Student Papers in Public Policy

Volume 2 | Issue 1 Article 6

2020

Smart Device Cyber Security

Shao-Chieh Lien
Purdue University, liens@purdue.edu

Nick Haythorn
Purdue University, nhaythor@purdue.edu

Yu-Chieh Tseng
Purdue University, tseng31@purdue.edu

Recommended Citation
Lien, Shao-Chieh; Haythorn, Nick; and Tseng, Yu-Chieh (2020) "Smart Device Cyber Security," *Student Papers in Public Policy*: Vol. 2 : Iss. 1, Article 6.
Available at: https://docs.lib.purdue.edu/sppp/vol2/iss1/6

Purdue Policy Research Institute

Student White Paper

Smart Device Cyber Security

Shao-Chieh Lien, Nick Haythorn, Yu-Chieh Tseng

HONR 399, Security: Technology and Society

April 21, 2020

Table of Contents

1. Introduction

In 2007, Apple released the iPhone under the direction of Steve Jobs. At the time people did not realize how revolutionary this invention would be. 13 years later, smartphones and other connected devices have completely permeated American society. According to Pew Research Center, in 2019 81% of Americans owned smartphones and 52% of Americans owned a tablet computer. Smartphones and other smart devices provide a large amount of convenience to their users, but the personal data stored on them presents a huge security risk.

Applications (apps) allow smartphones to provide important services, such as Apple's Apple Pay, which allows users to pay bills on their smartphones with their credit cards. People can access social media like Facebook, Instagram, and Twitter through their smartphone, and users can text each other, and post stories of their day: they are truly ubiquitous in modern life. The vast amount of sensitive information in a smartphone gives hackers a strong incentive to steal the data to make a profit. Kaspersky Lab (Fadilpašić February, 2019) reports that the number of mobile malware attacks doubled in 2018, topping 116.5 million last year compared to 66.4 million in 2017. There are numerous ways to hack into a person's smartphone, and one of the ways is via the Internet of Things (IoT).

The concept of IoT is "Taking all the things in the world and connecting them to the internet." (McClelland, 1-9-2020, p. XX). By connecting all kinds of devices, from a printer to a power generator, these devices can form a network in which the devices can communicate with each other, allowing the user to conveniently control the whole network from one end - like a spider web. Of course, this is hugely convenient for the user, but in contrast, it also allows hackers to find a breach and hack in the network. The bigger the network, the more difficult it is for people to protect the network. Since it is a network, everything is connected to each other, and if a hacker gains access to a single device, for example, a printer, they can use it as an entry point to control the whole network and steal valuable data.

The hacking of IoT is just one example of the cybersecurity problems that arise with the use of smartphones and smart devices. These technologies are still too new for people to pay attention to the potential problems. By one measure, "48% of companies that use IoT devices in the workplace don't have mechanisms in place to detect if any of their devices are hacked" (Schwab, 01-16-19, p. XX). (Gold, 8-6-2019, p, XX). The aim of this white paper is to increase public attention on the topic of smart devices and cyber security.

2. Security Risks

Cybersecurity is an endless arms race between those trying to get access to a user's data and those trying to protect it. Every new access point provides countless opportunities for malicious actors. As a result, the rise of smart devices has created millions of new ways for hackers to gain access to other's personal data. While these devices have provided incredible convenience, the risks they present cannot be ignored. Smart devices present security risks every day, not only to individuals, but also to the private and public sector.

2.1. Personal Security

Smartphones and other smart devices present many security threats to citizens. In some cases, the vulnerability is as simple as leaving a phone unsecured. According to a recent study, 28% of all smartphone users do not take any action to secure their phone, not even a pin code or dot lock to secure the screen (Mensch, Wilkie, July 2019). These preventative measures are incredibly simple: pin code requires a user to enter 4 numerical digits, and a dot lock is typically a grid of 9 dots which the user drags their finger across, touching each dot in a specific order. These security measures take only seconds for the user to complete but can present a major hurdle for a hacker. The fact that so many users avoid such simple deterrence is especially concerning because of the amount of sensitive information contained on most smartphones. By hacking into a smartphone, one could get access to the owner's identifying information, text messages and voicemails, personal or work email, credit card and bank account information, and many other usernames and passwords to various services.

