Student Papers in Public Policy

Volume 3 | Issue 1 Article 4

Lack of Cybersecurity in the United States' Critical Infrastructure

Dean Santos
Purdue University, santos57@purdue.edu

Jonathan Kovacev
Purdue University, jkovacev@purdue.edu

Kinsey Larson
Purdue University, larso101@purdue.edu

Lack of Cybersecurity in the United States' Critical Infrastructure

Dean Santos, Jonathan Kovacev, & Kinsey Larson | Purdue University

HONR 399: *Security, Technology, and Society* | Spring 2021

Instructors: Dr. Dwaine Jengelley (Honors College) & Dr. L. Allison Roberts (PPRI)

Introduction

Technology has revolutionized the nature of information, remote control, and communication itself, but it has also brought with it tangible dangers. Top minds in the United States, as well as the rest of the world, have seen those dangers and dedicated their work to mitigate them, developing the ideas and policies necessary to protect the nation from those dangers, and yet the actual implementation of safety measures within the nation lags behind.

In the meantime, as U.S. critical infrastructure remains woefully unprotected, the nation opens itself up to a plethora of cyber-attacks. These attacks can cause damage in many ways. There are the obvious, tangible effects like costing trillions of dollars [1], poisoning water supplies to cause illness [2], or causing power outages [3], but we must also consider more subtle, social damages caused as well, such as losing trust, questioning the legitimacy of polling machines, or losing a sense of security in general. Regardless of the damage caused, it is clear that these attacks cannot be allowed to continue, and the United States already has a number of policies and strategies in place to defend itself and its critical infrastructure. However, despite being theoretically applicable and effective, the nation routinely sees them go unimplemented even as preventable attacks repeatedly succeed.

What is it about the current U.S. policy that leaves it so vulnerable, and how can it be remedied? This brief addresses the question and offers a recommendation.

Current Policy

Cybersecurity and Infrastructure Security Agency (CISA)

The first piece of active policy highlighted is the newly formed Cybersecurity and Infrastructure Security Agency (CISA). Created in 2018, it works to secure the nation's critical infrastructure from cybersecurity threats by researching solutions to possible threats,

offering penetration testing to identify existing vulnerabilities and issuing cybersecurity directives [4]. Having a singular agency in charge of securing the United States' critical infrastructure streamlines the process of creating new security measures, implementing those measures, and responding to active threats when compared to giving the task to the Department of Homeland Security or the Central Intelligence Agency, both of which must also manage other responsibilities as well [5]. CISA's existence was proven to be a great benefit to the nation's cybersecurity in its first two years, but CISA could be doing much more than it is currently.

Process 1: Air Gapping

Air gapping is a process when a network of computers is completely disconnected from all other networks. Without outside network connections, it becomes impossible to hack a computer remotely, which is how the vast majority of cyberattacks are conducted. A cyberattack, especially one from another nation, becomes significantly more difficult to conduct if the attacker must be physically present in the facility. It is a functionally simple solution to what appears to be a complex problem.

There are numerous other individual policies equally varied in efficacy, application, and complexity; these just demonstrate the width of the scale

Process 2: Cybersecurity Engineering (CSE)

The second process is called Cybersecurity Engineering (CSE) and seeks to form a top-to-bottom security seal on an entire system, including all its component parts, from manufacturing and coding to operation. It is a more rigorous process that would require the government to have access to every level of production used in creating the infrastructure used in the sector, but the CSE philosophy creates functionally impenetrable systems. It can also be implemented more modularly as needed, securing specific, vulnerable components instead of entire systems, though with the modularity the completeness of the seal would be lost. All in all, it is a relatively high complexity solution that potentially offers more complete security in all situations.

Risks and Benefits

There are significantly more benefits than risks when it comes to employing cybersecurity systems. The majority of concerns lie in ethical considerations, over-reliance of the integrity of systems, and access to vital information. National cybersecurity has access to invaluable amounts of private data and business information that has been entrusted to it, a sacrifice that individuals make which comes with trusting that those people who are in charge of protecting data do not abuse their power. Additionally, failures in cybersecurity may go unnoticed for months or years, leading to massive loss of money and data while the security failure remains on other systems [6].

Sacrifices that exist are ultimately necessary ones compared to alternative of remaining undefended

Cybersecurity protects both the private and public sectors from threats intended to obtain vital information, disrupt communications, and destroy infrastructure. Governmental cyberattacks are being thwarted by the emergence of improved engineering techniques that employ secure devices, trusted suppliers and code with limited flaws. Public information and infrastructure are becoming more secure as prime targets, such as water purification systems and business revenues, are taking a priority in national defense [2]. As time goes on, systems are becoming increasingly secure at a rate that threatens cyber attackers, but there will always be more risks to cover and methods that bad actors will use to access various parts of a system. The ever-vigilant design of systems must allow for future changes and last as long as possible to ensure security for the

lifetime of the system. These systems save the country hundreds of millions of dollars every year, but failures still lead to massive losses that still need to be mitigated [1].

Ethical Considerations and Counterattacks

In an ethical review of cybersecurity, the authors considered a number of approaches to ethics, as ethicality is by no means a singular and obvious thing. For this, we consider the following three common approaches to determining ethicality: consequentialist ethics, non-consequentialist ethics, and agent-centered ethics [7]. Regardless of which of those approaches we choose to take, protecting food, energy, healthcare, and water (examples of critical infrastructure sectors according to CISA) [8], with any purely defensive policy would certainly be heralded highly by all approaches alike. Those sectors, in particular, are generally considered necessities or near necessities, and protecting them with no intent to harm the attacker would mean there is little to argue with. Other sectors with more questionable things to protect, while probably still supererogatory in the end for most, have much more to contend with as the thing being protected is itself ethically questionable, which makes the ethics of defending it more questionable.

The ethicality of certain options can be unclear when organizations start considering whether offensive measures need to be put in place, such as a counterattack. A counterattack is when an organization's systems are taken down by hacking them. This may be deemed necessary if an organization is under constant attack, so unless they take down the root cause of the attacks, the organization will be in constant danger. However, if it is possible to make the nation's critical infrastructure impregnable, then we need not worry about the ethics of a counterattack since there will never be any damage to use as justification to counterattack with. We thus conclude that cybersecurity as a whole should be considered as ethically sound, if not mandatory, depending on the philosophy to which one subscribes.

Any ethical sacrifices that may exist are ultimately outweighed

Costs

The obligatory nature of cybersecurity would mean that most costs are acceptable, so long as two things hold: (1) that the cost of security is less than the cost of damages and (2) that the cost is not so exorbitant that it detracts from the ability to provide obligatory services elsewhere. The costs can be put into three categories: monetary, privacy, and convenience. Monetarily speaking, Information Technology specialists predict cybersecurity funding will surpass $1 trillion over the next five years. However, projections for damage by cyberattacks are expected to be $6 trillion for 2021 with the average cost of a data breach of $3.86 million and taking 191 days to identify breaches [1].

Expensive, but less expensive than being attacked

Another cybersecurity cost is the loss of privacy and anonymity of people when they are online. While giving up a little bit of privacy for a large increase in security seems like a good deal, many people believe that government increasing online security could be problematic and fear that their privacy rights will be affected by people "watching" what they do on the internet. Another frequently acknowledged cost to cybersecurity is the social cost of convenience. Similar to the tradeoff between security and privacy, there is a tradeoff between security and convenience regardless of if that security is cyber or otherwise. The more secure something is, the more troublesome it becomes to operate it normally. The exact cost of widespread cybersecurity tends to be difficult to measure exactly

since it depends heavily on what policies get implemented where; in general, however, it is clear that the cost of an attack will far outweigh the cost of security.

Policy Recommendation

CISA needs to step forward and begin actively and forcefully managing the nation's cybersecurity. CISA already operates with the mission to mitigate risk to the nation's critical infrastructure, and the change in role would not require a very large change in terms of the powers it has been granted, as they are already capable of issuing mandates [9]. In essence, the United States government would have CISA execute the tasks it has done since its creation in 2018, but simply act more forcefully, requiring that all critical infrastructure be made secure instead of simply aiding those who want it. We are tempted to prescribe specific policies to specific sectors with specific timeframes, but such an approach lacks a certain nuance that must exist in the implementation of cybersecurity nationwide.

CISA appears to be in the prime position to take the lead in providing immediate, short-term solutions to stop existing defensive failures while having the expertise to manage the future of cybersecurity.

Conclusion

The problem the nation's cybersecurity faces is not a lack of ideas, it is a lack of urgency. The United States has in place organizations like CISA to manage the cybersecurity of critical infrastructure sectors as well numerous ways to create security through techniques, such as air gapping and CSE. When installed properly, these measures can be cost effective as well as functional, and yet they remain unimplemented. As individuals, we lack the ability to influence change ourselves, so we must rely on—and advocate for—CISA to step forward and forcibly effect those changes in our stead. As a collective, we can provide the impetus that the urgent changes the United States' cybersecurity situation deserves.

References

[1] "2021 Cyber Security Statistics: The Ultimate List of Stats, Data & Trends." Purplesec. [Online]. https://purplesec.us/resources/cyber-security-statistics/ (accessed March 30, 2021).

[2] K. Collier. "Lye-poisoning attack in Florida shows cybersecurity gaps in water systems." NBC News. [Online]. https://www.nbcnews.com/tech/security/lye-poisoning-attack-florida-shows-cybersecurity-gaps-water-systems-n1257173 (accessed February 14, 2021).

[3] BBC News. "US and Russia clash over power grid 'hack attacks'." BBC News. [Online]. https://www.bbc.com/news/technology-48675203 (accessed February 14, 2021).

[4] U.S. Department of Homeland Security. "Cybersecurity." Homeland Security. [Online]. https://www.dhs.gov/topic/cybersecurity (accessed March 2, 2021).

[5] Cybersecurity and Infrastructure Security Agency. "About CISA." CISA. [Online]. https://cyber.dhs.gov/directives/ (accessed March 2, 2021).

[6] S. McGraw (2020). "What Is Cybersecurity Engineering and Why Do I Need It?" Carnegie Mellon University. [Online]. https://www.youtube.com/watch?v=J1G_n6TDL4Y.

[7] S. Bonde and P. Firenze. "A Framework for Making Ethical Decisions." Brown University. [Online]. https://www.brown.edu/academics/science-and-technology-studies/framework-making-ethical-decisions (accessed March 16, 2021).

[8] Cybersecurity and Infrastructure Security Agency. "Critical Infrastructure Sectors." CISA. [Online]. https://www.cisa.gov/critical-infrastructure-sectors (accessed March 03, 2021).

[9] U.S. Department of Homeland Security. "Cybersecurity Directives." DHS.gov. [Online]. https://cyber.dhs.gov/directives/ (accessed March 03, 2021).