Advanced Cyber Exploitation and Mitigation Methodology

Oghene Augustine Onome

Abstract: The aim of this article looks into the comprehensive methods in re-architecting a security operations centre (SOC) to protect corporate computing frameworks. Through persistent exploitation using advanced technologies, cyber threat infiltration has caused financial losses to enterprises all over the world. No progress has been made yet in terms of technological improvements, particularly in combining cybersecurity equipment. Cybercriminals, on the other hand, are constantly improving their tools and methodologies in order to breach any business. Multiple exploitations through networks, systems, and phishing emails have resulted in incoming dangers, threats, and vulnerabilities in areas such as data privacy and security due to rapid technological advancement. To protect their working environment, several firms in many sectors have resorted outmoded technologies which are ineffective in the face of advanced persistent threats (APT). Cybersecurity actors are well-equipped groups with extensive knowledge that can infiltrate even the most secure of organizations. Cyber security is seen as a major issue around the world. As a result, dedicated cyber security researchers are analysing both existing dangers and emerging threat approach patterns in order to develop a technique that can be integrated with cybersecurity management.

Index Terms: Cyber Security, Data

I. INTRODUCTION

The evolution of technology has not helped in reducing the criminal act; it has rather reinforced the passion for it as it is a massive means of livelihood for the culprits. This begs the question: Is there any hope that this activity can be combatted for good? [1] states that people are curious as to whether this is possible either in the traditional sense, or in those areas in which there have been a unique evolution such as that within cyberspace, the internet; and the answer is yes, there is hope, but it will come with a price. However, this criminal activity should neither be considered insignificant nor be overlooked. The attitude and approaches adopted by enterprises and individuals in confronting this criminal activity must evolve. Before developing a model on how to control and stop the external threats, one crucial thing they need to keep in mind is that the enemy is within. And this demand was cultivating and developing a sense of surveillance which eventually results in the development and proliferation of those who seek to challenge the actions of the criminal. For enterprises and individuals to make headway in this mission, they need to devise means of detecting, identifying, and preventing the cybercrime as well as gain more insight into the subjective motivations and drivers behind these group of individuals. The ripple effect of this is, it will be easier for enterprises and individuals to understand the tactics, strategies, and plans developed to unleash attacks on their targeted victims to achieve their objective.

Furthermore, in the past two decades technological advancement has brought the entire world together without any boundaries. [1] states this is largely because of the evolution of modern telecommunication networks as well as the expansion of the internet and World Wide Web. This has changed the perceptions of communication, thus returning to the old ways is not possible. A single click of a mouse or swapping the LCD of a smartphone eliminates distance which in the past was a challenge facing humanity. The revolutionary drawback to the positive mark made by technology is the exponential increase in cybercrime activities which have increased both individuals' and organizations' risk posture. Like in the case of Sony pictures, the expectation was to block the release of a movie instead of sending the geopolitical message: "We can damage your companies and your economy."

Also, [2] mentions that though organizations make an effort to do the right thing and adhere to all the rules, they still get compromised and have their networks broken into. This, becomes a big surprise to the business owners after being notified of the incident in spite of the millions of dollars invested into safeguarding their assets. The takeaway, then, is that since there is no one hundred percent secure environment, the focus should be on controlling vulnerabilities on the network devices, systems, and applications. Since a large number of entities do not have an inkling of how cyber actors operate, they are often easy to compromise without much effort from the criminal. In order to be a step ahead of the attacker, organizations need to ensure that they understand how these criminals operate and develop an effective and working plan. In other words, safeguarding a threat that is not used by the attacker will lead to compromising the working environment of the organization. [2] states that fixing random vulnerabilities is a good thing; understanding how the attacker compromised an organization and focusing on those areas is the right thing to do. What this means is that, it is advisable to understand how the attackers break-in. This will make it easier to identify the common threats posture of the enterprise that could cause a possible high-risk impact.

Manuscript received on February 11, 2022.
Revised Manuscript received on March 02, 2022.
Manuscript published on March 30, 2022.
* Correspondence Author

Dr. Oghene Augustine Onome, Scholar, Post Doctorate Degree in Cybersecurity Management, Atlantic International University, Abuja Nigeria

