Scientific Research Publishing

Open Journal of Safety Science and Technology, 2023, 13, 231-248
https://www.scirp.org/journal/ojsst
ISSN Online: 2162-6006
ISSN Print: 2162-5999

Critical Role of Cyber Security in Global Economy

Emile S. Mbungu Kala[1,2]

[1]Department of Computer Science, Northrise University, Ndola, Zambia
[2]Department of Business, University of Zambia (UNZA), Lusaka, Zambia
Email: jackemile@gmx.com

How to cite this paper: Kala, E.S.M. (2023) Critical Role of Cyber Security in Global Economy. *Open Journal of Safety Science and Technology*, **13**, 231-248.
https://doi.org/10.4236/ojsst.2023.134012

Received: May 26, 2023
Accepted: December 22, 2023
Published: December 25, 2023

Abstract

The improvements that have been made in information technology have led to the creation of new dangers for the national security of several different countries. For the most part of military history, there has been a huge power disparity between the two opposing sides. This has been the case throughout the annals. This unequal allocation of resources might have been caused by a variety of circumstances, including economic conditions, advances in technology, or even just the disparities in the sizes of the parties involved. The modern battlefield is increasingly shifting its emphasis to one that is focused on information operations. In this particular arena, all of the warriors are making use of the same kind of armament, which consists of computers. These days, computers and network connections are what make up cyberspace, and it serves as a battlefield for a war that is still going on. The legal context in which this war will take place is currently being shaped by international law, and its framework is still being formed. This conflict is not just about collecting or protecting confidential material; it is also about preserving the critical infrastructures and institutions that are responsible for the preservation of domestic security and the economy. The stakes could not possibly be any higher. The presentations that are going to take place today are going to situate the work of defending our important infrastructures within the context of the role that cyber security plays and the influence that it has on economic security. This will take place in the context of the presentations that are going to take place today.

Keywords

Cyber, Security, Economy, Technology

1. Introduction

The critical role of cyber security in the global economy cannot be overstated. As technology continues to advance and businesses become increasingly reliant on digital platforms, the risk of cyber threats becomes more prevalent. Cyber-attacks can have devastating consequences for both individuals and organizations, leading to financial losses, reputational damage, and even national security breaches. Therefore, it is imperative that governments, businesses, and individuals prioritize cyber security measures to safeguard their interests.

In this new rising age, there is a substantial lack of knowledge and experience, which has resulted in a significant number of gaps within cyber systems. These openings can be exploited by attackers. To do damage to a certain organization in several distinct ways, those seeking to inflict harm may utilize a range of strategies. It has ramifications for a firm in a variety of ways, both fiscally and in terms of the interruptions it creates to business. These repercussions might be positive or negative. Losses in the range of $300 billion to 1 trillion dollars are incurred by the worldwide economy as a direct result of cybercrime, which amounts for 0.4% to 1.4% of total GDP [1].

One of the primary reasons why cyber security is crucial in the global economy is because of its potential impact on financial stability. In recent years, there has been a surge in cyber-attacks targeting financial institutions and payment systems. These attacks not only disrupt normal business operations but also compromise sensitive customer data such as credit card information and personal details. The resulting financial losses can be significant, with some estimates suggesting that cybercrime costs the global economy over $1 trillion annually [2]. By investing in robust cyber security measures, businesses can protect themselves against these threats and ensure the stability of their operations.

Furthermore, the interconnected nature of today's global economy means that a single cyber-attack can have far-reaching consequences. For instance, an attack on a critical infrastructure system like power grids or transportation networks can disrupt supply chains and halt economic activities across multiple countries. This was evident during the 2017 NotPetya ransomware attack which affected companies worldwide by targeting their Ukrainian subsidiaries [3]. Such incidents highlight the need for international collaboration in addressing cyber threats to prevent cascading effects on economies.

In addition to economic implications, cyber-attacks also pose significant risks to national security. Governments around the world are increasingly concerned about state-sponsored hacking activities that aim to steal sensitive information or disrupt critical infrastructure systems. For example, in 2015 it was revealed that Chinese hackers had stolen personal data from millions of U.S government employees, including those with security clearances [4]. These incidents underscore the importance of cyber security in protecting national interests and maintaining geopolitical stability.

To address these challenges, governments and businesses must adopt a proactive approach to cyber security. This includes investing in advanced technologies such as artificial intelligence and machine learning to detect and respond to threats in real-time. Additionally, there is a need for increased collaboration between public and private sectors to share threat intelligence and best practices. Governments should also establish robust legal frameworks that deter cyber criminals through stringent penalties.

The critical role of cyber security in the global economy cannot be ignored. The increasing reliance on digital platforms exposes individuals, businesses, and governments to significant risks that can have far-reaching consequences. By prioritizing cyber security measures, stakeholders can protect their financial stability, ensure national security, and maintain the smooth functioning of the global economy.

2. Research Purposes

The article "Critical Role of Cyber Security in Global Economy" highlights the importance of cyber security in today's interconnected world. The research purposes of this article are to raise awareness about the critical role of cyber security in the global economy, analyze the potential risks and impacts of cyber threats, and propose strategies to mitigate these risks.

Firstly, the article aims to raise awareness about the critical role of cyber security in the global economy. With advancements in technology and increasing reliance on digital infrastructure, businesses and governments are more vulnerable than ever to cyber-attacks. The article emphasizes that a breach in cyber security can have severe consequences for economies worldwide. By highlighting this issue, it encourages stakeholders to prioritize cyber security measures and invest resources into protecting their digital assets.

Secondly, the article analyzes the potential risks and impacts of cyber threats. It provides an overview of various types of cyber-attacks such as data breaches, ransomware attacks, and distributed denial-of-service (DDoS) attacks. It explains how these attacks can disrupt business operations, compromise sensitive information, and cause financial losses. By examining real-world examples and statistics, it underscores the urgency for organizations to address these risks proactively.

Furthermore, the article proposes strategies to mitigate these risks effectively. It emphasizes that a multi-layered approach is necessary for robust cyber security. This includes implementing strong access controls, regularly updating software systems with patches and fixes, conducting regular vulnerability assessments, training employees on best practices for cyber security hygiene, establishing incident response plans, and collaborating with law enforcement agencies for effective prosecution of cybercriminals.

Moreover, the article highlights international cooperation as a key component in addressing global cyber security challenges. It stresses that no single country

or organization can tackle this issue alone due to its transnational nature. The author suggests that governments should collaborate with each other through information sharing initiatives such as Computer Emergency Response Teams (CERTs) or by signing bilateral agreements on cyber security cooperation.

In conclusion, "Critical Role of Cyber Security in Global Economy" serves important research purposes by raising awareness about the critical role of cyber security, analyzing the potential risks and impacts of cyber threats, and proposing strategies to mitigate these risks. It highlights the significance of cyber security in today's interconnected world and emphasizes the need for proactive measures to protect digital assets. By addressing this issue, the article contributes to building a safer digital environment for businesses and governments worldwide.

3. Mostly Used Attacking Techniques to Organizations

Figure 1 below illustrates the mostly used attacking techniques employed by malicious actors to target organizations. In today's digital age, organizations face an increasing number of cyber threats that can have devastating consequences. Understanding these attacking techniques is crucial for organizations to effectively protect themselves.

One of the most common attacking techniques is phishing. This involves sending deceptive emails or messages to trick employees into revealing sensitive information or clicking on malicious links. Phishing attacks are successful because they exploit human vulnerabilities and often appear legitimate.

Another prevalent technique is malware attacks, which involve infecting systems with harmful software. Malware can be delivered through email attachments, infected websites, or even USB drives. Once inside a system, it can steal data, disrupt operations, or provide unauthorized access to attackers.

Denial-of-service (DoS) attacks are also frequently utilized by hackers. These attacks overwhelm a targeted organization's network or website with excessive

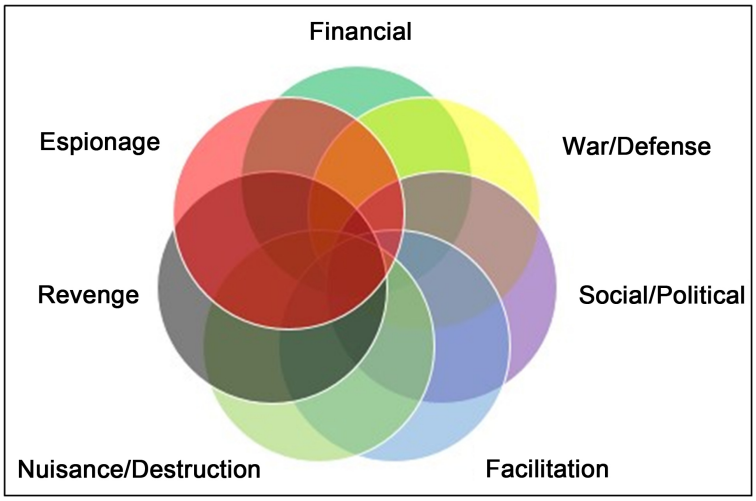

Figure 1. Illustration of attacks.

traffic, rendering it inaccessible to legitimate users. DoS attacks can cause significant financial losses and damage an organization's reputation.

Furthermore, social engineering is an effective technique that exploits human psychology rather than technical vulnerabilities. Attackers manipulate individuals into divulging confidential information or granting unauthorized access through tactics such as impersonation or manipulation.

