Spring 2020

Alexa, is my home network safe?

Schaefer Jones

Alexa, is my home network safe?

By

Schaefer Jones

An Honors Thesis Submitted in Partial Fulfillment of the

Requirements for Graduation from the

Western Oregon University Honors Program

Dr. Breeann Flesch,
Thesis Advisor

Dr. Gavin Keulks,
Honors Program Director

June 2020

ACKNOWLEDGEMENTS

Thank you to my mom and dad for helping motivate me and push me to be a better student and person throughout my life.

I would also like to thank my advisor, Breeann for supporting me and being understanding throughout the thesis process and my entire CS degree.

Finally, I would like to thank my friends for making college such an enjoyable time and the friendships that will last long after.

Table of Contents

ABSTRACT

This thesis was created to research the usability and ease of understanding of home network hardware, specifically routers. After the usability is researched, it will highlight the issues and insufficiency with informational documents from a layman's understanding and the issues that arise when home networks are not properly secured. Most technical manuals that accompany networking hardware are not built for ease of understanding for someone with little technical knowledge in the field and should prioritize securing the hardware and user awareness. Additionally, this thesis aims to bring to light the concerning situation of responsibility post-breach in home networks, business networks, or data-holding providers. In most cases, whichever business has the breach should be held liable for compensation to those affected and initiate better security standards in the future.

INTRODUCTION

Purpose of Thesis

The purpose of this thesis is to inform those without much technical experience about the dangers of unsecured networks and how to remedy them.

Objectives of Thesis

The objective for this thesis is to attempt to teach and inform the basics of home networking, primarily the router. Furthermore, to explain the potential security risks involved with unsecured networks. It intends to show that current router manuals are not well formatted for ease of use by the average person. Its secondary objective is to start the conversation on wherein lies the responsibility for data breaches on both home, business, and cloud networks, as well as what has happened in recent personal information data breaches.

Organization of Thesis

The first section of the thesis explains why the thesis was created and explains some of the main points and questions. The second section is the literature review of various articles and research. The third section will be explaining the extenuating circumstances created by the Coronavirus pandemic and how it affected the completion of this thesis. The fourth section is a brief explanation of the design choices for the website. Lastly, the responsibility section which will bring forth the conversation on the responsibility of data breaches.

LITERATURE REVIEW

Securing a home network is not something that is easily done in many cases. With a staggering 73% of United States adults with home broadband and 90% that use internet in general in 2019, according to Pew Research Center, more and more people are getting home networks, which might not be secure. For many, configuring a router (the main bridge between a computer and the internet) can be a difficult and frustrating process. Many people do not necessarily have a lot of technological experience which can make this even more difficult. On top of all of this, there are people that are constantly looking for vulnerabilities in a network to take advantage of them. An article by NetworkWorld states it well, explaining one of the major problems behind these questions, "gone are the days when operational technology (OT) was single-handedly responsible for securing IoT, often taking a "security by obscurity" approach by physically separating production operations and industrial networks from enterprise networks and the Internet." The problem of home network security and the responsibility of the post compromise situation is what will be concentrated on in this review.

First, to go over some of the many malicious things that can happen to an unsecured network. From the "Securing Your Home Routers" article from

Trend Micro, there are many possible ways to infiltrate a home network: Built-In Backdoors, Vulnerabilities, Web-Based Scripts, and Authentication Bypass. Built-In Backdoors are usually found in router firmware (software that is for low-level control for the hardware) from the manufacturer for faster development and debugging. These, if not properly removed or patched up, allow hackers to have a free pathway into a home network. Vulnerabilities in a network can be anything from a piece of malware to security flaws in management. According to Trend Micro, almost 600 vulnerabilities were reported by researchers from 1999 to present. There are also Web-Based Scripts (pieces of code for injecting into a network), which bypass various authentication for routers, allowing hackers to get into the administrative side of a network. Finally, there is Authentication Bypass, which is similar to Web-Based Scripts, but can be done in two ways. The first is locally which is where an attacker would reside nearby and could guess the administrative credentials for the router. The other is via the internet and is accomplished by brute force, in a similar fashion to the local version, and attempts to remote manage the router.

