General Review of the National Cybersecurity Strategy

Tyler Walker

Old Dominion University

CYSE 525

Professor Hamza Demirel

11/01/2024

Introduction

The National Cybersecurity Strategy released in March 2023 tries to take on something that honestly feels bigger every year: the growing mess of cyber threats surrounding everything we do online. With how much of our daily lives run through digital systems now, like banking, healthcare, and other utilities, it's not surprising that the government is trying to rethink who should actually be responsible for protecting all of this. What stood out to me right away was the strategy's push to shift responsibility away from everyday users and small businesses and toward the people and organizations that actually have the tools, budget, and expertise to defend against major cyber risks (White House, 2023). Honestly, that makes sense. Expecting individuals to keep up with nation-state attackers just doesn't feel realistic anymore.

Overview

The strategy lays everything out through five main pillars: defending critical infrastructure, disrupting and dismantling threat actors, shaping market forces, investing in long-term resilience, and working closely with international partners (CAI, 2023). It's a lot, but seeing all of it together gives the impression that cybersecurity can't just be one thing, it has to be a whole system that works from multiple angles at once. I found myself appreciating how balanced it is. Some parts deal with the "right now" threats, while others try to prepare the U.S. for what's coming later.

Defending Critical Infrastructure

The first pillar, defending critical infrastructure, feels like the foundation. Energy grids, water systems, hospitals, these are the systems we don't really think about but absolutely rely on. The strategy talks a lot about strengthening partnerships between public and private sectors and encouraging frameworks like NIST to help organizations understand their risks better (White House, 2023). When I read this section, it reminded me how fragile these systems can be, and how important it is that organizations communicate with each other before something bad happens, not just after.

Disrupting and Dismantling Threat Actors

The second major pillar focuses on taking the fight to cybercriminals and state-sponsored groups instead of always playing defense. I liked this part because it feels more realistic about how determined some attackers are. The strategy emphasizes identifying, disrupting, and even prosecuting threat actors when possible. With agencies like CISA and the NSA involved, plus support from international partners, the U.S. wants to make it genuinely harder for attackers to operate. It's basically raising the cost for anyone thinking about launching an attack.

Shaping Economic Incentives and Strengthening International Cooperation

Another interesting part is how the strategy tries to reshape economic incentives. Instead of punishing organizations after a breach, it pushes the idea that companies should be rewarded for doing cybersecurity the right way. International cooperation also plays a big role because cyberattacks obviously don't stay inside one country's borders.

Conclusion

This strategy feels like a step in the right direction. It doesn’t claim to magically fix everything overnight, but it sets a long-term direction that treats cybersecurity as something shared. As threats change, it seems like the only practical way to move forward is to have a plan that includes resilience, working together, and punishing attackers. What I took away most from reading it is that the country can’t afford to be reactive anymore. The plan is clear about the fact that cyber threats are getting more complicated, better organized, and more connected to everyday life. The U.S. is striving to develop a cybersecurity base that will last by focusing on better infrastructure, greater coordination, and wiser incentives. It's not ideal, but it seems like a good place to start to keep everything we depend on in the digital world safe.

References

CAI. (2023). Summary of 2023 National Cybersecurity Strategy. Retrieved from https://www.cai.io/.../summary-of-2023-national-cyberse…

White House. (2023). National Cybersecurity Strategy. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf