Cybersecurity Infrastructure Status in the United States

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Peng Zhang
Spring, 2021

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature _____ Date _____
Peng Zhang

Approved _____ Date _____
Tsai-Hsuan Ku, Department of Engineering and Society

Introduction

The United States is the most targeted country for cyberattacks, experiencing 156 "significant" cyberattacks between May 2006 and June 2020, followed by 47 in the United Kingdom ("The Countries Experiencing," 2020). The rapid digitization of society on a global scale has led to increasing dependence on the Internet, in addition to increasing amounts of sensitive data being stored. As the most targeted country, it is imperative that the United States has proper cybersecurity infrastructure to prevent devastating data breaches.

The United States experienced one of its most devastating federal government data breaches in December 2020 from the Sunburst cyberattack (Viou, 2021). This cyberattack was massive, affecting many organizations and federal agencies alike, which showed numerous high-risk vulnerabilities and entry points across multiple network levels. The breadth of the breach that occurred within different infrastructure sectors demonstrates the need for a cohesive national cybersecurity infrastructure to mirror the dependencies between sectors brought by advancing technology.

This paper will focus on case studies from the healthcare and public health sector and the transportation systems sector. These are critical infrastructure sectors, deemed essential to security, public health, and economic security on a national scale ("Critical Infrastructure Sectors," n.d.). By analyzing case studies, previous research, and discussing sociocultural factors, this paper will demonstrate how Actor Network Theory can be applied to understand the state of cybersecurity infrastructure within the United States.

Literature Review

The transportation systems sector efficiently and safely moves both people and goods both domestically and internationally. Management and control systems are becoming more dependent on information technology, increasing the complexity of respective systems and services. These dependencies also grow the need for cybersecurity to maintain the security of transit IT infrastructure. The Mineta Transportation Institute released a report in October 2020 revealing that over 80% of agencies felt prepared for a cybersecurity threat, yet only 60% had a cybersecurity program in place (Belcher, Belcher, Greenwald, Thomas, 2020). The lack of a cybersecurity program in a significant number of the transit agencies surveyed suggests that many agencies probably do not have protocols to prevent data breaches or system compromises.

The healthcare and public health sector has been under immense strain as a result of the COVID-19 pandemic, with over 500,000 deaths in the United States. COVID has had a unique societal effect, resulting in the transition of many businesses to remote operations. This has also led to an increase in telemedicine practice, where the patient and doctor interact remotely. The healthcare industry has established a history of less-than-ideal cybersecurity, and the rise in telemedicine has also resulted in an increase of over 55% in healthcare attacks in 2020 (Ikeda, 2021). Cyberattacks against healthcare computer systems are extremely detrimental, as not only do facilities work to keep patients alive, but they also process and store highly sensitive and personal data.

Foreign interference in the United States has become increasingly intertwined with cybersecurity in recent years. During the 2016 presidential election, the computer network of the Democratic National Committee was breached by Russian cyberespionage groups, leading to the leakage of stolen information (Lipton, Sanger, Shane, 2016). Leading up to the 2020 presidential

election, Microsoft also observed cyberattacks targeting both people and organizations involved with the opposing campaigns, by groups from Russia, China, and Iran (Burt, 2020).

Framework

Actor-Network Theory (ANT) focuses on the interaction of human and non-human actors within networks to effect social processes. These actors are a "source of action regardless of its status as a human or nonhuman" (Cresswell, 2010). The diversification between human and non-human actors makes ANT a social theory, intended to explore both the technical and social construction of heterogeneous actor-networks.

Previous research utilizing ANT to understand cybersecurity management analyzed the translation process from the introduction of a server until the computer system was compromised (Hedström, Dhillon, Karlsson, 2010). Translation of a network establishes or modifies a relation between actors, allowing for the network to be represented by a single entity. Hedström, Dhillon, and Karlsson state that a typical translation requires enrollment, where an actor tries to influence another actor's role in the network. In a heterogenous actor-network, enrollment introduces the interests of specific actors, and can become part of the technical systems as inscriptions. Enrollment also leads to the last phase of translation, mobilization (Callon, 1986). Mobilization is intended to ensure the proper representation of all actors within the network, and problems during mobilization may result in the unenrollment of actors.

Analysis of the United States cybersecurity infrastructure was conducted at three different levels: the federal level, the industrial level, and the citizen level. By discussing both technical and sociocultural factors in case studies at all three levels, it will be clear how

conflicting interests between actors leads to detrimental inscriptions within the network, and how sociocultural differences can result in problems during mobilization.

Analysis

One of the defining sociocultural attributes of the United States is that it is extremely diverse, both ethnically and culturally. This diversity reflects the heterogeneity of the network being analyzed, as there are highly individualized social interests that cause problems during mobilization of the network. This can be seen from the firing of Christopher Krebs, who was the director of the Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security. Conflicting opinions between Krebs and President Trump regarding fraud in the 2020 election led to Krebs' firing (Nakashima, Miroff, 2020). Clearly, this inscription utilized non-technical interests to leverage executive power and resulted in the unenrollment of an actor from the network.

This unenrollment of a key actor from the federal level of the network had effects that diffused throughout the other levels of the network. The Government Accountability Office (GAO) released a report during the Trump Administration which stated that there were insufficient leadership responsibilities outlined in the administration's national cyber strategy and implementation. According to the GAO, the lack of proper leadership responsibility delegation prevented the coordination of the cybersecurity programs of 23 federal agencies to support national cyber defense (Kass, 2020).

Another defining attribute of the United States is that it is an individualistic society, which prioritize the needs of an individual. The emphasis on independence and freedom largely contributes to the interests of the actors at all levels of the network, from the bottom up. A

growing technical topic of contention which reflects this individualism is user privacy. Apple's changes to data/privacy permissions and app tracking transparency starting with iOS 14 enable users to strictly filter which apps monitor personalized information (O'Flaherty, 2021). Leaving large cybersecurity problems such as user privacy to be resolved by relationships between actors at the industrial and citizen level further emphasizes sociocultural individualism. However, the United States cybersecurity network might experience more mobilization problems as a result of the lack of cohesion between all levels of the network regarding large data issues such as user privacy, when compared to collectivist societies such as China. The enactment of the Chinese Cybersecurity Law grants the Chinese government an immense amount of authority to monitor data protection, which directly inscribes the interests of the federal government throughout the rest of the network (Wagner, 2017).

The Mineta Transportation Institute report on transit agency cybersecurity showed that many transit agencies wrongly believed that they had proper cybersecurity programs. This demonstrates the lack of relationships between actors at the federal and industrial levels of the network. There was clearly a lack of initiative at the industrial level for transit agencies to maintain technological security. However, there is also a lack of regulation from actors at the federal level, who provide federal funding. The concluding recommendations from the report advocated for collaboration between the federal government, the industry, and agency leadership in order to set up adequate cybersecurity programs (Belcher et al., 2020). It was also emphasized that the Federal Transit Administration (FTA) should implement minimum cybersecurity standards requirements to continue qualifying for federal funding.

The Digital Imaging and Communications in Medicine (DICOM) standard was established three decades ago and is still the way that many medical professionals store and

transfer images (Ikeda, 2020). These images can include x-rays, MRI and CT scans, ultrasounds, dental records, etc. and can also include even more sensitive information such as social security numbers. The lack of security across the healthcare industry has resulted in data breaches totaling over one billion images. Similar to the maintenance of cybersecurity programs in the transportation systems sector, the security of computer systems in the healthcare industry is the responsibility of individual facilities. Failure to keep systems secure has resulted in the breach of trust between actors at the citizen level and those at the industrial level of the network. Despite the Health Insurance portability and Accountability Act including a security provision to protect sensitive data, some facilities appear to consider these finable violations an acceptable cost of doing business (Ornstein, Waldman, 2015). These business practices are extremely reflective of the individualistic society values, and it seems that actors at the federal level need to become more involved in order to inspire change.

The lack of cybersecurity program development in critical infrastructure sectors seems to stem from both a lack of industry wide initiative and federal government leadership. This could possibly be due to the effects of an individualistic society causing a combination of complacency and a lack of cohesion between actors on all three levels of the network. The case studies from the transportation systems sector and the healthcare and public health sector showed that when the maintenance and regulation of cybersecurity programs is solely left to actors at the industrial level, then the heterogeneity of the network results in a wide spectrum of results regarding the efficacy of the corresponding cybersecurity systems.