Once the threat patterns are ascertained, it becomes an area to channel all energy towards. Besides, enterprises fully aware of this trend will need to apply intelligence for information gathering and never be reluctant as the attacker keeps changing their mode of operation to get their targeted victims compromised forcefully. Traditional vulnerabilities are what make it easy for them to a break-in, as they are aware many organizations are to update application of patches to remediate vulnerable systems in the environment. An environment without updated patches can simply be compromised by a worm. So, once a single system or network device is compromised, the attackers will be in the network causing damages to data. Meanwhile, discovering a vulnerability early requires developing attack tools to automate the exploitation of the vulnerabilities. [3] suggests regularly examining technologies as they systematize computer hacking. With this, end-users of these technologies should adopt a more advanced way of studying the technologies they acquired, as in some cases vulnerabilities are embedded into the products. An example is a case with Juniper Networks. In December 2015, it was reported that a malicious group introduced a destructive code in the software baseline of the device. The discovery prompted the United States government to ban the importation and sales of the vendor product. A similar incident occurred with a checkpoint product by an Israeli company. The United States banned the importation and sale of the product. It is quite common for manufacturers of high-tech devices to embed codes that serve as a back door for easy access inbound and outbound into the network environment. Moreover, cyber exploitation causes more damages to data; though data exploitation leaves behind digital footprints which make it easy to capture traces within the environment. [4] states that Apple iCloud was hacked and hackers got their hands on 100's of nude celebrity photos including Kaley Cuoco, Avril Lavigne and Hayden Panettiere, Kim Kardashian, Hope Solo and Vanessa Hudgens. These affected victims thought their privacy was secure, until all their private data was stolen and brought to the public eye. These criminal acts are as a result of calculated efforts – physically and logically – by the attackers; each one making public what should have been private. Regardless of where your data is stored - even if in a space hosted by a cloud provider on your smartphone – attackers always make calculated efforts to steal it.

II. DATA EXPLOITATION

Data exploitation takes place when data is at rest and in transit. It could be physical or logical theft. Either of them could end up being exploited. The physical theft happens in varieties of ways. One is when a computer device is stolen, and the thief accesses the internal disks, memory in that order until data is retrieved from wherever it is stored. Another physical theft method is the stealing of a wallet, pocketbook, locating pay stub, ATM receipts, and credit card. The system of physical theft is not easy to curb, except when one is not directly threatened physically. There are multiple ways to protect one's self from being threatened physically threatened though. Personal security can reduce the risk exposure of the individual to an extent. Also, the individual must devise a better way of safeguarding their credit card, wallet, and other physical items. Organizations must consistently review the inventory of their assets and evaluate their risk exposure to reduce the threat of physical exploitation as well. On the opposite end of physical exploitation is logical exploitation, which is referred to as cyber-attacks. It commences through repeated surveillance until the targeted object is freely accessible. Logical exploitation of data takes place when data are at rest and in-transit. The data at rest means the data is stored in storage; whereas data in-transit is when the data is moving from a source to a destination through file transfer and via e-mail.

The exploitation of data at rest occurs in different dimensions based on the most effortless approach to access the data. The threats can be unleashed depending on where the data is stored. It could be via social media resulting from the exchange of login credentials between both parties. Also, data theft can be through remote attack such as penetration. The data could be stored inside a system, server, and storage devices such as external hard disk and memory stick. However, it is likely to be kept in an extremely secure location. Unlike data in-transit, it is accessed by attackers while the data is traversing the network and when it is sent from an employee device to the backend servers. According to [4], Data exploitation concerns are multiple; therefore, data saved in the local device and accessible by hackers can be used against the owner of the device, as well as data in the form of financial records, medical records, personal information, work-related information, family information and pictures. The only effective mitigation to addressing physical exploitation of data is by securely protecting the local device, as well as ensuring that the mobile device is not left open where it is accessible by attackers. Adopting locking code techniques on the device for extra-protection as a deterrent to the attacker's effort is another way. Any open logical port should be disabled and not open for a period. To protect data against intrusion data encryption technology should be deployed as a safeguard for data both at rest and in-transit. Data in-transit can be hacked when the data traverses through a network and when the transfer of data takes place between the clients and backend servers. This occurs when technology is used to sniff and is analysed to reveal information such as login credentials of an e-commerce website. Spoofing of the website can also be used to capture credentials as it transits from source to destination. Hackers can skim data from credit or debit card using a hardware device in between the card and the reader. This is the approach adopted by hackers to exploit financial information. [4] mentioned, that data loss prevention software suite can securely protect egress points as well as firewalls, making it easy to capture anything traversing from the network into the external network. The tool's capability can bring to visibility violation of security policies established in the enterprise.

A. Exploitation Mitigation Techniques

Ideally, it is advisable that entities perform due diligence in their operating environment; including assessing and analysing the processes that lead to the end state.

