ISM ORIGINAL WORK SET-UP & COMPLETION SUMMARY

MANAV SOOD, AKASH BASKARAN

Objective/Purpose:

The advent of ever-advancing technology and increased accessibility to network technologies has inevitably made way for the massive growth of the Internet of Things that the world is experiencing today. Each day, ordinary appliances such as stereos, thermostats, microwaves, even water bottles are being made with the technological capacity of being managed remotely through a user's smartphone. However, the growth of in-band, or internet-connected, devices has brought with it hosts of vulnerabilities to ordinary consumers due to popular corporate attitudes of manufacturing and vending devices without effective security measures for the purposes of maximizing sales and profits. These issues are starting to be addressed. Specifically, a recent piece of legislation, the Internet of Things (IoT) Security Improvement Act of 2017, was proposed in Congress as a way to implement and enforce security standards within businesses and their IoT products. Though the intent of the legislation is undoubtedly applaudable, the unfortunate truth is that it is dangerously weak and therefore ineffective in actually raising the security of IoT end users beyond a marginal amount. Therefore, our proposal is to draft a revised version of the bill that would implement IoT security standards that are much more stringent, and therefore effective, in protecting IoT users.

Throughout much of our research, we have found much regarding the lack of implementation of effective security standards within many industries, the consequences for which abound. In fact, many of the articles and corporate surveys we have researched suggest that a vast number of companies in the United States alone have been hit with IoT data breaches. It is evident that the impact of IoT breaches on the efficacy of companies' business operations have staggering magnitudes. However, IoT security flaws also pose dangerous risks to consumers, who sacrifice privacy and security for convenience when using IoT devices. The complex web of information networks formed by the rapid emergence of IoT devices presents a unique risk with implications not only for the private sector, but to infrastructure and national security. With the standards currently in place, this technology is conducive to cyber crime and exploitation on an unanticipated scale. Therefore, the end goal of our original work

would be to impose stricter regulation on IoT companies so that they as a well as their consumers are protected from those who would exploit obvious vulnerabilities to extort people and businesses.

Obviously, to be able to draft an effective bill that addresses all, if not most, of the current security vulnerabilities of IoT, we would have to conduct careful and in-depth research regarding the needs of IoT consumers, the costs for such implementations, and how companies can incorporate IoT security standards in practice in a scalable and practical way. We intend to conduct this research by scheduling more research interviews with cyber security professionals in hopes of gaining more perspective into what the world of IoT needs. Furthermore, we fully intend to conduct independent research into current security trends/practices and recent IoT-based exploits and data breaches to learn how to better protect and defend from common vulnerabilities being exploited repeatedly.

Invariably, this task will require not only the extensive research as mentioned previously, but we would also have to apply all of the knowledge we've already gained regarding cyber security into forming a set of standards that are geared towards the protection of all IoT consumers. Furthermore, learning how to draft an improved standard, as well as achieving the means to enforce it upon developers and manufacturers, will be a strenuous yet rewarding challenge. We believe that in exploring the relationship between cyber security defense and compliance as well as gaining a deeper technical background through research and industry connection is a unique and exciting way to develop greater understanding and insight into the field and have that knowledge culminate into our original work, which will work to improve society by improving the standards of security across the board for all IoT users.

Description of Process:

We set out to rewrite a bill that had originally been drafted for the purpose of proposal in congress. The first thing we had to do before we could justifiably alter the original bill was to learn everything we could about what the legislation encompassed. As a result, much of our initial research was comprised of definitions of terms included in the bill document and the ramifications of the bill itself. Next, we set out to define our own ambitions regarding IoT security in order to decide what we needed to edit from the original bill. Having delineating our goals for our original work, we went through the bill and picked apart which parts would prove effective in protecting IoT users in the greatest capacity and which parts would need altering in order to reach this specification.