Conclusion

The Actor-Network Theory is a useful framework which helps clarify both the social and technical aspects of cybersecurity, especially when applied to the infrastructure of an individualistic society like the United States. Actors at the federal, industrial, and citizen level of the network develop relationships in order to produce practices and protocols that protect sensitive data. Analysis of the mobilization of the network has shown that interests that may be inspired from the ingrained values of an individualistic society has led to less-than-ideal cybersecurity measures being taken. The reserved actions and unenrollment of actors at the federal level needs to change in order to promote more cohesive change in cybersecurity technologies across numerous critical infrastructure sectors. More cohesive collaboration between the government, industry facilities, and citizens will promote better national cyber security.

Bibliography

Belcher, S., Belcher, T., Greenwald, E., & Thomas, B. (2020). *Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness*. Mineta Transportation Institute. https://doi.org/10.31979/mti.2020.1939

Burt, T. (2020, September 10). New cyberattacks targeting U.S. elections. *Microsoft on the Issues*. https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/

Callon, M., 1986. "The sociology of an actor-network". In M. Callon, J. Law, & A. Rip, eds. Mapping the Dynamics of Science and Technology. London: Macmillan, p. 19–34.

Cresswell, K. M., Worth, A., & Sheikh, A. (2010). Actor-Network Theory and its role in understanding the implementation of information technology developments in healthcare. BMC Medical Informatics and Decision Making, 10(1), 67. https://doi.org/10.1186/1472-6947-10-67

Critical Infrastructure Sectors. (n.d.). Retrieved November 2, 2020, from https://www.cisa.gov/critical-infrastructure-sectors

Hedström, K., Dhillon, G., & Karlsson, F. (2010). Using Actor Network Theory to Understand Information Security Management. In K. Rannenberg, V. Varadharajan, & C. Weber (Eds.), *Security and Privacy – Silver Linings in the Cloud* (pp. 43–54). Springer Berlin Heidelberg.

Ikeda, S. (2020, January 24). *One Billion Medical Records, All Containing Images, Exposed Due to Common Security Oversight*. CPO Magazine. https://www.cpomagazine.com/cyber-security/one-billion-medical-records-all-containing-images-exposed-due-to-common-security-oversight/

Ikeda, S. (2021, February 26). *Healthcare Cyber Attacks Rise by 55%, Over 26 Million in the U.S. Impacted*. CPO Magazine. https://www.cpomagazine.com/cyber-security/healthcare-cyber-attacks-rise-by-55-over-26-million-in-the-u-s-impacted/

Kass, D. H. (2020, September 25). *White House Needs National Cybersecurity Director, Government Watchdog Asserts*. MSSP Alert. https://www.msspalert.com/cybersecurity-markets/americas/white-house-needs-national-cybersecurity-director-government-watchdog-asserts/

Lipton, E., Sanger, D., & Shane, S. (n.d.). *The Perfect Weapon: How Russian Cyberpower Invaded the U.S. - The New York Times*. Retrieved November 2, 2020, from https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

Nakashima, E., & Miroff, N. (2020, November 17). Trump fires top DHS official who refuted his claims that the election was rigged. *Washington Post*. https://www.washingtonpost.com/national-security/trump-fires-dhs-election-official/2020/11/17/97d3fa5c-251c-11eb-952e-0c475972cfc0_story.html

O'Flaherty, K. (2021, January 31). *Apple's Stunning iOS 14 Privacy Move: A Game-Changer For All iPhone Users*. Forbes. https://www.forbes.com/sites/kateoflahertyuk/2021/01/31/apples-stunning-ios-14-privacy-move-a-game-changer-for-all-iphone-users/

Ornstein, C., & Waldman. (2015, December 29). *Few Consequences For Health Privacy Law's Repeat Offenders*. ProPublica. https://www.propublica.org/article/few-consequences-for-health-privacy-law-repeat-offenders?token=Tu5C70R2pCBv8Yj33AkMh2E-mHz3d6iu

The countries experiencing the most 'significant' cyber-attacks. (2020, July 9). https://specopssoft.com/blog/countries-experiencing-significant-cyber-attacks/

Viou, S. (2021, January 7). *Sunburst malware: What we know about an advanced attack, and protective measures with Stormshield*. https://www.stormshield.com/news/sunburst-cyberattack-what-we-know-about-an-advanced-attack-and-protective-measures-with-stormshield/

Wagner, J. (2017, June 1). *China's Cybersecurity Law: What You Need to Know*. https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/