Marcus Sowers

Old Dominion University

CYSE 406 – Cyber Law

4/7/22

Writing Assignment #2

I am currently a legislative research aide for U.S. House of Representative member Tito Canduit in the 26th District of Virginia, who is facing a contested reelection bid in the fall of 2022. This reelection bid, Rep. Canduit wants to show the voters his commitment to enacting proposed laws or highlighting existing legislation that protects the American people from all different kinds of cybersecurity threats. With the plans to roll out a series of letters to constituents about proposed or existing laws designed to strengthen cybersecurity in the U.S, this background research memo will discuss and go into detail of the "Hack Your State Department Act." This was one of the first cybersecurity bill measures passed by the House during the 116th Congress.

The "Hack Your State Department Act" passed House on January 22nd, 2019. This bill requires the "Department of State to design, establish, and make publicly known a Vulnerability Disclosure Process to improve cybersecurity" (H.R.328). Within this Vulnerability Disclosure Process, the State Department has a few jobs it must complete. One of the jobs the State Department must do is identify which information technology should be included. They must also determine whether the process should differentiate among and specify the types of security vulnerabilities that may be targeted. Lastly, with the steps taken they must also provide an available form and a consistent ability to report. This specific bill also requires the Department of

State to “establish a bug bounty pilot program, where an approved individual, organization, or company is temporarily authorized to identify and report vulnerabilities of internet-facing information technology of the State Department in exchange for compensation” (H.R.328). With this being stated, this Act is basically the law passed to establish protection against cyberattacks within the State Department. This Act forces the State Department to provide annual reports of potential security vulnerabilities as well as previous unidentified vulnerabilities that may be a result of the bug bounty program used. This allows for the State Department to be fully aware of any threats or potential bugs that may affect them by the help of this program.

The “Hack Your State Department Act” is technically not trying to fix a law, but a continuously growing problem. Cyber threats and attacks are continuously evolving and growing in today’s cyberworld. Access to the internet and technology is becoming much easier, creating a serious problem for people and organizations who need their stored information fully protected. Some potential background and context that may help understand the creation of this Act is the current events that is repeatedly happening as time passes. The current event that’ll be discussed in this background research memo is when the State Department phones were hacked with NSO Group spyware. In December of 2021, US State Department employees who were serving in Africa were hacked with spyware developed by Israeli technology firm NSO Group in the previous months. The hacks targeted “11 employees of the U.S. Embassy in Uganda, including both foreign service officers, all of whom are U.S. citizens and local staff” (Joe Walsh). This is a great example of why this Law was passed, to help possibly prevent and stop scenarios like this from happening. This was a huge concern because the State Department contains tons of international information, data, and intelligence. When this event happened, a National Security Council spokesperson said that the Biden Administration was “acutely concerned that commercial spyware like NSO Group’s software poses a serious counterintelligence and security risk to U.S. personnel” (Joe Walsh). This event unfortunately happened after the law was passed, creating uncertainty for the belief if this Act is actually efficient or not.

Does the law fix the current problems happening today? It has been proven to not be 100% efficient in fixing protection against cyberattacks within the State Department. If this specific law can the law be improved, how could that be done? There are always techniques to improve the bug bounty program with continuous updates and increase time of use but cyberattacks will always continue to be a threat. This law is important to highlight because the more people are aware of these threats, the more knowledgeable they will be to prevent and possible completely stop these attacks while improving the security. This memo discuss that this Act was enacted into law, summarized the law as thoroughly as possible, described the problem, how to fix the problem, and helpful background information.

Work Cited

H.R.328 - 116th Congress (2019-2020): Hack Your State ... https://www.congress.gov/bill/116th-congress/house-bill/328/.

Walsh, Joe. "State Department Workers' Phones Reportedly Hacked Using NSO Group Software." *Forbes*, Forbes Magazine, 4 Dec. 2021, https://www.forbes.com/sites/joewalsh/2021/12/03/state-department-workers-phones-reportedly-hacked-using-nso-group-software?sh=14fedfb511c6.