International Journal of Scientific Research & Engineering Trends
Volume 9, Issue 4, Jul-Aug-2023, ISSN (Online): 2395-566X

Layered Security Defense, A Panacea to Loss Of Intellectual Properties And Damages To Information System

Odunayo Onaolapo Ajayi
Cyber Security Unit, Mcintire Solutions
aodunayo@mcintiresolutions.com

Abstract-Cybersecurity has become a continuous lifecycle event that every business owner must consider before setting up a firm. As a result, the strength of an organization is as good as the ability of an organization to protect its intellectual properties. As the threats are becoming rampant and complex, the measures to curb their spread can also be complex and sophisticated. The past and projected economic consequences of the crime are very huge and devastating. This paper x-rays some of the reported cybercrimes across the globe and the proposed economic worth of future occurrences. To minimize the effect and avert economic instability, this paper discusses a Layered security framework and why it is better than a single-layered framework either for On-premises or Cloud-based security solution platforms.

Keywords- Cybercrime, Cyberstalking, Cyberspace, phishing, and Spoofing.

I. INTRODUCTION

In partnership with McAfee, the Center for Strategic and International Studies (CSIS) published a report (Economic Impact of CybercrimeNo Slowing Down) in Feb. 2018 which affirmed that nearly $600 billion, that's almost a percent of global GDP, is lost to cybercrime each year. The report attributed the increasing trend to the unimagine prowess exhibited by cyber criminals in adopting new technologies from their hidden 'dark web'. The criminal activities in cyberspace are so much wide-ranging to point it accounts for almost two-thirds of global crimes nowadays. This fact is evidenced in a statement of one senior British official who was reported to have lamented that half of all reported crime in the UK is cyber-related. These phenomenal impacts of cybercrimes and their consequential effects on our cyberspace motivate this research work.

Several organizations today are used to the use of just antivirus solutions and basic firewalls. It may be a result of a lack of adequate resources to procure a raft of solutions and personnel that will run them. It may even be that the organization never tries any other measure than old ones. In this modern day, no organization should see cybersecurity as a one-and-done job. It is a continual process involving monitoring, threat hunting, and training of cyber-staffers.As the level of our technology composition becomes robust with the advent of some other features, Machine learning, Cognitive computing, Robotics, Neural network, Deepfake, Computer vision, and Expert system, human is engulfed in diverse philosophies as to what is adequate as a measure to protect the expansion of not only an organization but the whole world from cyberattacks. As a result, cyber-Security has become an integral part of information technology. The protection of information is now the biggest headache of today's organizations.

The threat of cyber security also known as the cyber threat has become a common phenomenon that every organization as well as governments at all levels consider most critical nowadays. The tide is on the rise. A greater part of organizational and government spending has never materialized due to this hydra-headed monster. No one is spared. It is delusional for anyone to believe single-layer technology (a single act of software) innovation can make an organization all-time secure. This is empirically believed to be untrue as pointed out by a "Certified Ethical Hacker and Mindsight's own Security Solutions Architect" - Mishaal Khan says: "You can never secure yourself 100% from anything. Even I cannot help you be 100% secure or 100% private." It is on this basis that this study is conceived. What security architecture is better to safeguard an organization – multi-layer or single-layer?
Security and Privacy of the data have become the topmost security measure that every organization considers important if it wants to remain stronger in the business. The evolution of information technologies in recent years has led to a global digital transformation across various organizations and governments. No iota of doubt, information today is being managed electronically. As a result, the process is prone to several threats. Thus, the system must be insulated maximally against these threats.

This work vividly explains what layered security defense entails and why it is better than single-layer security measures. The paper discusses the likely security gaps

inherent in a single-layered security framework in an organization. The framework is adaptable to any system; be it individual firms, private firms, corporate firms, or even government systems. The process allows a cyber-ecosystem that is sustainable anywhere in the world. The other sections of this work are as follows; Section Two centers on Related literature. Section Three discusses Global Cybersecurity Statistics, Section Four discusses On-Premises and cloud-Based Security Solutions, Section Five delves deeper into why layered (or Multi-layered) security architecture proves to be the better option over other measures, Section Six gives some Recommendations to governments and organizations, Section Concludes the paper while Section 8 comprises of all reference materials contacted on the subject matter.

II. RELATED LITERATURE

The complexity being experienced in the field of data management by organizations has forced every organization to be cybersecurity conscious. In the present day, Cybersecurity is the most concerning matter for every organization as cyber threats and attacks are overgrowing. The role of the internet in our day-to-day activities cannot be underestimated. The process has made communication easier across the globe. The interconnected world goals are achieved through the internet coupled with other internet-dependent innovations. According to Tan et al. (2021), the population of internet users is today over three (3) billion. Judge et al. (2021) added that apart from connecting the whole world, the internet also provides employment opportunities for many. In explaining the interconnectivity between security measures put in place and the essence of the organization, Robson et al., (2014) detailed that Information security must support business aims and objectives by curtailing dangers and evolving trust. A single-solution framework has been proven to be unreliable as it is believed to leave the network vulnerable to attacks from hackers. NIST Cybersecurity Framework (2020) advocates the use of multiple security layers that does not leave loopholes for attacks.

1. Cyber Attacks:

A popular saying that "assessing an enemy's strength before striking a blow is wisdom" shall be employed in this section. Let us look at various types of threat landscapes that an average organization is exposed to before discussing the appropriate measures to guide against them. Cybersecurity, according to Cybersecurity and Infrastructure Security Agency (CISA), is "the art of protecting networks, devices, and data from unauthorized access or criminal use, and the practice of ensuring confidentiality, integrity, and availability of information." This act of protection is considered effective when cyberspace is secure, reliable, and flexible. The main essence is to avert attacks on organizations' frameworks. Nowadays, the main essence had been extended to cover prevention, detection,response, and recovery. Empirically, cybersecurity professionals had proven beyond doubt that it is impossible to avert all attacks; but measures can be put in place to detect and prevent seizures (Leiva, 2015; ITU, 2018; Watson, 2019).A cyberattack is any offensive maneuver that targets computer information systems, computer networks, infrastructures, or personal computer devices. This is an attack, via cyberspace, targeting an enterprise's use of cyberspace to disrupt, disable, destroy, or maliciously controlling a computing environment/infrastructure; destroy the integrity of the data, or steal controlled information.