DDoS: When an attack is carried out using the technique known as distributed denial of service, the perpetrators of the attack render the resources inaccessible to those who are legitimately allowed to use them. When an adversary compromises a network by installing malware and botnets, they also produce zombie machines, which are computers that may be remotely controlled by the adversary. These zombie computers send requests to the server on an almost constant basis, which causes the server to become too busy to meet the needs of the intended users by providing the services or resources that those users demand. In a survey that was carried out by Neustar, it was discovered that more than 300 distinct businesses were victims of DDoS attacks. The vast majority of firms that are dependent on the internet, such as those in the banking sector, the telecommunications industry, retail, the travel industry, and information technology, were routinely attacked. If a company's website is down for maintenance, the business could potentially lose up to $10,000 in revenue every hour. Businesses utilize the internet to provide customer service, make direct transactions, and increase brand awareness. Despite this, a website that does not have enough protection can be swiftly taken down by aggressive competitors, unhappy customers, or demonstrators motivated by social and political problems.

Phishing: Phishing is an attempt to acquire sensitive information such as a username, password, credit card details, pin code, account number, or unique id by impersonating a reputable organization in order to fool the target into giving the information. This can be done in order to obtain access to the target's computer or to steal their identity. It is possible to do so by contacting someone by telephone, e-mail, or text message, among other methods. A survey conducted by the RSA Anti-Fraud Command Center found that the overall number of fishing assaults in 2012 was 59% more than in 2011. This increase was seen from 2011 to 2012. It is projected that the losses on a global scale amounted to $1.5 billion in 2012, which represents a 22% rise over 2011.

Social Engineering: Engaging in social engagement with the person who is the target of the information is one technique to get the essential information for verification and identity. This interaction can take the shape of a conversation or an interview. An outside hacker obtains access to the computer system of a corporation by employing critical personnel with the intention of applying socio-psychological techniques on such employees. As a result, with this approach, the needed information is gathered directly from the individual as opposed to gaining access to the system without the target even somewhat knowing that they have been misled in any manner. A breach of data or the loss of informa-

tion: It is essential for a business to save the data in the system in an electronic format so that it can be swiftly altered, examined, studied, and registered into the system. In many instances, this information is of such critical importance to their firm that, if it was obtained by a user who was not permitted to do so, their company would suffer a severe financial loss. It is possible for data to be corrupted because of either negligence on the part of the user or a deliberate attack on the system itself. This information might be altered by the attacker, sold to a third party, or publicized in any manner that could be detrimental to the organization's brand, reputation, and trustworthiness, as well as its income. Although it was announced in December as the most significant data breach ever, it actually occurred in November and resulted in the disclosure of forty million individuals' names [5].

Malware: The term "malware" is used to refer to any potentially destructive program that is downloaded and installed on a computer. It has the ability to talk with its creator in the background while being unnoticed by the system administrator, and it is skilled in theatrical performance. It is the single most effective method there is for wreaking havoc on a company or organization. E-mail, downloading an attachment, and even occasionally installing it using USB or other external devices are all legitimate means of installation. Occasionally installing it through USB or other external devices is even recommended. Malware is included in 72 out of every 100 emails issued by the government, 163 out of every 100 emails sent by educational institutions, 218 out of every 100 emails sent by banking institutions, 235 out of every 100 emails sent by marketing organizations, and 236 out of every 100 emails sent by lodging enterprises.

Insider Attacks: It is also possible for the employees of a firm to constitute a threat to the business they work for. The employees leak secret information to other parties in order to either advance their own personal financial interests or to place the organization in a difficult financial position.

Figure 2 below illustrates the alarming rise in insider attacks, a concerning trend that poses a significant threat to organizations worldwide. Insider attacks occur when individuals within an organization exploit their privileged access to compromise security measures. This malicious behavior can result in severe consequences, including data breaches, financial losses, and reputational damage.

One key factor contributing to the increase in insider attacks is the lack of proper security protocols and employee training. Organizations must prioritize implementing robust security measures that restrict access privileges and regularly update passwords. Additionally, comprehensive training programs should be provided to employees to raise awareness about potential risks and educate them on best practices for safeguarding sensitive information.

Another crucial aspect highlighted by the figure is the need for continuous monitoring and auditing of employee activities. By closely monitoring user behavior, organizations can identify suspicious patterns or anomalies that may

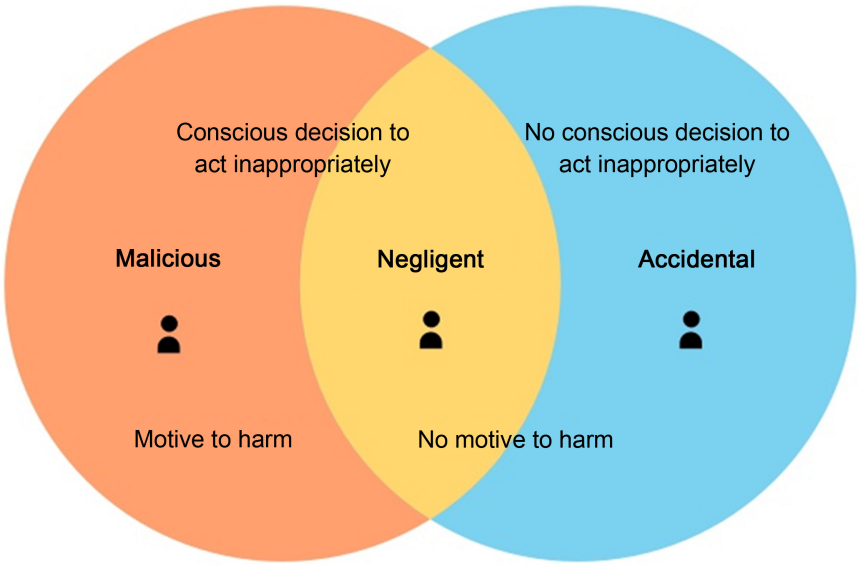

Figure 2. Illustration of insider attack.

