Cybersecurity essentials

understanding protection in a digital world[i]

Michael Heber

Bachelor of Science degree from
the University of Maryland, College Park
Cyber Security in the United States Federal Government
E-mail: graybeardsecure@gmail.com

Recebido: 10 set. 2025 Aprovado: 10 nov. 2025

Abstract: This essay on cybersecurity summarizes the virtual presentation held for students and faculty at Fatec Itaquaquecetuba in the second semester of 2025. This is an updated discussion with examples of emerging technologies in practice. The question is: how does protection occur in a digital world? I am going to touch on a couple of main topics and observe how that integrates into the job market. So, even in the cyber security career field, AI is an enhancement right now. That is not to say that it will not replace jobs, but it will create jobs.

Key words: Professional Career. Cybersecurity. Digital World.

Resumo: Este ensaio sobre segurança cibernética sintetiza a apresentação virtual realizada para estudantes e professores da Fatec Itaquaquecetuba, no segundo semestre de 2025. Trata-se de uma discussão atualizada sobre tecnologias emergentes na prática. A questão é: como ocorre a proteção em um mundo digital? Abordarei alguns tópicos importantes e analisarei como isso se integra ao mercado de trabalho. Portanto, mesmo na área de segurança cibernética, a IA já representa um aprimoramento. Isso não significa que ela não substituirá empregos, mas sim que criará.

Palavras-chave: Carreira Profissional. Segurança Cibernética. Mundo Digital.

Resumen: Este ensayo sobre ciberseguridad resume la presentación virtual realizada para estudiantes y profesores de Fatec Itaquaquecetuba durante el segundo semestre de 2025. Esta es una discusión actualizada con ejemplos de tecnologías emergentes en la práctica. La pregunta es: ¿cómo se produce la protección en un mundo digital? Cubriré algunos temas importantes y analizaré cómo esto se integra en el mercado laboral. Por lo tanto, incluso en el ámbito de la ciberseguridad, la IA ya representa una mejora. Esto no significa que no vaya a sustituir puestos de trabajo, sino que creará otros nuevos.

Palabras clave: Carrera Profesional. Ciberseguridad. Mundo Digital.

Introduction

Good morning, everyone. My name is Mike Heber. I am from Maryland in the United States of America. Today, I will talk with you about information technology and cybersecurity and help you understand how protection occurs in the digital world.

I was introduced very early in my life to computers. My father realized back in the 1970s that computers were going to become a very important part of how business would be conducted. At that time, he spent a lot of money buying a computer to put in front of his children so that they could be exposed to that technology. Little did he know that two of his sons would eventually turn that into a career.

I received a Bachelor of Science degree from the University of Maryland, College Park, in 1988. I have 30 plus years of experience in a wide range of Information technology and Cyber Security. I spent 21 years working for the United States Federal Government as a contractor doing cyber security and I spent a couple of years as an instructor in a specialized course for government employees.

About my background in five (5) points:

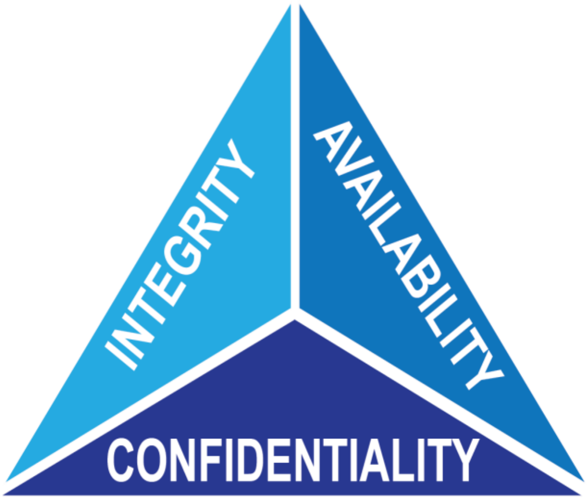
1. It was introduced to computers at an early age (9-10).
2. I received a Bachelor of Science degree from the University of Maryland, College Park (Dec 88)
3. 30+ years of experience in a wide range of Information Technology/Cyber Security.
4. 21+ years working for the United States Federal Government as a Contractor in Cyber Security.
5. Lifelong learner. I spend some of every week reading and trying to learn new things.

