Social Implications of Cybersecurity Policy

Adam Johnson

Old Dominion University

CYSE 425W: Cyber Strategy and Policy

Professor: Bora Aslan

November 13, 2022

Technology is constantly changing how our society functions, the capabilities to do business and conduct our day to day lives. In the article "Cybersecurity Decides on the Stability of Societies" published in the Database and Network Journal (vol.50 no.1) the impact of technology and the use of connected devices are becoming an integral part of our society and how it functions. The article shows how even medical devices are now connected to the "Internet of Medical things". Devices such as insulin pumps, heart monitors, defibrillators, pacemakers, CPAP and pretty much any home medical device are connected to a network that can be accessed or targeted by attackers. This connection to our medical devices creates opportunities for attackers to breach systems, target medical facilities and products with ransomware attacks, leveraging the health and well being of patients and citizens. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) is associated with combating these types of attacks in the future and has even identified the medical field as critical infrastructure. This would require the reporting of attacks targeting medical facilities and their devices to federal agencies to help secure them in the future.

Through the advancement of IOT devices it is estimated that by 2025 there will be over 75 billion networked devices that will have their own software package that could potentially compromise the networks they exist on(Vol.50 No.1). This advancement in technology can have major effects on society as more people start to rely on and use these devices in their everyday lives. These devices include smart speakers, fitness trackers, smart watchers, thermostats, energy meters, security cameras, smart locks and lights (Vol.50 No.1). The more our society becomes dependent on IOT devices the more focus on cybersecurity in these areas are needed as they will become major targets for attackers. Organizations such as NIST have created guidelines that are currently being used in the federal government that require IOT device

makers to create devices within specific standards and security capabilities. These devices will have expiration dates and will need to be replaced as software and hardware become outdated and subject to attacks. The use of these devices can have major impacts on our society as insecure devices are more widely used throughout society. Personal information and data collection is already taking place within our mobile devices and social media accounts but that can also extend to even IOT devices that are easily accessible to attackers who can now target home devices remotely while phishing for easy access to personal information.

Even the transportation infrastructure is moving towards a connected platform and in turn putting supply chains and everyday drivers at risk. Advancements are being made to produce and sell self-propelled vehicles operating on AI and connected smart devices. Everyday vehicles are using GPS, bluetooth, cellular networks, usb connections and WIFI to keep vehicles and their drivers connected to social media and mobile devices. The capability to connect ourselves to our vehicles and other everyday devices has led to attackers targeting those devices. Vehicles and the operation of them can be compromised through insecure wireless connections such as bluetooth that would allow an attacker to even control the vehicle while in operation.

It has become clear that our society is moving towards a connected existence as all aspects of our critical infrastructure and personal lives are being infested with connected devices. The ability to secure these devices and the role of cybersecurity protecting our society and the well being of individuals is becoming a critical necessity in our society. The CIRCIA ACT is still a work in progress and is trying to address these issues as they arise but our society is changing and adapting to the use of connected IOT at such a fast pace it will be a very hard task for cybersecurity policies and actions to stop cyber criminals from targeting the cloud and every device on it.

References

Cybersecurity Decides on the Stability of Societies. (2020). Database & Network Journal, 50(1), 16–17.

Carley, K. M. (2020). Social cybersecurity: an emerging science. Computational & Mathematical Organization Theory, 26(4), 365–381. https://doi-org.proxy.lib.odu.edu/10.1007/s10588-020-09322-9

Creese, S., Dutton, W. H., & Esteve-González, P. (2021). The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions. Personal & Ubiquitous Computing, 25(5), 941–955. https://doi-org.proxy.lib.odu.edu/10.1007/s00779-021-01569-6

Xu, S., Yung, M., & Wang, J. (2021). Seeking Foundations for the Science of Cyber Security: Editorial for Special Issue of Information Systems Frontiers. Information Systems Frontiers, 23(2), 263–267. https://doi-org.proxy.lib.odu.edu/10.1007/s10796-021-10134-8