indicate an insider attack in progress. Regular audits of system logs and user activity records are essential for detecting any unauthorized access attempts or unusual data transfers.

Fostering a culture of trust within organizations is vital in preventing insider attacks. Employees who feel valued and appreciated are less likely to engage in malicious activities against their employers. Organizations should promote open communication channels where employees can report any concerns or suspicions without fear of retaliation.

It is common for individuals in lower levels of management to mistakenly reveal sensitive and secret information with those who are seeking to breach the system. This is caused by the fact that these individuals have less awareness about the sensitivity of the topic.

It is quite simple for management at the intermediate level to make inappropriate use of the data since they are completely aware of the relevance of the data and yet they still find it easy to do so. Due to the greater number of duties, they have, those in the highest levels of management participate in data sharing as well, but to a lesser extent than those in the middle levels.

Social Sites: There are a lot of other competing businesses that are actively working, through the use of social media platforms that are accessible online, to hurt the brand and its reputation. They do this by publishing or tweeting false information about an organization in an effort to destroy people's faith in that organization and destroy trust among the general public.

4. The Concept of Economic Security

During the era of the bipolar world order, the idea of security was predominately centered on the primacy of military safety. On the other hand, as more time has gone by, the meaning of the phrase has shifted, and it is now necessary to in-

terpret it in a more nuanced way. It is possible that the idea of monetary safety could be seen as a crucial component of this perspective, maybe even the most significant one. It is impossible to have a conversation about the state of the nation or the economy using the phrase "stability" if the concept of security is not grasped in a nuanced manner. When discussing national and international relations, it is essential to make a distinction between the perception of economic security and the actual state of the economy. In the first theory, economic security refers to a state's power to safeguard its sovereignty and continuity of existence in the face of all pressures and hazards emerging from the rest of the world. Specifically, this theory focuses on the relationship between a state's economy and its ability to maintain its existence. This theory also considers the capacity of the state to ensure the continued survival of the nation in the face of these obstacles. Maintaining this in today's globalized world is an extremely challenging task due to the fact that numerous states and nonstate operators are layered on top of one another and, as a result, depend on one another to such an extent that it is nearly impossible to end or reduce this interdependence. This interdependence is caused by the fact that the state and nonstate operators are layered on top of one another. This dependency emerges as a result of the superimposition of a number of state and nonstate operators on one another. This trend will become much more prominent in the years to come as a direct result of the increasing connectivity that will characterize the global economy. This will occur as a direct result of the rising interconnectedness that will define the global economy. The fact that economic security is sensitive to more external reliance as well as external repercussions will make it even more difficult to identify the true substance that forms economic security. This vulnerability will make it even more difficult to identify the underlying substance that creates economic security. Interdependence and the introduction of new factors that threaten the financial stability of individual national economies are inevitable results of integration, despite the fact that integration offers the possibility of an improvement in economic efficacy.

Figure 3 illustrates the concept of economic security, which is crucial for individuals and nations alike. Economic security refers to the ability to maintain a stable income, access basic necessities, and withstand financial shocks. This

Figure 3. Economic security concept.

figure highlights the various components of economic security, such as employment opportunities, social protection programs, and access to healthcare and education. It emphasizes that a comprehensive approach is necessary to ensure economic stability for all citizens. By understanding this concept, policymakers can design effective strategies to promote economic security and reduce inequality in society.

This sort of superimposition of the economies would result in the collapse of the economies of other nations in a domino effect, as was illustrated by the worldwide financial crisis that happened in 2007. Within the scope of this article, we intend to emphasize neuralgic features that are crucial in the examination of connections between cyber security and economic security. The legal framework, the safeguarding of essential infrastructures, and the conduct of cyber-attacks on these targets are among these points.

5. Consequences for the Organization Because of Attacks

1) Damage to the organization's economy will occur regardless of the type of attack that is carried out, causing this type of harm to an organization.

2) Reputational: After a business has been the subject of a cyber-attack, people are less likely to have faith and trust in that organization, and they are also less willing to spend more money in that firm.

3) Loss of IP: Theft of an organization's intellectual property, such as a patent, copyright, or trade secret, can often result in a large financial setback. This can be especially problematic in situations when the IP in question is a trade secret.

4) The loss of confidential information pertaining to the company Data that has the potential to be transformed into monetary worth should be retained; nevertheless, the loss of such data can be damaging to the company since it may be put to use by competing businesses.

5) A Decreased Level of Trust: Once a firm has been the subject of a cyber-attack, the clients of that company will no longer consider it safe to conduct business with that particular company. It has a policy that compels customers to move to other kinds of services.

6) Disruption to Business Operations and Lost Sales: As a result of the myriad of different types of attacks, companies and sales have also been negatively impacted. During a denial-of-service assault, customers are unable to access the services, which leads to a loss of income for the firm in a relatively short period of time.

7) Loss of Equipment: Malware may occasionally destroy all of an organization's networking equipment, which will need the business to pay a substantial amount of money to replace all of it.

8) Stock values: An attacker may view the company's stock values as a tool to reduce the worth and image of a certain business through the deployment of malware. This interpretation may be based on the fact that an attacker has access to the stock prices of the organization.

6. Critical Role in Global Economy

The conversation at this week's World Economic Forum in Davos, which is being held in Switzerland, has changed to concentrate on the essential function that cyber security plays in the economy of the entire world. This comes after it was listed as one of the top five global hazards. This is certainly one of the most fascinating issues out there, and it is one that is receiving a lot of attention at the World Economic Forum this week.

"But before we get into the meat of the topic, since cyber security is related to the internet and securing the data it carries, stores, and transmits, we first need to examine the significance of the internet's data flows and its effect on the economy of the entire world. This is necessary because cyber security is related to the internet and securing the data it carries, stores, and transmits. The protection of the information that the internet transports, saves, and transmits is integral to cyber security, thus this is an essential step in the process".

Without a consistent flow of data, the global economy would be unable to function properly. The value of data not only as an input to "information industries", but also to other manufacturing sectors and conventional industries, has been growing. This is true not just of the information industries, but also of the other industries. This is occurring as a result of the present acceleration of the digitalization of global organizations, which is being supported by the quick adoption of rapidly growing technologies such as cloud computing and data analytics. This is causing the phenomenon. According to a survey that was compiled by McKinsey, traditional companies are accountable for 75 percent of the value that is produced by the Internet [6].

The expansion of the economy is strongly correlated to the rise in the number of individuals utilizing the Internet. "The fact that increasing internet penetration is closely connected with a wide variety of economic performance indicators suggests that obtaining universal access requires not only reforms to the sector" of the economy that deals with telecommunications, but also policies that are geared toward assisting individuals and businesses in getting the most out of their use of the internet. This is because increasing internet penetration is closely connected with a wide variety of economic performance indicators.

It is estimated that there are around "four billion people who are connected to the internet, which is close to half of the entire population of the" world, which is 7.7 billion. According to the Global Ecommerce Association, international online commerce is increasing at a phenomenal rate, and it is projected that one billion consumers will make purchases across international boundaries in 2020, up from 390 million in 2016. In 2016, the number of customers who made purchases across international boundaries was 390 million.

As a result, the growth of the internet and the rise of the economy both contribute to each other's success. The internet has caused significant shifts in the ways in which we go about our daily lives, the ways in which we make a living, the ways in which we engage socially and with one another, and the ways in

which we move forward as a society and as a nation.

In its study, McKinsey made a parallel between the growth of the internet and the expansion of the electric power business during the early phases of commercialization of the latter. The internet, much like electricity before it, has changed the geography of the world, bridged enormous distances, and made the globe flatter by providing instant access to a limitless stream of information. Electricity was the first technological innovation to do these things. A parallel may be drawn between this occurrence with the beginning of the industrial revolution. It has enhanced the standard of living, contributed to growth, and had an influence on the economic well-being of the general people.

As we have seen, the process of growing the economy of the entire globe includes a substantial and useful role for the many forms of cyberspace, including the internet and other forms of the internet. As a consequence of this, it is of the highest significance that proper security be given for the internet against activities that are not permitted and are criminal. Unfortunately, there are currently no ready-made solutions available for this problem. Attacks, which may be conducted against organizations as well as individuals, can result in considerable monetary damage.

According to McAfee and the Center for Strategic and International Studies, cybercrime is responsible for the loss of about one percent of global GDP each year, and the cost of cybercrime might be as high as $600 billion in the United States. This estimate is based on the fact that cybercrime is becoming increasingly prevalent. The study also underlines the fact that it appears to have become less difficult to monetize stolen data as a result of developments in cybercrime black markets and the use of digital money. This is another point that the research brings to light. This is one of the conclusions that may be drawn from the report.

"According to the 2019 Official Annual Cybercrime Report by Cyber Security Ventures, which was sponsored by Herjavec Group, cybercrime is not only the greatest threat to every company in the world" but it is also one of the most serious issues that mankind is currently confronted with. The global damages that are predicted to be incurred as a result of cybercrime are expected to approach $6 trillion yearly by 2021, up from $3 trillion in 2015, according to forecasts provided by Cyber Security Ventures. The paper goes on to state that this is the largest transfer of economic wealth in the history of the planet; that cybercrime poses a danger to the incentives for innovation and investment; and that it will be more profitable than the worldwide trade of all of the main illegal substances combined in the future.

It is abundantly clear that cyber security plays an essential role not only in the protection of global businesses and the infrastructures that support them, but also in the protection of the health and happiness of people in every region of the world, as well as in the maintenance of a thriving global economy.

Therefore, the following are some of the possible macrolevel measures that

can be taken to ensure effective cyber security across the globe:

- "In addition to providing comprehensive training to their workforce on the subject of safe and secure business procedures, every business organization ought to adhere to secure business practices, manufacture secure goods and services, and follow secure business procedures themselves".
- "In addition to aligning risk management and information technology operations and regulating private and public organizations for compliance, the government of every nation should take steps to educate its population on the need of maintaining a secure digital environment and raise cyber security awareness".
- "Greater predictability and stability in cyberspace would result from all nations voluntarily and universally adhering to established cyber standards and international law for responsible state action in cyberspace, as stated in the United States National Cyber Strategy of 2018".
- "Countries ought to collaborate with one another to ensure the safety of cyberspace and to accommodate legal requests for the extradition of criminals who are situated in other nations".
- "Organizations of all sizes, educational institutions, and trade organizations like ISACA are required to train and retain qualified human resources in the field of cyber security".
- "Countries ought to have significant capacities for both detection and deterrence in cyberspace, in addition to having a robust incident response structure, and this should be a priority".
- "Organizations should benchmark their cyber security practices using the NIST Cyber Security Framework as well as the guidelines provided by ISACA".
- "In conclusion, all nations should advocate for the freedom of the internet, promote a multi-stakeholder form of governance, and prioritize the development of communication infrastructure that is both interoperable and dependable, as well as the expansion of internet connection. This will result in a healthy economy based on information and knowledge, which will, in turn, lead to a successful economy on a global scale".

7. Cyber Security Policy

Because of cyber, the output of the community has increased, and the information that has been passed down through the generations has been transmitted effectively. It has never been a question as to whether or not the amount of output that is achieved through the use of cyber should be increased, and this is true irrespective of the type of application or industry that employs cyber. The speed with which data is sent into cyberspace nearly always results in a decline "in the level of system security. As a result of the fact that prevention indicators restrict, prohibit, or delay user access, consume indicators that identify critical system resources, and respond to management attention [7], security indicators fre-

quently come into direct conflict with progress for technology professionals who work to improve production". This is due to the fact that indicators of prevention employ indicators to consume indicators that indicate crucial system resources. The system is updated using hardware that is instantly accessible and also meets the requirements for it. Along the lines of the cyber security policy, the conflict that occurs between the present security situation and the goal for cyber performance is a crucial concern. This conflict may be seen as a potential threat. The term "policy" might refer to the rules and regulations that govern "the transmission of information, the goals of the commercial sector for the preservation of data, or the operational strategies for system control". There is a wide variety of scenarios in which the word "policy" is employed that are important to cyber security. On the other hand, depending on the setting in which the work is being done, the term "cyber security policy" can be used to refer to a wide number of different things. In the same vein as the word "cyberspace," the concept of "cyber security policy" does not have a precise definition; nonetheless, when this idea is used as an adjective in the field of policy, a general idea is intended to be communicated [8]. The policy on cyber security has been approved by the regulatory framework, and it is now in the process of being formally implemented throughout the entirety of the important components that comprise the regulator. According to the findings of the research that Cheng and colleagues published in 2020, the components of a security strategy may change based on the policy spectrum [9]. While the national cyber security policy, for example, applies to all citizens and possibly even foreign businesspeople operating in its sector, the corporate cyber security policy only applies to workers who are employed by the firm or have a formal relationship with the company and are required to manage their behavior toward the organization. This is in contrast to the national cyber security policy, which applies to all citizens and maybe even foreign businesspeople operating in its sector. It is not even realistic to expect resource suppliers who rely exclusively on one client to comply to the customer security policy unless there is a written contract in place. This is because there is no way to enforce the policy. The criteria that should be used to decide what should be included in the security policy are based on the objectives of the relevant regulatory body. There is a significant gap between the objectives of national security and those of businesses looking out for their own interests in terms of safety. The organizations that are responsible for the policy's implementation will be the ones to establish the way by which it is to be interpreted and registered. Additionally, the regulatory board and the components that are engaged will be the ones to decide whether or not the policy will be approved. Both the process by which aims in the government are changed into policies "and the process by which policies are transformed into legislation are distinct but intertwined processes. Laws are the end result of both processes. On the other hand, it is not unheard of for firms to have a centralized security unit that is liable for the company cyber security policy in addition to associated stan-

dards and solutions. This is becoming increasingly prevalent. The standards and solutions produced by a company's security department" are frequently the source from which the rules for regulations are generated. When safety is a primary concern for an organization, it is possible that one will become aware of the company's policy regarding cyber security. The many different internal entities that make up the common components wing are responsible for issuing this policy. According to Quigley [10], the utilization of these common components could lead to the discovery of policy inconsistencies that occur as a result of the simultaneous execution of these issues. This finding was derived from the research conducted by the aforementioned researchers.

The nation's cyber policy is now included into the nation's broader plan for ensuring the nation's continued safety and security. Even if we consider a country's cyber security policy to be in line with the policy of the State Department or the economic policy of the country, these types of laws and policies are not as sovereign as the constitution of a nation. This is the case even if we consider a country's economic policy to be in accordance with the policy of the country. In point of fact, new policies are formulated via the discussion and debate of a wide range of subjects and problems, which is subsequently written up in papers and presented in lectures. Policies serve as a compass for the formulation of rules and regulations; in addition, they are instruments for the decision-making process. The actual rules and regulations have no bearing on the policy itself; there is no relationship between the two. The best-case scenario is one in which laws, agreements, and conventions come together to form a policy that is both meaningful and clever. However, it is possible to provide cyber security enforcement orders, rules, and regulations without first developing a cyber security policy. This can be done in a number of ways.

In the setting of a company, it is anticipated by the various departments that they would observe the norms for fear of incurring sanctions, since it is believed that the sanctions will continue "until the delinquent sector is closed. For instance, human resource, civil, and costing rules are all crafted in such a way that any non-compliance with the notification requirements would result in the area in question being closed". This is the case regardless of whatever regulation is being discussed. The implementation of communication policies into the activities of departmental departments, as well as the creation of indicators at the departmental level to monitor compliance with policies, are both needed of middle managers. Middle managers are responsible for providing support with day-to-day activities such as hiring new staff and filing expense reports. In the study conducted by [11], the authors found that every sort of organizational subdivision that functions in the public sector is susceptible to the governance limits. "The security policy that was provided by the CEO is only applicable to the industry in which the company works, but the corporate security policy that was delivered by the CEO applies to the whole organization". This general rule has several notable exemptions, including instances in which certain aspects of the

information categorization are taken into highly serious consideration. The employment of technological workers is an ideal application. One of the recent advancements that have taken place across a wide variety of businesses is the appointment of a senior data security manager or a senior manager who is responsible for picking different components of the security situation of corporations. This is one of the recent developments that has taken place. This is one of the most recent changes that has been made to the organizational landscape. Another adverse contrast between corporate cyber security policy and policies surrounding human resources or legal concerns is that the determination of corporate cyber security policy is the responsibility of middle management. Because this may be a requirement of the cyber security policy, sensitive information should not be shared unless first a comprehensive investigation has been conducted into the capability of the receiver to keep the information secure. This is especially important when there is a significant risk that sensitive information will be compromised and leaked. This tactic assigns the task of identifying the amount of risk "posed by the data to a manager, who may be incentivized to reduce expenses by contracting out the flow of information into the office and by hiring people from outside the office to perform information analysis. It's probable that the same manager is the one trying to get away with avoiding inspection to save money. A situation such as this is the result of mistakenly delegating information responsibilities to a person who is not an expert in security; alternatively, the culture of the firm in question may be the one that is accountable for bearing the risk. In any case, the division of labor is an important component that must be present. These scenarios become increasingly difficult and complex as a direct result of the fact that the methods of cyber security have not yet attained the same level of maturity as the indicators for accounting or human resource management".

8. Conclusion

Napoleon's "the best way to defend yourself is to attack" may apply to cyber-attacks. More nations are realizing the importance of this and creating their own military groups trained to conduct cyber-attacks, like India gave its Defense Intelligence Agency and National Technical Research Organization permission to conduct undetailed offensive operations if necessary. Fearing an attack on India's critical infrastructure, this was done. The Pentagon Cyber Command wants 13 offensive teams by 2015. New teams will be formed as part of the government's massive efforts to protect the nation from attacks on Wall Street or the electrical grid. Cyberspace and its technologies are a major power source in the third millennium. Cyberspace's cheap entry fees, anonymity, susceptibility, and asymmetry cause "power dissipation". This means that if governments have shared power among themselves up to this point, then it must be other players, such as private enterprises, organized terrorist and criminal organizations, and people, albeit governments still play a significant role.

Acknowledgements

Technology plays a pivotal role in almost every aspect of our lives; cyber security has emerged as a critical concern. The global economy heavily relies on digital infrastructure, making it vulnerable to cyber threats that can disrupt businesses, compromise sensitive data, and undermine trust. Therefore, acknowledging the crucial role of cyber security in the global economy is essential for safeguarding economic stability and promoting sustainable growth.