Figure 1 – My other computer

The CIA Triad

To start a discussion about cyber security and give you some perspective on what that entails. I am going to touch on a couple of main topics and observe how that integrates into the job market. One of the key cornerstones of cybersecurity is called the CIA Triad (fig. 2). This consists of Confidentiality, Integrity and Availability:

Figure 2 – The CIA Triad: The Cornerstone of Security



Reference: The Author

1) *Confidentiality*: keeping secrets secret.

Any company or government has things that they want to keep in-house. They do not want their trade secret to get out without them having to look at it. How do we protect confidentiality? One way is to limit access. We can use passwords. We make shared documents only available to certain people, and emails are encrypted. In this way, we know that people are talking with the right person, because encryption keys are used to protect that communication.

2) *Integrity*: Ensuring data is accurate and unchanged.

The second piece of this triad is called *Integrity*. It ensures that the data has been unchanged. How do cyber security professionals protect the integrity of data? One way is something I've already mentioned. We can encrypt the data and evaluate people who have passwords for it. Another way is to back the data up. If the data should become corrupted, we can recreate it. And not lose whatever we have created.

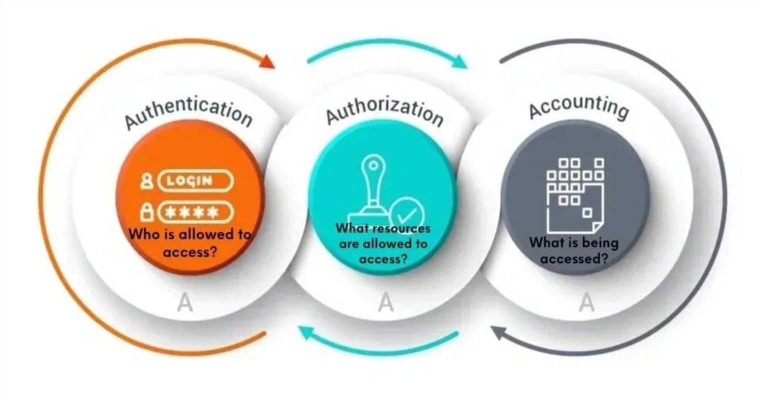
3) *Availability*: Making sure systems are up and running when needed. If I have a computer system and it's only available 10% of the time, it's not very useful. If you look at cloud computing people like AWS, they have 11 9s availability. What that means is that throughout the course of a year the data that you store in the cloud might only be unavailable for five minutes. That is a broad claim. But they have data that shows that it is exactly what they are doing.

The central theme in cyber security really rests on the pillars of Confidentiality, Integrity and Availability

The Security Trifecta: Authentication, Authorization, & Accountability

Another pillar is something called The Security Trifecta: Authentication, Authorization, & Accountability.

Figure 3: The Security Trifecta: Authentication, Authorization, & Accountability (AAA)



Reference: The Author

Authentication means who is allowed to access the data. When we talk about confidentiality, in the previous slide, we talk about the way that we protect confidentiality is through authentication. We protect certain areas of the network or certain devices on the network by using passwords or pass keys or multifactor authentication. If you have ever used Google's authentication, by logging into a website, you might put your username and password and then be asked to give a numerical string that changes every 60 seconds. That authentication is synced up to the computer system and your account. And only you are getting that string of characters. So, this authentication is an addiction layer of protection ensuring that whoever is connecting to the system is the right person.

In addition to Authentication, we have *Authorization*. An example that I can give is Cisco has a product called the Identity Service Engine (ICE) which embodies the concept of the AAA – Authentication, Authorization, & Accountability. And marries it to all network devices that are out there. So, if you are not in the ICE system, you cannot log into those devices. But you might only be able to see a couple of the devices that are out there. That's a way to protect those devices from everybody being able to get into them and manipulate them.

The last piece of AAA is called Accountability. One thing we want to be able to do in cyber security is if a chance is made, we want to know who made it and when it was made. If something goes wrong, that trail of information will help us to diagnose. And help us figure out why it was changed and if it was changed appropriately.

Another pillar inside of cyber security is this concept of AAA.

When security fails real-world examples

Here we have a real-world example of when some of these security principles fail. In 2017, there was something called Equifax Data Breach. In this data breach, 147 million Americans' data, their credit histories were taken by someone outside of the Equifax Organization. I happen to have personally been and my wife was personally affected by this. We got letters from Equifax letting us know afterwards that they were sorry, but our data was taken. Not a wonderful feeling and fortunately nothing was done with it.

Let's look at how those principles failed or if they failed in terms of this real-world example. Confidentiality in this case is personal information that Equifax held. Things like American Security social numbers, their home addresses, possibly email addresses, and their telephone numbers. The perpetrators of this theft of data used vulnerability in something called Apache Struts, which is a part of a web application. It allowed them to bypass the security that was in place and essentially elevate themselves to a position of being able to take whatever they want out of the system.

In the CIA triad, one of the things that failed was confidentiality because information escaped the system in a way that it wasn't intended to. We can look at integrity. The question is was any of the data changed. Fortunately, in this case, none of the data was changed. But suppose as a nefarious person, I wanted to affect some people. I got in that system, and I changed the credit history to make it look like they didn't pay their bills, and it made that harder for them to go to banks or credit organizations and try to get access to money. Or I could flip the script there and maybe I say “Hey, I’ve got the best credit there is. You should loan me as much money as I am asking for.” In this instance, The Equifax data breach, integrity was maintained, because the people that got the data didn’t change any of it.

The third pillar that we talked about was availability. In this case, Equifax must take down their systems to investigate what happened, making it hard for banks and creditors to ask: is this person a good debtor? Do they pay their bills? So, of our CIA triad, two of the legs were essentially broken and allowed for this breach to influence all of 147 million Americans. Let's now look at the pillars of AAA.

The breach occurred because Equifax failed to patch a vulnerability in a timely fashion. This is a very common theme in the cyber security world. If you work in this industry, you must balance a lot of things. Banks, the Federal Government, have computer systems that must stay up around the clock, 365 days a year, 24/7. But if they don’t patch, they become easily vulnerable to things that are occurring in the cyber world.

One of the things companies and governments struggle with is how do we patch this? How do we maintain access to the data but protect it? That's a constant struggle. I’ve worked in places where we had teams of people that all they did every day on a global network was go out and push patches out onto network devices. We had a lot of coordination that had to occur because they were literally hundreds or thousands of devices. When a patch came out, we had to come up with plans.

What areas of the network would get pathed when? Do we have people locally if something goes wrong that we can depend on to help us solve that problem?

The other thing that Equifax did was they were slow to notify individuals about the breach that occurred. That is a contentious point right now. If you follow the news about 10 years ago, Americans created an organization called CISA – the Cyber Security Infrastructure Security Agency. And one of the things that American did was it enacted into law a policy that said if a breach occurs, companies have a certain amount of time to report that to the government and to report that to the individuals affected. And if they fail to meet that requirement, they can be held liable in other ways. That was a good step in moving towards helping the community get educated and helping corporations to be accountable.

If you are a CISO of a corporation and you are breached, one of the things that you might do is say: “we don’t want people to know now about this.” And the Federal

Government said: “No, you need to tell us, and you need to tell the people it was their information. If you follow the politics in America at the end of September, some of those requirements lose their funding. But I think in the short term when that funding gets turned back on, those requirements will come back and snap back into place, because we have learned as a country that reporting that information has more benefits than hiding it. Here is a real-world example personally that affected me in which a security breach occurred, and it can have a long ranging reach into who it affects.

Another attack occurred back in 2020 which was somewhat startling and even now we are still as a community struggling with how to deal with it was the SolarWinds Cyberattack. SolarWinds is a computer program used by very large organizations to help manage their networks. You can imagine that a country, a continent or a global community who has a network struggle to keep the arms wrapped around the devices and the data that are flowing across those devices in their environments. In this case, the SolarWinds software which was used to monitor and help manage those was attacked. A back door was placed into the code in the company that writes the software for that and, for quite a long time, that back door went undetected. The software got pushed out into a lot of these organizations. It became a new and huge problem. Thousands of organizations including the government agencies and corporations discovered that they had a back door, and somebody was getting into their network that they did not know about.