Once the router has been compromised there are numerous attacks the hacker can perform. One of the most devastating post compromise threats is a Botnet. A Botnet is a group, usually very large, of infected devices that are

internet connected that can be managed by a hacker. These devices are then often used to carry out Distributed Denial of Service attacks. Distributed Denial of Service (DDoS) occurs when many devices, such as a botnet, floods a server with requests (example of a request includes opening a website, where a request to the server for the website is then sent to a computer for viewing). This is a very prevalent issue, especially with the growing number of Internet of Things (IoT) devices at 6.381 billion in 2016 and an estimated 20.415 billion by 2020 as mentioned in the article from Gartner. One of the most prominent botnets is the Mirai botnet. The Mirai botnet was at its peak in 2016. It sent DDoS attacks to groups from security journalist Brian Krebs to Netflix and other large companies. Before being taken down, the creators of Mirai botnet released the source code (the code used to create the botnet) to the public, allowing other hackers to create their own "strains" of the botnet.

Moving on to securing a home network before it becomes compromised, there are plenty of ways this can be done and make it much harder for a hacker to get administrative access. One of the simplest and a very effective countermeasure is to simply change the router password to a more secure version. This is recommended in most guides to home network security such as the Trend Micro article and the FTC's (Federal Trade Commission) "Securing Your Wireless Network" article. Most routers have

preset passwords for ease of set up, but not all require changing them after setting up. A recommended password length should be about 16 characters including upper and lower case, numbers, and symbols. For an average brute-force password cracker this can take around 41 trillion years. One of the next steps is managing the encryption level for the router. There are a few major types of encryption for wireless; WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), and WPA2 (a newer version of WPA). WEP is an outdated encryption protocol and should not be used but can still be selected on many routers. WPA is another older encryption protocol and more secure than WEP but does not use the more advanced encryption algorithm called AES (Advanced Encryption Standard), that WPA2 uses. Further explaining this in the Lifewire article, "WPA2 is designed to improve the security of Wi-Fi connections by requiring the use of stronger wireless encryption than WPA requires. Specifically, WPA2 does not allow the use of an algorithm called Temporal Key Integrity Protocol (TKIP) that is known to have security holes and limitations."

Another tip from the FTC is to log out from the administrative account so that attackers cannot piggyback off of the open connection and to disable remote management features which allow outside access (with credentials) to the device's controls. I believe that the Trend Micro article sums up this

issue well, saying “Becoming aware of how home routers can be abused for cybercriminal activities is one step toward securing these devices. Manufacturers have begun introducing changes with features like embedded security, password policies, CAPTCHAs, and users’ access control lists (ACLs), among others. These features, however, also mean additional costs for home users and thus become a big challenge for ISPs. As such, we believe that home routers will still be a prime target of cybercriminals.” Becoming aware of the problem is one of the largest steps towards prevention when it comes to cybersecurity.

Another large part of this thesis is the question of responsibility when a network, personal or enterprise, is compromised and sensitive personal data is stolen. Questions akin to “Who is at fault if a manufacturer makes the defaults of a router insecure and a consumer gets attacked?” or “If a company that you have given sensitive personal data has a security breach, should the consumer be compensated or forgiven on their credit score?” One of the main issues regarding manufacturers is the balance between security and cost. This is summed up well by Kranz from the Network World article, “However, device vendors have been slow to invest in security because it can add cost, complexity and time-to-market. With many makers committing clear security missteps – such as hard-coding default names and passwords into their

devices – consumer IoT gadgets have been incredibly easy to compromise." This is often the core reasoning behind manufacturing security faults and one of the things that will be independently researched in this thesis.

