughout areas such as government, business, and personal entities. These tools are among the many that are used in cybersecurity methodology and lower the risks of cybercrimes and vulnerabilities of weak systems and routine.

Business environments need adequate cybersecurity training and awareness to ensure the incapability of financial and data loss that can be devastating overall for a business due to vulnerabilities. In businesses, cyber-physical-social (CPS) systems drive the development of many digital processes such as enterprise management, transaction processing, and supply chain management which need thorough education and training to keep processes performing efficiently. Many businesses are slowly moving towards allocating processes towards implementing cybersecurity measures to mitigate risks and to keep business processes flowing smoothly without error within these CPS systems. Businesses implementing methods of proper cybersecurity training and education routines help minimize the risks and effects of vulnerabilities in cyber systems (Hsu, D, 2015). These vulnerabilities can lead to the risks of becoming a victim to cybercrimes such as ransomware, password jeopardizing, identity theft, malware, etc. The impact and occurrences of these cybercrimes disrupt the concept of having a safer economic cyber world and the importance of education supports the notability which helps mitigate these risks. Businesses and organizations such as Amazon and IBM have made efforts to allocate education and training to the public and educational fields. From the article “October is Cybersecurity Awareness Month–So what’s new?” it states that “Amazon announced it will make available to the public at no charge the security awareness training it offers its employees…IBM announced it will train 150,000 people in cybersecurity skills over the next three years and will partner with more than 20 Historically Black Colleges & Universities to establish Cybersecurity Leadership Centers to grow a more diverse cyber workforce." (michellehavich). It is also noted that Google pledged to help over 100,000 Americans earn cybersecurity skills certifications (michellehavich). These facts, if popularized by more companies and organizations can help significantly grow cybersecurity education and awareness in the workplace to help minimize risks and vulnerabilities that would alternately lead to devastating outcomes.

Familiarization with policies and frameworks for business intelligence techniques can mitigate cyberthreats within business environments. For example, the CIA Triad (Confidentiality, Integrity, and Availability) is a model that businesses can use to deter potential risks and vulnerabilities of information technology systems through implementation and research. The consistent familiarization of this model can benefit organizations greatly by having a baseline plan to execute for daily business operations that are digital to maintain safety and security (Sadik, 2020). The implementation of this framework within more businesses can help secure a safer cyber world economically due to the layout of the model that works to keep business security afloat. Apart from keeping systems secure it is beneficial to implement physical security devices such as firewalls, software systems, hardware devices, and authentication devices. Having this knowledge of physical security devices, the CIA Triad can act as the perfect formula for where to have these devices implemented which protects the confidentiality, integrity, and availability of security systems (LenelS2).

For education and awareness on the national level, the Networking and Information Technology Research and Development (NITRD) program is a strategic framework federally supported and developed through the coordination of government entities and academic institutions collaboratively through research and educational development (Hsu, D, 2015). The NITRD supports research that focuses on diverting the challenges within cybersecurity systems and acts as an educational foundation for research and development among these concepts and utilizes findings to support the federal government's strategy. Utilizing this program at the national level helps support the education and awareness of cybersecurity methods and research and should be frequently discussed and utilized daily to ensure a safer cyberworld. Consistent research and developmental strategies are among the many techniques used to support adequate education and awareness methods for a safer cyber world.

National Security Advantages

Protecting national security for the United States is an important factor in securing a safe cyberworld. National security in this context is the protection of the nation and its assets entirely, which includes its digital components of information and data. With the concept of nationally embarking on efforts to protect national security through a cybersecurity approach it is possible to secure a safer cyber world. The ways that this can be accomplished can be through international cooperation, national legislation, and other courses of action that are collaborated federally and state focused. The National Cybersecurity Strategy is essential to protecting national security through cybersecurity by collaboration of private and public entities and provides a strategic framework of actions and steps to take to protect national security. Understanding the developing trends of cybersecurity on a national level can help support better understanding and research that can be used to curate functioning standards of cybersecurity efforts (Craig). The emerging usage of artificial intelligence, developing usages of the internet, and the questions regarding data usage factor into the safety of the cyber world. These questions that need to be addressed are how they can be secured fully to protect national security with the growing number of cybercrimes that impose threats on critical infrastructure and economic structures. Concerns can be addressed with the five pillars of national cybersecurity: Defend Critical Infrastructure, Disrupt and Dismantle Threat Actors, Shape Market Forces to Drive Security and Resilience, invest in a Resilient Future, and Forge International Partnerships to Pursue Shared Goals (National Cybersecurity Strategy). All of these pillars, if taken seriously through thorough national implementation and effort, contribute adequately to securing the national security of this country through a cybersecurity approach. The importance of securing the national security of this country helps build a safer cyber world (Craig).

Pillar one, “Defend Critical Infrastructure” discusses the importance of collaboration between national cybersecurity affiliated organizations such as CISA to develop strategic plans to protect national security and critical infrastructure entities by implementing guidelines. These guidelines help critical organizations in the private or public sector by allowing the opportunity to seek assistance when needed. The CISA will also work to support implementation of the National Cyber Incident Response Plan to strengthen processes and fortify systems with the confidence of proper assistance.