Identity exploitation leads to fraud and creates more loopholes for hackers to acquire employee's personal information for criminal activity. It brings about substantial financial loss and increased insurance rate. Many individuals and business owners have lost so much money through identity theft. But the risk exposure can be reduced when users reduce their digital footprint, especially on social media sites. At the same time, the private and public sector should manage their social media engagement. Furthermore, shunning the practice of paying for goods online through non-protective channels, and embracing specific credit cards with fraud protection in place; as well as taking an inventory of one's personal belongings is a sure way to protect one's self. Always remember where you save vital information, and practise personal safety mitigation mindset. [4] states that all the techniques may not eradicate the threats, but it reduces the landscape. Personal action, like viewing your statements frequently, can better aid in protecting valuable individual assets and noticing a compromise immediately.

B. Hardening Systems

Devices should be hardened as a safeguard measure to protect it. The hardening could be in the following format: locking it down, automatically applying operating systems updates, service packs, and patches. These eliminate the medium of hackers by patching vulnerabilities; turning off non-important services; and deploying security controls through systems configuration such as password management, file permissions, and closing unused network ports. The hardening has a process to follow safely to protect the device and is not limited to hardware but includes operating systems and application. Computers: Hardening a computer device requires securing access to it. The device should not be powered and open. The login credentials protection must adopt the best security. Ensure anti-malware software is installed and place the device behind the firewall. Background applications and the operating systems should have up-to-date security patches. The automatic system update should be enabled to allow update installed in the background without user intervention. Another important security measure is installing anti-phishing software within the browser; and the e-mail notification should be enabled to filter spam and ensure that they are not opened. Lastly, auditing setting is enabled to run at the level of the operating system. This hardening approach should apply to the following devices: laptops, mobile devices or smartphones, network devices, and game consoles. Malware Protection is adopted to protect both data at rest and data in-transit securely. Primarily, data at rest is more protected as compared to the one in transit. Conventionally, when an anti-software may be malware, phishing, and virus, it is protecting the data in the systems. According to [4] there are other forms of threat protection such as host-based intrusion detection (HIDS) software, that will alert you to the fact that an attempt to access your data was made. Such a type of solution functions off a threat database that uses heuristics to look for seemingly malicious trends in traffic. On the other hand, surveillance revolves around data gathering to understand and learn about the hacker's pattern, and prepare in the event of another advanced attack higher than the previous one. Attackers always leave behind a footprint of their earlier attempt to probe into the network and systems. The digital trace can be extracted from the systems, firewalls, and occasionally can be flagged by IDS and IPS device. [4] advocates that IPS and similar intrusion software are meant to block attacks such as I.P. fragmentation attacks. They can be a reference when scans are actioned to understand network designs and architecture.

C. Data Encryption and Data loss Protection

Data encryption protects both data at rest and in-transit. It is a process of applying a cipher layer to make data unreadable to those without the means to decrypt and read it. So, it can be applied to data in-transit. Hackers, however, have what it takes to decrypt encrypted data; it is therefore necessary to encrypt your data with a more robust data encryption method to protect the data when intercepted securely. The technology can apply as software on directories, on the hard drive, and memory sticks to protect it against malicious activities. Data loss protection (DLP) is a suite of applications that make it impossible to exploit data at rest and in-transit. It works perfectly well only when the inventory of data is recorded at the initial stage before implementing the solution. With this, any data traversing from the network is flagged because of the capability embedded into the software. Likewise, data can be classified based on their intimate level, and DLP will be flagged when such data classification is exiting the organization as a violation against the policy. In any case, to enable the DLP software have a holistic view of data movement within the network all the devices such as database, file shares, e-mail, local computers, and servers are to be defined on it as endpoints. Similarly, network and all its periphery device are DLP configured to protect it against confidential data exiting the environment into a public network

D. Firewall Device

The device is a program to control ingress and egress traffic within the network. These ensure that malicious activity, like network and system penetration, cannot take place. In this case, logical exploitation will be impossible, unlike physical theft. All online threats are blocked, and the device sends out notification in the event of any persistent threats. Also, protocol analysers - referred to as sniffers - can capture data in-transit for analysis and review purpose. This technology allows attackers to come into the network and then it captures useful information about their pattern. Eavesdropping is another form data exploitation that uses a program such as sniffer to exploit data in-transit. Like physical eavesdropping, it acts as a middleman where the attacker injects itself into a conversation and acts as one of the participants under the pretext of gathering information from a trusted communication. The protocol analyser then captures and analyses the trend of their pattern.

E. Digital Forensics

Data exploitation can be uncovered through digital forensic investigation; where the evidence of recovered information can expose the platform through which the criminal activity ensued.

The process can extract evidence from all the devices of those who conducted the crime as well as their identity. According to [4], from a surveillance point of view, any data - even data you think you may have erased - could be resurrected with digital forensic tools and software.