* * *

Let’s look at those the CIA triad and the AAA foundations, in this case, were affected.

In terms of *confidentiality*, the attackers were able to get at information that was sensitive to both government agencies and Fortune 500 companies. Again, the confidentiality leg of our CIA triad was broken.

In terms of *Integrity*, it wasn’t the integrity of the data. Although they could have manipulated the data, it was the integrity of the software. The company that manufactured the software programmers did not detect that a change had occurred and that allowed a back door to be inserted. Then when that software got rolled out globally, a lot of organizations were now vulnerable to this attack.

In terms of *Availability*, a lot of organizations had to take their monitoring systems offline. They had to take their computer systems off the internet. So, businesses impacted, the ability of their employees to do their jobs were impacted. I don't know what the number was, but you can take a pretty good guess that financially many of these organizations ended up losing a lot of money, because something that happened and, in many cases, it was not even in control. It was the manufacturer of the software that they had purchased. They trusted that it was ok, only to discover later that the supply chain had been compromised, and this is called a supply chain attack.

In our Triad AAA arena, authentication and authorization are breached. The attackers were able to bypass normal authentication mechanisms. They were allowed to grant themselves higher authorization in the system. It is a nightmare when you must go back behind and try to figure out what accounts were breached. If new accounts were added and what authorization they had. From an incident response perspective, it can take a long time to clean up these messes. That means companies are spending dollars that might have gone to people's salaries. It might have gone to expansion of their business.

Cyber-attacks can have a wide-ranging effect both inside of countries, inside of corporations and sometimes even globally. This attack was not detected for more than a year. I cannot remember the exact timeline, but a year is a long time for an attacker to have unfettered access into a computer system. I am sure there were some corporate executives who had taken a lot of Advil because of what occurred.

Common cyber threats & attack methods

Let's move away from the core tenants and talk about some things related to cyber security. There are common cyber-attacks and threats that are out there. A term that you will hear is Malware. This is a broad term about viruses, trojans and other software. Some of you have heard right now about an attack inside WhatsApp that is spreading software that allows an attacker to gain access to computer systems. It is essentially a worm which is another term for malware that gets into your phone and then spreads via people in your personal contact list. This malware movies quickly. There have been cases in which it can burn through computer systems like wildfire.

At the beginning of my career, I don't know if I am going to date myself here because this goes way back in history to the 1980s. There was something called the Morris worm. It was the first malware ever created. Mr. Morris was a student at Harvard or Yale University and at the time the internet didn't exist. It was a connection of education computer systems. He discovered a vulnerability in one of the standard programs on that computer system and he used it to create an attack, and he thought that his attack was going to affect the local computer system. So, he ran his attack, and it was successful. He shut off his terminal, and he went back to his dorm. Unbeknownst to him, it began to spread and across the next 24 to 48 hours, it infected many of the mainframes in educational facilities across the country. It was so bad that many of these universities had to unplug from the education net that existed. It took days for them to figure out what happened. Remember, they're now offline.

So, at that point in time, they had to call other universities and work together through the phone system to try and figure out what this was. In the end, Mr. Morris was prosecuted by the federal government and spent several years in prison. When he got out of prison though, the National Security Agency called him and offered him a job. This is a long time ago. You can see that sometimes viruses have unintended consequences and even get out of control of the creators of that virus.

Let's move on to Social Engineering. This is a broad term. In general, it is a manipulation of people to gain access to something. It could be access to money, It could be access to computer systems. You can research the literature and see many cases where someone who has what is called a "gifted tongue" makes a phone call and convinces the recipient that they are part of the organization or that they are acting on behalf of the CEO. As a result, they can gain access to information or resources that they shouldn't have access to. Social Engineering is a broad term.

Underneath that term is something called phishing. This is when you get an email and it appears to be a legitimate email and at the backside of that email, it is used to manipulate or attack the person who it was sent to. This is a big problem right now globally. I get phishing emails probably 10 times a week and so do my friends, and it is getting harder to detect them.

We are talking about artificial intelligence (AI) a little later. One of the downsides of AI is that an attacker who is not native to a particular country uses it to craft an email. In such a way that is grammatically and culturally correct. So, it can be hard for the receiver to even know that it is illegitimate. It is a big problem and if you enter the cyber security community you will see this happening. Hopefully at some points we will be able to get our arms around it. I don't have a good example off the top of my head, but if I come up with some, I will let you know.

The first attack method, which is probably the hardest to deal with, is called Insider Threats. It is a disgruntled employee or bad actor within the organization. Who uses their position and manipulates access to resources. Just yesterday, I was watching a television show and again I will date myself. This goes a long way. A system administrator in a company here in the United States that manufactured electronics for the military. They manufactured sensors and electronics components for the National Aeronautics and Space Administration. They were a small business at the time, but small is a relative term. They were doing millions of dollars in business a year. What this individual did is create what is called a *time bomb*. He created a script that on a particular day would go out and erase all the data from a computer system. In this case, he quit his job, left the company and at that *time bomb* went off. It shut down the production facility. It cost them $10 million dollars to recover from that incident. Now, fortunately, this company reached out to the FBI, which is an American law enforcement agency that deals with domestic incidents. After a long investigation, they uncovered the fact that the perpetrator was an employee. Then, they found the evidence to prosecute him, and he ended up spending about four years in jail. Also, he ended up having to pay the company $2 million dollars. That is a small price compared to the $10 million dollars and the loss of reputation that this company incurred. They are still in business today, but you must wonder how large of an organization they are. Could they have been bigger had they not had to deal with this insider treat?

I am sure you hear of probably one of the most famous insiders, that was Edward Snowden. He was an insider in the federal government, and he used his position to gain access to things that he was not supposed to, and he left the country with that data. To this date he is an American citizen who cannot return to this country because if he does, he will prosecute.

The human factor: the weakest link

We were talking about insider threats. In a computer system in an enterprise in a network, the weakest point is the human being. Human beings are subjects emotionally that can be manipulated through social engineering. They are often the easiest target. As an employee in a company, you always want to do the best for your job. You want to do the best for your company, but that can place you in a position of being vulnerable. How do we compensate for that? Well, strong security habits. Education is probably the best way to deal with this. In many of the companies that I worked for, every year we had training that we were mandated to go through that talked about how to look for the insider threat, how to look for phishing attacks. To mitigate this as best as possible, some companies will test this. The way that they test is to hire someone to send out a phishing email that has a link in it. If you click the link, it records your email address and it reports back to the company – this person followed the link and went to the unquote vulnerable website, or in many cases, there is a mechanism inside the company to report this. I mentioned earlier that I get probably 10 phishing emails a week. One of the things I do is I forward them on to my service provider and I say – hey, this is spam, a phishing attack. I do that so their systems can look out for and learn what kind of attack is occurring or where they are occurring from. My hope is that maybe it stops someone from getting a phished, falling victim to this.

A huge problem in the world now is the elderly. They are very susceptible to phishing attacks because computer systems were never part of their upbringing. For me, it was ingrained in me because it was something that I was exposed to early on. For my children, they were three years old when I put the computer system in front of them. So, they are more apt to see these things coming. But it is in the realm of billions of dollars that are taken away from elderly people, because they fall for phishing attacks. The adversaries know that the weakest link is the person. If an attacker can gain access or get your trust in your bank account, he can clean you out.

As a global community, we need to do better in teaching and protecting everyone, children and the elderly. And educating people about how to mitigate these attacks. But, again, we human beings are the weakest link that there is in this chain of cyber security

Building a security-aware mindset

How does one go about building a cyber security mindset? As a cyber security professional, you will be exposed to these things on a regular basis. Honestly, everyone – our children, our parents, our friends – need to educate themselves about these concepts so that they can protect themselves.

One of the ways is the Use of strong passwords. There is a lot of literature out now saying that passwords are a bad idea. As a matter of fact, the person that created the password recently passed away, but he thinks one of the worst things he ever did was this concept of password. If you look at it, what else were we going to do? Cyber systems develop over time. The best thing you can do is have a strong password. And what do I mean by a strong password? It consists of alphabetical, numerical, and special characters on the keyboard. But it is not just that, it is how large they are, how random they are. I have a password manager that I use personally called *BitWarden*. It contains the passwords to my accounts. What is nice about it is that I have generated random 20-character passwords.

If you look at a computer system doing what is called brute force attacking that size password can take millions of years of computer time. What that means is in terms of computer time, if I submit a password every second, and I do it 24/7, 365 days a year, it will take millions of years through a brute force attack for it to figure out my password. So, it is layer protection. A good and strong password, a randomized password can make it harder for adversaries to gain access to a system.

Another layer of this is Multi Factor Authentication. It is typically composed of something you have. Something you know and you are. Something I have is my password. Something I know might be that authenticator string that regenerates every 60 seconds. For most of my career, every morning when I logged into the computer system, I had to give it my account. I had to give it my password, and I had to give it my randomized string from the authenticator. If you really want to go to another level, you can do something called something you are. That might be your fingerprint. That might be an Iris or a facial scan. There are a lot of things that go into consideration there, because when you start using something you are, you start looking at a person's personal privacy. Those added layers of security incur certain levels of thought into what policy is.

We continue with our "what security mindset" is being suspicious of unsuspecting emails or phone calls. Like I said, I've gotten phished in emails. I tend to be very skeptical of how I enter this sweep stake when I never actually entered it? I try to be a little bit suspicious but not paranoid. It can go a long way in helping protect yourself from these types of scams. As cyber security professionals, we not only protect ourselves, but we must go help organizations implement policies about security mindsets and help the staff understand what it is they should be doing to protect the company and to protect themselves.

Defensive tools & techniques

I want to give a broad overview of the kind of things that you might be interfacing with when you enter a cyber security career. You might be involved in firewalls which control network traffic. Who can get in or out? I learned about firewalls because I installed one in my home to protect my access to my service provider. You might be involved in antivirus or endpoint detection systems (EDR) that try to detect and remove malware, before it can gain a foothold into a network. I have mentioned this before, encryption. You can spend a lot of time depending on how much you want to really understand encryption. It is a very important tool in the cyber security practitioner's toolkit.

One thing that is very important is backups. If a system becomes compromised (encrypted) not by me, but by an adversary or data becomes corrupted it does happen, having good backups allows you to easily recover and mitigate the losses that might be incurred. Also, testing those backups on a regular basis. Several companies have backed up their systems and have not bothered to test their backups only to discover in their time of need that the backups were corrupted too.

So, think about system backups, how often do they occur? Or how is that data protected? We used to keep off-site backups early on in my career. Where we would take a tape backup and we would move it out of the facility. If the facility had a catastrophic event – let's say a flood – we did not lose everything. As a cyber practitioner, you must think about how those things can be protected, not just in a digital realm, but in a physical world too.

Network Monitoring is a big thing currently. Especially with large networks, how do you monitor the devices and traffic? How do you predict when a particular link is becoming overwhelmed, and maybe do you need to rearchitect a portion of the network? My brother currently works for a service provider that has 300 data centers globally.

And one thing that he is working on is a more robust monitoring system that looks at the devices on the network and tries to detect where vulnerabilities might be or where systems need to be patched. How far down that rabbit hole are they? It is as if he has systems that have been patched in three years. He is probably going to prioritize those to get patched to try mitigating the vulnerabilities.

A lot of the time, companies deploy hardware and then forget about the fact that it is deployed. As an adversary, that is a place where you can look to gain a foothold and access into a network. Along with network monitoring is logging.

I have worked in facilities where we logged every command that was run on a network device. We could literally query that system and say: “tell me over the last 90 days what commands were run and where they were run or who ran them?”

That is also a massive amount of data to try to filter through and figure out what is going on. We talked about artificial intelligence (AI), but that is a place where AI can be used to rapidly look at that and point out where things might have occurred and instead of taking hours or days, might only take seconds.

Another tool or technique is something called Incident Response. Some of my friends are involved in incident response teams. And what they do is when an incident occurs, they have a set of policies and procedures where they go in and they try to diagnose what, where and how that occurred. And how are they going to recover from the event? It is an intriguing field, but you can get lost in a lot of information there.

I have never actually participated in an incident response team. I would consult with them. So, this is to sort of give you a flavor. Cyber security is a very broad field. There are a lot of ways that you can go with this type of career.

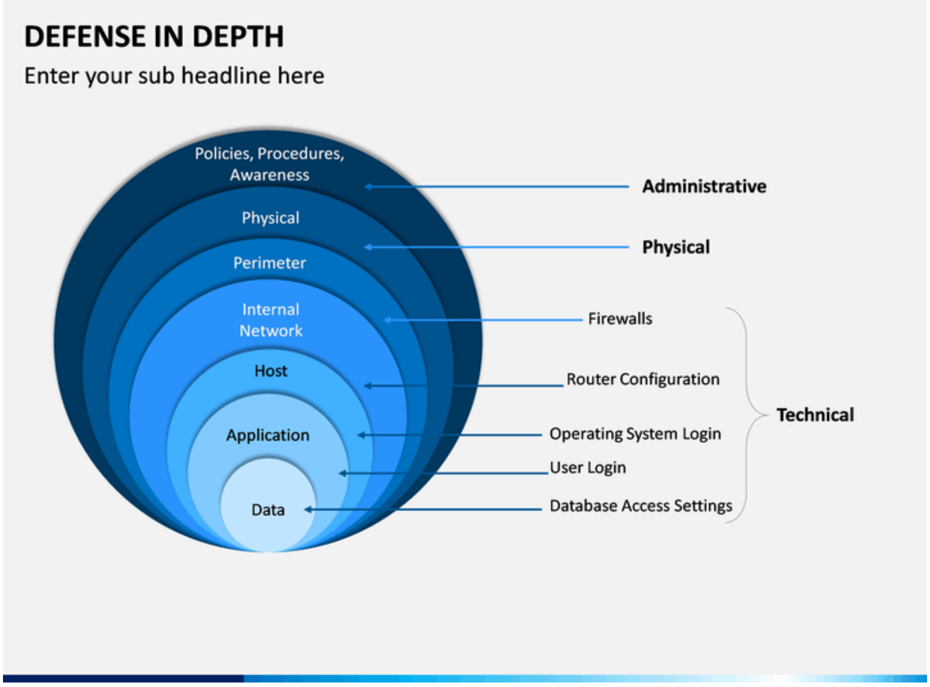
Layer security: defense in depth

You might hear something called defense in depth. This is a concept that gets applied across an organization and it is a multi-layered approach on how to protect computer systems and data. If one layer fails, there are other layers that will hopefully catch and protect your data or your computer systems.

As you can see from the next figure you have policies and procedures. Which does not do you any good to put policies and procedures in effect after an incident occurs. It is better to have them in place before because it will help you deal with the problem, and it helps protect your system.

Cyber security can also involve physical manifestations. Computer rooms that are locked and only certain people can get into them. I worked in facilities where when you went into computer rooms, you did not go in alone. You went in as a pair.

Figure 4 – Defense in Depth



DEFENSE IN DEPTH

Enter your sub headline here

Reference: The Author

You logged into a computer system, both people had to be present to attest to what you did. There are physical ways that cyber is being protected. There are perimeter defenses, fences, guards, doors that have pass keys that have to be used to access them. Those are perimeters where we are layering the protection of the computer system and the data. There is internal network protection. We segment networks. I do not want the engineering network to have access to the financing network. So, I do things in architecting the network itself. I put in a firewall, or I put in an access control list that controls who can get to what areas of the network and try to protect it so that if one area is breached, they do not necessarily automatically get access to all the data in a network.

There is application security. Even though you log into a network, you may have logged into a particular application. Again, we might have a financial system that handles payroll. Everybody can get access to that data. There is another password or pass key that is used to help protect that in a layered fashion.

And the final way is to access data itself by encrypting that data at rest on a hard drive. If somebody wants to access it, they must have that password. All this together basically is called a layered defense. As you can see, a computer system can get very complicated quickly. It takes a lot of people to work in concert to make it work efficiently and effectively.

Careers & pathways in cybersecurity

What kind of career paths are there out in the cyber security world? There are Systems Administrators. There is a Network Administrator. There is a Database Administrator. I have worked as both a Systems Administrator and a Network Administrator at different times in my career. There is a Security Engineer – people who help architect policy and physically set up and manage a network.

There is something called the blue team, which is analyzing networks from a defense perspective. There is something called the red team, which is analyzing networks from an offense perspective. I have been on red teams before. There is a purple team which is sort of a hybrid. That looks at a network both from an offensive and defensive perspective and makes recommendations to corporate executives or security departments about how they can improve the network's posture.

There are Governance, risk, and compliance (GRC) roles. My last job was to work with a compliance team. They had a lot of policies that they had to ensure and every few years they had to attest to a higher authority that we were following those policies, and we were implementing the directives from higher up in protecting the networking. My capacity at that time was as a lead engineer. So, I consulted with information system security officers who were responsible for the paperwork, but I was responsible for letting them know where the system was currently at.

The pathways in cyber security involve Certifications. There is something called security plus and network plus. There is a certified ethical hacker. I held the certified ethical hacker certification for a while. There are ten to hundreds of certifications that are out there and there are good ways to get acquainted with a particular area of cyber security and have a steppingstone into a career path.

Fortunately for me, I came about cyber security early on when the internet did not even exist. And certifications did not exist. My son who followed somewhat in my foot path was required to get the security plus certification; he maintained that to keep his job. There are a lot of places where you can look for good information online. It just depends on what you as a person want to explore and to develop your career.

Final considerations

What things are coming? One of the problems that has come about is something called Coding Hygiene. Vulnerabilities in software have come about because it was written from a time perspective. It provides us with income. And those vulnerabilities went out the doors. Remember back to the example of the Solar Winds that exists because the program that was written was not a bad program. It just has flaws in how it was written. And the language to write software can prevent vulnerabilities from arising.

Automation is a big thing. I mentioned before that artificial intelligence (AI) could be used to scan the reams of logs that come out of networks and look for problems. Network Detection Systems (NDS) is now starting to implement AI to analyze data on the fly of the network and try to find vulnerabilities and attacks in more real time as they are occurring and try to block them before they can get a foothold.

The last thing I will mention in the future is artificial intelligence (AI). This term is very broad. It involved creating intelligent machines. There is a lot of hype in the media now about AI. What we have right now is generative AI – or large language models that have been built. You have probably heard of chatGPT, Claude, or Gemini. These are all large language models, but they are not intelligent. They are a neural network that has been trained on a lot of data. And you can ask it a question, and it uses probabilities to predict what the next word in a response would be, but it is not really thinking.

The next step which is not here is Agentic AI. That is when machines understand context, but we are not there yet. I sort of envy you guys, because I have used AI at the end of my career to help me solve problems. Before, I had to slog through manuals and look for solutions in other places. AI can help cut through a lot of that chaff and get the solutions a lot faster than it used to be. Is AI going to take away jobs?

There was a study done recently I heard in a podcast, done by The Brookings Institute. They looked at the last five years of AI to answer the question “how many jobs have been lost to AI”? At the end of this study what they came up with was in certain very well-defined niches, a couple of jobs were lost. But zero jobs have been lost to AI. It really is not replacing jobs. It may be in the future. I tend to think of AI as an enhancement to human beings in doing their jobs. A very good example of this is helpdesks. When you call a company and you have a problem, they can link AI to this and they can zero in on answers much faster, making the helpdesk more efficient. And they help the human being zero in providing answers.

So, even in the cyber security career field, AI is an enhancement right now. That is not to say that it will not replace jobs, but it will create jobs. If you look at some other technologies, the internet itself came about in the 1970s and did not really get big until the 1990s. That was a 20-year gap. Computers came about in the mid-1970s but did not become commonplace in business till the late 1980s or early 1990s. AI right now is in its infancy. There are a lot of governments and organizations that are struggling to understand this, because it is changing rapidly. But I do not think it is as much of a problem in the long run as people are making it out to be. I could be wrong, but I think it is helpful.

[i] This activity, organized by Professor Aparecido, was supported by Professor Paula Pudo. Disponível em: https://www.youtube.com/watch?v=8cN5d0ClifQ