International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838, Print ISSN: 2664-682X
Received: 24-03-2023, Accepted: 11-04-2023 Published: 26-04-2023
Volume 5, Issue 2, 2023, Page No. 7-11

Cyber security: Functioning & its domains

Vidita Saini
Assistant Professor of Law, Bharat College of Law, Rurki, Haryana, India

Abstract
In the present technology driven world, we are surrounded by gadgets and machines all of which functions through internet. Internet has revolutionized the human lives. The combination of machines and internet has no doubt made the life of human being easier but it also has its own drawbacks. Anyone can hack into someone else's device and can steal the vital information. In fact nowadays hacking, phishing has become a business for some to earn their bread. It thus becomes necessary to secure our devices from any form of cyber-attack. This is where the role of cyber security comes into the picture. This research paper showcases the ancient way of securing information as well as the modern methods for the same. Further it is discussed that who is a cyber security expert and what functions does he perform. Thereafter, the various factors associated with the cyber security are discussed in detailed manner followed by functioning of cyber security and its domains. In the end conclusion presents a wholesome idea of cyber security and give some suggestions to practice cyber hygiene.

Keywords: cyber security, cyber-crimes, cyber criminals, encryption, hacking, network, network security

Introduction

From the time of civilization, it has been an important aspect to keep the information safe. Different ways were practiced to secure the messages. When messages were sent through a messenger, it used to be sealed by special material like clay etc. along with the seal of the King or authority as the case may be. Other than this, encryption method was also popular where after encoding the message on a strip of cloth, it was then wrapped on a cylinder to be later on decrypted by the receiving party. But to make it more complex the cylinder and cloth were sent separately and had to be combined later on to make out what was written on it. See Fig 1.

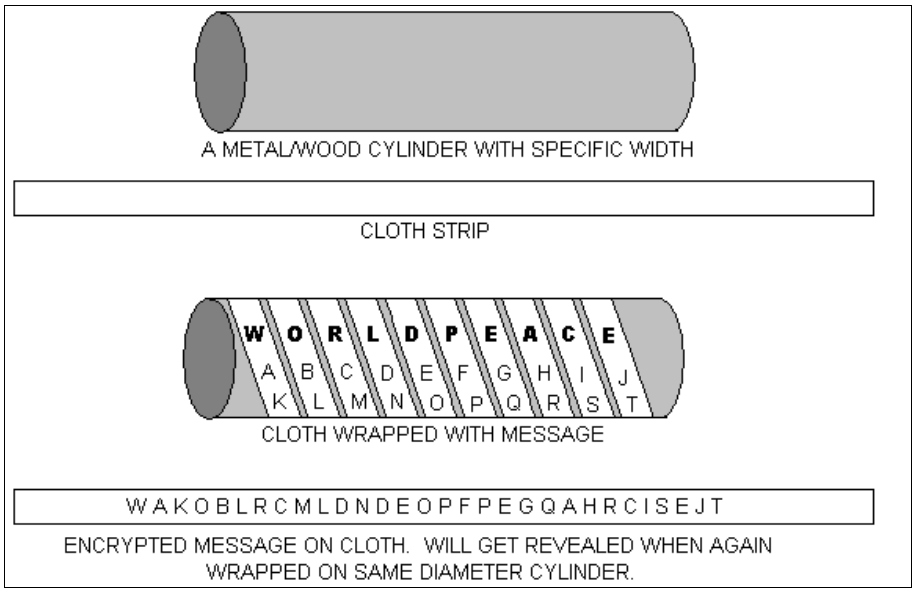

Fig 1

In Fig 1, the message is not revealed when the cloth is spread but it can be read when it will be wrapped on the same cylinder. The term *"WORLD PEACE"* is kept in bold to comprehend easily. The similar technology is used in present times to save the original message. This is nothing but the process of encryption and decryption as it is referred today.

Who is a cyber security expert

A cyber security expert is an individual employed by an organization to protect their infrastructure. This person is responsible to identify potential flaws and what fits the organization faces and then streamline or create or design or architect methodology which is going to protect all the assets that the organization has. They do this through a variety of techniques such as

- **Finding weaknesses**
  So that vulnerability management could be performed through vulnerability scanners in the organization infrastructure. It could be in applications or in servers or in desktops or operating systems or network based flaws as well.

- **Monitoring systems**
  Then the expert monitor these systems and look at the data flow that is going through the internet and the network and find out if there is anything malicious going on in that network.

- **Network breach**
  So over these techniques, you can monitor the system on day to day basis and try to identify if anything extraordinary is happening. After you find the weaknesses, you test those weaknesses to identify the complexity of those weaknesses. Then you will repair them, patch them and install updates or mechanisms like firewalls or anti viruses to mitigate those weaknesses. This will result in strengthening the area where an attack may have occurred.

Factors of cyber security

Cyber security works in the similar way to fulfill the same purpose of keeping information safe. Cyber security by itself is an architecture created to protect networks and devices from the damage, attacks or the unauthorized access. Essentially the cyber security helps to achieve here a design to be implemented in a manner which will allow some factors to function in a standardized manner. These factors of the cyber security are

- **Protection of the business from hackers**
  This includes saving the files, company server and their web application from being compromised and databases being leaked out.

- **Increased Productivity**
  People would be in very controlled environment concentrating more on their work than worrying about cyber criminals.

- **Inspire customer confidence**
  Where an organization ensures that it is complying with certain regulations, its clients would feel more confident about sharing their information with the company. It will then help to make applications and websites more stable and protect them from external threats.

- **Protection for the customers or clients from cyber attacks**
  Now organization would be holding some amount of data for the customers and clients as well and then it becomes responsibility of the institution to protect their information along with its own data.

- **Stop the websites from crashing**
  The websites are the face of any company or organization. They have to be protected from attacks by securing them with protection layers. Once the website is secured, it works in an efficient manner.

The three main pillars of cyber security that we deal with since the inception of the computers are confidentiality, integrity and availability triad. (The triad is also known as CIA). They have served as the industry standard for computer security since the time of first mainframes.

Confidential

This pillar aspires to keep the data confidential. The principles of confidentiality assert that the information and functions can be accessed only by authorized parties. For example: military secrets.

Integrity

To maintain the integrity of the data by keeping it intact. This is where the trustworthiness of the data comes into the picture. The principles of integrity assert that information and functions can be added, altered, or removed only by authorized people and means. For example: incorrect data entered by a user in the database or modified by the unauthorized person.

Availability

To made the data available at all points in time. The principles of availability assert that systems, functions, and the data must be available on demand according to agreed-upon parameters based on levels of service. For example: G-mail as a service is always made available to the users.

Threats to CIA

The threats to CIA can be discussed in two different parameters: cybercrime and hacking. Cyber crime is any criminal activity or any unauthorized activity that would involve the usage of any computing device which would result as a security incident at the victims end. Most cyber crimes are carried out in order to profit from them. Criminals would try to do phishing attacks to steal the money out of bank accounts or to con into the credentials and thus compromising the e-mail accounts or the social media accounts and try to gain access to the identity of someone else. Cyber crimes are generally carried out against the computers or devices directly to damage or disable them, spread malware, steal secret information, etc. This is about the motivational aspect for a person to conduct such an activity to cause damage.

Functioning of cyber security

It is all about securing the computers and there are various methodologies and factors that come in on how one can secure his computer.

1. Authentication Mechanisms

Authentication is the part where the person is identified and he is then authorized for some access controls and then further authenticates the person to ensure that the person is the same person who they claim to be. This process begins with creating a username and associating a password with it. The username is used to identify the account that person wishes to access. The password is the authentication mechanism to prove that the person is who they are. The authentication mechanism can be enhanced by using a two-way authentication mechanism. For example: With banks when you type in the username and password, they send an OTP which is auto generated by a server and sent to a register device that the person owns (cell phone). This is one

added layer of security where you are not only relying on the password which can be cracked but you are relying on a third party device as well which the person needs to have physical access to. Every time they try to log into, a new OTP will be generated.

2. Secure the password
Just having a password may not be sufficient. You have to ensure that the password meets some complicating standards to ensure that the security of those passwords or the complexity of that password is high enough where cracking programs will not be able to easily crack the password.

3. Regular updates
All the operating systems or the applications that you use will be receiving regular updates. It could be for functionality but more for security so as new vulnerabilities in applications or operating systems are found out. The software vendors or the developers of the software over a period of time start sending out these updates also called patches to the end users. It is very important for the end users to identify these security patches and install them on their devices as soon as possible otherwise they remain open for those vulnerabilities and unpatched systems thus can easily be hacked.

4. Usage of an Antivirus
To protect yourself from viruses, worms, Trojans essentially malware, there needs to be a software that is installed on your computer that is going to watch out for them. You cannot rely on the operating system itself to protect you. So there has to be an antivirus which will be scanning the connections that you are making, the websites that you will be visiting, the files that are getting executed in the background and ensure that everything that is happening is legit.

5. Installing a Firewall
A firewall essentially is software or a hardware that allows or disallows some functionality. For example: a port to be opened or closed or a service to function on a computer or not. Thus by disabling unwanted services one can limit the threat landscape that are created for the computer. If a service does not exist on your computer, it cannot be hacked. So the essence here is first to identify which ports and what services one is using and then create a policy on the firewall to ensure that only required ports and services are running.

6. No Phishing
Phishing as discussed could be a malicious website that is being hosted by a hacker and sending a fake mail looking like a genuine one asking to connect to the particular server and fooling to give the confidential information to him. So one should install antivirus or in addition to that should have a handy phishing tool bar which would identify the websites that you are visiting and give the risk rating of that website and this will give an idea whether this website was ever reported as a phishing website or not. The court declared phishing on internet as an illegal act that entails injunction and recovery of damages in the landmark case of *National Association of Software and Service Companies v. Ajay Sood & Ors*. (2005) Del HC.

7. Cryptography/Encryption
The best way to keep everything secure is to encrypt it. However, what kind of encryption is required, what should be encrypted and what should be not encrypted, how that encryption should function and how this encryption enhances the business value is needed to be ascertained. So, the knowledge here that will be required is what protocols you want to encrypt. For that you first need to identify which protocols you are going to consume, what data is going to be transmitted and how valuable that data is to your organization and then you are going to add encryption or cryptography on top of it to prevent any attacks from hackers.

8. Securing DNS Servers
DNS is a Domain Name Server which is basically an index that maps the domain names to the IP addresses. On the internet, computers do not know domain names. They can only identify the IP addresses and MAC addresses. So, when we type in for instance, google.com on the browser, the computer doesn't know what google.com is. What it does is, it sends the packet to the DNS server and in the DNS server, it queries where the google.com is located. It is given the corresponding IP address because of which the packet then goes to the relevant server. There are attacks where DNS can be compromised and the pointer pointing to your particular website can be changed to point to a malicious server that a hacker is hosting. So to prevent that from happening you need to secure your DNS servers.

Domains in cyber security
1. Asset Security
Assets could be applications, networking devices, computers, routers, wireless access points and all these devices have their own operating system and their own functionality and it is important that we look at the security of each and every asset that the organizations owns.

2. Security Architecture and Engineering
Not everyone can just walk in an organization and start implementing the security in particular manner. We have to standardize the security in such a way where security is constant for a long period of time and is consistent as well. For that to happen there is an architecture and engineering phase where we have to plan a way for how the security needs to be implemented. For example, if a particular antivirus is installed in on computer, it has to be ensured that the same antivirus is installed in all the computers in the organization as only then would be able to get report from the proper owner. So for this proper policies and procedures has to be created and implemented in standardized manner for security to work properly.

3. Communication and Network Security
With cloud computing coming in and deployment of physical infrastructure talking to something that is on cloud (AWS OR Microsoft), data flaws are happening globally these days. One has to be careful how the data is transmitted across the network. Thus it becomes necessary to create those paths and ensure that these paths are monitored and regulated properly and to not have any data leakages.

4. Identity and Access Management
The person accessing the data must be authorized to do so. The owner must be able to authenticate his actions, track him and hold him accountable. Even if the person is authorized to do something, we have to hold him accountable for the activity so that if something happens later on; it could be identified who made the change. So identity and access management module consists of groups, policies, users, roles and interlinking them with the assets to ensure that only authorized people are able to access those devices.

5. Security Operations
On a day to day basis, security of the organization has to be monitored. For example, if today a person starts witnessing Denial of Service Attack or an attack to crack the password, there should be some internal mechanism that are in place to identify these attacks. So regular monitoring is a must.

6. Security Assessment and Testing
Now when the mechanism is in place, it does not mean they are going to perform similarly their rest of the lives. Information Technology is an ever evolving scenario. So we need to test and assess our security controls on regular basis to ensure that there are no gaps left. What may be configured today will be irrelevant tomorrow. So, constantly looking at latest security trends, patches that are being installed, comparing the security infrastructure to check whether compliant with the latest security standards or not is the necessary steps to be followed.

7. Software Development Security
For the organization developing and selling software, security becomes a huge part because the end user will ask what kind of security testing was done in that application. So that brings to a software development life cycle which talks about how you are going to create and test that code and ensure that the code is secured enough. So there is need to follow secure coding practices and test the software over and over again till you are satisfied with the outcome.

8. Security and Risk Management
Risks are basically events that may occur compromising the security of an organization. So it is very important that we identify these risks, map these risks and verify how the risk is going to impact the business and then try to figure out security controls to mitigate that risk or bring it down to manageable aspects.

Conclusion
The cyber world or the cyber space is a lot more than just the internet. It is an online environment where countless number of participants are caught up in social interactions with the capability to influence and manipulate each other. Digital medium becomes the tool to establish communication in the cyber space. However, it is fact that the rapid communication system has evaded the personal space of an individual. Every new invention is helping cyber-warriors to twist the game. Every different connection creates another opportunity for a hacker to get in. We are expecting technology to do more and more things for us. Because of that greater vulnerability is being built into our everyday lives. Cars that are internet enabled are being hacked so that they would stop on the highway. Webcams are being turned on for spying purposes. The cyber criminals are speaking to the children through baby monitors in their rooms. They are more sophisticated than ever before. Security is always a battle with hacker and defender. What we find is that on the internet attackers generally have the upper hand. The hacking has become a business. It's like an industry where they actually have expenditures and payroll that have benefits attached to be given to their employees. One cannot personally buy an atomic bomb or hire SEAL Team 6 but one have the equivalent platform online to do that. Today, computer viruses and Trojan are designed to do everything from stealing data to watching you in your webcam to the theft of billions of dollars. One can go online and buy a hacking service to knock the business competitor offline. Cyber criminals are checking the quality of their viruses before releasing it into the world and getting paid for it. This is how advancement in technology and latest developments gave birth to many cyber crimes in recent years.

To combat cyber crime, cooperation and collaboration among national governments, computer and crime authorities is vital. If national governments work with one another as well as with business communities to modify institutions by defining appropriate policies for the security of the digital world, it will result in lower transaction costs. Some signs of success have materialized, but nations have very far to go before they can achieve even a moderate level of success. Secondly, there is need to enact laws and establish organizations to set up appropriate defence mechanisms and make reporting of cyber crimes mandatory which will then eventually help to combat these crimes. U.S. government, for instance, requires commercial banks to secure their networks.

Thirdly, some of the countries are altering the regulative landscape towards harshness of punishment. For example- the "*U.S. Patriot Act, 2001"* has brought cyber attacks into the definition of terrorism with penalties of up to 20 years in prison. However, the chances of arrest in cyber crimes are quite low since traditional law enforcement agencies are not up to date with the mechanism of cyber space. In place of severity of punishment, to enhance cyber safety is more important.

However, the most important subject above all these points is "The Netizen" i.e. the user. The user must be well informed and aware of latest advancements. One must have the basic knowledge of Internet and Internet's security. He or she must have the ability to respond in crisis and be able to do that with confidence. Once you get hacked, you must know how to react to it. First thing we need to do is to take that computer off the network. These are the skill sets one has to gain by doing it. In order to be updated, one can go online and find the simple best practices:

- Don't be an easy target. Find out how to update and patch the computer.
- Get a secured password and never share it with anyone.
- Make sure you use a different password on each of your sites and services online.
- Find the resources on internet and apply them.

In order to prevent cyber crimes, we need to adhere to simple rules such as:

- Avoid disclosing your identity to any strangers.
- Use the latest antivirus software always to guard against virus attacks.

- Never send your credit card number to any site which is not secured.
- Use of firewall.
- Uninstall unnecessary software.
- Change passwords frequently and enable two-step authentication in webmail to keep social account secure. One should not set simple password that could be easily decrypted.
- Do not share the personal information like bank account number, ATM pin, password etc over an unencrypted connection including unencrypted mail. The websites that does not have the lock icon and https on the address bar of the browser are the unencrypted site. The *"s"* stands for secure and it indicates that the website is secure.
- Trusted application from trusted site should be used for protection of one's sensitive information or data.
- Don't sign to any social networking site until and unless one is not old enough.
- Don't forget to update the operating system.
- Firewalls, anti- virus and anti-spyware software should be installed in ones PC and should be regularly updated.
- Visiting to un-trusted website or following a link send by an unknown or by an un-trusted site should be avoided.
- Don't respond to spam.
- Make sure while storing sensitive data in the cloud is encrypted.
- Try to avoid pop-ups: Pop-ups sometimes comes with malicious software. When we accept or follow the pop-ups a download is performed in the background and that downloaded file contains the malware or malicious software. This is called drive-by download. Ignore the pop-ups that offer site survey on ecommerce sites or similar things as they may contain the malicious code.
- One should not download the nastiest creations of cyber criminals.

In addition to these, cyber law awareness programs and schemes must be conducted by the government. A set of rules and guidelines should be developed by within the law enforcement agencies in order to address the various categories of computer crime.

If anyone falls in the prey of cyber attack, he must come forward and register a case in the nearest police station. If the criminals won't get punishment for their deed, commission of these crimes will never stop. Awareness regarding the cyber-crimes and punishing the criminal behind cyber-crime with strict implementation of laws is the only cure to this disease.

"Can we secure the world from a bloodless war? I'm talking about Cyber Security. India must take the lead in cyber security through Innovation."

Narendra Damodar Das Modi

References

1. Charles P. Pfleeger, Shari Lawrence Pfleeger and Jonathan Margulies, *Security in Computing* (Pearson,2015 Edition)
2. https://www.academia.edu/34263657/Online_Certificate_Course_on_Cyber_Law_paper_2_regulatory_framework_part_b_domestic_legal_regime
3. https://en.wikipedia.org/wiki/Scytale
4. https://en.wikipedia.org/wiki/Encryption
5. https://en.wikipedia.org/wiki/Computer_security
6. https://digitalguardian.com/blog/what-cyber-security
7. https://www.sciencedirect.com/topics/computer-science/vulnerability-scanner
8. https://blog.gigamon.com/2019/06/13/what-is-network-security-14-tools-and-techniques-to-know/
9. https://sipmm.edu.sg/six-crucial-factors-cyber-security-healthcare-procurement/
10. https://www.preferreditgroup.com/2019/08/27/the-three-goals-of-cyber-security-cia-triad-defined/
11. https://www.certmike.com/confidentiality-integrity-and-availability-the-cia-triad/
12. https://foresite.com/5-core-functions-of-effective-cybersecurity-1-identify/
13. https://www.sciencedirect.com/topics/computer-science/authentication-mechanism
14. https://it.uottawa.ca/security/identity-authentication-theft
15. https://us.norton.com/internetsecurity-how-to-the-importance-of-general-software-updates-and-patches.html
16. https://www.forcepoint.com/cyber-edu/firewall
17. https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html
18. https://www.techrepublic.com/article/10-things-you-should-know-about-securing-dns/
19. https://library.ahima.org/PB/SecurityDomains#.X5ubQ1uWbIU
20. https://searchsecurity.techtarget.com/securityschool/Top-cybersecurity-techniques-to-prevent-data-breaches
21. https://www.coursera.org/lecture/cyber-security-domain/software-development-security-wpuHY
22. https://resources.infosecinstitute.com/certifications/cissp/
23. https://www.mercurynews.com/2018/12/20/im-in-your-babys-room-a-hacker-took-over-a-baby-monitor-and-broadcast-threats-to-kidnap-their-child-parents-say/
24. https://www.theatlantic.com/magazine/archive/2006/12/how-to-get-a-nuclear-bomb/305402/
25. https://blog.malwarebytes.com/101/2016/08/10-easy-ways-to-prevent-malware-infection/
26. https://www.pcmag.com/how-to/12-simple-things-you-can-do-to-be-more-secure-online
27. https://www.thesslstore.com/blog/how-to-prevent-cybercrime-9-helpful-tips/
28. https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack
29. https://economictimes.indiatimes.com/tech/internet/do-you-know-how-to-report-a-cyber-crime-heres-a-guide-for-victims/articleshow/61464084.cms?from=mdr