Dilanian (2013) asserted that cyberattacks were considered a bigger threat than Al Qaeda in the United States. A cyber-attack is a manipulation of computer systems and networks. It is not a strategy, but rather a tactic employed among several others toward the attainment of a broader strategy. The aim and target of a cyber attacker could be for personal delight, political revolution, intellectual property theft, terrorism, or even international war. It involves the use of malicious code to adjust computer code, logic, or data and leads to cybercrimes, such as identity theft and information.
For simplicity, cyber-attacks can be classified as follows.

2. Web-based attacks:

These involve all the attacks which occur on a website. Below are some of the most common web-based attacks.

3. Injection attacks

This attack comes in various forms but the most common one is SQL injection which communicates with the database, code injection which happens when an attacker, Cross-Site Scripting (XSS) which happens when the attacker injects an arbitrary script into a legitimate web application to perpetuate a criminal act. If the systems are unable to clean this unwanted information before it is submitted into the database, the destructive code can change, delete, or even reveal the data contents in the system to the attacker. A perfect example is Stuxnet, a worm that was used back in 2010 by US intelligence to interrupt Iranian Natanz uranium enrichment facility activities by burning out numerous centrifuges. It is amongst the most dangerous and oldest attacks aimed at web applications.

3. DNS Spoofing

DNS (Domain Name Service) spoofing is the process of poisoning entries on a DNS server to redirect a targeted user to a malicious website that resembles its intended destination under the control of the attacker. This mostly occurs in public Wi-Fi environments. It can as well occur anywhere. The hacker uses a malicious site that looks like the original website a user knows to give the hacker a perfect phishing scenario to collect sensitive data such as passwords, credit card pins, bank details, contact

information, geographic data, and some other personal identity information (PII)

4. Session Hijacking

Transport Control Protocol (TCP) session hijacking, sometimes also known as cookie hijacking, is the exploitation of a valid computer session—sometimes also called a session key—to gain unauthorized access to information or services in a computer system. In contrast, Anastasios Arampatzis (2021) defines session Hijacking as a method of taking over a web user session using source-routed IP packets to intercept an ongoing communication between two nodes on a network through an inserted commands and pretend to the authorized user. Once the user's session ID has been accessed, the attacker can undetectably operate as that user and do anything the user is authorized to do on the network. In this type of attack, the hacker does not need to authenticate the server; he/she gains access to the server directly unhindered. If the communication session remains active, the authentication remains intact throughout the session.

5. Phishing

This is a cybercrime where a hacker tricks an individual using malicious software, email, telephone, or text message to reveal sensitive information needed by the attacker to carry out his action. This attack has become sophisticated over time, more than ninety percent of a data breach in an organization starts with spear phishing. According to Akarshita et al., (2019), this attack can occur in four different ways.

a) Deceptive Phishing
b) Spear Phishing
c) Whaling Phishing
d) Pharming Phishing

It was reported by the US Department of Homeland Security about the breach of the US power grid which was orchestrated by a Russian attacker by infiltrating some supplier companies through phishing methods.

6. Cyberstalking

According to (Kobets&Krasnova, 2018; Nobles et al., 2014), the definition of cyberstalking is, is ad Infinitum. However, cyberstalking is known to be a means of using the internet by some set of people to intimidate their target with defamation, slander, blackmail, identity theft, threats, solicitation for sex, monitoring, vandalism, and slandering. In October 2016, Uber's database was breached by an attacker who stole more than 57 million customers' personal information. Uber paid the attacker sum of $100,000 to cover up the attack and delete the data. This incident and a couple of others remain one of the reasons cyberstalking is a big threat.

7.Brute force

It is a type of attack that uses a trial-and-error method. In this type of attack, the hacker uses a 'trial and error approach to gain access to the location of **data of the victim(s). It may be** guessing passwords or just the login details of the victim(s). There are several types: Simple brute force attack, Dictionary attack, Hybrid brute force attack, Reverse Brute force attack, and Credential Stuffing. Cybercriminalsuse this method to de-encrypt data from an organization's network.

8. Denial of Service

Under this attack, the attacker makes the network temporarily unavailable to the users. During that time, the attacker steals the needed information. This is done by trafficking the user with unnecessary information that may eventually lead to the crashing of the network or server. It mostly uses just a single system and just a single internet connection to attack the user's server. This can be classified into -

- Volume-based DDoS attacks: This is targeting the bandwidth of the user's server. This happens when there is a bunch of small requests for the server to respond to at a time and mostly cause the crashing or instability of the server.
- Protocol attacks- this involves exhausting the resources of a server It consumes actual server resources, measured in packets.
- Application layer attacks- Involves gaining unauthorized access to an organization server via a vulnerability of software.
- vii) Dictionary Attacks

This type of attack stored the list of commonly used passwords and validated them to get the original password.

9. URL Hijacking

It is a type of attack where the attacker changes certain parts of a URL and makes a web server deliver web pages for which he is not authorized to browse. That is Domain address is deliberately misspelled and this misspelled domain is registered legally. This is sometimes called typosquatting.

10. File Inclusion attacks

It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the included functionality.

11. Man-in-the-middle attacks

It is a type of attack that allows an attacker to intercept the connection between the client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.Thomas A Johnson's book, Cyber-Security: Protecting Critical Infrastructure from cyber-attack and cyber warfare, discusses various cybersecurity threats landscapes as follows.

1.Traditional Threat (TT): This includes

- Worm: Here, the attacker develops a stand-alone malware that can replicate itself and attack the network

by using up the network bandwidth until it reaches the vector and exfiltrates the target data.