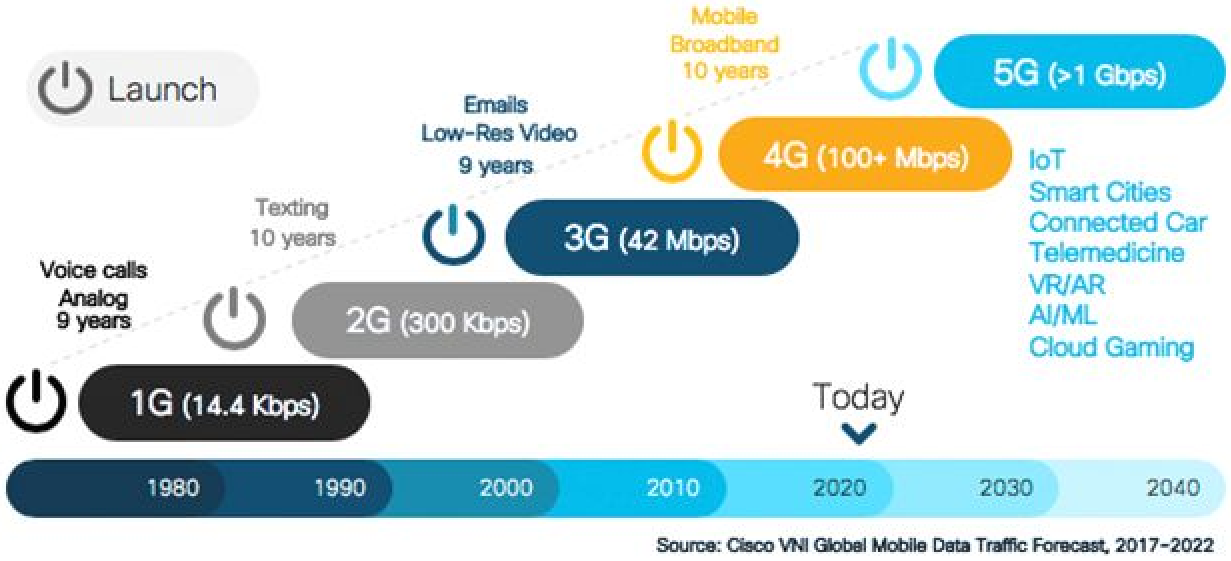
Even if a malicious actor doesn't have physical access to an individual's phone, they can still access and retrieve personal data in various ways. While there are very complex ways to get data from a phone--for example, a "man in the middle attack" which intercepts network communication--one of the simplest ways is through one of smartphones' greatest conveniences, apps. In 2015, a study showed that 17% of all Android apps were malware, and approximately 24,000 additional malicious apps were blocked from the app store every day in 2017 (Mensch, Wilkie, July 2019). The growing number of 'grayware' apps is even more concerning than malware. Grayware typically comes in the form of adware or spyware, and while not directly harmful, these apps can still range from annoying to dangerous. Adware typically serves users additional advertisements on their device. These ads are usually intrusive, negatively affecting the user experience and earning the adware creator advertisement revenue (Malwarebytes, n.d.). Spyware is the greatest concern from a personal security perspective. These applications typically infect a device without the user’s knowledge and gain access to personal information such as the user's phone number, email address, browsing history, or even location data, and then leaks it to companies or other potentially malicious actors (Malwarebytes, n.d.).

