Political Implications of Information Systems Security Policies

Samantha Riggs

Old Dominion University

CYSE 425W: Cyber Strategy and Policy

Dr. Shideh Yavary Mehr

June 16th, 2025

The very quick progression of technology as a whole since the 1970's has changed and modified our society at almost all levels. National and world politics are no exception to this as cybersecurity attacks have every potential to be politically motivated just as much as ones that are financially motivated. Cyber incidents have come to hold a prominent position in national and international security (Cavelty & Wenger, 2019). In order to adapt to the growing and rapid progression of cyberspace, including cyber threats, the federal government has made an effort to address security concerns by creating new or modifying preexisting laws and policies in order. The creation of these policies and establishment of them can sometimes be difficult to put into place because, as Beyer describes people's perspectives on cybersecurity are often defined by where they "sit" professionally (2023). However, given this hurdle of potential differing opinions, the notion that cybersecurity measures are required in order to ensure online safety on a national level is, more often than not, agreed upon.

When it comes to security policy concerning information systems, more often than not the private sector comes to mind before federal implementation. However, there are national cybersecurity guidelines like the CIA Triad and the NIST's Cybersecurity Framework that aim to provide guidelines and protect citizens from potential cyber threats. These are provided by the federal government not only for their own organizations and agencies to use but also are adaptable to any size of business as well. At the Cybersecurity and Consumer Protection Summit in 2015 at Stanford University, President Barack Obama stated gave this quote: "There's only one way to defend America from these cyber threats, and that is through government and industry working together, sharing appropriate information as true partners." This statement makes note of the importance of collaboration between a nation and its citizens, especially in today's modern digital world.

However, there are some significant challenges that come with cybersecurity and digital privacy legislation. One of the most noticeable of these challenges is simply attempting to keep up with the high rate at which technology is developing (Sumartono, et.al, 2024). Keeping up with cybersecurity within any system is difficult since just as quick as vulnerabilities are patched in a system can a new one be exploited. This makes the passing of effective laws or policies difficult, since they are the result of a relatively long process. What was an effective method when a bill was written could potentially be obsolete once it gets passed and signed executively. This is not to say that all federal legislation is obsolete and ineffective. There are integral laws like the Federal Information Security Management Act which mandates comprehensive information security programs for federal agencies and the Cyber Incident Reporting for Critical Infrastructure Act which requires and sets a streamlined path for critical infrastructure entities to report incidents. These more broad, all-encompassing laws, along with more targeted regulations like the Health Insurance Portability and Accountability Act (HIPPA), provides a strong national standpoint on the importance of protecting digital spaces.

References

Beyer, J. L. (2023). The politics of cybersecurity and the global internet. *Perspectives on Politics*, *21*(2), 664–668. https://doi.org/10.1017/s1537592723000361

Cavelty, M., & Wenger, A. (2019). Cyber Security Meets Security Politics: Complex Technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

National Archives and Records Administration. (n.d.). *Remarks by the president at the Cybersecurity and consumer protection summit*. National Archives and Records Administration. https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit

Sumartono, E., Harliyanto, R., Situmeang, S. M. T., Siagian, D. S., & Septaria, E. (2024). The legal implications of Data Privacy Laws, cybersecurity regulations, and Ai Ethics in a Digital Society. *The Journal of Academic Science*, *1*(2). https://doi.org/10.59613/29qypw51