Kayvaun Khoshkhou

Professor Tomasevich

CSC300G-04 GWAR

5/16/21

Why Cybersecurity should be Emphasized and Expanded

In this day and age, the process of growth in expansion of businesses and information are exploding to new heights for the world consumers. Most notably, it is the technological area that is paving the way and it is inseparable from what some call the virtual world. Kim Andreasson, editor in charge for the book "Cybersecurity Public sector and Responses," adds on this in the preface, "In an illustration of how rapid progress can be, the average availability of 20 important online public services in the EU27 increased from 69% in 2009 to 82% in 2010, according to Europe's ninth e-government benchmark report" (Andreasson 16). This is why for continued growth, cybersecurity needs to prioritize and expanded to aid this growth. The growth and connection with cybersecurity will be looked at from the perspective of its rise to its importance to the present. Then in detail, it will be fruitful to look at three areas of discussion that cover the different levels of impact and issues pertaining to cybersecurity. Where the first area is the federal security level and where its status is currently at, its history and its effects. Which in turn leads to discuss a more consumer area in specifically individual's banks and information. To get the broad picture of cybersecurity, it is also needed to cover its controversies and drawbacks to help those with doubts feel more comfortable knowing that there is an awareness of these issues and that there are potential solutions. Let's take a look at cybersecurity's rise in importance along with the global trend.

As we look into the rise of technological globalization, the concept of cybersecurity has become a concept that is now a concept heard by much of the world's governments and businesses of the modern day for a means of protection. Daniel Castro convenes that governments like the U.S. government now in the early twenties wanted to make sure they had secure information and telecommunication systems, but the idea of cybersecurity has been here since the seventies with the network and computer revolution (p. 129). The rise of cybersecurity followed closely with the rise of computers in the nineteen-seventies as computers would include forms of communication with bits of data and code attached to them that meant there were certain risks involved. Today computers contain a whole virtual world with the internet that has whole businesses, entertainment and forms of social media available for everyday users which means whole areas of new opportunities in this frontier. The big expansion means positive growth for the economy and new goods and services available for consumers. However, these are also areas added as new potential targets for maliciousness.

There are individuals who are familiar with computer programs and applications' data infrastructure can choose to use their knowledge to invade systems and perform illegal activities that some call "Cyber Attacks." Those individuals are commonly addressed as hackers who choose to attack web and computer systems. There are functions of cyber-attacks that should be covered for the reason why cybersecurity is needed. Chris Bonk, in a chapter titled "U.S. Federal Cybersecurity Policy", wrote, "A cyber-attack will generally render three possible results: one a denial of availability to information, two a compromise of confidentiality of information, or three a subversion of the integrity of information" (Bonk p.257). The first function entails that hackers can pull down web programs that may have certain types of information up for users. The compromise of information means that information that may have been needed to be kept private

for certain groups such as bank account information can also become leaked to the public and then advantage of by others. The third function is addressing how some hackers attempt to take down authority figure sites or web programs to rebel against them by taking down one of their platforms. Another level that Bonk should add is also "DDOS" or denial of service attacks that take down web services for common reasons where either the hacker wanted to test their abilities or for them to unfairly win video game matches. Clearly there are notable risks for systems that comprises of a huge slice of the globe and so cybersecurity is comprised of the individuals knowledgeable in the system's infrastructure that instead defend against such vulnerabilities. One big area of risks is the many governments which are meant to be systems that hold society together from unstable chaos. They are the vulnerable level that encompasses a very large impact that must be analyzed before diving in at the consumer-based level area for cybersecurity.

Governments usually create the laws and programs that create rules and support for all citizens to be a part of. Governments of yesterday are much different than the governments of today as governments are have towards "E-Governments", or governments that can be interacted with through the web rather than going in person. This however means more openings of risks. Jeremy Millard, author for the chapter "Global Rise of E-Government and Security Implications," touches on this writing, "For example, they can pose profound challenges to cybersecurity in terms of unauthorized access to, or use of, data and public sector information. Public sector managers need to be just as aware of these unintended consequences as they are of those they expect when e-government is introduced" (Millard p.39). This goes back to the functions of cyber-attacks discussed earlier where unauthorized access can lead to leaks of government data or subversion on their authority. This in turn is already why governments are heavily invested in cybersecurity. Governments are not foolish to expand further as E-

governments either. Millard writes further “For example, according to ongoing benchmarking reports led by Capgemini, a consultancy, full online availability of a basket of the most common 20 e-government services in Europe increased from 20% in 2001 to 82% in 2010, while online sophistication increased from 45% in 2001 to 90% in 2010. Globally, the 2010 UN benchmarking survey “finds that citizens are benefiting from more advanced e-service delivery, better access to information, more efficient government management and improved interactions with governments, primarily as a result of increasing use by the public sector of information and communications technology” (p.41). People find so much more benefit having wider opportunities to interact with government programs and services that they may not have had the time or commuting resources before available to do so. Having more available knowledge of qualifying for programs, tax policies and penalties such as not having certain insurances is a dire benefit that communities rely on to float financially. It is easy to see that governments affect communities on a big level, and it is important that they are able to connect with each other.

The importance of Governments and them going electronic is why cybersecurity needs to be emphasized upon by their resources and not slowly approached as a solution. People usually picture governments as secure strong areas and impenetrable but governments have actually not shown such strength on the virtual side. “For example, three-quarters (75%) of 217 senior level IT executives at U.S. federal organizations said they experienced one or more data breach incidents in the prior year, according to a 2009 survey conducted by the Ponemon Institute, a consultancy” (Bonk p. 256). Seventy-five percent is an outrageous number of attacks occurring and those numbers are concerning as breaches indicate that the hackers were successful in one or more of their attempts. Such volatility can bring down the trust people have in interacting with E-government and because governments operate heavily electronically it can bring distrust

people have in the stability of the government's security. Millard further adds that a government needs transparency and accountability for them to survive as an E-government and that distrust needs to be a trend that becomes reversed (p.55). Without those factors, it can have big consequences on holding people united as a country. For example, in the U.S. it has led people to question presidential legitimacies with suspicions of foreign cyber-attack involvement such as the U.S. presidential run between Donald Trump and Hilary Clinton. If governments encompass such a large portion of the way society is run then trust needs to be built and can be done so by having a ready number of individuals that notice vulnerabilities, can track hacker patterns, and implementation of more developed encryption or anti-virus applications to combat the maliciousness of hackers. Yet, governments have been slow to do so. Where, "according to a 2008 Organization for Economic Cooperation and Development (OECD) report, there is limited availability of data on public sector efforts. Even in highly advanced e-government countries like Norway, only a minority of public administrations have been offering secure ways of communicating with their websites, despite many surveys showing that fears of data insecurity are perceived by users as the biggest deterrent to their use of e-government" (Millard p.42). This smaller scale effort should not be adopted for the modern-day governments. Where there are number of instances where cyber-attacks can cause economic concerns when they have chosen to deny network service for large scale government transports. It is clear that with the importance of the responsibilities governments hold they should do all they can to secure their systems to be able to govern. Unfortunately, cyber-attacks occur outside of the public sectors of government and happen on the private sector level as well.

As consumers, we all partake in businesses, social media and entertainment online as it has seemingly unlimited uses. However, one area close to our hearts that is especially vulnerable

is the private sector where our financial transactions and bank systems take place. Private sectors have been more apt to be diligent in improving their means of cybersecurity. The *Deloitte Center for Financial* Services shares, "The average annual cost of cyber-attacks has been ballooning for many organizations. So, it was not surprising to find that cybersecurity spending rose among the financial institutions surveyed compared to those responding in the prior year. Respondents to our most recent survey spent about 10.9% of their IT budget on cybersecurity on average, up from 10.1% a year earlier. This equaled about 0.48% of company revenue on average, again up from 0.34%." (Karen Edelman et al. p.4). Business institutions realize more and more the need to invest in cybersecurity and are beginning to pour more of their resources in doing so. It makes sense that you would want to build up your customers trust in knowing the safety and stability of their financial transactions. A merchant would be more likely to take trade routes guarded by soldiers then risk routes plagued with bandits and no guards. Rather than small foot trade caravans, Cyber-attacks have posed as bigger threats on users as they invade identity documents and bank account information. These attacks have happened on big scales affecting many unfortunate people in the millions.

Cybersecurity can be the only thing holding banks back from losing people's hard-earned money as can be shown in a specific case in one of the biggest bank heists of all time. This bank heist was not like the classics in the movies with four armed men with a hostage and a shoot out to get to a getaway car. This took place in Bangladesh and was responsible for a loss of eighty-one million dollars to thieves. *The One Brief*, a site that explores globalization and cybersecurity break down the incident in several parts. The thieves had manipulated the system to trick the bank system in transferring money to their fake accounts. The notifications system for orders was shut down by their malware virus and they did not successfully rob more than eighty-one

million dollars because of a typing error on their part! (The Bangladesh Bank Heist, N.D.). This incident was a prime way of expanding upon areas inside cybersecurity itself. Where cybersecurity is not only an anti-virus computer program or an encoded application, but it also boils down to human people being involved with measures of cybersecurity like we have regular security guards. “You can have the most sophisticated state-of-the-art security systems in the world, but if people are cutting corners or failing to follow instructions, then criminals can exploit that. And human error played a great part in the BCB attack, at several points during which the theft could have been stopped. There is evidence that the workers who installed the SWIFT system in BCB did not follow official guidelines and that could have opened up security vulnerabilities” (The Bangladesh Bank Heist, N.D.). Cybersecurity also involves individuals to understand secure measures that are practiced in the real world also apply to the electronic systems that are in place. Employees trained and aware of guidelines of the ways of cyber-attacks would have them more prepared to prevent such suspicious activities. Had such cybersecurity measures been taken they could have saved those millions of dollars.

It may not seem like it at first but there are some drawbacks and glaring issues for the means of cybersecurity both in the public and private sector that can have some question how far cybersecurity needs to be expanded. First of two points, is that the aspect of cybersecurity of gathering lots of information to be prepared could instead be counterintuitive to being effective as a security measure. The *Harvard International Review* addresses the first point stating, “Overwhelmed by data, analysts lose the ability to pick out what is important and fail to make good judgments. In a 1970 book, futurist Alvin Toffler of the International Institute for Strategic Studies coined the term "information overload" to describe situations in which an excess of information results in poorer decision making” (Young, 2019). Having too much data means that

there would have to be extra resources involved in being able to look through and analyzing all the information which can pose an issue if there is a lack of manpower. That expanding cybersecurity through the means of information gathering leads the system to become spread too thin and instead can also lead to more vulnerability when evaluating too much data. This is further addressed where *Harvard International Review* writes, "Secondly, institutions may face the challenge of circular reporting. In the process of collecting massive amounts of information, agencies may collect the same information twice from different sources. When faced with high volumes of incoming reports, intelligence agencies cannot easily prevent this duplication of data" (Young, 2019). With already lots of information pouring in, information can also be collected many times over without individuals knowing if the database effort is too wide. A process that can end up wasting a lot of time for unneeded effort for information already obtained. If a cyber-attack were to occur the system may be slow to react or detect because it has its hand full.

The second issue for cybersecurity is that it is a concept that can be abused for the means of stepping on others to secure oneself. For example, many countries can use cybersecurity as an excuse to do some hacking of their own to protect their own interests. Nicole Perlroth, an author for *The New York Times*, writes, "Among the leaks on Friday was an extensive list of PowerPoint and Excel documents that, if authentic, indicate that the N.S.A. has successfully infiltrated EastNets, a company based in Dubai that helps to manage transactions in the international bank messaging system called Swift" (2017). The N.S.A being an American agency that possibly had hacked into another regions system to possibly secure U.S. policies in the area or to prepare plans for whatever information they could find would be a breach of trust. Already rumors float around that other countries such as Russia hack into U.S. systems to gain an

information advantage over us. An argument could be made that further expanding into cybersecurity would only lead to those in power to have more power to abuse in the name of cybersecurity. Perlroth indicates an example of the U.S. having been accused of using cyber-viruses to compromise Iranian nuclear facility systems to secure the Nuclear Deal set between them and Iran (2017). Cybersecurity for some means to use cyber-attacks as a part of a defensive strategy like the saying a good defense means a better offense.

It is already clear that I endorse stronger investments into cybersecurity on both a public and private sector and agree that there are some glaring issues that need to be addressed. However, these issues do not lessen the need for cybersecurity but instead means that further expanding cybersecurity means analyzing its ins and outs as a whole to change its path. Instead, there should be a concept within cybersecurity called "Human Behavior" that is studied and then have the results used to change the future path towards cybersecurity's improvement. Millard elaborates on this writing, "Human behavior, whether rational or not, lies at the core of cybersecurity—how people think about their identity, data about their identity, who owns it, has access to it, and how it is used" (p. 48). Human behavior is what drives those to secure assets thoroughly or lazily and drives others to abuse cybersecurity methods or use inefficient methods. Millard speaks further that finding a good balance is still unclear but there needs to be more effort of figuring things out through trial and error, evidence collection, as well as the conscious application of ethical and democratic principles" (p.48). If we focus on the idea of human behavior in cybersecurity, it will need trials to show the results for what will work best. For example, the discussion of the U.S. being rumored to use viruses to secure policies near Iran is a perfect example of the public's involvement with cybersecurity. A common solution for foreign issues is having the public vote on more transparency, and regulations being introduced by their

representatives in both house and state. It does not mean that the public will vote on the best choice or that the perfect bills or laws will be introduced. However, it is a means of getting the ball rolling and having a collective being more aware of a system of defense that they also rely on and should be a part of in the public sector.

Human behavior also involves how cybersecurity professionals perform their duty of encryption, awareness or information gathering. With the issues of too much information being a hindrance, this of course was found with studies done. With study results, there can be implementation of training on this matter for those involved with cybersecurity. A focus on what is important or not and learning from other case examples. From the bank heist in Bangladesh, it was mostly due to human error that they were robbed and that an understanding should be built between the professionals and their systems. The bank heist concluded that there were numerous inconsistencies within the SWIFT program that should have raised alarm (The Bangladesh Bank Heist, N.D.). A system can tell you all kinds of information, but the individuals need to be trained in investigating the information they receive and to avoid circular reporting of information. This training would mean a need to expand resources in cybersecurity to educate and improve the way people handle things behind the computer defense systems. This is just another issue that needs further focus in and either reallocating or pushing more resources in.

To conclude, the world as we know it is pushing new boundaries in the electronic world of computer systems and applications and that means new territory that needs to be protected with cybersecurity. “Cybersecurity is a moving target that evolves with such speed that it is difficult to capture an up-to-date picture of it. New threats, or variations of old ones, emerge every day as do strategies to defend against them” (Andreasson p.327). The way hackers try to invade will surprise many with new viruses, data duplication, and code cracking techniques and

so the ways of cybersecurity need to match them in being trained, up to date on new threats and the new systems being introduced for both sides. Governments have so much importance in confidentiality and controlling E-commerce but are still so vulnerable. It is quite clear that not investing in increasing their efficiency of cybersecurity means delays in their programs and less trust in their stability to run smoothly. This trust runs down to private consumer businesses as well that many regular people rely on to interact with the financial world. Volatility of security for private businesses can introduce a new type of problem of anarchy in the virtual setting if consumers cannot have trust in systems like banks to keep their money safe. The glaring issues that cybersecurity faces of greedy information gathering and having cyber-attacks abused under the guise of cybersecurity are issues that clearly will be here for the future. It must be addressed and then run through the lens of an analysis of human behavior being the key player. Much more studies and trials must be done either through political reform and the way sectors train their cybersecurity professionals. It is not going to be left up in the air for waiting for the new anti-virus program. It will also involve the minds and hands of the people being involved in this system. Realistically, a perfect result is less than likely for the outcome of cybersecurity for governments and the private sectors, but the world is not going to quit growing through the electronic world and it’s in everyone’s best interests to be kept up to date and aware to protect themselves.

Works Cited

Andreasson, Kim. *Cybersecurity: Public Sector Threats and Responses*. CRC Press, 2012.

Bachman, Hannah, et al., editors. *Reshaping the Cybersecurity Landscapes*. Deloitte Development LLC, 2020.

Bonk, Chris. "The Civilian Cyber Incident Response Policies of the Federal Government." *Cybersecurity Public Sector Threats and Responses*, edited by Kim Andreasson, CRC, 2012, pp. 255–275.

Castro, Daniel. "U.S. Federal Cybersecurity Policy." *Cybersecurity Public Sector Threats and Responses*, edited by Kim Andreasson, CRC, 2012, pp. 127–159.

Millard, Jeremy. "Global Rise of E-Government and Security Implications." *Cybersecurity Public Sector Threats and Responses*, edited by Kim Andreasson, CRC, 2012, pp. 1–27.

Perlroth, Nicole. "Hacking Group Claims N.S.A. Infiltrated Mideast Banking System." *The New York Times*, The New York Times, 15 Apr. 2017, www.nytimes.com/2017/04/15/us/shadow-brokers-nsa-hack-middle-east.html.

Young, Alex. "Too Much Information: Ineffective Intelligence Collection." *Harvard International Review*, Harvard International Review, 18 Aug. 2019, hir.harvard.edu/too-much-information/.