2.2 Private Sector Security

The security risks from smart devices to individuals are substantial, but smart devices present risks to groups as well. In this decade, most information is digitized. Financial institutions, banking systems, research projects, and other assets that belong to companies are connected to the internet. Cyberattacks on these systems can lead to the loss of money, customer privacy, and important technologies including weapons developed under government contracts. Take a cyberattack on Cathay Pacific two years ago as an example: this attack compromised thousands of Cathay Pacific’s customer’s credit card information. This great loss to Cathay Pacific’s customers was due to the vulnerability of the company's cybersecurity. The article from CISCO, mentions that the total volume of cyberattacks has increased four times between 2016 and 2017, and it’s still rising. 53% of the attacks results in a loss of $500,000 or more (Cisco, n.d.). This issue is even more critical to companies like Facebook and Google, where people save lots of personal information, or defense companies like Boeing and Lockheed Martin, where there is lots of classified technology.

Industry is being revolutionized by the emergence of 5G. 5G is the fifth-generation communication technology, it allows devices to connect to each other and form a decentralized network, rather than communicating through hubs like routers or cell towers. This allows data to be transferred at faster speeds, with greater efficiency, and lower latency (Ericcson, n.d.). The idea of Industry 4.0 is an extension of 5G, wherein devices on a factory floor will all be smart and communicate with each other directly. That means every machine in a factory will be interconnected and autonomous. The machines will be able to share resources, manage the transportations of materials, and timing of interactions by themselves. This will greatly increase the number of smart devices in industry settings. Productivity will undoubtedly be increased, but so will the risk of cyber-attacks. More smart devices mean a larger number of potential entry points for hackers and a larger amount of control possible if access is gained. A malicious actor could shut down production or worse, gain control of dangerous equipment around human operators.

For companies that are responsible for cybersecurity such as CISCO, a cyberattack can also lead to a great loss of profit. Companies like CISCO are responsible for the cybersecurity of many businesses and governments. One of the tasks of CISCO is to control the backdoor



Source: Cisco VNI Global Mobile Data Traffic Forecast, 2017-2022

Figure 1: Progression of wireless communication technologies. (Jain)

program in missiles sold to other countries. If a hacker were to gain access to CISCO's network, they could potentially gain control of missiles.

2.3. Public Sector Security

Beyond individuals and businesses, smart devices have become a new and advanced weapon which could threaten national security. Through the IoT, which is the network where every device is interconnected, hackers or the military can attack governments or public facilities and turn personal devices into national security threats.

From the attack of an individual to a government, IoT devices can be used to create a national security attack. In 2016, Paras Jha created malware which could carry out large-scale network attacks through the IoT. (Bours, December 13, 2017). It has temporarily brought down portions of America's internet including some public facilities like CCTV cameras. Another example is the hacker group, APT28 in Russia, which is believed to be controlled by the GRU military intelligence. It focuses on attacking military and government organizations using IoT devices. Unlike the internet attack carried out by Paras Jha, APT28 focuses on stealing data and controlling big companies' networks to influence a country's security. (Doffman, August 5, 2019). In 2019, Microsoft spotted a cyber-attack using IoT technology from APT28. They tried to exploit VOIP phones, office printers, and video decoders in order to gain access to the companies' network. Luckily, it was blocked by Microsoft in the early stages, which prevented it from becoming a problem for other big companies, and furthermore, a threat to national security. (Doffman, August 5, 2019).

Other than the potential loss of information and data in the government, cyberattacks can also cause damage to critical infrastructure. Through the IoT, hackers will be able to get access to the control systems of critical infrastructure, such as power stations. The control systems of these infrastructures are sometimes totally unsecured, making them easy targets. If these systems were controlled by hackers from other nations or governments, it can become a great threat to the security of the nation.

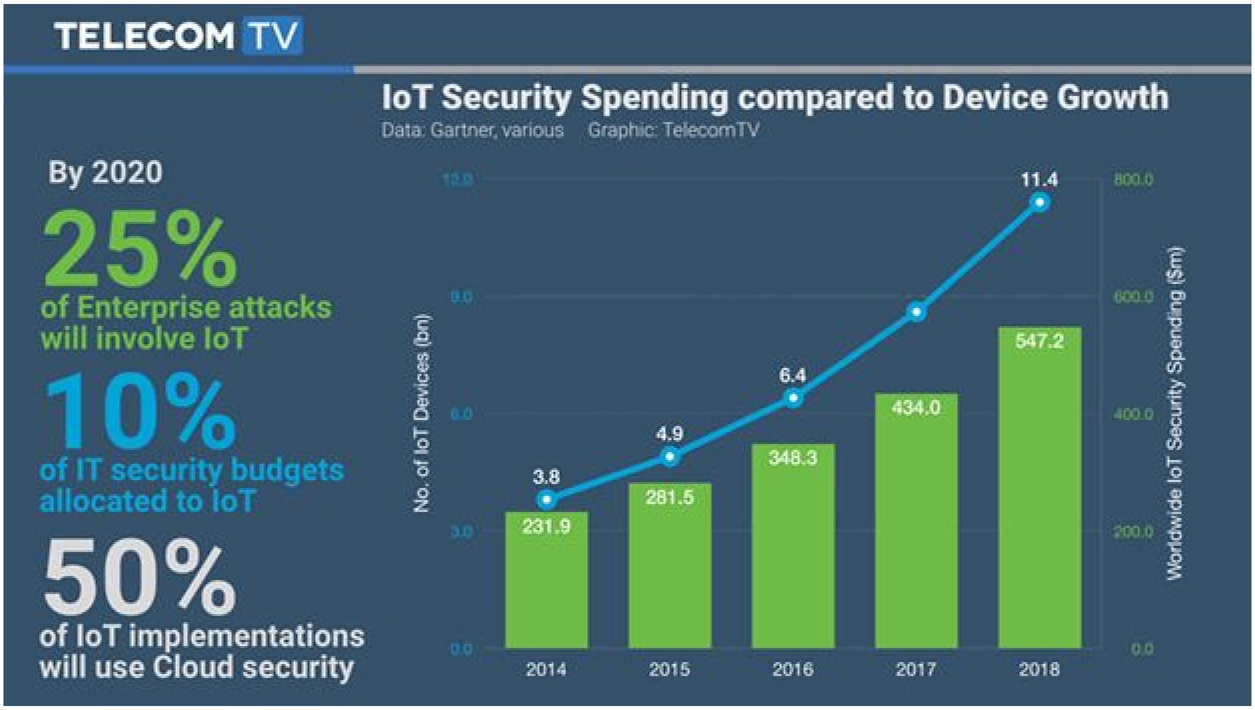
3. Security Cost

The importance of cybersecurity has increased as informational, networking, and computational technologies have developed. Governments, businesses, and civilians rely increasingly on smart devices such as in smartphones, computers, smart locks, and smart cars to complete various tasks more efficiently. Important data is like online payments information is often stored on these devices, which results in a higher societal and financial cost when these devices are attacked. As a result of this, more money is spent on the security systems of these devices to prevent attacks or reduce the cost of them when they happen.

The societal cost associated with cyber technologies has increased year by year at both the individual and national level. According to the report from the White House, a total of 42,068 security incidents and 1,935 breaches were reported in 2016 (The White House, 2018). The societal costs of these security issues vary with severity and the industry. The average cost of a cyber-attack is reported to be 1.1 million dollars for large firms and around 500,000 dollars for small firms (Dynasis, n.d.). This is the cost of a single cyber-attack, but many companies experience many attacks. According to the report from Accenture, a consultant company, an average of 2.8 percent of a company's annual revenue might be lost as a result of cyber-attack in the next five years for an average company with a 2018 revenue of 20 billion dollars (Accenture Security, 2019). The cost of each attack is still growing as the economy develops. Cyber-attacks on industry cost a great deal of revenue, thus negatively affecting the GDP of a country.

One cause of the decline in GDP is the result of attacks on smart devices in different industries and government branches. Among the societal costs of all industries and government branches, the attacks on manufacturing, government, finance, and healthcare are the greatest. The industry percentage of the 2016 GDP loss as a result of the attacks is around 18 percent for the manufacturing industry, 7 percent for the finance industry, 7 percent for healthcare, and 12 percent for the government (The White House, 2018). This data shows that the attack on cyber or smart devices can cause a great deal of societal cost.