III. NETWORK EXPLOITATION AND MITIGATION TECHNIQUES

The dynamism of network exploitation is extremely extensive, and it continues in a persistent trend until the hackers have exhausted all their mechanism without reaching their target. This outcome is not always the case. In some, it depends on the enterprise and the degree of security controls implemented to safeguard the business assets. The size of the organizations and their sensitivity to security matters also contributes to either of the success or failure of the hacker's effort. According to [2] back in the 1990s, understanding and assessing why organizations were compromised was straightforward. There was always a gap by the organizations that made it easy for them to be compromised. In some cases, it was intentional; in other cases, it was not. Many of the reasons were obvious mistakes. A deeper dive into investigations revealed that in many of the cases inadequate controls and absence of security appliances were the root cause. All of this became transparent after an incident had occurred. Cybersecurity is never simple. Yet it is obvious knowledge, that the threats are identified and quickly handled, giving the organizations a clear understanding of what to do to protect their environment.

Attackers are persistent in their current threats; thus, they maintain remote access to their victims for as long as they want, without the knowledge of the targeted enterprise. They leverage on this to gather information and unleash more attacks to the targeted enterprise and others. [5] states that operators behind the threat utilize the spectrum of intelligence gathering techniques. Inclusive of this computer intrusion technologies and techniques, and conventional intelligence gathering approach are telephone interception technology and satellite image capturing. These work by intently focusing on a specific task instead of seeking information for financial gain. The hackers continuously monitor their target and interact gradually until they achieve their objective. [5] mentioned, that the most advanced forms of threats are the best-funded ones; ones which generally fall in line with world governments, criminal entities, and large corporations. In contrast, there exists another group of individuals motivated by money; whose goal is financial gain. Their target organizations are mainly small to medium sized organizations. Hackers are aware this size of entity will not do much implementing of security controls required to keep their network and environment highly secured, compared to the big enterprises. According to [6] the attacker is a person or a group of people; they operate as one body - a well-ordered hierarchy, but regardless the attacker is human. So, their mindsets are not same, planning their operations from a human perspective causes them to become narrowly focused on trying to create a perfect technical solution. [7] Small businesses make great targets for exploitation operations. This is simply because their employee's numbers are low and overworked; their networks and infrastructure are misconfigured; and they are often negligent in their use of technology to avert cyber threat actions. Furthermore, the hackers rely on their experiences with small business exploitation to connect to larger enterprises. The heinous actors take advantage of access to find a vulnerability or something that can be exploited on any of the unsecured areas of the entity's network. Therefore, the interconnection between enterprises and strength of business relationship can be leveraged to enable exploitation; as a failure with one enterprise network becomes a failure with others.

Besides, according to [7] Verizon data breach investigation report, roughly 43% of breaches in 2019 involved small businesses. Also, 47% of the compromise was because of both negligent employees and contractors. Majority of compromises take place through mistakes committed by employees and operating model of the enterprise; including dependency on e-mail and business applications managed by a third-party company. Large numbers of research work revealed that complete neglect of security tooling and systems, and mismanagement are responsible for many cases of exploitation happening in organizations. The criminal act will extend entry into more extensive networks as many of them fail to defend their networks. In other words, malicious actors and cyber warfare will have to adapt a new technique of exploitation. Multiple technologies deployed by organizations which the hackers have access to today will provide the venues from which the attackers will unleash the target. It is therefore imperative for every organization to understand the failure points and the complexity that makes the technology highly vulnerable in order to make it secure.

A. Network Exploitation Techniques

[2] Although cyber-attacks are rife and any network could be compromised, you don't need to let fear make you unplug your systems and go Amish. The reality is that network, systems, and any applications will be compromised. Therefore, energy should be directed to areas of major concern to ensure the right cybersecurity solutions apply so that the performance of organizations are enhanced. It is essential though, that the threat pattern is understood, and a calculated plan to prevent, minimize, and detect a threat before it inflicts damage is established. The common saying in cybersecurity is paranoia is your friend; meaning being in a state of paranoia is better as it positions you steps ahead of the attacker. Hackers are persistent in recent times, thus, a strategic plan to minimize and control them is necessary. Investment should be focused on detection, as there are cases where an entity could be compromised for months and they remain unaware. Popular network attacks vector is outlined below. Network Attacks Vector is the cluster of techniques adversaries use to leash or infiltrate the network. It could occur in different dimensions ranging from malware and ransomware to man-in-the-middle attacks to credentials compromised phishing attacks.

- Compromised Credentials
- Weak and Stolen Credentials
- Malicious Insiders
- Missing or Poor Encryption
- Misconfiguration
- Ransomware
- Phishing
- Trust Relationships
- Zero-day Vulnerabilities
- Brute Force Attack
- DDoS

In developing a measure to control these attack vectors, organizations should scale up their focus beyond just prevention because that alone is not adequate to stop the attacks from taking place. [2] admits that since the attacks have changed, it is necessary that the defensive measures are scaled against all threats. [3] also mentioned, that to engage in computer network defence, you need to establish a firm base of protection. What most organizations define in their security program for countermeasures are mainly assumptions that come with risks. Thus, they are prone to attacks through the various attack vectors the firm never anticipated. In such cases, they are aware of the attacks, but that is not enough to mitigate the vulnerabilities exploited. Strictly put, the cybersecurity program should consider developing a dynamic program. The following are required to scale and detect all forms of attack vectors, including advanced persistent threats:

Automation: The controls implemented must be automated to stop all forms of the attack vectors since criminals are sophisticated and keep changing their mechanism of compromising organizations; both small and large ones. Also, the manual controls should be limited, especially when needed in areas such as analytic perspective.

Adaptation: The cybersecurity solutions should be adaptive as the attackers naturally are persistent and continuously maintain their encroachment into their targeted victims' space. With this approach by attacks, security controls need to be adaptive. [2] states that attackers keep figuring out a way into the system. Organizations' strategy then must take into consideration this pattern and deploy a defence mechanism to prevent it from happening.

Proactive: Traditional enterprises only focus on financial investment to curb and controls threats. This model is operated by the reactive approach; waiting for hackers to inflict damage, detect it and fix it. But this results in extreme reputation damage and financial loss. The system of waiting for the enemies to come in before reacting is no more the norm of providing security. Therefore, security best practices must be proactive and quickly fix the issues once identified.

Predictive: As attackers adopt advanced persistent threat mechanisms to compromise their target, a predictive intelligence is necessary to uncover the trend pattern. By gathering more information about the types of attack vectors the hackers use, and developing a defensive measure to counter it predictively, entities can be assured of success.

IV. ENHANCED CYBERSECURITY PERFORMANCE

The exponential rate of cyber-attacks is increasing daily worldwide. Yahoo was in the heart of a planned transaction with Verizon to sell its core businesses. Unfortunately, it experienced the most significant data breaches in its data centre; with sensitive information of more than one billion users' accounts in 2013 and five million in 2004 stolen from their environment. This criminal Act led to the postponement of the acquisition; it also resulted in a U.S Securities and Exchange Commission probe into the breaches disclosure. According to [8] in the past several years, the list of companies whose internal systems have been hacked has multiplied; extending to thousands of small and medium sized organizations, including high profile organizations such as JP Morgan Chase, Ashley Madison, and Yahoo. The news of these cybersecurity attacks continues for weeks because of the reputational damage that comes with it.

Financial gain is the motivating factor for most hackers, though this results in financial loss to companies. [8] mentioned that many hackers are drawn to the possibility of earning from thousands to millions of dollars. Hackers are sophisticated and intelligent in how they unleash attacks on their targets. Thus, for companies to checkmate them successfully, they need to know the hacker mindset. Companies are encouraged to invest in comprehending the expertise of successful hackers to be aware of their model and confront them. They should venture into this journey thinking like a hacker; mainly knowing the attribute of a sophisticated hacker.

[8] additionally states, that attackers have two mindsets during the phases of infiltrating their victims' space; explorative and exploitative. In the initial phase of an attack, hackers generally use an exploration mindset that combines deliberate and intuitive thinking and relies on intense experimentation. Regardless of the outcome of the first phase, the attackers, continue to search for the vulnerable systems. When access is identified through a vulnerable system, next he/she adopts the exploitation mindset to achieve their goals. As already discussed, to be ahead of the hackers, enough time and energy is required to comprehend their tactics and develop a strategy on how to checkmate their encroachment into the network. But the execution of the criminal act spans multiple steps until success is attained. These are: identifying vulnerabilities, scanning, and testing, gaining access, and finally, consistent access. The latter is based on performing exploration on the targeted network whilst the former focuses on efficiently exploiting the environment. Primarily, organizations need to understand that monitoring the trend pattern of hackers is necessary to safeguard their environment and effectively put together the best cybersecurity practices. Complementing this first step are the following recommendations to help meet security expectations:

Executive Buy-in: Getting executive buy-in is mandatory to sustaining essential action plan to mitigating cybersecurity risks. The support is needed from the top hierarchy down to the employees. This should go hand in hand with attending meetings in the presence of the stakeholders. [8] seeks executive-decision makers on board, and it's important to emphasize the role of cybersecurity in addressing the market, privacy, technology, and regulatory risks and demands. The executive can only support requests when there is an outline of cybersecurity strategy with the business objectives, highlighting security governance to protect the interest of the business owners and assurance of external customers. Besides, the profitability and resilience of the organization are dependent on the security strength in place.

Develop a Robust Security Strategy: A good cybersecurity strategy should speak to the entire security posture of the organization. It requires viewing cybersecurity from inside out and outside in to develop security perception from a holistic perspective; to ensure a broad approach to critical planning and make sure the enterprise prepares well and positions itself ahead of threats. [8] mentioned, that executives and information managers should examine how up-to-date their information systems are and assess their level of cybersecurity.

They should also determine how secure each asset needs to be, and assess whether they have the right skill set as well as good organizational architecture to be aware of an incident and proactively respond to cybersecurity threats. Multiple choices need to be made when developing security strategies such as starting to build full-fledged in-house security capabilities; depending on third-party expertise, and adopting a hybrid model.

Developed Cybersecurity Sensitization: Developing cybersecurity sensitization programs across the enterprise is needed to create awareness. All employees must know about the dynamism of cyber threats as their approach keeps evolving. This awareness can be deployed by adopting various models suitable for the employees to have a grip of information security best practices.

Create Partnership: According to (Ramalho, Elisabeth and Gu illermo) skilful hackers can replicate successful attacks when a vulnerable system is identified for exploitation purpose. Subsequently, they keep exploiting those systems consistently until the vulnerabilities are remediated. Eventually, those systems become entry and exit point for hackers. It's crucial that information about cybersecurity incidents and vulnerability is shared within the enterprise and industry. Partnership in the industry is equally mandatory for matters of a cybersecurity incident, management, and challenges with securing the network.

Adopting Best Practices: Compliance to regulatory requirements has not been adhered to, as many organizations have not put in place the rigorous, continual way of monitoring compliance. This is evident from the exponential rate of data breaches reported in the industry. Threats pattern are becoming sophisticated as they keep moving with new security vulnerabilities identified, resulting in the release of new malware. Best practices must be adhered to confront modern cybersecurity threats. Adopting best practices like maintaining an up-to-date process in approaching cybersecurity risks; and continually training I.T. security teams with the dynamics, creating controls that proactively detect, analyse, and quickly respond to the security incident is essential. According to [8] new approaches to cybersecurity and new threats will undoubtedly continue to evolve. This compels all security stakeholders to think and act like hackers; to better protect their network.

V. CYBER SECURITY LAW AND POLICY

The increasing threats emanating from computer hacking has prompted the governments of many nations to enact laws that will checkmate the practices and serve as a measure to reduce it. The U.S government and European countries have established laws to protect individuals and organizations from quickly falling victims to the criminal act negatively impacting the world economy and causing severe financial losses to entities leading to their early bankruptcy and closure. The laws were introduced to prosecute individuals who accessed computers, software, and data without seeking authorization. Majority of the laws established were not reviewed while technology consistently evolved, creating room for cybercriminals to go free, as the law had disagreements on what constituted illegal hacking that amounts to criminal sentences and civil liability. [9] Few prosecutors, plaintiffs, and courts have adopted extraordinarily broad views of these anti-hacking laws. The laws prohibit traditional unauthorized access as well as unauthorized use and transfers of information, and circumvention of access controls. Although some organizations share concerns, the laws are not adequate to deter worst behaviour, and this is becoming a significant pain to companies who are victims of widespread theft and data breaches. There are multiple controversial laws enactments to control cyber risks faced by individuals and organization, and this has attracted the attention of many requesting for amendments to all laws.

Computer Fraud and Abuse Act is the first U.S. Federal bill designed to prohibit and penalize a limited form of computer hacking. The Act imposes both criminals' civil penalties for actions committed by individuals who violated authorization laws by accessing computers, as well as exceeding the authorization limit. The U.S. Congress passed this bill as the rate of devices networking without any guarantee of protection of compromised vital information related to personal credit card numbers. [9] states the modern version of the Computer Fraud and Abuse Act based on a 1986 amendment of the 1984 law, the counterfeit access device and Computer Fraud and Abuse Act, which was focused primarily on the hacking of financial institutions and the federal government. Also, the Act has seven subsections primarily applying to individuals who access the computer without authorization and exceed authorization limit. The bill equally applies to the defendant without authorizations. Following are the seven subsections of the Computer Fraud and Abuse Act (CFAA):

- Hacking to commit espionage.
- Hacking to obtain information.
- Hacking a federal government computer.
- Hacking to commit fraud.
- Hacking to commit damage.
- Trafficking in passwords.
- Threats of hacking.

However, other countries have taken similar decisions to enact a bill to prohibit and penalize cybercrime committed by individuals in all forms. Apart from the Computer Fraud and Abuse Act (CFAA) other laws are created to protect the interest of the state, organizations, and individuals; each tailored to specific areas of information technology, as well as people and organizations. Outlined below are the bills:

- Digital Millennium Copyright Act: This law provides authors of creative works and expressions with copyright, which allows them a limited right to exercise their control over the distribution, publication, and performance of their works.
- E.U. Agency for Cybersecurity: This Act is intended to enhance trust through the EU-wide certification framework in a combination of cybersecurity certification schemes in addition to cybersecurity requirements and evaluation criteria across national markets and sectors.
- The United Kingdom Data Protection Act: The law was updated in 2018 by the U.K. parliament. It is a national law that complements the European Union General Data Protection Regulation. Everyone responsible for using personal data must follow strict rules called data protection principles outlined below:

- Data should be used legally, lawfully, and transparently.
- Data must be used for a specified, explicit purpose.
- Data must be used in a way that is adequate, relevant, and limited to only what is necessary.
- Data must be accurate and, where necessary, kept up to date.
- Data must be kept for no longer than is necessary.
- Data must be handled in a way that ensures appropriate security, including protection against unlawful or unauthorized processing, access, loss, destruction, or damage.

VI. CYBERSECURITY POLICY AND GOVERNANCE

In the words of [10], we live in an interconnected world where both individuals and collective actions have the potential to result in inspiring goodness or grievous harm. Cybersecurity was orchestrated to provide the necessary protection to individuals, organizations, and the essential infrastructure assets need from cybersecurity adversaries. Cybersecurity policy is the document that guides the practices of securities in every enterprise. [10] defines policy as the seminal tool used to protect enterprise infrastructure assets and individual liberties. It merely directs the affairs of the technology to conform to regulatory requirements. These make it the bedrock of organizations operations. Absence of policies create an environment of uncertainty but not in all cases; policy brings about positivity and negativity. Again, [10] mentioned that cybersecurity programs and policies recognized that organizations must be vigilant, resilient, and ready to protect and defend every ingress and egress connection as well as organizational data wherever it is stored or transmitted. Cybersecurity programs and policies encompass traditional security programs. Moreover, cybersecurity policy serves as a directive for enterprises on how to protect its infrastructure assets and systems and ensure there is compliance with legal and regulatory requirements. Ultimately, the policy and other comparable programs safeguard the enterprise, its entire employees, customers base, third-party organizations, and vendors from being exposed to threats. Occasionally, the security policies are triggered by strategic cybersecurity position to exceptionally protect the network from persistent threats, such as defence-in-depth and other similar controls. Universally, organizations, both private and public focus no more on the adoption of a new technology concept to seamlessly provide services to their customers; instead, the need is to provide a more secure and effective technology platform. [10] This is especially true with the adoption because it has the potential to alter the paradigm of how business is done and whoever owns the task of creating and enforcing such policies. Following are attributes common to creating impacting polices:

- Endorsed: Get executive buy-in.
- Relevant: The policy is suitable for the enterprise.
- Realistic: The policy has a positive impact.
- Attainable: The implementation of the policy is successful.
- Enforceable: The policy is mandatory.
- Inclusive: The policy scope encompasses all stakeholders.

The policy meeting enterprise expectation depends mainly on how organizations approach the development, publication, adoption, and review. The combination of all these tasks is referred to as the policy life cycle. The approach differs from organization to organization depending on the specific regulatory requirements.

VII. CYBERSECURITY FRAMEWORK

The NIST cybersecurity framework serves as the common language in communicating cybersecurity risks to organizations' internal and external stakeholders. It is the right tool to adopt in addressing cybersecurity risks' emanating threats. Also, it is used to coordinate policy, business, and technological approach in mitigating cybersecurity risks. It plays a significate role in mitigating methodologies in both the private and public sectors. On the other hand, it can easily co-exist with other best practice standards and guidelines to allow similar frameworks and controls align with an enterprise's unique security needs. The framework provides guidance in implementing specific controls to mitigate threats, and it's applicable to an enterprise's unique needs depending on their sizes. [11] hammers on the need to identify the types of threats and typical vulnerabilities it faces, besides determining its risk appetite. Furthermore, the framework can be leveraged to facilitate the development of the cybersecurity program, as well as enhance existing and better organizations' cybersecurity practices. So, the implementation should be in alignment with the organization's current security circumstance to meet their expectations and provide business assurance. [11] said it is also an excellent approach to communicating cybersecurity requirements to stakeholders, ensuring they are made aware of any risks to the organization. This will facilitate board decisions on cybersecurity investment to mitigate security risk, increase awareness across the enterprise, and secure customers' confidence. The framework structure has three critical components, namely: Core, Profiles, and Implementation tiers. Each has a unique attribute and benefit [12] [13] [14] [15] [16].

VIII. CONCLUSION

Cyber exploitation is more advanced, and the actors have gone sophisticated in their approach to persistently encroach organizations' networks and maintain surveillance without being noticed. As technology evolves with new security controls to put an end to the criminal act, hackers are equally consolidating mechanism and building means to overpower these controls. However, the mid-sized entity is mostly the target as they do not adequately implement in-depth defence controls in their operating environment. Beyond that, vulnerabilities status determines what makes hackers enter the organization. When a system is identified to be vulnerable through multiple exploratory efforts, this becomes an easy pass into the network. The criminals follow a process to cause damage to an organization, namely:

- Reconnaissance: This is the exploratory activities done to gather more information about the targeted victims.

□ Infiltration: Naturally, this is the act of gaining access to the physical and logical environment without authorization.

□ Identification: This is the process of ascertaining the vulnerable state of the environment.

□ Acquisition: This is referred to as the act of obtaining things from the operating environment.

□ Security: This refers to how secure is the environment.

□ Extraction: The hackers leave without being noticed and unscathed.

□ Delivery: This is the end state. The hackers achieve their objective.

As cyber risks exponentially increase the only measure to an extremely secure operating environment is defining a countermeasure which has protection, detection, and reaction capabilities. Ultimately, this will lead to implementing advanced persistent security to protect the entire organization's infrastructure assets holistically. Therefore, the different categories of countermeasures such as technical countermeasure, operational countermeasures, personal countermeasures, and physical countermeasures, are implemented as mitigation methodologies to curb cyber exploitation. Combining the benefits of all the countermeasure categories will guarantee and provide the acceptable assurance to meet the expectation of business owners. Cybersecurity law is established by each country as a control measure to help protect the interest of individuals and organizations who are victims of cyber-crime. Although, many of these laws were created years back without any reviews to update them to match current technology. So, this has resulted in several disagreements and controversies without the attackers getting the actual punishment for their crime. Cyber laws should be reviewed as technology evolves to allow the right litigation decisions be taken to the full benefit of the victim of the incident. Thankfully, many countries have noticed the drawback and have addressed the gap with their updated law. This enhances the mitigation of cybersecurity risk.

REFERENCES

1. Gragido, P. Will and John, Cybercrime and Espionage, St. Rockland, Massachusetts : Syngress , 2011.
2. Cole and Eric, Advanced Persistent Threat, St. Rockland, Massachusetts : Syngress , 2012.
3. Winkler and G. A. T. Ira, Advanced Persistent Security, St. Rockland, Massachusetts : Syngress , 2016.
4. Shimonski and Robert, Cyber Reconnaissance, Surveillance and Defense, St, Rockland, Massachusetts: Syngress , 2014.
5. Kilger, C. Dr. Max, J. Gregory, B. Jade and Sean, Reverse Deception: Organizsed Cyber Threat Counter-Exploitation, New York City : McGraw-Hill, 2012.
6. Monte and Mathew, Network Attacks and Exploitation, Hoboken, New Jersey: Wiley , 2015.
7. Cunningham, T. Chase and G. J, Cyber Warfare - Truth, Tactics, and Strategies, Birmingham: Packt Publishing , 2020.
8. Ramalho, H. Elisabeth, E. Guillermo and Jose, To Improve Cybersecurity, Think Like a Hacker, Boston : MIT Sloan Management Review, 2017.
9. Kosseff and Jeff, Cybersecurity Law, 2nd Editon, Hoboken, New Jersey: Wiley , 2019.
10. Greene, S. Sari and Omar, Developing Cybersecurity Programs and Policies, Third Editon, New York City : Pearson IT Certification, 2018.
11. Calder and Alan, NIST Cybersecurity Framework - A pocket guide, United Kingdom: IT Governance Publishing, 2018.
12. Vacca and J. R, Cyber Security and IT Infrastructure Protection, St. Rockland, Massachusetts : Syngress, 2013.
13. Haber and M. J, Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations, New York City : Apress, 2020.
14. Winterfeld, A. Steve and Jason, Cyber Warfare, St, Rockland, Massachusetts: Syngress, 2011. C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.
15. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interfaces(Translation Journals style)," IEEE Transl. J. Magn.Jpn., vol. 2, Aug. 1987, pp. 740–741 [Dig. 9th Annu. Conf. Magnetics Japan, 1982, p. 301].
16. M. Young, The Techincal Writers Handbook. Mill Valley, CA: University Science, 1989.

AUTHORS PROFILE

Dr. Oghene Augustine, Serves Currently As Technology Recovery And Operations Management Head for eProcess International, the technology hub for ECOBANK TRANSNATIONAL INTERNATIONAL. Prior to joining eProcess International, Dr. Augustine Oghene held senior technology engineering management positions with CBC EMEA and Net Solutions.