- Trojan: Here, a malicious program masquerading as a normal application (like a game app, social medial app, etc.) infiltrates the system and destroy/damage the files on the system.
- Computer Virus: Here, malicious codes are introduced into the system to damage intellectual property and spread the effect like a virus.
- Spyware: Here, a malicious program secretly gathers information about the user for advertising known as adware.

Botnet: Here, it involves a group of internet-connected malware-compromised computers to launch a denial-of-service attack on the victims.

(2) Social Engineering Threat: This involves popular but dangerous threats such as Phishing, Spear-Phishing, Whaling, and Bailing.

(3) Structured Query Language (SQL) Injection and Buffer Overflow

a. SQL: Here, through a web-based application, the database of the victim is attacked, and critical /valuable assets such as passwords, credit card numbers, etc., are discovered and exfiltrated.

b. Buffer Overflow: Here, the attacker introduces more data than necessary into the memory buffer than its capacity. This will cause the spilling of valuable information into the adjacent memory. This may cause malfunction or crashing of the system.

(4) Next generation Threat (NGT): These are:

a. Polymorphic Threat (PT): This is a collection of constantly changing threats (i.e., morphs) such as Trojans, worms, or spyware.

b. Blended Threat (BT): Here, the attacker uses multiple attack vectors to inflict damages on the victim's system.

c. Zero-Day Attack (ZDA): Here, the attacker launches an attack on the application within the system before its "day zero" of public awareness of the vulnerability.

d. Advanced Persistent Threat (APT): In this type of attack, the attacker covertly gets connected to the system without the knowledge of the victim for a long time to monitor the series of activities on the system and steal information when needed without damaging the system. APT is designed to steal high-valued information from an organization.

III.GLOBAL CYBERSECURITY STATISTICS

It is a known fact that our world is digitally more connected than ever before. As a result, the hackers take advantage of this opportunity to explore the weaknesses in the process. The economic and social impact of this Monster is extremely damaging to governments, businesses, and individuals globally. These cybercriminals are increasingly becoming organized and coordinated in their attacks on governments, businesses, and individuals globally.According to Steve Morgan and Sausalito (2022) and Cyber Threat and Trends Report, Worldwide cybercrime damages are predicted to cost $10.5 trillion annually by 2025. As of 2021, the global annual cost of cybercrime damages is estimated to be $6 trillion. Cybercrime cost has been estimated to be worth 1% of the global Gross Domestic Product – GDP. It is estimated that cumulatively between 2021 and 2025, the global cybersecurity expenditure will exceed $1.75 trillion.

Moreover, it has been reported that an average of 71.1 million individuals fall victim to cybercrime annually and the top among such crimes are Phishing, Extortion, identity theft, personal data breach, and non-payment .

In addition, Global Market Insights (GMI) predicts that the cybersecurity market shall grow to $300 billion by 2024. It has also been confirmed that small businesses are being attached the most. As a result, they are considered "Lucrative Targets" to the attackers. Juniper Research attributed the cause of these constant attacks to a meager expenditure of less than $500 been spent by small businesses.

In contrast, Allianz Global Corporate and Specialty reports that the cyber insurance Market will hit $20 billion by 2025. Also on this note, Cybercrime Magazine is reported to have hinted to companies against ransomware attacks as companies are predicted to be attacked every 14 seconds. This stance was supported by a University of Maryland report that cyberattacks on companies will occur every 39 seconds. On the same matter, Statista reports that 37% of global cyberattacks are perpetrated towards businesses and KnowBe4 adds that over 90% of successful attacks against businesses come from Phishing. Juniper Research has it that the United States stands the risk of being the target of 50% of global cyber-attacks in the next five years. The CPO Magazine claims that just 10% of cybercrimes are being reported.

1. Cybersecurity Charts

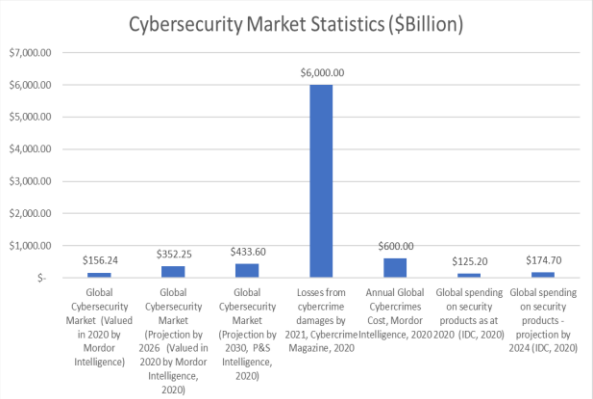

Fig. 1. Cybersecurity Market Statistics($Billion).

Source: Baker Hostetler, 2020
Source: Hiscox, 2020

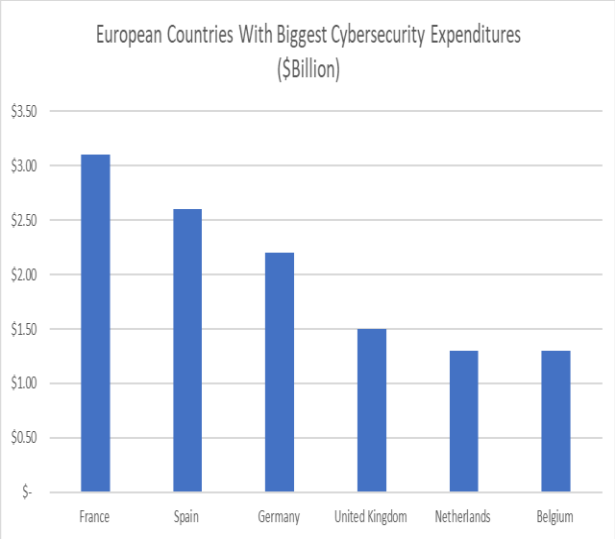

Fig. 2.List Of European Countries with Biggest Cybersecurity Expenditures ($Billion).

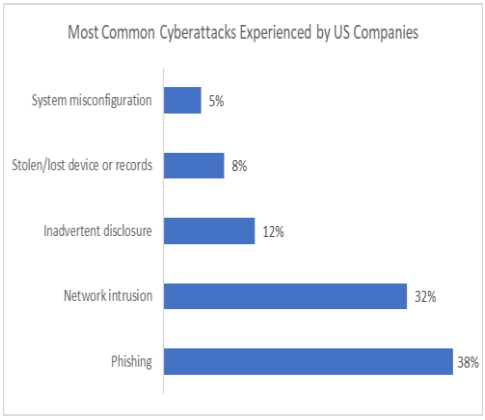

Fig. 4.Most Common Cyberattacks Experienced by US Companies.

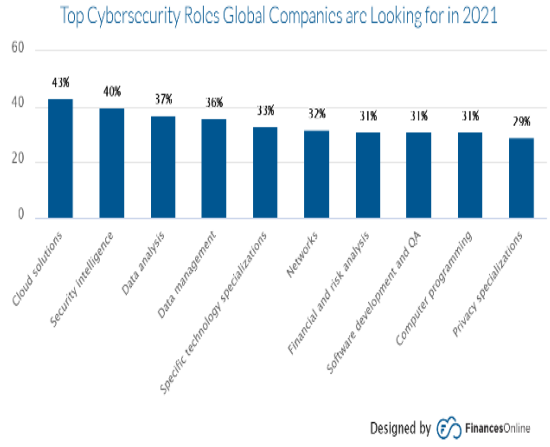

Fig. 3.Top Cybersecurity Roles Global Companies are looking for in 2021.

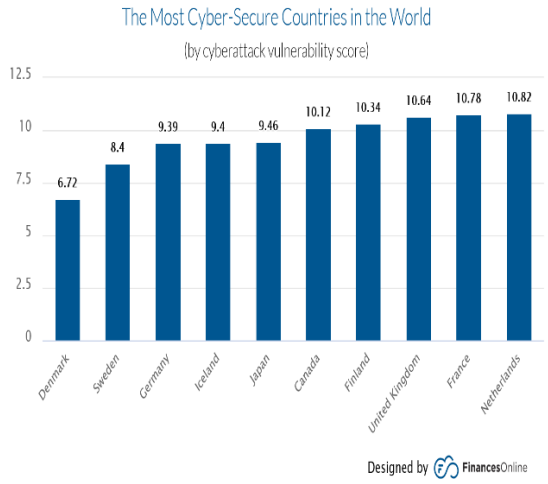

Fig. 5. The Most Cyber-Secure Countries in The World.

Going by the above facts and figures, there is a need for urgent and deliberate action plans to curb the tide of ever-growing cases of cyber insecurity across the globe. At this juncture, it is safe and appropriate to look at the layered security framework and why it is better to curb the tide of cyber insecurity.

IV. ON-PREMISES AND CLOUD-BASED SECURITY SOLUTIONS

One critical decision that every organization needs to intelligently decide when thinking of the protection of its data system is located. In taking such a decision, every organization is enjoined to involve the service of an experienced Managed Service Provider (MSP) to educate the organization in choosing the right choice. Majorly, two solutions are popular: namely (I) On- Premises Solution and (II) Cloud–Based Solution.

1. On-Premises:

In this type of security solution, the software, hardware, servers, backups, and Enterprise Resource Planning – ERP, security framework, etc.) are warehouses in a specific enclave/building. The security framework included may be single-layered or multi-layered. The organization would have to employ the service of an IT guru/specialist to be managing the security architecture of the organization. The strength of the security framework depends largely on the capacity of the employed IT specialist. Hence, the IT specialist must be abreast of happenings in the cyber world across the globe. One major weakness of this cyber solution is the recovery of an organization after a major natural disaster like an inferno.

2. Cloud-Based Solution (CBS)

In the cloud – base solutions, organizational critical information is kept in a cloud-based infrastructure, platform, and application. To efficiently achieve this, the services of a firm or experienced individual(s) who

specialize in the Service of Cloud Provider (SCP) will be needed. The provider ensures constant internet connection to host the Services of an organization – the client. CBS helps organizations in the recovery of any data loss, storage, and network protection against cyberattacks, etc. Depending on the choice, size, and financial capability of an organization, either of the security solutions can be adopted. The two security solutions can be layered but CBS is the most efficient.

V. WHY LAYERED (OR MULTI-LAYERED) SECURITY ECOSYSTEM

This is an age where no two cyber threats are exactly alike. As a result, we must accept the fact that the cyber security measures are as many as various series of threats to our data. However, we must acknowledge also that an array of security tools may not be sufficient to completely protect an organization from any form of cyberattack.
When it comes to technology and tooling, the first thing that comes to mind is cyber security's one-layer approach. this can further be explained as having variegated standby security measures to secure various pathways. e.g., web application firewall being deployed, utilizing encryption tools for email gateway, and protecting the endpoints, rather than adopting the archaic practice of perimeter defense common in our today's organization.

Professionally, layered security means a system of security where every component of the security framework is protected in a coordinated manner so that the operation of an organization is difficult to infringe upon by unauthorized people. Just like an onion, every layer serves as a protective envelope to the operation of an organization. Even if a hacker manages to infiltrate one layer of security, all the data and resources inside the network remain safely guarded by the other layers of security which are in place".

In a layered security framework, multiple components are put into use to protect the whole operations of an organization. It is a collection of technologically driven in-depth measures integrated into the organization's system that hinders, slows, or delays any likely threat from an attacker. It is essential since just one cybersecurity measure cannot guarantee the full protection of data in an organization against all cyber threats in these days of ever-evolving threats and viruses. In this system of cyber threat prevention, an individual layer of the cybersecurity plan is designed to be able to counter any likely flaw or threat from unauthorized sources.

Only a layered security ecosystem is in line with the cybersecurity framework recommended by the National Institute of Standards and Technology (NIST). NIST has five basic functions. These are Identify, Protect, Detect, Respond, and Recover. The NIST framework helps an organization design its security architecture in such a way that it will be able to identify a threat and protect the system against the identified threat. Where the cybercriminal has been able to breach the system, the security framework should be able to position the organization for the best possible result when Responding and Recovering from the attack. Thus, NIS synergizes the strategies and the best-known industrial ethics to help organizations manage and understand their cybersecurity risks.

However, maintaining total compliance with standards cannot guarantee the security of a system, rather, there is the need to go far -far beyond the known best practices and norms. As of today, no known 'almighty' measure has ever been designed or developed to protect a system permanently.

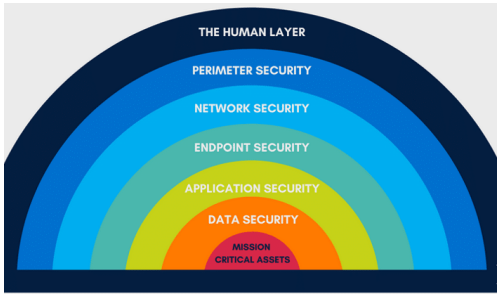

Fig. 6.The Seven Layers of Cybersecurity.

1.Layer Security Framework
In a layered security framework, the foundational component is perimeter defense, which involves the prevention of malicious traffic from ever reaching the network. Perimeter defense begins with a firewall, which can be implemented using software, a hardware appliance, or a cloud-based solution.

2. Cyber Security Fundamentals
Effective and efficient cybersecurity diminishes the risk of cyber-attacks and consequently protects organizations as well as people within the organization from the unauthorized manipulation of systems, the network itself together with the technologies. A very strong cybersecurity framework is roughly based on three key terms: people, processes, and technology.These fundamental principles are the building blocks of security and will help the organization to develop a strong foundation in security. Confidentiality, Integrity, and Availability (CIA) are the driving forces behind Information Security.

To enhance the security of an organization viz-a-viz data management, cybersecurity should be layered; it is not expected to be a single piece of technology that organization security will depend on. This ensures comprehensive protection. In essence, the security framework prevents any observable security

compromise/weakness in one layer to extend to others due to different security plans in place. Thus, every organization ought to understand what a layered security architect is all about. Here is a brief of what each layer contains.

1. Mission-Critical Assets
This is a collection of vital properties (such as application software, gadget, database, etc.) upon which the smooth running of a business enterprise or organization rests. The absence of them will spell doom for an organization or a business entity. Such critical assets ought to be protected. To achieve this, the security architecture of an organization should be built in layers with each performing a specific/unique protection role.

2. Data Security
Data security: This is the enhanced protection mechanism put in place to protect the integrity of the data during storage or transfer. This may be in terms of developing codes or passwords to protect the data. Data security mainly includes data confidentiality, availability, and integrity. This is so because data is the backbone of any organization. Sophisticated security measures should be in place to protect the sanctity (i.e., confidentiality, availability, and integrity) of the data. Such measures include encryption of data using an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) to alert and prevent any attack on the stored data. Also, the paths through which the data are being transmitted should be credible and made immune to attacks. For instance, data shared on encrypted Hypertext Transfer Protocol (HTTP) are saved. The encrypted HTTP (i.e., HTTPS) uses TLS. HTTPS is a secure form of HTTP. HTTPS encrypts HTTP requests as well as responses. If information is intercepted on HTTPS, the attacker only sees a set of unmeaningful strings of characters.

3. Endpoint Security
Endpoint security is also called endpoint protection. It is the protection of computer networks that are remotely connected to user devices. The larger system allows for common access to files, the internet, and software. A user accesses a network via a connection to an endpoint, (person or remotely). Depending on the arrangement of the system, they will then have access to part or all of the network. An organization system or network connects various endpoints. This includes connecting a computer to a printer and the internet, database, intranets, and/or extranet. The susceptibilities of endpoints appear endless. The setup makes it easy for the compromised endpoint(s) to easily penetrate the organization set up to steal desired information needed. Yue Shi (2018) confirmed that 70% of successful corporate exploits target endpoints, rather than servers or other internal infrastructures.

Endpoint protection platforms (EPP) can verify files as they enter the network. There are versions of EPP that can leverage on strength of the cloud to manage and free the endpoint database of an ever-increasing database of cyber threats. This assesses the data easy and faster. Installation of EPP helps to promptly detect any malware as well as any other cyber threats. An Endpoint Detection and Response (EDR) component can detect zero-day attacks, file-less malware, and polymorphic attacks. There are versions of EPP that are compatible with an on-premises solution and cloud-based solutions.

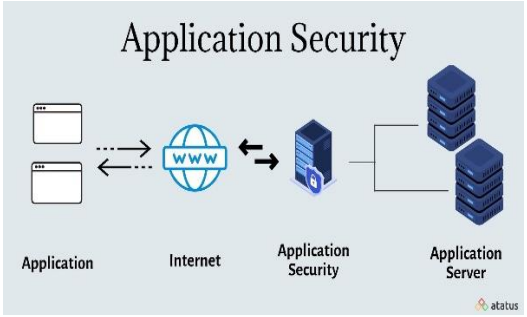

Fig. 7. Application Security.

4. Application Security
This is a security measure designed to prevent data theft within the application. This security measure is implemented at the application design and development level. So, at the level of application deployment, the security is already embedded.Application security is increasingly becoming necessary nowadays in that applications are hosted on the internet and vulnerabilities of these applications to threats are as well increasing. The application security can detect weaknesses at the application level and appropriate solutions can be proffered. This is because of various features embedded in the configuration such as logging, authentication, encryption, and authorization.

5. Network Security (NS)
This is a security measure where the networking infrastructure is protected from unauthorized misuse/access even modification through the adoption of some policies or processes which make it extremely difficult for an intruder(s) to gain access. This requires a continuous update of the process and the system in general for necessary security patches as well as encryption. This may be informed of disabling unused system interfaces to further safeguard against any possible threats.

NS is critical in shielding the data and information of the clients. It keeps shared data in a secure database and ensures easy and reliable access to the internet/network by protecting it against cyber threats For instance, Firewalls manage both the incoming and outcoming network traffics following the laid down rules and regulations. For instance, Next Generation Firewall focuses on blockage of all application-layer – attacks, and malware.

6. Perimeter Security

This is a security measure where a network of an organization is protected against attackers or intruders via the installation of surveillance detection, pattern analysis, designing of firewalls, threat recognition, and effective response.

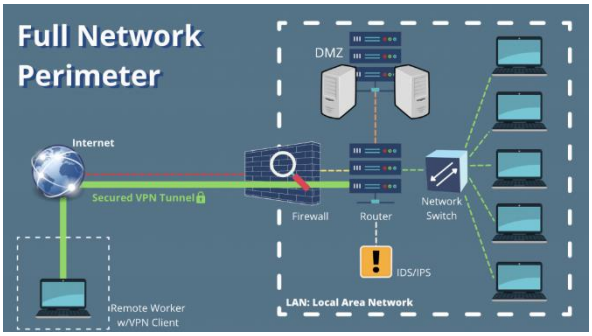

Fig. 8.Fulll Network Perimeter.

Source: https://digital.com/best-vpn-services/what-is-perimeter-security-architecture/ The perimeter security framework has the following components: Firewall, Intrusion Prevention System (IPS), Intrusion Detection System (IDS), DMZ, and Virtual Private Network (VPN).

7. The Human Layer

Under this security control, the organization puts in place measures that automatically detect and prevent likely people–oriented security attacks. In this control measure, a unique security identity is developed for every member of the organization. Regular update is done to this control to prevent compromise from within and outside intruders. Majorly, this layer turns the human elements of an organization into security assets. This is based on the use of intelligent technology to help a man make the wisest decision when alerted on infringement on the network framework illegally.

RECOMMENDATIONS

- To Governments The government of every nation should see cybercrime as a great economic challenge that requires concerted efforts of all stakeholders. The cyber environment should be protected with Laws and legislation that will make it impossible for cybercriminals to thrive. Law enforcement agents should be supported to be able to confront the situation no matter the level of sophistication.
- The capacity of our security agencies should be enhanced to be able to manage the existing cyber risks. There must be collaboration among the agencies to be able to identify, assess, track, and manage various cyber threats emerging across the globe.
- To Organization: Every organization should ensure it adopts a layered security framework in setting up its security solution. The best security solution is cloud-based type. Any organization that has the capacity should adopt a Cloud-Based Solution to be immune from cyber criminals.

VII. CONCLUSION

Today, cybersecurity has become a scary monster that the global economy must be immune against. The colossal sum of money has been estimated to be gulped by this economic threat in the next few years to come, if not checked. Empirical evidence is around to support the havoc already caused by cybercriminals around the World. To avert this impending calamity, efforts have been made to sensitize the likely 'Targets' of this heinous act ahead of its manifestation. Every organization (Business, Corporate or Private) has been encouraged to adopt either On-Premises or Cloud-Based Solutions. In addition, the organization has equally been exposed to the danger of adopting a single-layered security framework in either of the adopted security solution. Every organization has been enjoined to adopt a Layered (or simply Multi-Layered) security framework to safely guide the important information of the firm.

REFERENCES

1. Abdulaziz Alarifi, Holly Tootell, and Peter Hyland. (2012). A study of information security awareness and practices in Saudi Arabia. International Conference on Communications and Information Technology (ICCIT) (pp. 6-12). Hammamet: IEEE.
2. Aimee O'Driscoll (October 2, 2018), 100+ Terrifying Cybercrime and Cybersecurity Statistics & Trends [2018EDITION], https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/#Global.
3. Alansari, M. M., Aljazzaf, Z. M., & Sarfraz, M. (2019). On Cyber Crimes and Cyber Security. In M. Sarfraz (Ed.), Developments in Information Security and Cybernetic Wars, pp. 1-41. IGI Global, Hershey, PA, USA. doi:10.4018/978-1-5225-8304-2.ch001.
4. Alex Antoniou and Gauri Sinha. (2012). Laundering sexual deviance: Targeting online pornography through anti-money laundering. European Intelligence and Security Informatics Conference (pp. 91-98). Odense: IEEE.
5. Alex Roney Mathew, Ayad Al Hajj, and Khalil Al Ruqeishi. (2010). Cybercrimes: Threats and protection. International Conference on Networking and Information Technology (pp. 16-18). Manila: IEEE.
6. Alexios Mylonas, Anastasia Kastania, Dimitris Gritzalis. (2012). Delegate the smartphone user? Security awareness in smartphone platforms. Computers & Security, 34, 47-66.
7. Aloul, F. A. (2010). Information Security Awareness in UAE: A Survey Paper. Internet Technology and Secured Transactions (ICITST), 2010 International Conference (pp. 1-6). London: IEEE.

8. Amber Stabek, Paul Watters, and Robert Layton. (2010). The Seven Scam Types: Mapping the Terrain of Cybercrime. Second Cybercrime and Trustworthy Computing Workshop (pp. 41-51). Ballarat, VIC: IEEE.
9. Andreasson, K. (2011). Cyber security: Puplic sector threats and responses. U.S.A: CRC press.
10. Anti-phishing Working Group. (Sep,2013). Phishing Activity Trends Report. Phishing Activity Trends Report.
11. Articl19 Group. (2012, Feb 2). Brazil: Draft Cybercrimes Law. Brazil: www.artical19. com.
12. Balkhi, S. (2013, MAY 6). 25 Biggest Cyber Attacks In History.
13. Barnes B. and Perlroth N. (2014, DEC 3). Sony Pictures and F.B.I. Widen InquiryIntoHackers' Attack. The New York Times.
14. Berg, D. (2013). Social Media and Online Defamation. NOLO law for all.
15. Bhanu Sahu, Neeraj Sahu, Swatantra Kumar sahu, and Priya Sahu. (2013). Identify Uncertainty of Cyber Crime and Cyber Laws. International Conference on Communication Systems and Network Technologies (pp. 450 - 452). Gwalior: IEEE.
16. Bhatt S. & Pant D. (2011). Cyber Crime in India. International Journal of Advanced Research in Computer Science, Vol. 2 Issue 5, 153-156.
17. Box, J. F. (1987, Feb). Guinness, Gosset, Fisher, and Small Samples. Institute of Mathematical Statistics, Statistical Science, Vol. 2, No. 1, pp. 45-52.
18. Broadhurst R. &Grabosky P. (2005). Cyber-crime. Hong Kong: Hong Kong University Press.
19. Brokenshire, J. (2013, Mar 14). UK government. Retrieved Aug 1, 2014, from http://www.gov.uk.
20. Bruce S. Schaeffer, Henfree Chan Henry Chan and Susan Ogulnick. (2009). Cyber Crime and Cyber Security:A White Paper for Franchisors, Licensors, and Others. business.cch.com.
21. Chang Yew, Wong. (2002). Malasian Law and Computer Crime. Malaysia: SANS.
22. Cyber Security Ventures, (2018). https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.
23. Diane Lending & Sandra A. Slaughter. (1999). Understanding differences in ethical beliefs and behaviors toward software copying: the effects of organization culture. SIGCPR '99 Proceedings of the 1999 ACM SIGCPR conference on Computer personnel research (pp. 253-260). NY, USA: ACM.
24. Dilanian K (2013) Cyber-attacks a bigger threat than al qaeda, officials say. Los Angeles Times, March 12, 2013. http://articles.latimes.com/2013/mar/12/world/la-fg-worldwide-threats-20130313. Accessed 5 August 2013
25. Dixon, P. D. (2005, December). An overview of computer forensics. Potential, IEEE, 24(5), 7-10.
26. DogrulM.,AslanA&Celik E. (2011). Developing an international cooperation on cyber defense and deterrence againts cyber terrorism. International conference on cyber conflict (pp. 1-15). Istanbul: IEEE.
27. Erbschloe, M. (2004). Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code. Oxford: Butterworth-Heinemann.
28. Fawn T. & Paternoster R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. International Journal of Cyber Criminology, 5, 773-793.
29. Frances S. Grodzinsky and Herman T. Tavani. (2002). Cyberstalking: moral responsibility, and legal liability issues for Internet service providers. International Symposium onTechnology and Society, 2002. (ISTAS'02). (pp. 331
30. Global Cybersecurity Index 2017, (2017). International Telecommunication Union (ITU), https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.
31. Gorazd Mesko,and Igor Bernik. (2011). Cybercrime: Awareness and Fear: Slovenian Perspectives. European Intelligence and Security Informatics Conference (EISIC) (pp. 28 - 33). Athens: IEEE.
32. Hamdi M., Safran M. and Wen-Chi Hou. (2014). A Security Novel for a Networked Database. Computational Science and Computational Intelligence (pp. 279 - 284). Las Vegas, NV: IEEE.
33. Hernandez-Castro E.,Boiten E. (2013, Aug 23). About Us: Kent University. Retrieved Sep 22, 2014, from University of Kent website: http://www.cs.kent.ac.uk.
34. Hussainat, M. (2013). Computer Crimes in the Jordanian Society: Ajloun/Empirical Study. Asian Social Science, 9, 85-93.
35. IIBF. (2012). IT Security. India: M/s TaxMann Publishers.
36. Ilyin, Y. (2013, AUG 15). Kaspersky Lab Business Web site. Retrieved MAY 22, 2014, from Kaspersky Lab Business Web site: http://business.kaspersky.com/threats- in-q2-2013.
37. International Journal of Digital Evidence,1(3),1-12.
38. Jeffrey M. Stantona, Kathryn R. Stama, Paul Mastrangelob, Jeffrey Joltonb. (2004). Analysis of end user security behaviors. Computers & Security, 24(2), 124-133.
39. Johnson, M. (2013). Cybercrime: security and digital intellience. U.S.A: Gower publishing LTD.
40. Kabay, M. E. (2008). A Brief History of Computer Crime. An Introduction to Students conference. Norwich University.
41. Kenefick, S. (2008). Real World Software Configuration Management. Newyork: Apress.
42. Kumar, A. P. (2009). Cyber Crime. Bangalore: The Banner of YFI &Anupa p Kumar.
43. Kuwait Times. (2016, 12 1). Kuwait times. Retrieved 1 25, 2016, from http://news.kuwaittimes.net/website/electronic-

