Social Meaning and Impact of Cyber Security-Related Technical Systems

John Wilson

Old Dominion University

CYSE200T_28570

Christopher Bowman

April 25, 2022

Social Meaning and Impact of Cyber Security-Related Technical Systems

The current society is largely reliant on technology as part of routine living. Primarily, companies and businesses have turned to digitalization on majority operations. As this occurs, the social media meaning alongside the effect of cyber security technical frameworks will change along with it, and not mostly in a positive manner. There exist many components and elements of the system that operate in a way to safeguard businesses and their information. Evaluating multiple perspectives and issues assists in the development of alternatives to enable guide counteracting cybercrime (Brazevich et al., 2020). As such, the paper will dwell on the social meaning and impact of cyber security and related technical systems.

Cyber-policy and Infrastructure

A cyber security policy depicts a guideline that assists in preserving data alongside technological infrastructure. Companies and businesses have a duty of ensuring information are always safe to enhance the efficiency of operations. Since the field of the cyber market is considerably widening, infrastructure and policies are yet to keep up with the pace. The more companies and businesses trust technology to keep, collect, and control information, the more it becomes susceptible to numerous threats consisting of hackers and malfunctions in technology. Such attacks are propagated for numerous reasons, including personal assaults and business concerns. The United States, for instance, has in place numerous complex systems that are connected to national security and the country's economy (Malatji et al., 2019). To rely on such systems is founded on the dependence of organizational success in the private and public sectors, and this incorporates infrastructure. Primarily, such infrastructure makes operations vulnerable to attackers.

The Department of Defense holds concern for public and private networks. It recommends the development of strategic plans to enhance the response rate in identifying and preventing attacks from happening. Cyber security should be prioritized and be all peoples' responsibility event with or without similar knowledge. Maintaining a cyber strategy or policy provides defense against attacks and assaults. While hackers routinely change their approaches, information technology teams and businesses are compelled to evolve to safeguard companies from imminent risks. Being a step ahead of cybercriminals is an uphill task but maintaining specific strategies to prevent damage and help recovery is very essential (Malatji et al., 2019). There is also a need to bounce back from an attack and ensure such a problem never happens in the future.

Threats within the Workplace

Cyber technology has developed opportunities for a place of work deviance. Primarily, this is a growing pattern that is not yet to stop any time in the future. Cyber technology leads to undesirable traits with ramifications that many regards as negative or adverse on groups, businesses, and groups. Research by Moon et al. (2018) supports that deviance in technology leads to momentous costs for companies both in the form of finances and human capital. Adverse effects experienced by companies incorporate disciplinary actions, loss of employees, terminations, and breaches of corporate confidentiality. Others include losing personal and organizational information, loss of productivity, and connected legal expenses. Compared to aspects in the form of demographics, situational and personality elements are largely connected to counterproductive work character. As cyber deviant behavior typically happens when people have access to their information communication and technology gadgets at their place of work. As such, there are situational triggers alongside context effects that mediate moderate or

immediate outcomes and behaviors. Primarily, different factors and triggers connect to specific behavior. As such, organizations and businesses should execute strategies meant to limit the utilization of hyper-connected technology to workers (Moon et al., 2018). As the boundaries of technology haze between work and daily personal operations, the more challenging management and prevention of cyber deviant character in companies become. In general, research into this topic is restrained and requires further exploration.

Developing Cyber Security Programs

Small business enterprises play a critical role in the United States cyberinfrastructure and economy. Currently, corporations of all sizes and magnitudes are even more dependent on their networks, data connectivity, and the internet to manage routine operations. Cybercrime is an expanding concern and is on the rise in small to medium to big sized corporations because of the lack of education and resources on approaches to controlling the problem. The main aim of cybercriminals is to gather intellectual property, sensitive data, and personal information for their various needs. Cybercrimes cost companies hundreds of dollars when dealing with the issues, including laying down strategies or recovering after the assault (Payne, 2018). This is despite the numerous plans and strategies that companies have put across to handle the damaging situation.

There are numerous gains and expenses of developing cyber security programs in companies. Principally, businesses today look to the NIST Interagency Report (NISTIR) for guidance on approaches to assist safeguard operations. The NIST offers critical security for their data, networks, and systems. It was developed via coordination between the private sector and governments as a resource template for planning cyber security risk management procedures and processes in critical infrastructures. A robust information security program assists companies attain and holding their clients, alongside employees and affiliates. Developing or enhancing the

information security program further makes it less complicated for entities to innovate. Ideally, the programs allow companies to take advantage of modern technologies as a way of lowering expenses while creating commodities to ensure customer satisfaction (Rosengarten, 2018). The NISTIR further involves worksheets that compute an overall ranking alongside risk score for all information types and factors. There are numerous practices and steps companies have in place to create cyber security programs in which they can confidently address the growing risks.