However, there are some administrative organizations that are attempting to hold the router and IoT industries to higher security standards. Organizations such as ODVA (Open DeviceNet Vendors Association), OPC (Open Platform Communications), ISA (International Society of Automation), IIC (Industrial Internet Consortium), IEEE Internet of Things Initiative (Institute of Electrical and Electronics Engineers), and the IETF (Internet Engineering Task Force), all exist to hold companies to standards in one way or another. Another group that has been previously mentioned is the FTC, which has already held large companies accountable ie: charging ASUSTeK Computer, Inc. for "critical security flaws" in their routers. Some of these flaws include "a vulnerability in the AiCloud service to bypass its login screen and gain complete access to a consumer's connected storage device without any credentials, simply by accessing a specific URL from a Web browser."

That being said, companies and organizations are not the only ones that are starting to tighten up security standards, especially when it comes to IoT devices. Multiple laws have been passed or are in the process of being

passed that limit these insecurities in IoT devices. The California Senate passed Senate Bill 327 in September 2018, a bill for information privacy for internet connected devices. The bill states “Manufacturer of a connected device shall equip the device with a reasonable security feature or features that are all of the following: 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.” The United States Congress also passed bill 1691 which exists to “provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes.” This bill was introduced into the Senate on the first of August of 2017 and has not made much progress since, but is an important piece of legislature that could help protect large groups of individuals and consumers by requiring that these manufacturers that could be cutting corners in security, use more robust security standards.

Another bill closer to home is the Oregon legislation bill 646A.622 which moves to the other question of responsibility. This legislation requires that “A person that owns, maintains or otherwise possesses data that includes a consumer’s personal information that the person uses in the course of the person’s business, vocation, occupation or volunteer activities shall develop,

implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including safeguards that protect the personal information when the person disposes of the personal information." The question of post compromise responsibility for data breaches is an interesting topic that does not have nearly enough awareness for how big of a problem it is or could be. Most likely this is a situation where people do not worry about a problem until it happens to them. However, this problem reaches a larger group than many may think, as stated in the article "A Case of Mistaken Identity? News Accounts of Hacker, Consumer, and Organizational Responsibility for Compromised Digital Records" by Erickson and Howard, "In early 2005, a series of high-profile cases culminating in the loss of more than 140,000 customer credit records by the data mining firm ChoicePoint helped generate significant public interest in the dangers associated with digital records of personal information." While this is an older statistic and rather low, it is an important fact in showing how large of a problem identity theft has been and that it is even larger now. For more recent data, the FTC stated that they received 1.4 million identity fraud reports in 2018. There is a great analogy in regards to the little that is done to prevent or come up with solutions to data security, from the article "From data breach to information stewardship" by Mike Small, "People would not treat money with the same disregard that they treat

information and data. Taking care to look after property that is not your own is called stewardship, and what is needed is better information stewardship." This kind of information stewardship is needed more than ever as more and more internet connected devices are put into use and have access to home or enterprise networks.

With the growing amount of identity theft, what happens to those who are not at fault when their data is compromised? With so many data breaches happening it would seem like this is an easier question to answer, but it is rather gray. An example would be a background check agency that requires the submission of a person's social security number. Let us say that agency then has a compromise for any reason, for this example it will be an insecure router. From this compromise, all those that have gotten background checks have now had at least their social security numbers stolen and potentially much more. Where the gray area comes into play is who should be at fault for this incident and what should happen to those that have had their identities stolen? Should the fault lie with the router company that left the security to low standards and did not require a password change and set a simple default password for the administrative account? Should it lie with the background check agency for not making sure that there is better security around the personal data that they store? Should it be the ISP (Internet Service Provider)

that does not have security for what is transferred over their provided connections? Or should it be the person who submitted the data to the background check agency, should they have asked and made sure that it would all be secure? These are all questions that seem to be lacking in concrete answers but will be explored later in the thesis.