Pillar two, “Disrupt and Dismantle Threat Actors” emphasizes the importance of collaboration between organizations federally and locally to dismantle threats against entities. On the federal level, actions would be taken through both diplomatic and law enforcement strategies to assist the prevention of cyber-attacks that deter the progress made by cyber criminals. Sharing the information regarding characteristics of the attack, methods used, and outcomes between federal and non-federal entities help build a relationship of deterring incidents (National Cybersecurity Strategy).

The third pillar of the National Cybersecurity Strategy discusses the resilience strategies that will be taken to hold accountable the wrongdoings of poor cybersecurity practices while also keeping the liability off of vulnerable organizations and businesses that may not have the position to rebuild and take countermeasures for losses such as data and finances. This pillar "Shape Market Forces to Drive Security and Resilience" gives organizations both private and public the motive to invest properly into cybersecurity measures and to develop secure Internet of Things services.

The fourth pillar elaborates on the motive to secure a better secure digital future. The pillar elaborates on key takeaways such as strengthening national security in ways that would benefit future developments and practices and subsidize research and practice of cybersecurity at the federal level to build awareness and education National Cybersecurity Strategy).

The last pillar "Forge International Partnerships to Pursue Shared Goals" explains the concepts of collaboration through foreign diplomacy that builds better relationships with neighboring companies. With this, collaborative techniques can help with sharing information that can support a partnership of cybersecurity forces that could aid in combative and countermeasures if events occur. This international cooperative motive builds up a safer cyber world among several allied nations, securing a safe digital environment for our nation and other nations. The administration in which constructed the pillars states that "We have used multilateral processes such as the United Nations (UN) Group of Governmental Experts and Open-Ended Working Group to develop a framework that includes a set of peacetime norms and confidence-building measures, which all UN member states have affirmed in the UN General Assembly" (National Cybersecurity Strategy). This showcases the characteristics of international collaboration taken by the federal government, cooperative with organizations such as the United

Nations (UN) to elaborate and develop international strategy to better support a secure cyber world. These methods of development on the international level can help support better education, collaboration, and implementation of physical cyber security devices throughout all areas of government and private entities.

Throughout the discussion of concepts that ensure a safer cyber world, there has been coverage regarding the benefits of more education and awareness, implementation of policies and security devices, international collaborative discussion, and national security fortification that ensure a safer cyber ecosystem nationally and internationally. The consistent development of digital technology throughout the past several years imposes risks of information and data security, fraudulency, and theft which tarnishes the progress of keeping a secure digital environment. Following the many available methods and research that have been discussed can better enforce a safer cyber world if popularized and considered by the rights of information and data stakeholders.

References

1. Hsu, D. Frank, et al. "Cybersecurity: Toward a Secure and Sustainable Cyber Ecosystem." *Computer (Long Beach, Calif.)*, vol. 48, no. 4, 2015, pp. 12–14, doi:10.1109/MC.2015.103. https://ieeexplore.ieee.org/ielx7/2/7085638/07085950.pdf

2. Shillair, Ruth, et al. "Cybersecurity Education, Awareness Raising, and Training Initiatives: National Level Evidence-Based Results, Challenges, and Promise." *Computers & Security*, vol. 119, 2022, p. 102756, doi:10.1016/j.cose.2022.102756. https://www-sciencedirect-com.proxy.lib.odu.edu/science/article/pii/S0167404822001511?via%3Dihub

3. michellehavich. "October is Cyber Security Awareness Month—So what's New?" *The American City & County* (2021)*ProQuest.* Web. 20 Apr. 2024. https://www.proquest.com/docview/2586936785?accountid=12967&parentSessionId=mWV2BD%2FP2J9RIXDhEbwnycYcANjV2UrJW4ExqbHkOGg%3D&pq-origsite=primo&sourcetype=Trade%20Journals

4. Craig, Anthony J. S., et al. "Building Cybersecurity Capacity: a Framework of Analysis for National Cybersecurity Strategies." *Journal of Cyber Policy*, vol. 7, no. 3, 2022, pp. 375–98, doi:10.1080/23738871.2023.2178318. https://www-tandfonline-com.proxy.lib.odu.edu/doi/pdf/10.1080/23738871.2023.2178318?needAccess=true

5. *National Cybersecurity Strategy*, www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf. Accessed 20 Apr. 2024.

6. LenelS2. "Physical Security and Cybersecurity: How They Work Together." *LenelS2*, www.lenels2.com/en/news/insights/Physical_and_Cybersecurity.html. Accessed 20 Apr. 2024.

7. Sadik, Shahrin, et al. "Toward a Sustainable Cybersecurity Ecosystem." *Computers (Basel)*, vol. 9, no. 3, 2020, p. 74, doi:10.3390/computers9030074. https://mdpi-res.com/computers/computers-09-00074/article_deploy/computers-09-00074.pdf?version=1600329902