Importance of Cybersecurtiy in Big Infrastructures

Omarion Branch

Old Dominion University

IDS 300W

Dr. Patricia Oliver

December 8th, 2023

Abstract

"It takes 20 years to build a reputation and a few minutes of cyber incidents to ruin it."(Unknown), This short but meaningful quote is something I found on a blog posted on Balbix and is the heart of the purpose for this paper. See cybersecurity is a new major field that is still getting its feet wet in the industry and is starting to spark an interest in many people ranging from high schoolers to 40 year old adults. But what exactly is cyber security? Why is it important? What are the pros and cons? There are an endless amount of things you could ask about cybersecurity, but for this research paper I'm just going to go over the basics. I will be taking an interdisciplinary approach in order to present the importance of cybersecurity. We will be taking a look at economic, computer science, psychology, and political stand points. Cybersecurity in simple terms is the practice of protecting systems, networks, and programs from digital attacks according to Cisco. In order for any big company or business to achieve the goal of "secure network", one must be able to have valuable knowledge in multiple categories of disciplines. Now before we get into depth completely here we must address that each thing listed within this research will not guarantee a 100% safe network. Sadly there is no such thing as a 100% secure network, but there are measures in place that allow for companies to manage gains and losses without it being a total disaster within the organization. Now I know what you're thinking "Why don't they just put in proper training and people in order to be more secure?," well sadly it's not that simple and leads us into our first area of discussion. Economics.

Economics

Now as we all know money makes the world go round and money also makes a difference into how much a company is willing to put in to achieve its goals. "Cybercrime is estimated to have

cost the global economy just under USD 1 trillion in 2020, indicating an increase of more than 50% since 2018. With the average cyber insurance claim rising from USD 145,000 in 2019 to USD 359,000 in 2020(Frank Cremer). As you can see there is a major growing necessity for improvement in cyber information, stabilizing databases, and public awareness but it all comes down to money. As an organization there should be a budget rule of 10% in place that goes directly into IT workers and computer security needs. For example if your business is bringing in $3 million dollars annually then you should be spending at the least $300,000 in your IT area. Now of course this number varies depending on what exactly your business is in charge of and how valuable the information you're holding is. But there will always be room for improvement because we are in a time period where technology is growing faster than we can imagine. Putting forth money in the latest tools and softwares can not only benefit your company security but allow for your employees to be familiar with the latest trends.

On December 25, 2014 , Sony and Xbox were victims of one of the most devastating Christmas day events in the world. A group of professional hackers known as Lizard Squad, hacked into Playstation networks and Xbox live and launched a DDoS attack against both gaming companies. A DDos is a malicious attempt to interrupt the normal traffic flow within the targeted server or network by overwhelming the target with an extra flood of internet traffic that it is not prepared for, causing it in most cases for the network to freeze or completely shut off. This attack caused over 160 million gamers to not be able to use their gifts. This also made Sony and Xbox lose collectively over $25 million dollars on Christmas day. "losses from cyber-related risks might reach US$ 6 trillion in 2021. Due to the digitalization of business and economic activities via the Internet of Things (IoT), cloud computing, mobile, blockchain, and other innovative technologies"(pavel). The growth of technology is extremely dangerous and has already started

to have its impact on society as we speak. A lot of countries cannot afford to lose this type of profit as that causes inflation within the communities. Companies would start charging more for their services or network servers in order to cover up some of the loss and this just goes to show hackers are starting to become much more money hungry as they are motivated by these large sums of cash.

Computer Science

"Cybersecurity strategies are considered increasingly central and crucial aspects of the transformations. Cybersecurity relates to processes and networks designed intelligently to digitally protect unauthorized access" (Medoh). In order to have a secure network that is stable and completely thought through one must have an understanding of computer science. Computer Science primarily focuses on the development and testing of software and software systems. While cybersecurity focuses more on securing networks, we wouldn't be as successful without them. One famous quote said by Doug Linder is "A good programmer is someone who always looks both ways before crossing a one-way street", now this is a great analogy to use when speaking on the interconnection between cybersecurity and computer science. In order for a programmer or company to be successful one must look at both fields in order to gain the knowledge needed. Of course there are multiple ways of solving the problem but most importantly the foundation all starts here. Having the understanding of this will allow for a company to analyze data more effectively and communicate amongst their employees exactly what they;re looking for. A computer science specialist makes up roughly around 45% percent of the IT team. Each member of that 45% will all be assigned a task where most of their focus will be. For example a team of 4-5 people will be in charge of constructing the software and the other team will be in charge of pointing out the flaws of the software before moving into the hands of

the overhead supervisor. Once the supervisor has approved the program it is then released to the cybersecurity unit where they will be inserting all the security measures needed to insure the software is ready for public or private use. But that's just the start, once this software is officially released they are to monitor it for any flaws that were possibly missed or need improvement. This is just the constant cycle it goes through daily to make sure all data is where it needs to be and that nothing has fallen into the wrong hands.

Psychology

Now when it comes to constructing a plan for your company, one must understand how a hacker thinks or operates. We must determine if there is a relationship between the age, gender, and nationality of hackers and characteristics of the cyberattacks that they perpetrate. This takes a serious amount of effort and research due to the fact that you're trying to identify and describe people who sit behind a computer screen. But yet not all hackers are considered bad people either. Hackers typically fall into three categories based on the attack that was executed. You have your black hat hacker who illegally crack into systems with malicious intent with hopes of getting into unauthorized systems and exploit them. Then we have the White hat hackers, these people are the ones who have permission from the company to hack into the system and find weak points. Once the weak points are spotted they typically create a blueprint and fix them before a criminal finds it. Lastly we have Grey hat hackers, these people don't have the malicious intent like a black hat hacker but yet they don't have permission to do what they're doing either. These hackers typically will get into the computer systems and then email the company telling them what they did but won't tell them in full detail until a certain amount of payment is given to them. It's almost like blackmailing. Over the past 10 years black hat hackers are starting to increase more and more each year, especially in the younger age groups. From 2018 to 2022

there has been an increase of 10% for hackers in the age group of 18-30 with about 91% of them being males. “studies found that nationalistic hackers are more likely to hack enemy nations than their own”(Joshua). This means when protecting your system one must be able to prepare for anything. We are in a new era where war is being taken through network battle instead of physically. It’s been happening for a while now but it's just now being seen by the public eye. Many of these hacks going on now are done by hackers from other countries in more of a statement saying hey this is what we’re capable of and should watch how to approach us. This kind of hacking done by hackers is referred to as respect. They have no intentions of leaking information nor gaining money. They just want to be known for what they’re capable of and the damage your systems can be in. why yes it's still alaming and can hurt your organization but this gives you an understanding that some criminals just enjoy playing mind games. “Motivations for hackers include ego, exposure, monetary gain, revenge, sabotage, disinformation, and Infowar (cyber-war related)” (Shoemaker & Kennedy).

Political

The most common statement people say is that IT should just secure the networks better so that nothing can ever get hacked. But there’s a problem with that statement and doing so. See when it comes to cybersecurity there’s a thin line you thread between right and wrong.. “The protection of an individual’s and a citizen’s rights and freedoms was used in an approach that calls for the implementation of political conflict…” (Liudmyla). This has been one of the biggest debates the past few years in the cyber world. We the people trust these big companies and organizations with very sensitive information that could change a lot if put into the wrong hands. Most hackers are looking to steal this type of information in hopes of making a profit. Now there have been several policies made over the past few years that try to protect human rights but however most

of them are little too broad and lack a clear understanding. This is why most cyber criminals get away with most of the crime they do. Usually if a criminal is actually caught they get a few years in jail maybe, but if they get away with the crime how can we fully trust anyone with our information or data. Government officials have been trying to push for better laws and regulations on the internet but it's hard to control something when people are always finding loopholes and let alone trying to regulate over a billion people isn't an easy task either.

In conclusion, the importance of cybersecurity is a major deal in the world we live in today. Everything is starting to be shifted into an era where our devices can control everything and as long as we have these devices hackers will always be around to try to steal information. It's up to us to start promoting smarter tactics on the internet or promote the cybersecurity field to more people. We cannot afford for these major companies to keep losing money or hackers to be a step ahead. Within the next 10 years the amount of IT people we have in the world is going to make a difference in whether we are able to compete in the cyber world or not. Everything must be protected and all data should have the same amount of security regardless of how important it is. The technology is changing in front of all of our faces. We can either embrace technology and enhance what we have or we can stay in the dark and let the darkside of the internet control and steal from us on a daily basis.

WORK CITED

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022, February 22). *Cyber risk and cybersecurity: A systematic review of data availability*. The Geneva papers on risk and insurance. Issues and practice. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8853293/#:~:text=Whilst%20it%20is%20an%20emerging,2020%20(Maleks%20Smith%20et%20al

Gerstenfeld, J. (2023, March 31). *Understanding the connection between hackers and their hacks: Analyzing USDOJ reports for Hacker Profiles*. Virtual Commons - Bridgewater State University. https://vc.bridgew.edu/ijcic/vol6/iss1/5/

Kormych, L., & Zavhorodnia, Y. (2023, August 10). *The concept of modern political confrontation in cyber space*. Academic.oup.com. https://academic.oup.com/cybersecurity/article/9/1/tyad017/7240366

Shevchenko, P. V., Jang, J., Malavasi, M., Peters, G. W., Sofronov, G., & Trück, S. (2023, January 24). The nature of losses from cyber-related events: risk categories and business sectors. Academic.oup.com. https://academic.oup.com/cybersecurity/article/9/1/tyac016/7000422

Medoh, C., & Telukdarie, A. (2022, March 8). *The Future of Cybersecurity: A system dynamics approach*. Procedia Computer Science. https://www.sciencedirect.com/science/article/pii/S1877050922002393