With the potential problems growing more and more each year, this thesis hopes to add to the conversation of others that have researched this and bring some of these issues that do not have enough attention to the foreground. Laws, organizations, or company policies all could help bring attention to manufacturing issues and "information stewardship." While more conversations about where the responsibilities lie when it comes to post compromise data loss are also needed, until the question of where the responsibility lies is answered or better defined, people need to continue to talk about it until there is more precedent either legally or as an industry. These are huge problems that this thesis hopes to add to the conversation and bring as much awareness to the issues while also trying to provide some information to also stop the issue of uninformed consumers with insecure home networks.

WHY SECTION

One of the major points of this thesis is to be informative for the average person so that they can be knowledgeable and make smart decisions for their own home networks. It would seem like this information would be readily available online and would not take much effort to find, however that is not the case. The reasoning behind the existence of this thesis and the evidence for the difficulty of finding simple information is the topic of this section.

To find out just what information would show up when having an average person look up information regarding their own home network security, different search terms were tested. For each set of search terms the top three to five results were gone through to see how easily accessible the information was for someone with little to no technological background.

The first search term was “home network security guide.” The top result and the Google featured snippet was the Home Network Security Page from the US Cybersecurity and Infrastructure Security Agency (CISA) which is a division of the US Department of Homeland Security. The guide was adept at describing various potential threats to a home network and solutions to fix each of the described problems. However, the terminology and explanations of the solutions would not necessarily be easy to understand without a

technological background. Furthermore, while it describes what solutions could be followed to mitigate the problems illustrated, it does not give any in-depth instruction on how to carry out said solutions. This site would be best used by someone with moderate technological background, as a checklist for things to accomplish to make sure they have properly secured their network. The second link was to the Home Wireless Network Security page of the blog for Heimdal Security, a consumer and enterprise security suite company. The blog is comprised of both Heimdal employees and guest authors that pitch article ideas that must be approved by Heimdal. This specific article was written by Ioana Rijnetu, a guest author who is a Marketing and Communications Specialist and Cybersecuirty Enthusiast. This article specifically went through twelve steps to "enhance your home wireless network security." This article was much easier to understand from a layman's point of view. It went through various steps from as simple as changing the name of your home network to increasing encryption strength and changing default IP addresses. Be that as it may, the article did not provide full step by step instructions for each section. Moreover, many of the instructions that were given merely linked to other articles and websites such as WikiHow and Lifewire. The third link was to the Lazy Admin website, which is a blog operated by Rudy Mens, a System Administrator and IT-Specialist at Thunnissen Groep, a Netherlands real estate company. This blog

post was less helpful than the Heimdal Security article, but it still did well in explaining issues in layman's terminology. Similar to the US Department of Homeland Security, this blog does not do a great job in adequately explaining how to solve those problems and where they do, they often lead to other articles. The fourth and final result for the first search term lead to Hackernoon, an independent tech media site. The article was written by David Balaban, an editor at Privacy PC, a security and privacy news site. This was a rather short and straightforward article that did explain things such as changing the SSID (Service Set Identifier), encryption, and firewall. While this article is rather informal, it is not very helpful when it comes to explaining in easy to understand language. It also does not explain how best to solve the problems or tips that it covers.

By changing the search term to "home network security for beginners" it was actually surprising to find out that the top three links were ones that were already covered in the first search term: the Heimdal Security Blog, Lazy Admin Blog, and Hackernoon website. Since the first and second search terms were similar, the third search term was changed to try and find differing results. The third search term was "how to secure home wifi." The top result was for Tech Radar's article "How to secure your Wi-Fi at home and in your business" by Paul Rubens. This article starts by talking about increasing encryption, using a strong password, making sure there are no extra wifi

access points that are unmanaged, providing a separate network for guests, hiding network names, using a firewall, enabling MAC authentication, and using a VPN. All in all, it is a pretty decent guide but it is not very helpful for a beginner. The second link for this search term was for the Heimdal Security Blog again, showing there is not variation in search results that are shown on the front page of Google for this topic. The third and final link was to a blog for CompariTech. The article by Stephen Cooper was very similar to other articles however, there were a couple non-traditional tips such as just turning off the router, using aluminum radar dishes to make the wifi more directed, or filling your house with aluminum in the ways to build a home faraday cage. These are more complicated and what most would consider unnecessary tips that might overly worry or complicate things further for someone who is not technically adept.

