How Exactly Does Cybersecurity work?

Omarion Branch

Old Dominion University

Intro-Tech & Scientific Writing

Professor Garcia

February 28, 2022

When people begin to think about the cyber world, they look at it as a complex program with just and never know exactly where to begin when it comes to trying to understand how it all works. Like most people know we are in a time where all our data and personal information is being placed into clouds and databases instead of the old fashion paper in a file cabinet method. Now I'm not saying we don't use papers anymore but it's slowly starting to become something businesses are stepping away from which is where the cyber world and security come into place.

To make this simple as possible when organizations look to go into storing data, they typically break it down into these categories: budget, construct, apply, and maintain. These 4 words all go hand and hand with each other when it's time to secure personal information. The problem is not everyone knows how hard this is and when they hear a company has been hacked or breached, they just automatically assume they didn't prepare for it.

According to the resource center's 2021 data breach report, "there were 1,862 breaches, up 68% from the prior year, and exceeded the 2017' record of 1,506". Now before we all start to panic, these numbers are not as bad as they look. Whoever had a hacker may have gotten into the system, but most of those companies were able to secure their data back before it was too late.

Now the questions present themselves, how does a company budget? How to construct? How is it applied? And how can one maintain their information?

To identify this topic I used a computer, databases, and online articles & blogs made by professional cybersecurity experts. Limiting down to exactly what I was looking for was troubling at first, but I soon gathered the idea to attack the key points listed above after every article I read consisted of those points. Gathering the information needed by taking out what seemed to fit the scheme of my paper became easier after words.

Getting more in depth with the information I decided to go investigate a few notes that were presented within my cyber course that I'm currently in right now. This allowed me to take down notes on the different types of organizational patterns that were presented within the infrastructure of constructing a secure database within a company. I also looked at a few YouTube videos that were able to break down step by step how it all starts, so that I could explain the points that I will be trying to make.

To explain everything in this paper I will be using a chronological pattern so that way everything can flow in order, and nothing will seem out of place. Allowing this will keep my reader engaged and when terms from past paragraphs come up, that can easily go back and look at the definition, so they aren't confused. Also, the information will be given in a mixture of both quantitative and qualitative data, so that everything can be supported with high quality facts and precise numbers.

Now as far as the order we will be going from which is: budget to construct to applied then to maintained. I chose this order only because it allows me to provide great details and definitions as the terminology gets a little difficult as the paper goes. But as you follow along with me, you'll be able to have enough basic knowledge to understand that the cyber world isn't as confusing as people make it out to be.

According to Deloitte reports, "the average business will invest between 6% and 14% of its annual IT budget in cybersecurity." Which is quite good because at a certain point companies used to spend only 10% and call it a day. Although these numbers may seem low, we still must take into consideration how they must pay their employees, cover training and manage other maintenance. When deciding where to put your money it can become extremely difficult when breaking up the percentages. The average person will always say, "put more money into technology instead of the employees." But understanding why that isn't the best idea can be difficult to understand so let me break it down for you.

While our world is becoming more advanced day by day, the technology we use is also growing at a rapid speed. But as many people know technology will have errors here and there which will need fixing, correct? This is where the employees come into play. Being able to take out enough money to cover the employees pay and training is critical. Because no technology is good enough to take out what humans can bring to the table. Jason (2021) "Cyber professionals continually educate themselves on changing and growing cybersecurity threats so they can protect the agencies that depend on them. Humans update systems with new knowledge to eliminate advanced and persistent attacks from cybercriminals seeking sensitive data."

Being able to go into systems and update them with new knowledge is the main reason we cannot rely completely on just technology itself. Humans bring in the knowledge and the systems react based on what we implement into them, which is the reason you need a firm budget and balance between training your employees and security systems.

Now that we have balanced out where your money is going it's time to construct your plan for how you'll be securing the data.

When constructing the plan for how you want to build your security system, many organizations use the CIA triad model. The CIA triad is an information security model that helps guide organizations when it comes to keeping their data secured. The CIA is made up of three key components, which are confidentiality, integrity, and availability. Confidentiality goes for only allowing authorized users to be able to access data. Integrity means data should be in the correct state and no one can modify it improperly and availability just goes for the authorized user to be able to see and access the data at any given time and point when needed. But most foundational concepts, CIA doesn't have a creator, it was more of just three separate components that were established over time that then came into one big group. Which was proven by this sentence here, "It's also not entirely clear when the three concepts began to be treated as a three-legged stool.

But it seems to have been well established as a foundational concept by 1998 (Fruhlinger, 2020)." For example, PayPal provides confidentiality because it not only asks you to sign into your account, but it'll also send a verification code to your phone to allow full access. Data integrity is presented by presenting you with information anytime an order is placed through them, and last availability is shown because PayPal allows for their services to be used 24/7 whenever you want too. But all this falls under one category/rubric which is confidentiality. This leads into authentication (a process that allows systems to determine if a user is who they present themselves to be) and authorization (determines who has the right to access whatever data they need to get into). In conclusion the CIA is a great tool to use for planning your infosec strategy and getting a foundation laid out for your organization. If you utilize each category correctly it can provide great security for important data which is going to be explained below.

When applying and maintaining your security system everything above is put into consideration. Once you have found out how you want to structure your system, applying and maintaining it becomes a lot easier. Most companies when it comes to this part tend to try to organize certain roles within the organization. Meaning that everyone within the cyber security part has a hand in all of this. Most of the information is presented to the works through a SCADA system. Within the SCADA system it allows for multiple networks to be run at once and gives overview of the systems data in charts. Yes, this may be very effective, but it can lead to disasters if it is done incorrectly, which is why companies tend to hire top notch candidates for the position they are trying to fill. But the networks they use are not just regular everyday networks, they avoid using default network ports for several reasons. The main reason is default ports are often under fire for brutal attacks due to how common they are. When avoiding default ports, it makes the hackers try different port variation numbers. This usually leads to the hackers getting frustrated and just giving up.

Another way is using encrypted data. This allows for your data to be put into all kinds of crazy formations when moving or storing sensitive user information. Therefore, if a hacker were to somehow get the information during transitions, it will remain safe because they cannot quite make out what they are looking at. According to Verizon, “80% of data breaches are caused by compromised passwords.”, meaning that passwords are not as secure as we think they are. To cover for this companies usually will add another layer of security known as the multi-factor authentication process. Which most people have in common with today. For example, when you log into your Instagram accounts it will send a code to your phone number after you have typed in your password. So even if your password is somehow guessed correctly, they are going to need the other codes to get in.

Lastly, make sure to use database and web application firewalls. These are usually the first line of defense for keeping out cyber attacks anyway. There are three most common ones that people use: packet filter firewall, stateful packet inspection which is known as SPI, and proxy server firewall. Making sure that the firewall can cover certain loopholes correctly is vital to random cyberattacks. This also means that you should keep your data in backup saves on a regular basis. This limits the risk of losing sensitive information due to attacks or even just a simple data corruption error. Being able to retain any data that may have been lost can save a company a lot of money and customers.

All companies do a great job when it comes to planning out their security systems. Starting off with the budget allows for them to send the correct amount of money throughout the whole organization while weighing in the risk factors that come along with it. Being able to split the money between training, technology, and employees allows for a great start to the foundation. Constructing the plan you want to use may seem difficult but if you follow the CIA triad you will be able to look at most of the vulnerable points within your infrastructure and limit yourself down to something that is the most effective for the company. Lastly, you must apply and maintain your systems. Having the most qualified people for your systems allows for your company to be able to really focus on the points you want covered. Using different methods to mitigate the risk of a data breech is surely helpful and should always be used in order to decrease the risk that could be presented.

As the world of technology evolves day by day, it is important for us to stay in the loop of ways to keep our own data safe. We cannot predict when attacks are going to happen, but we can limit the amount of damage that can possibly be done. Hackers are only going to get more creative as time goes on, so we have to be prepared for any that comes. The more people and security we have on the front line, the easier it will be for us to win the cyberwar battle. So take your information and be very careful how you store it.

References

SecurityScoreboard. (2021, November 10). *What is the CIA Triad? Definition and Examples*.

SecurityScorecard. Retrieved March 28, 2022, from https://securityscorecard.com/blog/what-is-the-cia-triad#:%7E:text=Confidentiality%2C%20Integrity%2C%20and%20Availability.,organization’s%20security%20procedures%20and%20policies.

SCADA systems. SCADA Systems. (2022). Retrieved March 22, 2022, from http://www.scadasystems.net/

Capone, Z. T. Z. B. J., &amp; Capone, J. (2018, May 25). The impact of human behavior on security. CSO Online. Retrieved March 22, 2022, from https://www.csoonline.com/article/3275930/the-impact-of-human-behavior-on-security.html

Cichonski, P. (2012). Computer Security Incident Handling Guide. *Computer Security Incident Handling Guide*, 1–51.

Opurum, P. (2021, December 21). *The Importance of a Security Budget*. FieldEdge. Retrieved March 26, 2022, from https://fieldedge.com/blog/importance-of-security-budget/

Authors, T. G. (2021, February 24). *10 Database Security Best Practices You Should Know*. The State of Security. Retrieved April 13, 2022, from https://www.tripwire.com/state-of-security/featured/database-security-best-practices-you-should-know/

Howarth, F. (2014, March 11). *5 Key Steps to Ensuring Database Security*. Database Trends and Applications. Retrieved April 17, 2022, from https://www.dbta.com/Editorial/Think-About-It/5-Key-Steps-to-Ensuring-Database-Security-95307.aspx