crimes-law-threatens-to-further-stifle-freedom-of-expression-amnesty-intl/.
44. Lesisko, Lee James. (2003). Analyzing Software Piracy in Education. ERIC.
45. Linda L. Edwards, J. Stanley Edwards, Patricia Kirtley Wells. (2008). Tort Law for Legal Assistants. Cengage Learning.
46. Louw C. , Von Solms S. . (2014). Online social networks to online social malworks. The evolution an industry conference (pp. 1-7). Africa: IEEE.
47. Lynch, J. (2002). The United States: department of justice. Retrieved Aug 3, 2014, from http://www.justice.gov.
48. Majid, M. D. (2012). Cybercrime: Malaysia. Malaysia: Royal Malaysia Police. May, M. (2004). Federal computer crime law. U.S.A.: SANS institute.
49. Menshawi, A. (2003). The size and style of the most common Internet crimes among Internet users in Saudi society, and a research paper.
50. Montgomery, D (2001). Design and Analysis of Experiments (5th Edition). NewYork: John Wiley & Sons.
51. Moon B., Mccluskey J., Mccluskey C. (2010). A general theory of crime and computer crime: An empirical test. Journal of Criminal Justice, 38(4), 767-772.
52. Neff, R. (1994). Software Piracy: International Copyright overview. WESCON/94. Idea/Microelectronics. Conference Record (pp. 190-195). Los Angeles, CA: IEEE.
53. Norton. (2012, April 2022). aitnews. Retrieved (2014, Dec 2) from http://aitnews.com.
54. Obrien A. &Marakas G. (2007). Introduction to Information System. Boston: McMagraw-Hill International irwin.
55. Ogilvie, E. (2000). Cyberstalking. trends & issues in crime and criminal justice (pp. 12- 19). Australia: Australian Institute of Criminology.
56. Oweis N., Owais S., Alrababa M., Alansari M. (2014). A Survey of Internet Security Risk Over Social network. Computer Science and Information Technology (pp. 1-4). Amman: IEEE.
57. Paganini, P. (2012, April 23). Analysis of cybercrime and its impact on private and military sectors. PenTest Auditing & Standards. Available: http://securityaffairs.co/wordpress/4631/cyber-crime/analysis-of-cybercrime- and-its-impact-on-private-and-military-sectors.html
58. Ping, Y. (2011). Study on the Main Form of Network Crime from the View of Criminology. International Conference on Human Health and Biomedical Engineering (pp. 1108-1111). China: IEEE.
59. Reith, M., Carr, C., &Gunsch, G. (2002). An examination of digital forensic models.
60. Rekha A. & Radhakrishna R. (2014). Piracy in the digital age: Is ethical awareness turning into action? Ethics in Science, Technology and Engineering, (pp. 1-4). Chicago, IL: IEEE.
61. Rekouche, K. (2011). Early phishing. Available: http://arxiv.org/abs/1106.4692v1.
62. Researcher. (2007). Retrieved Aug 2, 2014, from cyberlawsinindia: http://cyberlawsin india.net.
63. Riccardo Satta, Javier Galbally, and Laurent Beslay . (2014). Children Gender Recognition Under Unconstrained Conditions Based on Contextual Information. International Conference on Pattern Recognition (pp. 357 - 362). Stockholm: IEEE.
64. Richard Mankiewicz; Ian Stewart. (2001). Story of Mathematics. New Jersey, U.S.A: Princeton Univ Pr., Ewing.
65. Royakkers, L. (2000). The Dutch Approach to Stalking Laws. Berkeley Journal of Criminal Law, 3, 1-14.
66. Rubino, F. A. (2014). Federal Criminal Defense Lawyer Frank A. Rubino. Retrieved NOV 7, 2014, from http://www.frankrubino.com.
67. Russell, J. (2011, OCT 25). Japanese government hit by Chinese Trojan horse attack.
68. Saini Das, Arunabha Mukhopadhyay, and Girja.K. Shukla. (2013). i-HOPE Framework for Predicting Cyber Breaches: A Logit Approach. 2013 46th Hawaii International Conference on System Sciences (HICSS) (pp. 3008 - 3017). Wailea, HI, USA: IEEE.
69. SchaeffB,Chan H. and Ogulnick S. (2009). Cyber Crime and Cyber Security. A White paper for Franchisors licensors, and others, p.1-15.
70. Sebastian. (2013, 25 DEC). Security 1:1 - Part 1 - Viruses and Worms. Security, Symantec Protection Center (SPC).
71. Shahabuddin, S. (1987). Computer Crimes and The Current Legislation. ACM SIGSAC Review, 5(3), 1-8.
72. Sharma, D. (2013, 7 10). Retrieved Aug 2, 2014, from India largest cyber security solution: http://www.indiancybersecurity.com.
73. Shimbun, T. A. (2011, Aug 20). Editorial: Japan should play active role against cyberattacks. Adventure works weekley.
74. Sterling, B. (1992). The Hacker Crackedown. New York: Bantam Books.
75. Swain, B. (2009, JUN 25). What are malware, viruses, Spyware, and cookies, and what differentiates them? Inside Symantec, Security, Endpoint Protection (AntiVirus).
76. Symantec Enterprise. (2014, DEC 3). Retrieved DEC 5, 2014, from Symantec Corporation: http://www.symantec.com.

77. Symantec. (2014). List of Top 20 Countries with the highest rate of Cybercrime. USA: Business Week/Symantec.
78. Tabuchi, H. (2011, Sep 21). U.S. Express concern about new cyberattacks in Japan.
79. Totarotech. (2013, JAN 31). TotaroTechBlog. Retrieved OCT 10, 2015, from https:// totarotech.wordpress.com/2013/01/31/5-motivations-for-cybercriminals/
80. Velasco, C. (2007). The Legal Framework on Cybercrime and Law Enforcement in Mexico. Mexico: Contribution to the Second WSIS Action Line C5 Facilitation Meeting.
81. Warner, G. (2010, Aug 26). Major Fraud Ring Busted in largest Chinese Cybercrime Operation. Malcovery, UAB.
82. WD Kearney & HA Kruger. (2014). Considering the influence of human trust in practical social engineering exercises. Information Security for South Africa (ISSA) (pp. 1-6). Johannesburg: IEEE.
83. Siobhan Climer and Mishaal Khan (2020): What Are The 7 Layers of Security? A Cybersecurity Report
84. Secure Your Information: Information Security Principles for Enterprise Architecture. Available online: Allianz supports the European Championships Munich 2022. https://www.allianz.com/en.html Assessed on 22/08/2022.
85. Market Insights. https://www.gminsights.com/Assessed on 22/08/2022
86. Juniper Research. https://www.junipeearch.com/home Assessed on 22/08/2022.
87. CPO Magazine. https://www.cpomagazine.com/ Assessed on 22/08/2022.
88. JPMorgan Chase & Co. https://www.jpmorganchase.com/ Assessed on 22/08/2022.
89. KnowBe4. https://www.knowbe4.com/ Assessed on 22/08/2022.
90. Steve Morgan and Sausalito (2022): The past, present, and future of cybercrime by Cisco/ Cybersecurity Ventures, 2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics
91. Akarshita Shankar, Ramesh Shetty and Badari Nath K (2019): A Review on Phishing Attacks; International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 9 (2019) pp. 2171-2175 © Research India Publications. http://www.ripublication.com
92. Thomas A. Johnson (2015): Cyber-Security: Protecting Critical Infrastructures from
93. Frayssinet, M., Esenarro, D., Juárez, F. F., y Díaz, M. (2021). Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations. 3C TIC. Cuadernos de desarrolloaplicados a lasTIC, 10(2), 123-141. https://doi.org/10.17993/3ctic.2021.102.123-141
94. Economic Impact of Cybercrime (Feb. 2018): At $600 Billion and Counting - No Slowing Down
95. Cyber Attack and Cyber Warfare, Webster University St Louis, Missouri, USA.