Focusing on a more specific reason why this thesis is important would be the lack of easily readable manuals for what many people have as their extent of a home network, the home router. Five router manuals were examined of varying costs, technicality, and seemingly commonness. The first router manual that was researched was for the NETGEAR Nighthawk AC1900. This is a higher-end model router priced at $145 on Amazon as of November 2019. The manual goes through various security features such as allowing

and blocking access via IP address on page 59, blocking various programs and services from your network on page 61, and setting up email notifications for security alerts on page 64. However, it is not until page 125 that they begin to explain “Basic WiFi settings.” Furthermore, how to change the WiFi password and encryption level is even farther into the manual at page 127. Perhaps the most surprising is that how to change the router administrator password is not explained until page 147. The commonality between all this information is that many people might become frustrated reading the manual, especially to page 147, and some might not even read the manual at all.

The next router manual that was analyzed was the Cisco DPC3939, which is the primary router that Comcast uses for their internet packages and provided routers. This manual was much shorter than the last being about 57 pages. Most of the critical security information is around page 26-32, again well into the manual. This manual did a good job explaining the user interface, but also used a lot of technical language at times such as ASCII, Hexadecimal, and MAC addresses but does not go about explaining what those are.

The manual for TP-Link AC1750, which was rated as Amazon's best-selling router as of November 11th, 2019, was the third manual reviewed. This manual did an excellent job segmenting the manual with a well-designed table of contents and an interactive PDF which allows you to jump between

sections with a click. Moreover, the manual does not use technically complicated terminology and shows frequent pictures of the router's GUI (Graphical User Interface) which is extremely helpful for explaining how to accomplish certain settings. It also explains how to set up limited guest networks which can help with keeping a home network secure. However, it does not explain much when it comes to encryption settings and simply mentioned WPA and WPA2 without explaining what they are, their meaning, or which is better or more secure. Similar to other manuals changing the login password is not found until almost the end on page 90 of 98. Additionally, network security is not found until over halfway through the manual at page 53. It does explain how to setup the firewall and Denial of Service (DoS) protection settings, access protection, and IP and MAC address binding, which is beneficial.

The inconsistency and complicatedness of these manuals show one of the largest problems with home networking equipment. These manuals can be so convoluted that it could cause frustration and impatience. This frustration can then turn into overlooking and ignorance to properly setting up and securing their home networking devices. Thus creates the problem of easily accessible networks for bad actors to take advantage of and potentially obtain personal information of those owning the network.

WEB DESIGN

It seemed that creating a website to be able to alternately host the thesis or home security guide would be a good idea. Creating the website was rather simple since its main purpose was to be an information repository. Due to the simple nature of the website, a Wordpress designed site seemed an efficient choice. Designs were sketched up on paper to get an idea for what the site would roughly look like. For a homepage, the Wordpress Morden page layout was utilized. Four pages total were designed: a homepage, thesis page, download page, and a short about page.

The homepage contains a small section stating the purpose of the thesis, a synopsis of the abstract, and a short about the author section as well as links to the other pages of the site. The thesis page will contain the written entirety of the thesis with occasional pictures to break up blocks of text and keep it fresh. The download page will have links to the WOU (Western Oregon University) thesis page for download of the entire thesis including the home security guide, and a link to just the home security guide for those who wish to only have the home security guide for reference. Finally, the About page contains a short introduction by the author for people to know where the information is originating from.