There is a rising realization that businesses and people have a lot to learn to enable preserve the fundamental values of the collective history while including the positive elements of the new digital future. Primarily, deviance in the place of work and the numerous threats able to harm companies show proof of failure in keeping up with technology. Such are just a few illustrations of the possible consequences of cyber security-connected technology networks for people and companies. The combination of human reliance on technology alongside the contemporary system permits the present situation in cyber security (Rosengarten, 2018). To move forward, there is a need to regard the requirements for effective comprehension of social meaning alongside the effect of cyber security technical systems and entails a new analytical approach.

Fido Alliance and the problems ii Addresses

By definition, the FIDO alliance is an entity offering multifactor authentication services, including biometrics and PINs, to firms to aid secure their systems. Primarily, FIDO Alliance uses the thought approach; and this is something they are, know, and possess when validating users. The issue FIDO Alliance handles are the authentication matters of passwords. Principally, this happens using private and public keys between the user's precise grid and the company's servers to help eradicate illegal access using passwords and usernames (Rosengarten,

2018). FIDO Alliance also maintains biometrics innovation, including facial recognition and fingerprints, using equipment users possess.

How Cryptography helps with Authenticity and Integrity

Cryptography refers to the science of counseling information. Primarily, the approach utilizes mathematical algorithms and applications that change plain text into a decoded communication. The approach of encrypting information and text makes it challenging for unauthorized outside people to easily interpret interceded communications. An illustration of cryptography applied to safeguard information was during the Second World War when the United States utilized Indigenous Americans to communicate to others over the radio using tribal language during the Pacific Campaign (Shozi & Mtsweni, 2019). Another illustration was during a similar period when Germany constructed the Enigma Machine that utilized cryptography to conceal strategic radio chats from the allied forces. Luckily for the Alliance Forces, the Enigma Machine's encoded algorithm was broken by Marian Rejewski, a Polish Mathematician, in the 1930's. In the contemporary world, cryptography is largely dependent on the integrity and authenticity of systems to offer secure communications from one point to the other and keep them from unofficial access. Cases of communications that need encryption are things like financial data, such as bank account details and stock trading accounts. Intellectual information that should be encoded includes things like soda pop recipes, wind turbine source codes, and car battery schematics. Additionally, there is also a need to encrypt medical records among others (Shozi & Mtsweni, 2019). It is essential to use cryptography since it better provides the authentication and reliability of sent together with received information from reputable sources.

Conclusion

The threat landscape of the technological globe is changing fast. It has become complicated to keep up with the possible impact of threats thanks to a variety of elements. The rapid evolution of modern-day technology provides new issues for preventing threats. This problem might arise numerous arguments on how technology can be applied against defenseless victims, alongside how ethical the assessment of such innovation is as well. Ideally, the opposing opinion might inform that such innovations have rendered the world a more appropriate and safer place alongside making life easier in several aspects. Over the ages, technology has developed largely in ways that the average individual could not even anticipate. Many individuals currently cannot tell how a text message is delivered or what procedure is applied to relate to their home observation grids. Technology has become so complicated and has been included in our daily lives.

References

Brazevich, D. S., Safronova, Z. S., Kosheleva, T. N., & Biryukova, A. V. (2020). Analysis of the Problems of Ensuring Information Security in the Terms of the Contemporary Society. *Open Journal of Social Sciences*, *8*(02), 231. http://www.scirp.org/journal/Paperabs.aspx?PaperID=98599

Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information & Computer Security*. https://doi.org/10.1108/ICS-03-2018-0031

Moon, Y. J., Choi, M., & Armstrong, D. J. (2018). The impact of relational leadership and social alignment on information security system effectiveness in Korean governmental organizations. *International Journal of Information Management*, *40*, 54-66. https://doi.org/10.1016/j.ijinfomgt.2018.01.001

Payne, B. K. (2018, June 25). Criminology, Criminal Justice, Law & Society. https://scholasticahq.com/criminology-criminal-justice-law-society/.

Rosengarten, J. (2018). "Three Critical Components of a Cyber Policy." www.insurancebusinessmag.com/us/news/cyber/three-critical-components-of-cyber-policy-99482.aspx.

Shozi, N. A., & Mtsweni, J. (2019, February). A socio-technical systems analysis of privacy issues in social media sites. In *Proc. 14th Int. Conf. Cyber Warfare Secure.* (pp. 369-377). ISBN: 1912764121, 9781912764129