Besides loss due to attacks, governments, industries, and individuals also spend money on security technologies to protect their devices. The security systems can be briefly divided into information technology (IT) security and network security. IT security is about the protection of the physical and digital data stored in smart devices and while moving through the network, and the network security is about the protection of IT infrastructure from the network (Norton, n.d.). The security systems can be hardware, software, and services at different costs. The spending by private sectors on cybersecurity products in 2016 is 56 billion dollars and is estimated to double to 128 billion dollars in 2020 by Morgan Stanley (The White House, 2018). The financial cost of cybersecurity systems increases as the scale of business or government branches increases. Based on the report from Kaspersky, there are three main approaches that businesses use for the security of smart devices: classical and traditional, cloud-based security, and outsourced (Kaspersky Lab). The classical and traditional approach is the approach that uses anti-virus software; cloud-based security is the approach that uses hardware to manage the endpoints; the outsourced approach is the approach that has an engineer to manage the devices from other places. The approximate annual cost of a company with two offices and 100 endpoints for these approaches is 54,300 dollars for classical approaches, 33,500 dollars for cloud-based security, and 36,000 dollars for outsourced approaches (Kaspersky Lab). For personal smart devices, people use different anti-virus software at different costs. More expensive computers and cellphones, such as iPhone and Pixel 4, may include security chips and algorithms in the CPU and GPU to protect against security incidents and breaches.



IoT Security Spending compared to Device Growth

Data: Gartner, various Graphic: TelecomTV

Figure 2: Rise of IoT and related security budgets. (Daniels)

The cost of security technologies to protect smart devices is relatively low compared to loss it can prevent to industries, individuals, and governments. As the impact of attacks on smart devices increases year by year, it’s a fair trade to invest more in security technologies.

4. Ethical Considerations

With all the security issues and expenses created by the rise of smart devices, one must consider whether this technology is worth developing. One must realize that “The Internet of Things (IoT) is changing industries across the board – from agriculture to healthcare to manufacturing and everything in between.” (McClelland, 1-9-2020, p. XX). The variety of services IoT could provide is so wide that numerous industries, companies, and schools have been impacted by its powerful functionality and are now studying ways to implement it.

The wide adoption of IoT presents some ethical issues, like big data. “Big Data and its manipulation can result in potentially high impact, for instance, on privacy, security and consumer welfare. This is particularly so as the process of data collection in IoT is done automatically, often without any human intervention.” (Antoniou, Andreou, 1-20-2019, p. 03). Big data is the technique of processing a huge amount of data using advanced processors to analyze the data. The collection of personal data and consumer data has been an issue for the past few years. Big Data can have huge benefits. As an example, the collection of thousands of examples of the human genome and analyzing them with big data will allow the prediction of certain diseases and conditions well before symptoms appear. However, big data also has many downsides, political candidates have been able to sway voters with targeted advertisements crafted based upon their Facebook profiles and internet history. This is an unethical use of data because candidates are presenting themselves differently depending on who is viewing their advertisements. With IoT collecting all kinds of data from the devices in the network and big data capable of storing and analyzing the huge amount of data, it gives companies powerful tools to create good but also invade personal privacy and data. Personal data has been an issue and handing the tools for people to use it is becoming another issue.

The IoT could provide lots of convenience in our daily life, even for companies and governments. However, it is important for people and industry to acknowledge the risks and mitigate them before implementing it widely. Besides the potential risks, new technology requires new regulation to make sure the tool doesn't fall into the wrong hands.

5. Policy Overview

In terms of policy relating to smart devices, the internal policy of many companies is far ahead of any public policy. Broad reaching, Federal regulations about smart devices are lacking and state regulations have just started to pop up recently. Internally, individual organizations, like the Internal Revenue Service (IRS), use their own experts' knowledge, or other consultant companies to help prepare policy, and as a result tend to hold their employees to much higher standards of security practice than the federal government requires.