At this point, one of our greatest concerns regarding the efficacy of the bill was that the legislation only aimed to institute security standards for IoT devices sold to and owned by the United States government and related executive agencies. However, the largest IoT market is not any one government. Rather, it is the consumers of the United States that make up one of the largest demographic group of IoT consumer products. Therefore, in order to increase IoT security beyond marginally and to secure IoT consumer data from external threats for the most people, we had to broaden the scope of the bill from federally owned and operated IoT devices to every IoT device sold, owned, and operated inside the United States, including those used by consumers as well as those owned and operated by Federal organizations.

Our collective experience with bill-writing, gained through participation in youth government, came into play quickly. We recognized the need to define important terms in anything we endeavored to add to the bill. Terms such as “threat actor”, “two-factor authentication”, and “encryption” were not originally part of the bill. However, we set out to establish greater security measures against external threat actors through requiring more secure verification and data transport services such as two-factor biometric authentication and state-of-the-art encryption standards such as the Advanced Encryption Standard, or AES. After adding in the definitions we considered necessary, we separated responsibilities for the actual editing and formatting of our revised version. One of the more tedious tasks involved in this original work project was the correction of spacing issues that arose when copying over the original text of S. 1691 from Congress.gov. Upon completion, however, the next step was to parse through the bill once more and revise the lines that limited the scope of the legislation to only Federally owned and operated IoT devices. We accomplished this through defining the term “purchasing entity”, which incorporated both executive agencies and “commercial enterprises”, which was incorporated for the purpose of expanding the bill’s scope. Finally, we recognized that the latest trends of IoT usage in industry suggested that certain

commercial sectors held much clout in the demographic of IoT device consumption. The industries in question are those of Healthcare and Finances. We considered the devices used in these industries more important than other device information, as in healthcare, user data can include health information, medical records, and prescription details, and in finances, user data may include consumer bank information such as social security numbers, credit card information, and bank records. Therefore, we added separate clauses to the end of the bill that would set different security standards for devices based on their uses in the Healthcare and Financial industries: Section 4 and Section 5, respectively.

Utilization of Higher-Level Thinking Skills:

Throughout the development of our original work, analysis, synthesis, and evaluation played critical roles. In order to determine the criteria by which the bill would require IoT devices to operate within the United States, we turned to several industry articles, professional publications, as well as government and organizational standards relating to IoT operation and security. We analyzed the common occurrences between documentation, also finding rationale behind each of the recommendations made for the secure operation of IoT, especially in the medical and financial sectors. Further, we evaluated suggestions from industry leaders such as InfoSys and HITRUST compared to the original bill in order to create a more effective policy regarding IoT operation. For example, the conflicting wireless communications between healthcare-oriented IoT devices was a concern across the board for industry publications. In our bill, we sought to ease this by requiring IoT devices to be able to change working-state and operation mode in regard to the devices around them. Finally, with all our solutions for industry concerns as well as professional recommendations for the regulation of IoT, we synthesized all the information we had gained with the original bill, therefore creating a much more secure, effective, and futureproof piece of legislation.

Results/Conclusions/Application:

Our final bill addresses the concern of IoT security and regulation sector not only for the United States Government operational use, but for commercial, medical, and financial applications as well. Through combining our own knowledge of IoT with manifold sources of industry opinion regarding the regulation of this emerging technology, we have created an effective set of operating guidelines for not only the United States, but any area where Internet of Things technology will be leveraged. As a result of the exposure to current IoT views and regulation within the Cybersecurity and business industries, we have arrived to the conclusion that although some may view the regulation of IoT to the degree proposed in our Original Work unnecessary, the reality is actually to the contrary. With the number of internet-connected devices set to well outnumber the human population in the coming years, this legislation becomes even more paramount as the role of technology in everyday life increases exponentially. The tremendous security risks associated with IoT generating data about user location, biometrics, financial transactions, and even medical care are not going to disappear because of manufacturer conscience or attacker passivity. Rather, the Internet of Things industry needs to be regulated -- before it expands out of control -- in order to ensure a secure future for all.