Old Dominion University

Social Implications of Protecting Critical Infrastructure with Cybersecurity Insurance.

Clarence V. Kimbrell Jr.

CYSE 425W Cyber Strategy and Policy

Professor Lora Pitman

April 10th, 2022

The National Institute of Standards and Technology[1] created a framework in 2014 for national cybersecurity. This frame work is used by thousands of businesses across the United States. It provides a simple understanding of cybersecurity issues and how to prioritize and solve them accordingly. It is broken into five different stages Identify, Protect, Detect, Respond, and finally Recover. Cybersecurity insurance for critical infrastructure uses this framework to conduct analysis to prioritize financial losses. When it comes to cybersecurity insurance it falls under the functions of respond and recover. These two functions are important because cybersecurity insurance for critical infrastructure correlate well with these functions. The financial or information loss in a cyberattacks could be reversed with these functions if used correctly. The National Cybersecurity Framework was updated in twenty sixteen and twenty eighteen to compensate with the rapid increase in cyberattacks worldwide. The United States being the third most cyberattacked country worldwide the respond and recover aspect of the framework is invaluable. Within the framework the functions are defined as the following respond, create and apply accurate endeavors to take actions concerning a detected cyberattack. Recover is defined as create and apply accurate endeavors to maintain plans for resilience and to restore any capabilities or services that were afflicted by a cyberattack.

Social implications of cybersecurity insurance for critical infrastructure are reputational damage, financial loss and legal actions. If given the example such as an energy plant was cyberattacked and it disrupted the distribution of electricity to a neighboring town. The demand for change would be forced upon the business's insurance and defenses by the surrounding population. The trust that has been built the business and the customers will be shattered and struggle to recover for decades to come. If critical infrastructure has weak cybersecurity insurance or none to begin

[1] This is commonly referred to as NIST.

with it could cause a series of devastating events that would harm the surrounding population. Such as millions of U.S. dollars' worth of property and protentional for loss of human life. Cyber security insurance policies for critical infrastructure provides coverage against many losses associated with cyber-induced incidents for example data destruction and theft, extortion, malicious code, denial-of-service attacks, response activities and legal claims. (Young, 2) If any of these cyber-induced incidents occurred on critical infrastructure the amount of financial loss could lead to debt or bankruptcy if not dealt with properly. If there is competition in a designated area with critical infrastructure and ones fall victim to a cyber-attack many of its customers will seek other alternatives if possible. The consumer would have severed its trust in the company and cut ties with its products if possible. So not only will companies have to payout with insurance to subsidize the cost of the attack but will lose income from its consumers. This could lead to a series of substantial financial loss that could even lead to bankruptcy. In the years of twenty seventeen and twenty eighteen a substantial lawsuit was filed and named Warren V. DSG. This is a great example of the social implications of cybersecurity insurance because an individual challenged legal actions against the insurance company. Stating that their information was comprised and had a strong case that took on the insurance company of the business on four different fronts. This is becoming more common as critical infrastructure is a necessity to allow individuals to live comfortably.

The social implications of cybersecurity insurance for critical infrastructure are very in depth. It allows a population of an area to not have to worry about an event that could cause catastrophically devastating effects that could hinder generations to come. There is an increasing amount of cyber-attacks worldwide and it is up to cybersecurity insurance to recover information or equipment damage caused by cyber induced attacks.

References:

AUERSWALD, P., BRANSCOMB, L. M., LA PORTE, T. M., MICHEL-KERJAN, E., & MICHEL-KERJAN, E. (2005). The Challenge of Protecting Critical Infrastructure. *Issues in Science and Technology*, *22*(1), 77–83. http://www.jstor.org/stable/43314287

Collier, S., & Lakoff, A. (2008). The vulnerability of vital systems: How 'critical infrastructure'became a security problem. *The politics of securing the homeland: Critical infrastructure, risk and securitisation*, 40-62.

Karagiannis, G. M., Turksezer, Z. I., Alfieri, L., Feyen, L., & Krausmann, E. (2017). Climate Change and Critical Infrastructure—Floods. *EUR-Scientific and Technical Research Reports, Publications Office of the European Union, Luxembourg*.

Kaspersky, Eugene. "Kaspersky Cyberthreat Real-Time Map." *MAP*, 2 Apr. 2014, https://cybermap.kaspersky.com/.

Plėta, T., Tvaronavičienė, M., Casa, S. D., & Agafonov, K. (2020). Cyber-attacks to critical energy infrastructure and management issues: Overview of selected cases.

Rudkin, Thomas, and Kay Lubwika Bartlett. “Court Ruling Undermines Cybersecurity Compensation Claims.” *Farrer & Co*, Farrer & Co, 10 Sept. 2021, https://www.farrer.co.uk/news-and-insights/court-ruling-undermines-cybersecurity-compensation-claims/.

Young, Derek, et al. “A Framework for Incorporating Insurance in Critical Infrastructure Cyber Risk Strategies.” *International Journal of Critical Infrastructure Protection*, Elsevier, 13 Apr. 2016, https://www.sciencedirect.com/science/article/pii/S1874548216300439?casa_token=oXM2ie1kik0AAAAA%3A9HdKG8aA48v3EndzRVqczNfwkZ5LNg7_WpchrcxjSnbKK8EeuYkUg-_W42shP8f9C9OHRITDbg.