Firstly, cyber-attacks pose significant risks to businesses and organizations worldwide. According to a report by Accenture [12], the average cost of cybercrime for an organization increased by 13% from 2018 to 2019. These costs include not only financial losses but also reputational damage and legal consequences. A single successful cyber-attack can lead to severe disruptions in supply chains, halt production lines, or even force companies out of business entirely. For instance, the NotPetya ransomware attack in 2017 caused an estimated $10 billion in damages globally [3]. Acknowledging the critical role of cyber security ensures that businesses take proactive measures to protect their digital assets and mitigate potential risks.

Secondly, protecting sensitive data is paramount for maintaining trust among individuals and institutions involved in economic activities. In an increasingly data-driven world, personal information such as credit card details or social security numbers are valuable commodities for hackers seeking financial gain or engaging in identity theft. The loss or compromise of such data erodes public confidence and undermines consumer trust—two pillars upon which economic transactions rely heavily. By acknowledging the importance of cyber security measures like encryption protocols and secure networks, governments and organizations can foster an environment where individuals feel safe conducting online transactions without fear of their personal information falling into malicious hands.

Furthermore, recognizing the critical role of cyber security is crucial for fostering innovation and technological advancements within economies worldwide. The fear of falling victim to cyber-attacks can hinder the adoption of new technologies and slow down the pace of innovation. For instance, businesses may be reluctant to embrace cloud computing or Internet of Things (IoT) devices due to concerns about their vulnerability to cyber threats. By acknowledging the importance of cyber security, governments and organizations can invest in research and development efforts aimed at creating robust security frameworks that enable safe adoption of emerging technologies. This, in turn, promotes economic growth by encouraging innovation and enhancing productivity.

Acknowledging the critical role of cyber security in the global economy is essential for safeguarding economic stability, protecting sensitive data, and fostering innovation. Cyber-attacks pose significant risks to businesses worldwide, leading to financial losses and reputational damage. Protecting sensitive data is crucial for maintaining trust among individuals and institutions involved in

economic activities. Finally, recognizing the importance of cyber security fosters an environment conducive to technological advancements and innovation. Therefore, it is imperative that governments, organizations, and individuals acknowledge the significance of cyber security measures as a means to ensure a resilient global economy.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] McAfee (2020) The Economic Impact of Cybercrime and Cyber Espionage—Amazon Web Services, The Economic Impact of Cybercrime and Cyber Espionage. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/60396rpt_cybercrime-cost_0713_ph4.pdf

[2] McAfee & Center for Strategic & International Studies (CSIS) (2018) The Economic Impact of Cybercrime—No Slowing Down: Economic Impact of Cybersecurity II. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-economic-impact-cybercrime.pdf

[3] Wired UK (2017) NotPetya Malware Attack Cost TNT $300m in Lost Revenues Alone. https://www.wired.co.uk/article/notpetya-cyberattack-tnt-revenues

[4] Fruhlinger, J. (2020) The OPM Hack Explained: Bad Security Practices Meet China's Captain America. CSO Online. https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

[5] Lukic, D. (2020, September 22) Target Data Breach, How Target Almost Lost Everything. Data Breaches. https://www.idstrong.com/sentinel/that-one-time-target-lost-everything/

[6] Kamalnath, V., Lerner, L., Moon, J., Sari, G., Sohoni, V. and Zhang, S. (2023, December 5) Capturing the Full Value of Generative AI in Banking. McKinsey & Company. https://www.mckinsey.com/industries/financial-services/our-insights/capturing-the-full-value-of-generative-ai-in-banking

[7] Katrakazas, C., *et al.* (2020) Cyber Security and Its Impact on CAV Safety: Overview, Policy Needs and Challenges. *Advances in Transport Policy and Planning*, **5**, 73-94. https://doi.org/10.1016/bs.atpp.2020.05.001

[8] Cavelty, D.M. and Wenger, A. (2022) Cyber Security Politics. Routledge, London & New York, Vol. 12, 141-160.

[9] Cheng, S., Zhao, G., Gao, M., Shi, Y., Huang, M. and Marefati, M. (2021) A New Hybrid Solar Photovoltaic/Phosphoric Acid Fuel Cell and Energy Storage System; Energy and Exergy Performance. *International Journal of Hydrogen Energy*, **46**, 8048-8066. https://doi.org/10.1016/j.ijhydene.2020.11.282

[10] Quigley, K., Burns, C. and Stallard, K. (2015) "Cyber Gurus": A Rhetorical Analysis of the Language of Cybersecurity Specialists and the Implications for Security Policy and Critical Infrastructure Protection. *Government Information Quarterly*, **32**, 108-117. https://doi.org/10.1016/j.giq.2015.02.001

[11] Alghamdi, M.I. (2021) Determining the Impact of Cyber Security Awareness on

Employee Behaviour: A Case of Saudi Arabia. *Materials Today*: *Proceedings*, p. 122. https://doi.org/10.1016/j.matpr.2021.04.093

[12] Accenture (2020) Cost of Cybercrime Study: Insights on the Evolving Threat Landscape and Cost to Business. https://www.accenture.com/_acnmedia/PDF-112/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf