Private Sector Compliance with Federal Cybersecurity Requirements

KELLEN CARLETON

The cybersecurity of our critical infrastructure impacts almost every aspect of our daily lives. The 2017 National Security Strategy states that “cyberattacks offer adversaries opportunities to seriously damage or disrupt critical infrastructure, cripple American businesses, weaken our Federal networks, and attack the tools and devices that Americans use every day to communicate and conduct business.” Protecting networks, data, and intellectual property means protecting the things that give the United States its vast and unique competitive advantage as a nation compared to its enemies.

Why are some companies better able to comply with cybersecurity requirements than others? This question has several layers and implications for both the academic and public policy communities. Understanding compliance with cybersecurity requirements can help policymakers adjust federal policy to more accurately and effectively govern the cybersecurity of critical infrastructure.

One of the most important sectors of critical infrastructure is the Defense Industrial Base (DIB), defined by the Department of Homeland Security (DHS) as the “worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet [US] military requirements.” The DIB provides products and services that are essential to “mobilize, deploy, and sustain military operations.” The Defense Industrial Base is a useful case study to examine how the private sector interacts with federal cybersecurity requirements.

Throughout this study, several hypotheses were used to test the research question. My first hypothesis is that there is a clear link from policy cohesion to compliance and a clear link from compliance to security. If policy is not cohesive and clear, then intuitively, it will be difficult to follow. If policy is cohesive, then compliance becomes easier and security also improves drastically.

The second hypothesis is that the primary driver for noncompliance is that federal cybersecurity policy is ineffective. Private companies will not comply with federal policy if it is ineffective. The White House, National Security Strategy of the United States of America, (December 2017) https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.


Kellen Carleton graduated with a BS in Policy and Management in 2018 and an MS in International Relations and Politics in 2019. During his time at CMU, he was a member of Sigma Alpha Epsilon, serving on the executive board in several positions. He was also President of the Club Hockey Team. His internships include work in the US Senate during the Washington Semester Program as well as research in cybersecurity. He currently works for Accenture as a Security Analyst.
not successful in prevention and mitigation. One sub-hypothesis for the second hypothesis is that the cost of cybersecurity regulations and policies are a primary driver of noncompliance. Another sub-hypothesis for the second hypothesis is that a perception of the effectiveness of the policy is important to compliance as well. There is a slight difference between the idea of actual policy effectiveness and perceived policy effectiveness. They are intertwined, but perception is also a significant aspect of compliance.

A third hypothesis is that the private sector believes that they can and should be doing this on their own. This speaks to the overall disconnect between the public and private sectors. The relationship is in a precarious place right now. There is deep mistrust as hinted before. Both the government and the private sector want the relationship to work in their favor.

To investigate the case study of the Defense Industrial Base (DIB), interviews were conducted with cyber professionals. In order to have a truly representative sample of all of the relevant perspectives, a wide range of people would need to be interviewed. The key stakeholders in this problem are the following types of people: government employees, think tank and academic researchers, and private sector cybersecurity officials. Throughout the interviews, there were a couple of claims that were agreed upon and were relatively straight forward in their explanations.

The DIB is a unique slice of critical infrastructure because of the mission they are tasked with. Collectively, they create many of the weapons and systems for the US military. A senior cyber researcher remarked that “the DIB, out of all of the critical infrastructures, is the most targeted. They have the most to lose and they are very vulnerable to an attack because of that. The current policy is not effective for the current level of threat.”

The idea that DIB cybersecurity was a major national security risk was agreed upon by everyone that was interviewed. A former US Attorney stated that “cybersecurity is growing into one of the single greatest threats to the United States.” A senior think tank engineer echoed a similar sentiment. “Intelligence and data are exploited every day. Hacks are happening to everyone on a daily basis, it is just a matter of how bad it was. The DIB is a specific risk because they create our weapons systems and equipment for our armed forces.” The respondents also collectively felt that it was only a matter of time until the rest of the country begins to fully understand the pervasiveness of this threat.

The rest of the interviews were based around four major sets of claims that pertain to the hypotheses. The first claim was that current policy is not cohesive. The second set of claims pertained to reasons for noncompliance. The third claim surrounded the importance of perception in cybersecurity policy and how that differs from policy itself. Perception of the policy and the actual policy are distinct, and each is important in this area. The fourth claim surrounds the relationship between the public and private sectors and that in order for any improvement in this area, that relationship must improve.

Current cybersecurity policy and regulations are not cohesive. The policy is disjointed and

---

5 Interview with Senior Cyber Researcher, March 20, 2019.
7 Interview with senior think tank engineer, March 4, 2019.
needs to be reformed. If there are multiple policies, they need to work together in an intuitive way; if there is one policy, it needs to be both cohesive and robust. The main question that was asked to test this idea was to assess if the interview respondents viewed current policy in a positive light and found it clear and easy to follow.

Nine of the ten respondents agreed that the current policy was not clear and easy to understand. A former senior DHS official said that “the overall policy is not quite there yet. It is improving and people are working every day to ensure that the policy space as a whole becomes better. However, it is not fully there yet.” Many believe that the policy is becoming better as we learn more about cybersecurity and how to both defend it and regulate it properly. Others shared perspectives on prioritization, saying that “the current cyber policy needs more clarity from the government on what to prioritize.”

There were three major reasons for noncompliance: cost, ineffectiveness, and the fact that policies were difficult to follow. While eight of the ten respondents agreed that cost was the biggest barrier to compliance with federal cybersecurity requirements, it was not as simple as that. Many pointed to other reasons that were of equal importance or were also major contributing factors.

Ultimately, cost is what the private sector will fixate on, but the other issues of ineffectiveness and the fact that policies are difficult to follow are also important factors. A former FBI Special Agent said that “usually cost is the biggest issue in compliance. Coupled with cost, there is also some credence to the idea that people are unsure of what will be effective, so they do not want to spend on something that is not proven to be successful.” Regulations are expensive to implement and maintain, and cybersecurity regulations and compliance structures are among the most expensive to implement and maintain.

The private sector argues that most regulations are ineffective and not worth the investment. Because there is no standard to assessing cybersecurity efficacy, then it is really a perception problem that is causing the idea that government cybersecurity regulations will be ineffective. This perception factor reveals a larger public-private disconnect, but it is mainly about how the private sector views the policy as ineffective, disjointed, and too costly. Changing this narrative will be a major challenge for the public-private relationship to improve. A common thread from many interviews was that there is so much uncertainty that exists in this field. People are unsure of what to do, what is effective, and how to measure success.

The relationship between the public and private sectors is the crux of the problem in critical infrastructure cybersecurity. These two entities must align their goals and foster a better working relationship. They need each other, and each side is an important piece of this conversation. There are a few facets of note here: talent disparity, agility of organization, organizational goals, and structure. As stated before, the relationship is in a precarious place, and neither side wants to give concessions in terms of information sharing.

On the changing nature of the relationship, a senior think tank political scientist stated that

---

8 Interview with former DHS official, March 11, 2019.
9 Interview, March 20, 2019.
10 Interview with former FBI special agent, March 16, 2019.
“the issue today is that the government and the private sector have never been so intertwined and dependent on each other. Now they will be forced to work together, even though they do not necessarily want to.”12 This reluctance to work together is a major problem in this issue, and is one that must improve. Most respondents strongly reiterated the importance of the government in this equation, stating that “[the private sector] needs to realize that they cannot do this themselves. They may believe they are better equipped to do this, which they may be, but the government must have a piece of this. The interests are different, and they need to find a way to bridge that gap.”13

One last area that was common throughout the interviews was the idea that accountability and enforcement must vastly improve in order for critical infrastructure cybersecurity to improve. Eight of the ten respondents believed that more enforcement capabilities were needed for federal agencies to hold those accountable who continue to breach the systems of private companies and the government. When asked about enforcement capabilities of the federal government, a think tank cyber researcher stated that “more enforcement capability is needed. New laws and regulations will have to be crafted just for this. There is enough uniqueness about cybersecurity that we don't have enough to apply current and existing laws to this problem.”14 As jurisdiction over the cyber domain becomes clearer, the enforcement capabilities of those oversight agencies also need to become clearer.

Last, these findings from the interview process were able to yield a framework that can be applied to improvements in policymaking. Four major steps were identified: standardizing definitions, clarifying and crafting new policy, prescribing clear implementation strategies, and driving international legal standards. This study recommends using these findings to execute a policy framework that can serve as an iterative process to continually improve critical infrastructure cybersecurity.

12 Interview with senior think tank political scientist, March 13, 2019.
13 Interviews with cybersecurity practitioners, March-April 2019.
14 Interview with think tank cyber researcher, March 15, 2019.