Federal regulations of IoT and smart devices have had a lot of trouble getting passed into law (Lindsey, 2019). One recent attempt to introduce regulation on smart devices at the federal level was with Senate Bill S 2234, known as the "IoT Consumer TIPS Act of 2017". The main purpose of the bill was to require the Federal Trade Commission to develop "cybersecurity resources for consumer education and awareness." The bill defined the Internet of Things(IoT) as "devices, applications, physical objects that are internet-enabled, networked, or connected." It went on to explain how IoT has been rapidly and widely adopted by consumers and businesses, and that the security of these devices is paramount to the United States digital economy. The bill outlined that the Federal Trade Commission (FTC) should make “technology-neutral resources that include guidance, best practices, and advice for consumers to protect against, mitigate, and recover from cybersecurity threats or security vulnerabilities” (Hassan & Wicker, 2017). It also included requirements that the FTC keeps these resources up to date and makes them available to the public via the internet. The bill contained no regulations on the construction of devices by companies nor the usage of devices by companies and consumers. Unfortunately, the bill never came to a vote.

At the state level, California is the first state to have introduced any legislation regarding IoT and smart devices (Lindsey, 2019). Unlike the IoT Consumer TIPS Act of 2017, California’s SB 327, titled “Information Privacy: connected devices,” was passed in 2018. The bill took aim at regulating the connected devices being manufactured by companies to help increase their security. The bill requires manufacturers of connected devices to equip the device with reasonable security feature(s) that meet a variety of requirements like being ‘Appropriate to the nature and function of the device’, ‘Appropriate to the information it may collect, contain, or transmit’, and ‘Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure’” (Jackson, 2018). While this bill is a step in the right direction, it is rather weak in terms of actual regulation. Much of the terminology in the bill, like “reasonable” and “appropriate,” is left up for interpretation, meaning companies could argue that any level of protection is “reasonable” or “appropriate.” Additionally, the bill specifically notes that it in no way implies that device manufacturers are responsible for unaffiliated third-party software on their devices (Jackson, 2018). This means companies like Apple do not have to protect consumers from malware on their application stores.

While there is a distinct lack of public policy protecting consumers from smart devices, companies and many government organizations tend to have robust internal policies in regards to security. Part 10, Chapter 8, Section 26 of the IRS's Internal Revenue Manual provides a good example of current government policy on smartphone usage. The policy is detailed and all-encompassing, and in many cases links to additional and more detailed policy for individual bullet points within larger sections. It begins by explaining the differences between government-provided devices and personally furnished devices, including the numerous additional responsibilities that participants in the "Bring Your Own Device" program incur. The policy then goes into a strict definition of Access Control, including who can access the devices and what resources devices can access. One interesting note is that the policy contains specific guidelines for access to sensitive information, noting that mobile devices shall not download sensitive information and shall not access, process, transmit, or store classified information. The policy continues to cover training, assessment, management, incident response, disposal and many more topics regarding smart devices (IRS, 2017).

6. Policy Suggestions

It has become abundantly clear that there is a large disparity between public and private policy on smart devices in the US. The people who create private policy for government organizations like the IRS clearly understand the risks presented by smart devices - this is evidenced by their strict and thorough usage regulations. It is very important that new policies be implemented in the United States to educate the public of the threats they face from their smart devices and protect them from them.

First, the Consumer TIPS Act of 2017, or another similar bill, should be passed to educate the public of the threats of smart devices. This is important because 28% of all smartphone users do not take any action to secure their phone (Mensch, Wilkie, July 2019), leaving a vast amount of personal information completely unsecured. The TIPS bill would help decrease this fraction by educating the public on the importance of cybersecurity and some of the steps to keep themselves safe. Ensuring that the general public has access to information about security would be relatively cheap and likely require minimal upkeep. This bill could also include information on things like how to spot potentially dangerous applications and software, helping consumers protect themselves.

