PRIVATE SECTOR AND GOVERNMENT COOPERATION: AN AGENDA FOR IMPROVING THE CYBERSECURITY OF CRITICAL INFRASTRUCTURE

Introduction

CISA defines critical infrastructure as any “physical and cyber systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety” (Infrastructure Security, 1). Currently, the Department of Homeland security has identified 16 different sectors that fall under the category of essential critical infrastructure. These include, but are not limited to, the communications, food and agriculture, transportation, and financial services sectors. Defending these sectors is of paramount importance to the security of the United States. However, given the unique properties of cyberspace, protecting critical infrastructure is becoming increasingly difficult. The convergence of information technology systems and their dependence on the internet make critical infrastructure systems more accessible and expand their attack surface. The difficulty in attributing a cyberattack to a particular malicious actor makes deterrence and punishment difficult to carry out. The wider availability of cyber hacking tools and their lower barriers for entry make cyberattacks easier to perform and increase their frequency. (Lewis 2014, 166). As an example, in May 2021, Colonial Pipeline was the victim of a ransomware attack which caused gas shortages and increased gas prices on the east coast. Gasoline stockpiles dropped, four states declared a state of emergency, and Colonial Pipeline suffered huge reputational damage (Eaton and Volz 2021, 2). This incident illustrates the far-reaching harm that can occur when critical infrastructure is the target of a cyberattack.

Current Policy Practices

Broadly speaking, the U.S. government has adopted a voluntary, nonregulatory, incentive-based framework for protecting the information systems of critical infrastructure sectors. Companies that operate in this space are encouraged to join CISA, an information sharing program where private companies exchange cyber threat indicators and defensive measures with the federal government. CISA participants are incentivized to join by receiving limited liability protection, antitrust exemptions, and exemptions from federal and state disclosure laws. Companies are also encouraged to adopt the NIST Cybersecurity Framework, which provides "industry best practices and methods for cybersecurity risk management" (Questions and Answers 2022). So far, this voluntary strategy has worked well at encouraging private sector critical infrastructure companies to improve their cybersecurity, particularly because it sidesteps the bureaucratic process of legislation. However, this approach has its limitations since it relies on well-established incentives as a substitute for mandatory guidelines in order to motivate companies. Should these incentives prove insufficient or should trust on federal information sharing programs be eroded, there are few penalties for companies neglecting their cybersecurity. What follows is a realistically adoptable agenda for improving the cybersecurity of critical infrastructure that takes into account the current incentive-based relationship between the government and private sectors.

A Jumble of Incentives

One must first understand the various incentives at play for both stakeholders and attackers. More importantly, we must consider these incentives as a whole, not just from the point of view of individual participants. While everyone may be acting in their best self-interest, the interaction between these incentives can create feedback loops that ultimately result in reduced cybersecurity. For instance, companies care a great deal about their public image and are therefore incentivized to protect it. This encourages companies to not disclose cyberattacks and deal with them behind closed doors. The disclosure exemptions and liability protections that CISA offers address these concerns. However, they also inhibit the natural feedback loop of reputational damage motivating companies to improve their cybersecurity measures. If a critical infrastructure business suffers a data breach but they aren't required to disclose it because the data was encrypted (The Definitive Guide 2018, 8), how can the general public know not to trust that business?

In general, there are three incentive categories that can be used to cohesively improve cybersecurity in the critical infrastructure space: economic, social, and moral incentives. (Mariani et al. 2022, 8)

Economic Incentives: Businesses that operate on small profit margins are incentivized to cut costs wherever possible. This can lead businesses to avoid spending too much on their cybersecurity and ultimately become the victims of ransomware attacks or data breaches. In light of this, market pressures can be used to prevent these negative externalities from being offloaded onto the public. A good starting point could be the widespread adoption of cyber insurance. While cyber insurance is still in its infancy and has issues ranging from the difficulty of quantifying cyber risk to "moral hazards" (Porup 2018, 6), it's still a useful source of economic incentives. Specifically, cyber insurance with premiums that go up in proportion to the damage caused by a cyberattack will incentivize critical infrastructure businesses to invest more in cybersecurity.

Another economic incentive, this one inspired by the critical infrastructure section of the Cybersecurity Act of 2012, would be to promote a minimum baseline of cybersecurity or face fines. By adhering to basic “performance requirements” (Cybersecurity Act, 2012, 1), businesses in critical infrastructure would need to ensure they comply with basic cybersecurity standards. This single piece of legislation would of course require action from Congress. However, given the nonpartisan nature of national security and the focused target of this proposed legislation, it shouldn’t be too difficult for it to pass.

Social Incentives: The two most basic types of social pressures are public shaming and showcasing of good examples. A great way of making the adoption of the NIST Cybersecurity Framework more commonplace is by publicly recognizing companies that do so. While NIST does share “success stories that demonstrate real-world application and benefits of the Framework”, they currently don’t “offer certifications or endorsements of Cybersecurity Framework implementations” (Questions and Answers 2022). Even though NIST isn’t a regulatory body, their power as a ubiquitous standards organization should be leveraged to encourage good practices. Should NIST issue certificates of Framework implementation, the government may give preferential treatment to critical infrastructure companies that abide by the Framework.

Moral Incentives: Public opinion and moral trends can have an impact on the behavior of companies. For example, the rise in awareness towards a need for privacy has created a demand for privacy-conscious messaging apps in the last several years. Thus, public opinion can be swayed towards placing importance on cybersecurity. This can be done by not hiding the bad news of a cyberattack and raising awareness on the effects data breaches have on the general public. From the point of view of companies, information sharing programs such as CISA should encourage companies to understand their place in protecting critical infrastructure. The use of table-top exercises with other companies operating in the same critical infrastructure sector can help their employees understand the criticalness of their business. As such, the role of CISA should expand to include information sharing on cyberattacks through public channels and foster company-to-company communications for the critical sectors.

Loose Ends

Of notable exception from the definition of critical infrastructure are “commercial information technology products or consumer information technology services” (Obama 2013, 6). Dubbed the “Google Exception”, this definition excludes commercial technology companies from being considered critical infrastructure. While it may seem reasonable to exclude them in the interest of promoting innovation and competition, the widespread dependance on technologies such as Google’s G Suite or Amazon’s AWS should qualify them as critical infrastructure. Many businesses rely on these services to the extent that a debilitating cyberattack to any of these companies would result in large economic damage. Given that Information Technologies are part of the 16 essential critical infrastructure sectors identified by the Department of Defense, this exception should be closed (potentially through the use of another Executive Order) in order to bring more cohesion to the definition of critical infrastructure. Furthermore, while the definition of critical infrastructure is broad enough to encompass a wide range of sectors, periodic review of what is considered critical should take place on a yearly basis. Proposed in this agenda is the addition of Democratic Institutions. Seeing that foreign powers have a vested interest in interfering with U.S. elections (Nakashima et al. 2018, 1) and the wide-reaching effects this could have, Democratic Institutions, including the governing bodies of political parties, should be considered critical infrastructure.

If we are to fully embrace the American way of promoting cybersecurity, namely through lax regulation and strong incentives, it's time to untangle the web of incentives currently in place. Even though it can be difficult to pass regulation, at a minimum, it should be used to set a basic bar of security measures for critical infrastructure. Outlined in this agenda are tangible ways of improving cyber hygiene through a more coordinated and aligned set of incentives. Given the tremendous risk that cyberattacks pose on critical infrastructure, adopting a comprehensive and consistent framework is of utmost importance in defending the nation's government and assets.

References

[1] Eaton, Collin, and Dustin Volz. 2021. "Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom." *The Wall Street Journal*. Dow Jones & Company. May 19. https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636.

[2] "Infrastructure Security." 2022. *Cybersecurity and Infrastructure Security Agency CISA*. Accessed November 25. https://www.cisa.gov/infrastructure-security.

[3] Lewis, Ted G. 2014. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. New York: John Wiley & Sons, Incorporated. Accessed November 23, 2022. ProQuest Ebook Central.

[4] Mariani, Joe, Tim Li, Chris Weggeman, and Pankaj Kamleshkumar Kishnani. "Incentives Are Key to Breaking the Cycle of Cyberattacks on Critical Infrastructure." Deloitte Insights.

Deloitte, June 20, 2022. https://www2.deloitte.com/us/en/insights/industry/public-sector/cyberattack-critical-infrastructure-cybersecurity.html.

[5] Nakashima, Ellen, and Shane Harris. "How the Russians Hacked the DNC and Passed Its Emails to WikiLeaks." The Washington Post. WP Company, July 14, 2018. https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html.

[6] Obama, Barack. "Executive Order -- Improving Critical Infrastructure Cybersecurity." National Archives and Records Administration. National Archives and Records Administration. February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[7] Porup, J.M., "Does Cyber insurance make us more (or less) secure?" CSO. IDG Communications, June 18, 2018. https://www.csoonline.com/article/3280990/does-cyber-insurance-make-us-more-or-less-secure.html.

[8] "Questions and Answers." 2022. *NIST Cybersecurity Framework*. September 8. https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics#framework.

[9] "The Cybersecurity Act of 2012." 2012. *U.S. Senate Committee on Homeland Security & Governmental Affairs.* Accessed November 26. https://www.hsgac.senate.gov/imo/media/doc/CYBER%20summary%20Final%20-%202-13%206pm%20-FINAL1.pdf

[10] "The Definitive Guide to U.S. State Data Breach Laws." n.d. Digitalguardian.com. 2018. https://info.digitalguardian.com/rs/768-OQW-145/images/the-definitive-guide-to-us-state-data-breach-laws.pdf.