COVID-19 EXTENUATING CIRCUMSTANCES

With the start of the global COVID-19 pandemic, there were circumstances that caused this thesis to become harder to complete. Due to quarantine and its mental health impact, there was one section that was not able to be completed and one that was not fully implemented. The section that was not complete is the Home Guide for securing home networks. It was planned to be an easier to read explanation of general settings and how-to for a generalized router with links or suggestions on how to search for anything not covered in the guide. The second section affected was the website. The basic design and layout of the website was complete, spare some content from the thesis. While partially done, it does not feel right to submit not fully complete or refined work.

RESPONSIBILITY

When a data breach does eventually occur, it can be quite shocking and difficult to figure out just who is at fault and where responsibility lies. This section attempts to shed some light in that area, but by no means should be taken as absolute fact for every case, as laws and regulations can vary by country, state to state, or individual case. According to Thomson Reuters Law there is "no current central federal mandate that covers data breaches affecting personal information." Thus, many cases and outcomes are quite different as any laws regarding data breaches are primarily state based and regulated.

One of the first steps to understanding these laws is looking at the terminology regarding data and their subsequent breaches. The end user or customer is the individual or organization whose data is being stored. The data owner is the business that asks for the end user's data for any of a multitude of reasons. Finally, the data holder is the business that is storing the end user's data. Examples of data owners would be PayPal, Amazon, Google, or Walmart. Meanwhile examples of a data holder would be AWS (Amazon Web Services), or other cloud-based data companies. It is not infrequent or impossible for the data owner and the data holder to be the same company, as many have their own servers to store the information

without needing a third-party to store it. Now that the terminology has been defined, what are some examples of data breaches that people might know, and what was the result of these breaches?

The first example is the retail company Target which was hacked back in November 2013. Access to Target's network was exploited by using the network credentials of a third-party HVAC provider, Fazio Mechanical Services, used by Target. Through Target's network, the exploiters were able to access Target's payment system network and gain access to Target shopper's personal information. The question being: why did the HVAC providers have remote access with high privileges on the Target main network? It was later discovered that the connection to the Target network was "exclusively for electronic billing, contract submission and project management." The problem then changes to why the HVAC company was connected to the main Target network and why was their so little security to prevent the breach.

The next example is a well-known data breach: Equifax. The Equifax data breach affected 143 million Americans. In this case Equifax was both the data-owner and the data holder. Equifax announced their breach in September of 2017, although the breach had occurred four months earlier in mid-May of 2017. The vulnerability was through their use of the Apache Struts web-application software. However, the vulnerability was found by the

Apache company and they created a patch in March of 2017. The breach occurred due to the negligence of applying the patch to the Equifax servers. It is estimated that the hackers had access to the system for roughly 134 days. It is unknown if the user's personal data was encrypted at all, but if it were, there would have been plenty of time to decrypt the data in that timespan. Due to this, full names, social security numbers, addresses, dates of birth, and driver license numbers were stolen or compromised. This is an example of an extremely avoidable data breach that caused one of the most well-known and damaging data-breaches in recent history.

Another example is the Israeli cybersecurity company Imperva. According to their official statement from their Chief Technology Officer (CTO), Kunal Anand, there was "unauthorized use of an administrative API key in one of our production AWS accounts in October 2018, which led to an exposure of a database snapshot." In this scenario, the company's data was accessed through their data-holder, however the security flaw was not in the data-holder, but in the security control of the data owner. Imperva created an AWS database snapshot for testing "an internal compute instance that we created was accessible from the outside world," which happened to have the AWS API key to the created snapshot test database. The internal instance was "compromised," and the API key was stolen, thus the API key was used to access the snapshot for testing. At first glance this seems to be a no-harm

done scenario, it was a test database that was compromised, so there should not be any issue. However, Imperva was using actual data from the live databases for testing, rather than fake test data.

A fourth and more recent breach was of bank holding company Capital One in July of 2019. Capital One was hacked by Paige Thompson, previously employed by Amazon AWS, a data holder company. According to Capital One, roughly one-hundred million people in the United States and roughly six million people in Canada were affected by this breach. Krebs on Security, a blog by security journalist Brain Krebs, further researched the breach. It was discovered that the hack took advantage of a misconfigured Web Application Firewall. The firewall was assigned too many permissions, including access to list all the files associated with the web application and read said files. Paige Thompson was later caught by the Federal Bureau of Investigation and charged with wire fraud and computer fraud and faces up to 25 years in prison.

So, what came of these data breaches? Target had their CEO and CIO resign a year later in 2014 and settled for $18.5 million United States Dollars (USD), split between the affected users of 47 different US states. Meanwhile, in the Equifax case, the Chief Executive Officer (CEO), Richard Smith, was given a compensation package with nearly $20 million USD in bonuses, before his resignation in September of 2017. In the case of Equifax, the company

agreed to a settlement of $575 million USD, however not exceeding $700 million USD. This entitled the nearly 150 million Americans affected to receive a total of $125 for nearly all their personal information being stolen in their breach. After Imperva's breach the Chief Technology Officer (CTO) made an official statement and update about the breach. The CTO, Kunal Anand, is still the CTO. The CEO however, submitted their resignation eleven days after the security incident. In the case of Capital One, Paige Thompson was captured by the FBI and faces two charges and a lengthy prison term. She was held solely responsible and there was no compensation to those affected and no one held accountable in the company so far.

With so few and often complex regulations and laws, it begs the conversation that this thesis tries to cultivate. In the case of Equifax, who was it that made the decision or lack thereof, to not update to the most recent web-server patch? Should the CEO be the one to have resigned, should it have been the web developer, or should it be the responsibility of the entire company while understanding that mistakes could happen. In the case that there is a breach, should $125 be all that is owed to someone who has potentially lost their identity, credit score, tax returns, money, and more? Should the government, business, or consumer be held liable for the results of a data breach? What about the internet service provider that provides internet access for the hackers that exploit these businesses? The dates of

each attack show that this is a constant problem that has not gone away over the years even as technology has improved since 2013. With the problem still being relevant it is imperative that more defined and clear laws and regulations be put in place.

CONCLUSION

The average user manual for home networking equipment is often too complex or not optimally organized for a layman to easily secure their home network. This could be alleviated by creating a simple guide in the front of the manual for easy access and readability. This thesis attempted to create a website and generalized home guide for that exact scenario. Many of the issues that are found in the informational documents that come with home networking equipment could be potentially solved with rather simple solutions. The issue of default passwords on routers could be solved with a myriad of solutions ranging from as simple as a sticker over the power button, telling them to change the password, to a much more sophisticated solution of not letting them have access to the internet until the password is non-default. The organization of manuals could instead focus on basic setup then immediately proceed into security to protect the consumer. Just some of these changes could make a difference on the security of the average person's home network.

Furthermore, this thesis sought to bring light to the conversation of where responsibility should lie when a network home or otherwise is breached and personal information of the users is compromised. Current laws and regulations are too obscure or not standardized. Because of this

many people end up uncompensated or under compensated when sensitive personal information such as social security numbers get stolen. This issue could be further expanded if the company is a creator of home networking equipment such as ASUSTeK. The opinion of this thesis is that the business or data-owner should be held liable in most cases of a personal information data breach. When a data breach occurs, the consumers or customers should be notified as soon as possible and without interfering with the investigation. Once notified the data-owner should put forth a program to improve their security of personal data in the future as well as explain the fix of the vulnerability in a reasonable manner. Once this has been done the data-owner should properly compensate the consumer based on data leaked, scale of breach, and other factors if necessary.

These two points can become a combined problem when looking at examples like recent Google Nest hacks and other IoT device hacks. These breaches most likely are caused by a combination of unsecured networks due to frustrating manuals and lack of proper setup for the devices combined with potential vulnerabilities from the developers or manufacturers that will go without compensation. These are problems that still happen every day and will continue to happen until action is taken to fix issues like default admin passwords and convoluted manuals or regulations and clear and concise laws relating to post-breach actions are enacted.

BIBLIOGRAPHY

ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk. 28 July 2016, www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put.

Balaban, David. *How to Set up a Secure Home Network*. 1 Feb. 2019, hackernoon.com/how-to-set-up-a-secure-home-network-a3d0f829fd6c.

Cooper, Stephen. *How to Secure Your Home Wireless Network from Hackers*. www.comparitech.com/blog/information-security/secure-home-wireless-network/.

Crosby, Lance. *Who Is At Fault For A Security Breach?* 30 Sept. 2016, www.forbes.com/sites/ciocentral/2016/09/30/who-is-at-fault-for-a-security-breach/.

Costoya, Joey et al. Securing Your Home Routers. Web. 28 Apr. 2019.

Small, Mike. "From Data Breach to Information Stewardship." Network

Demographics of Internet and Home Broadband Usage in the United States. 12 June 2019, www.pewinternet.org/fact-sheet/internet-broadband.

Erickson, Kris, and Philip N. Howard. “A Case of Mistaken Identity? News Accounts of Hacker, Consumer, and Organizational Responsibility for Compromised Digital Records.” *Journal of Computer-Mediated Communication*, vol. 12, no. 4, 2007, pp. 1229–1247., doi:10.1111/j.1083-6101.2007.00371.x.

Hylen, Chris. *Imperva Security Update: Imperva*. 10 Oct. 2019, www.imperva.com/blog/ceoblog/.

Information on the Capital One Cyber Incident. 23 Sept. 2019, www.capitalone.com/facts2019/.

Kranz, Maciej. *IoT Security: Whose Job Is It Anyway?* 6 Mar. 2018, www.networkworld.com/article/3260984/internet-of-things/iot-security-whose-job-is-it-anyway.html.

Kranz, Maciej. *IoT Security: Whose Job Is It Anyway?* 6 Mar. 2018, www.networkworld.com/article/3260984/iot-security-whose-job-is-it-anyway.html.

Krebs, Brian. *Tag: Capital One Breach*. 2 Aug. 2019, krebsonsecurity.com/tag/capital-one-breach/.

Krebs, Brian. *Target Hackers Broke in Via HVAC Company*. 5 Feb. 2014, krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

Mens, Rudy. *Home Network Security Guide for Beginners*. 31 Jan. 2019, lazyadmin.nl/home-network/home-network-security/.

Mitchell, Bradley. *WPA2 Vs. WPA: What's the Difference for Wireless Security?* www.lifewire.com/wpa2-vs-wpa-for-wireless-security-3971350.

Newman, Lily Hay. *The Equifax Breach Was Entirely Preventable*. 14 Sept. 2017, www.wired.com/story/equifax-breach-no-excuse/.

O'Dwyer, Michael. *Who Is to Blame in Wake of a Data Breach?* 25 Nov. 2019, blog.ipswitch.com/who-is-to-blame-in-wake-of-a-data-breach.

Rijnetu, Ioana. *12 Steps to Maximize Your Home Wireless Network Security*. 18 Apr. 2019, heimdalsecurity.com/blog/home-wireless-network-security/.

Rubens, Paul. *How to Secure Your Wi-Fi at Home and in Your Business*. 10 Oct. 2018, www.techradar.com/news/networking/wi-fi/five-tips-for-a-secure-wireless-network-1161225.

Securing Your Wireless Network. 13 Mar. 2018, www.consumer.ftc.gov/articles/0013-securing-your-wireless-network.

Security Tip (ST15-002). 15 Dec. 2015, www.us-cert.gov/ncas/tips/ST15-002.

Surane, Jennifer, and Anders Melin. *Equifax CEO Richard Smith Resigns After Uproar Over Massive Hack*. 26 Sept. 2017, www.bloomberg.com/news/articles/2017-09-26/equifax-ceo-smith-resigns-barros-named-interim-chief-after-hack.

Who Is Liable When a Data Breach Occurs? legal.thomsonreuters.com/en/insights/articles/data-breach-liability.