Additionally, a bill like California's SB 327 should be passed at the federal level. The bill created an outline for ensuring the companies that make smart devices provide their consumers with protections against hackers. The only issue with California's SB 327 is that it used weak legal terminology like "reasonable" and "appropriate" (Jackson, 2018). The bill could be improved to include specific requirements that manufacturers must adhere to for specific classes of devices. For example, requiring that data on smartphones be encrypted to a certain minimum standard could greatly increase the security of consumers data.

Finally, it would be wise to all companies to implement minimum software and account security standards. Technologies like two-factor authentication, which requires a user to confirm a new account access on secure devices, can greatly increase the security of personal and company accounts by notifying users of attempted access to their accounts. Company-wide password strength policies are also a very simple way to increase account security. Simple passwords can be cracked by hackers in a matter of seconds but every increase in password complexity multiplies the time taken to crack it. The most secure passwords are uncrackable by even the most powerful computers on earth.

7. Conclusion

As a result of developments in the networking and informational technology, the costs of cyberattacks and the importance of cybersecurity on smart devices is rising. These technologies are expected to develop further in the coming years. This will lead to an rise in cyberattacks as the profits brought by these cyberattacks increase. As discussed above, the amount of money lost due to these attacks is increasing every year and the frequency of attacks increases daily. The cyberattacks can not only affect the privacy and interests of an individual, but also that of a company, an organization, and a nation. The impact can range from the loss of personal passwords to a reduction of the GDP of a country. To protect important information and personal privacy against cyberattacks, individuals, organizations and companies, and governments must invest more money on cybersecurity devices which reduce the financial cost of cyber attacks. More frequent collection of an individual's data using networking technologies and smart devices also leads to new ethical concerns. Although research and experience have shown the importance of increasing cybersecurity and considering the ethical questions brought about by these technologies, and despite the fact that companies have been working on the solution to these issues, no government regulations or guidelines have been passed at the national or global level. The need for regulations on cybersecurity at the national level is an urgent topic that should be discussed in the next decades.

Works Cited

Accenture Security. (2019). The Cost of Cybercrime. *Accenture.* Retrieved from https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

Antoniou, J., Andreou, A. (Feburary 20, 2019). Case Study: The Internet of Things and Ethics. *Orbit*. 2(2) doi:https://doi.org/10.29297/orbit.v2i2.111

Bours, B. (December 13, 2017). How a Dorm Room Minecraft Scam Brought Down the Internet. (2017). *WIRED.* Retrieved from https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/

Cisco. (n.d.). What Are the Most Common Cyber Attacks. *CISCO*. Retrieved from https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

Daniels, G. (June 10, 2016). Improving IoT security with smart edge devices. *TelecomTV.* Retrieved from https://www.telecomtv.com/content/iot/improving-iot-security-with-smart-edge-devices-13673/

Doffman, Z. (August 5, 2019). Microsoft Warns Russian Hackers Can Breach Secure Networks Through Simple IoT Devices. *Forbes.* Retrieved from https://www.forbes.com/sites/zakdoffman/2019/08/05/microsoft-warns-russian-hackers-can-breach-companies-through-millions-of-simple-iot-devices/#680495a4617f

Dynasis. (n.d.). The Price of Security: How Much Does a Cybersecurity Attack Actually Cost. *NOVATECH DynaSis*. Retrieved from https://dynasis.com/2019/03/price-security-how-much-cybersecurity-attack-actually-cost/

Ericcson. (n.d.). A Guide to 5G Network Security. *Ericsson.com.* Retrieved from https://www.ericsson.com/en/security/a-guide-to-5g-network-security

Fadilpašić, S. (February 8, 2019). 2018 Saw a Drop in DDoS Attacks. *ITProPortal.* Retrieved from https://www.itproportal.com/news/2018-saw-a-drop-in-ddos-attacks/

Gold, J. (August 6, 2019). Microsoft finds Russia-backed attacks that exploit Iot devices. *Network World*. retrieved from https://www.networkworld.com/article/3430356/microsoft-finds-russia-backed-attacks-that-exploit-iot-devices.html

Hassan, Wicker. (2017). S. 2234 IOT Consumer TIPS Act of 2017. *Congress.gov.* Retrieved from https://www.congress.gov/115/bills/s2234/BILLS-115s2234is.pdf

IRS. (September 10th, 2017). 10.8.26 Government Furnished and Personally Owned Mobile Device Security Policy. *IRS.gov.* Retrieved from https://www.irs.gov/irm/part10/irm_10-008-026r#idm139679955975536

Jackson. (2018). SB-237 Information Privacy: Connected Devices. *California Legislative Information.* Retrieved from https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

Jain, S. (February 26, 2019). Mobile VNI Forecast 2017-2022: 5G emerges and is here to stay!!. *Cisco Blogs.* Retrieved from https://blogs.cisco.com/sp/mobile-vni-forecast-2017-2022-5g-emerges

Kaspersky Lab. (n.d.). Cyber Security For Business -Counting The Costs, Finding The Value. *Kaspersky Lab.* https://media.kaspersky.com/en/business-security/cybersecurity-for-business-counting-th e-costs-finding-the-value.pdf

Lindsey, N. (May 10, 2019). New IoT Security Laws Seek to Protect Consumers From Hacks of Internet-Connected Devices. *CPO Magazine.* Retrieved from https://www.cpomagazine.com/data-protection/new-iot-security-laws-seek-to-protect-consumers-from-hacks-of-internet-connected-devices/

M.W., S. (July 26, 2019). 7 Biggest IoT Risks Facing Businesses Today - And What to do About Them. *TechGenix*. retrieved from http://techgenix.com/biggest-iot-risks/

Malwarebytes. (n.d.). Adware - What Is It & How To Remove It. *Malwarebytes.* Retrieved from https://www.malwarebytes.com/adware/

Malwarebytes. (n.d.). Spyware - What Is It & How To Remove It. *Malwarebytes.* Retrieved from https://www.malwarebytes.com/spyware/

McClelland, C. (January 9, 2020). What is IoT? - A Simple Explanation of the Internet of Things. *iot for all*. retrieved from https://www.iotforall.com/what-is-iot-simple-explanation/

Mensch, S., Wilkie, L. (July 2019). Smart Phone Security Practices: Item Analysis of Mobile Security Behaviors of College Students. *International Journal of Cyber Behavior, Psychology and Learning.* Vol:9 Iss:3. Retrieved February 13, 2019 from https://pdfs.semanticscholar.org/4706/885ead1197bb161a8ad5c0e8cd1e85554f80.pdf

Norton. (n.d.). What is cyber security? What you need to know. *Norton.* https://us.norton.com/internetsecurity-malware-what-is-cybersecurity-what-you-need-to-know.html

Norton Team. (2015). What is Grayware?. *Norton UK Blog.* Retrieved from https://uk.norton.com/norton-blog/2015/08/what_is_grayware.html

Pew Research Center. (2019). Mobile Fact Sheet. *Pew Research Center.* Retrieved from https://www.pewresearch.org/internet/fact-sheet/mobile/

Schwab, K. (January 16, 2019). IoT security is so bad, many companies can't tell when they're hacked. *Fast Company*. retrieved from. (https://www.fastcompany.com/90292568/iot-security-is-so-bad-many-companies-cant-tell-when-theyre-hacked

Silverio, M. (December 29, 2019). What is a smart device?. *Towards Data Science.* Retrieved from:https://towardsdatascience.com/what-is-a-smart-device-the-key-concept-of-the-internet-of-things-52da69f6f91b

Suny Cortland. (n.d.). The Internet of Things. *Suny Cortland.* retrieved from https://sites.google.com/a/cortland.edu/the-internet-of-things/home

The White House. (2018,Feb.) The Cost of Malicious Cyber Activity to the U.S. Economy. *Whitehouse.gov.* https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf