Scientific Research Publishing

Open Journal of Safety Science and Technology, 2023, 13, 51-65
https://www.scirp.org/journal/ojsst
ISSN Online: 2162-6006
ISSN Print: 2162-5999

The Impact of Cyber Security on Business: How to Protect Your Business

Emiles Mbungu Kala

Department of Computer Science, Northrise University, Ndola, Zambia
Email: emile.kala@outlook.com,emile@emkaconsulting.com

How to cite this paper: Kala, E.M. (2023) The Impact of Cyber Security on Business: How to Protect Your Business. *Open Journal of Safety Science and Technology*, **13**, 51-65.
https://doi.org/10.4236/ojsst.2023.132003

Received: April 20, 2023
Accepted: June 27, 2023
Published: June 30, 2023

Abstract

This book presents knowledge and grasp of numerous sorts of computer attacks, as well as the reasons and targets of those attacks. The introduction of the article includes a brief dictionary of relevant terms that are laid out in a manner that is simple to comprehend. Following this, the paper analyzes "the patterns and severities of cyber attacks and their impact on routine computer-based operations, the furtherance of business, and electronic commerce, as well as on some Critical National Infrastructure (CNI), which supports such essential areas as power, transportation, communications, defense, and banking and finance". In the field of cyber security, which is now a highly popular topic of debate, the definition of cyberspace or cyber risk is currently a prominent issue of controversy. The major goal of this article is to educate the audience about the dilemma that is offered by cyber security and to make them aware of the possible attacks and cyber threats that now exist in the world of information technology or cyberspace. This piece will also make them aware of the attacks and cyber threats that now exist in the realm of information technology or cyberspace.

Keywords

Cyber Security, Business

1. Introduction

The phrases "cyber security" and "information security" are synonymous to some extent, although they are not the same thing. Information security, as it is often known, refers to the ability of an organization to protect the flow of information across all of its departments. Cyber security, on the other hand, refers to the ability to protect a user's assets and the environment in which they operate from intrusion by an outside party. The problem of cyber security has recently

surfaced "as a matter of worry on a global scale, and all of the countries have started to create outlines associated with their involvement in cyber worries. At the same time, information security is making strenuous efforts to execute the general security objectives, which include safeguarding confidentiality, integrity, and availability while also assuring accountability and carrying out audits. Even though the definitions are relatively analogous to one another, the scopes of each are unique and get progressively more extensive when compared to one another. Our article will be organized as follows: in the first section, we will give an overview of the present state of the art by focusing on the impact that cyber security has on businesses and governments. Following that, we will talk about the significant financial harm that has been inflicted by breaches in cyber security. [1] After that, we will present a rundown of some of the countermeasures that are used in the realm of cyber security in the subsequent section of this article. In the second part of our conversation, we will examine the key differences between information security governance and cyber security. After that, we will highlight the new framework that is based on EAS-SGR. This new framework will aid us in the process of putting together an action plan for cyber security.

2. What Is the Cyberspace?

The science fiction author William Gibson first used the term "cyberspace" in the title of his novel "Burning Chrome" which was published in 1982. Since the release of his novel "Neuromancer" in 1984, which first popularized the word "cyberspace" to describe the virtual world of information networks, science fiction has never been the same again. The term "cyberspace" was originally popularized by William Gibson in his novel "Neuromancer". The word "cyberspace" refers to the common digital universe that exists across all of the computer networks of the globe and has come to be used to characterize the total information space. This shared digital universe is referred to as the Internet. The use of automated teller machines, conversing on the phone, engaging in online chat rooms, transferring information through computers, and other similar pursuits are all examples of activities that take place in cyberspace. Because "cyberspace" has more or less become a mainstream euphemism for the internet, one may use the word "exits in cyberspace" to metaphorically allude to the internet as a website. This is because the term "cyberspace" has grown popular in recent years. The use of electronics and the electromagnetic spectrum to store, alter, and otherwise convey information (or data that has been processed) via networked systems and the physical infrastructures that are linked with them is what defines the region known as cyberspace. It is a method of characterizing the virtual three-dimensional environment that is formed by computer networks and through which electrical signals can travel in text, audio, and video format. This environment can be thought of as being similar to the world of a video game. [2] Cyberspace is the name given to the geographical region of the world in which the use of computers and other forms of electronic processing is most common.

It comprises all parts of human undertakings, whether they are business initiatives or private endeavors, which are either driven by or focused on any component of computer usage or support. This is true regardless of the type of endeavor: private or commercial. Simple desktop publishing tasks (such as Word, Excel, PowerPoint, and Outlook) are examples of such disciplines. Other examples include scanning and accessing the web online. The fields of data mining, data networks, artificial intelligence, robotics, cyber forensics, biometrics, and computer imaging are among the most complex subfields in computer science. Additionally, the word "cyberspace" is used to refer to all operational regions that are dominated by human-computer interactions and are driven by a range of high-tech computer systems. These places are referred to as "operating regions" in this article. These computer technologies may take the form of data networks, software systems, or computer-centric intellectual communication. Alternatively, they may be used in combination. In a nutshell, the word "cyberspace" refers to the ubiquitous information society, which is distinguished by the fact that the promotion of day-to-day activities is possible by continuously increasing electronic technology. This society is defined by the pervasive information society. Cyberspace is the name given to the domain of all things digital. [3] [4]

Cyber Threats to Business Organizations

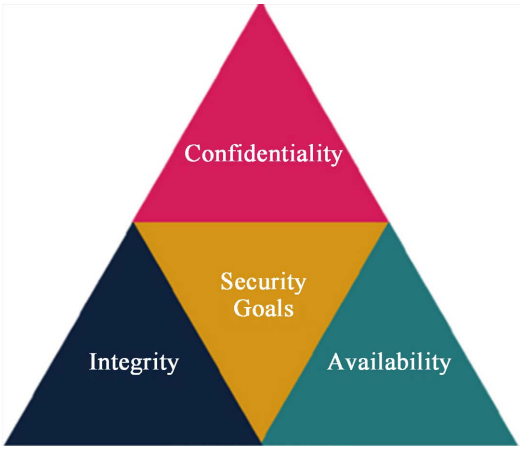
The fact that we all live in a society that is centered on information and education has a beneficial effect on the growth of enterprises on a variety of scales, including the local, national, and even the worldwide level. We are becoming increasingly dependent on a huge number of systems, which leaves us open to cyberattacks that have the potential to inflict significant harm. This is one of the drawbacks associated with the process of establishing a knowledge society. This is the case regardless of the perspective one adopts when examining the situation. According to Green, "a cyber-attack is an electronic attack on the systems of several different companies or organizations," and the result of such an attack is frequently the theft of the accessible assets of the targeted companies or organizations, which are held in the form of accessible digital information. In today's world, enterprises that operate in the domains of power, transportation, banking, finance, and infrastructure; medical services; sewage and potable water supply systems; and digital infrastructure (e-shops, clouds, etc.) are typical targets of cyberattacks. Attacks carried out online are growing more and more frequent. It is expected that the rate of development of cyber dangers will increase at a pace that will be dizzying. It is projected that future cyber assaults would concentrate primarily on the backup storage systems of important corporate organizations. [5] These attacks may be carried out to undermine the targets' objectives and inflict damage within a competitive setting. The propensity of consumers to click on potentially malicious URLs that are placed in their email inboxes is one of the most pressing concerns that exist at this time. The credentials can be encrypted, and it is conceivable to launch an assault on the system with nothing more than the push of a button. The distribution of potential cyberat-

tacks throughout the globe in 2016 and 2017 is depicted on the map that can be seen below.

Definitions: What Exactly Is Network Security?

If one wants to have a complete comprehension of the idea of network security, it is necessary to first have a comprehensive comprehension of the idea of security in general. The practise of consistently securing anything against unauthorised access and guaranteeing a condition or perception of safety from potential threats is what we mean when we talk about security. This object can be a person, a firm, an organisation, or a piece of property like a computer system or a file. Among the numerous possible manifestations of this item are those listed above. On the other hand, network security is a more precise word that refers to the numerous protocols and preventative measures that are put into place to safeguard the underlying networking infrastructure of an organisation. This infrastructure may include wireless networks, wired networks, or both. The primary objective of network security is to monitor and prevent unauthorised access to an organization's network, resources, and assets. This is accomplished through the use of authentication and authorization protocols. By doing so, the company may protect itself from a wide array of possible dangers, including cyberattacks, data breaches, and system outages. When attempting to gain a deeper comprehension of the idea of security, it might be useful to examine it from the perspective of privacy. Security is what ensures that something is protected from unauthorised access, whereas privacy is the requirement that something should be shielded from such access. The danger of cyberattacks and data breaches is larger than it has ever been in today's digital age, when individuals and organisations routinely engage in online activities such as surfing the web, making purchases from online retailers, and uploading data over the public internet. Consequently, the likelihood of these types of incidents has increased. Intruders on the same network have the possibility of gaining access to sensitive data such as personal identities, credit card details, account numbers, and passwords, which can lead to fraud and other forms of criminal activity. They are also capable of causing a large amount of harm to an organisation by bringing its infrastructure to a halt or stealing precious assets, such as prototypes of projects or other forms of intellectual property. [6] Therefore, it is very necessary for businesses to put in place efficient network security measures in order to prevent viruses, malware, hackers, and other types of intruders from gaining access to or manipulating their important data or assets. Organisations may guarantee that they are effectively secured against a broad variety of possible attacks by appropriately protecting the network infrastructure that supports their networks. (**Figure 1**)

The average cost of a data breach for corporation organisations in the United States as of 2022 is expected to be $9.44 million, which includes the expenditures of remediation, forensic investigation, and litigation, as stated by statista.com ("statista.com", 2022). This estimate comes from statista.com ("statista.com", 2022). It is possible to save undue suffering and money by addressing weaknesses



Source:
https://www.open.edu/openlearn/ocw/mod/oucontent/view.php?id=104794&section=1.1

Figure 1. Concept of information security.

in the security posture of your organisation in advance and in a proactive manner. When it comes to building a comprehensive governance model for your company, there is no need for you to start from scratch. Instead, you can make use of the CIA triad, which is the fundamental concept behind information security. [7] Concerning the safety of computer networks, the CIA triad is widely regarded as one of the most important models that should be used to regulate information security policies inside an organisation. Confidentiality, Integrity, and Availability are the meanings denoted by the abbreviation CIA.

Confidentiality

Maintaining confidentiality means limiting access to information only to those individuals for whom it is meant. When talking about information that is sensitive or classified, the phrase "confidentiality" refers to the ability of only authorised people or systems to view that information. It is imperative that no unauthorised users or systems may access the data stored on the network. Utilising encryption techniques such as AES (Advanced Encryption Standard) and DES (Data Encryption Standard) to protect your data is an essential component of the fundamental approach for avoiding this issue, which is to make use of a VPN tunnel (Virtual Private Network), which enables data transit securely across the network. so that even if the attacker gains access to your data, they are unable to decode it even if they try. [8]

Integrity

Integrity refers to the state of not having communications and messages intentionally corrupted or changed in any way. Integrity is the reliability of data throughout its lifespan while retaining both the external and internal consistency of the data. It refers to the process of safeguarding data against any kind of alteration that might be made by unauthorised users. Encryption techniques may be utilised to accomplish this goal, which helps to retain a level of data integrity as well as accuracy. [9] The mechanism of the encryption system should be able to prevent the message from being changed or corrupted, or at the very least be

able to notify that this has occurred. Just picture the massive amount of trouble that would be caused if someone's medical records or medicine prescriptions were changed.

Availability

When it comes to information and services, accessibility is ensured when there is availability. This suggests that users of the network should be able to quickly connect to the network whenever they require it. This is something that applies to both the systems and the data, since they need to be available whenever it is necessary. In order to ensure that the network and its data are always accessible, the administrators of both the network and the system should ensure that their hardware and software receive regular updates. In addition, the administrators of both the network and the system should have backup plans and fail-over strategies for the infrastructure of their organisation, just in case a failure occurs or DDoS attacks bring the company's infrastructure and resources to a halt. [10] They have the capability to easily fail over to alternate infrastructure, which will lessen the impact of any failure or assault. In general, all of the data that you want to keep safe needs to be kept secret, preserve its integrity, and be accessible. The term "confidentiality" refers to the act of merely concealing the information in question, namely from those who are not authorised to read it. Integrity implies preventing unauthorised parties from making changes to the data, either on purpose or inadvertently, while availability ensures that the information is accessible whenever it is required.

Possible Impacts of Cyber Threats on Business

Costs Will Go Up Businesses and organizations that are serious about defending themselves against scam artists online will need to dig deep into their pockets to cover the increased costs. In general, for companies to comply with the standards for internet safety, they may be needed to confer with a wide variety of legal consultants and professionals. This is so that they can ensure that they are not breaking any of the rules. In addition, if they are the victim of an attack, they may be obliged to pay significantly more in legal expenses and damages as a consequence of ordinary processes brought against the organization. This is based on the assumption that they are the intended target of the assault. Costs Will Go Up Businesses and organizations that are serious about defending themselves against scam artists online will need to dig deep into their pockets to cover the increased costs. [11] [12] In general, for companies to comply with the standards for internet safety, they may be needed to confer with a wide variety of legal consultants and professionals. This is so that they can ensure that they are not breaking any of the rules. In addition, if they are the target of an attack, they may be required to pay much more in legal expenses and damages as a consequence of ordinary processes brought against the organization. This is in addition to the fact that they may be the subject of an assault. This is predicated on the assumption that they are the intended target of the assault. Reputational Harm: If severe breaches in a company's information security cause its brands to suffer, the company's reputation might take a serious hit,

which would be extremely damaging. Customers and even providers could be cautious to entrust a firm with their sensitive information if that organization's information technology system has already been breached at least once. Following an assault, the value of the firms whose stocks had been hacked dropped by an average of 3.5 percent, falling behind the Nasdaq by 3.5 percent in the process.

3. Information Security Governance and Cyber Security

Because cyber security is such a vast area of study, we felt it necessary to compile a list of some of the key concepts underlying it to have a deeper understanding of the subject. We need to define governance as the process of maintaining an effective corporate structure so that we can talk about the connection between ISG and cyber security. Governance may be thought of "as the act of maintaining an efficient corporate structure. The following are some major concepts related to governance:

- "The vision"
- "The mission"
- "Transparency"
- "Equity"
- "Accountability"
- "Corporative Responsibility"

Because every company needs a clear vision for each of the tasks that their staffs are tasked with completing, these suggestions must be respected and adhered to by any company that has as its primary goal the accomplishment of its business objectives. Indeed, the company's task force has to maintain open communication with one another and take responsibility for the consequences of their activities.

Information Security

Information security is recognized as the most valuable asset because of its well-known properties, which include confidentiality, integrity, and availability (CIA). This is the reason why information security is considered to be the most valuable asset. When it comes to cyber security, these criteria are not adequate to deal with the ludicrous vulnerability that flows across the internet; nonetheless, the CIA triangle model is no longer an appropriate response to the ever-evolving environment of the computer industry." [13] In today's world, these criteria are not sufficient to deal with the absurd vulnerability that flows across the internet when it comes to cyber security. Therefore, we need to add additional features like accountability and audit, and after we have done that, we will give it the name CIAAA. CIAAA stands for the Comprehensive International Accounting and Auditing Association. The following is a description of how the new components can be categorized:

- When we talk about accountability, what we mean is that there is a requirement for us to be able to trace any acts that are carried out by an entity back

to only that entity alone. It is possible to attribute any action or omission on the part of an employee to that employee;

- Audit: The auditing of security to relevant events is a crucial component for identifying security breaches and attacks, as well as for recovering from the effects of those occurrences. Auditing security to relevant events.

Information Security Governance (ISG)

ISG is an abbreviation for information security and governance, both of which are components of corporate governance. We are in a better position to cope with potential dangers as a result of the addition of accountability and auditing procedures to the capabilities of the CIA. [14] "Mark Brown, Director for Advisory Risk & Information Security at Ernest and Young" was given the task of conducting an assessment on the use of information systems in companies in the year 2013 as part of a commission from EY. This examination was carried out following Ernest and Young's instructions. The findings of the research point to the fact "that":

- 88% of businesses report an increase in external threats;
- 57% of businesses report an increase in internal threats;
- 61% of businesses cite a lack of budget as the main hurdle;
- 57% of businesses view information security resources as lacking necessary skills;
- 62% of businesses do not align information security to enterprise architecture or business processes;
- 38% of businesses do not align with organizational risk appetite.

"Even when all information security researchers and practitioners are doing their very best to prevent risks from delaying or even obstructing" is the path that enterprises follow to achieve their business objectives. This is still often considered to be the most critical obstacle that businesses must overcome. At the same time, the volume and scope of attacks continue to increase, and hackers are concurrently accessing information systems increasingly deeper to obtain extremely sensitive data. Based on this analysis, we need to take a more cautious approach to IT risk management and cyber security threats, and we also need to develop a new framework that will assist IT managers in protecting their systems, and more importantly, preventing their systems from being used for cybercriminal activity, which has recently taken center stage in the security arena. Both of these steps are necessary for us to meet our responsibilities.

The Risks and Consequences of Cyber Threats

Cyber threats are any hostile acts that are carried out by individuals or groups making use of technology to inflict harm to individuals, businesses, or even nations. These activities can be carried out by anyone, anywhere, at any time. These dangers can manifest themselves in a wide variety of ways, including cyberattacks, data breaches, hacking, identity theft, ransomware, phishing, and many more. The dangers and repercussions that might result from cyber attacks can be serious and widespread, affecting many facets of our life, such as the ones listed above:

1) Financial Loss: Individuals and businesses are both susceptible to suffering big monetary losses as a result of cyberattacks. Cybercriminals may steal critical financial information, carry out fraudulent transactions, or demand ransom payments to decrypt material that has been encrypted. The financial expenditures that can be incurred in detecting and managing cyber assaults, in addition to the possible legal obligations and fines, can be significant.

2) Reputational Damage: Individuals, corporations, and even national governments all run the risk of having their reputations damaged by cyberattacks. A loss of confidence on the part of customers, partners, and the general public can be the result of data breaches and the leaking of sensitive information. The damaging effects of unfavorable publicity and reputational harm to the brand can have lasting repercussions, including the loss of consumers, partners, and commercial possibilities.

3) Loss of Intellectual Property: Theft of intellectual property (IP) can be the consequence of cyber threats, and examples of IP include trade secrets, private information, and data relating to research and development. This can have a substantial influence on the competitive edge and market position of a firm, which can ultimately result in financial losses and a loss of market share.

4) Disruption of Operations: Attacks on computer networks have the potential to sabotage crucial commercial and government activities, leading to downtime, decreased productivity, and delays in the provision of services. Attacks using ransomware, for instance, can encrypt data and make systems or networks unavailable, which can result in disruptions to businesses and financial losses.

5) Legal and Regulatory Consequences: As a direct result of cyber attacks, organizations run the risk of experiencing legal and regulatory repercussions. There are a variety of legal requirements, including data protection and privacy laws, industry rules, and contractual duties, that may need the implementation of particular security measures by businesses to safeguard sensitive information. Should you fail to comply with these rules, you may be subject to civil and criminal penalties, as well as litigation.

6) National Security Risks: The potential dangers posed by cyberattacks on the nation's infrastructure cannot be overstated. The disruption of important services, the compromising of sensitive information and the influence on national defense capabilities are all potential outcomes of cyberattacks directed at critical infrastructure, government networks, or military activities. This can have extremely negative repercussions for a nation's security as well as its sovereignty.

7) Psychological and Emotional Consequences: Individuals may also have psychological and emotional repercussions as a result of being exposed to cyber dangers. People who are victims of cyber assaults, such as having their identities stolen or being harassed online, may experience a variety of unpleasant emotions, including tension, worry, and panic. [15] These repercussions have the potential to have an impact on an individual's mental health as well as their quality of life.

To reduce these risks and safeguard against cyber attacks, it is essential to establish comprehensive cybersecurity measures, such as frequent upgrades, strong passwords, personnel training, and other best practices. In addition, people and businesses may strengthen their defenses against future cyberattacks by keeping up to date with the most recent cyber threats and by implementing best practices for cybersecurity.

Common Cyber Threats to Look Out for

You should be aware of the most frequent forms of cyber threats, such as malware, phishing, and ransomware, to maintain your level of protection against them. These attacks can have a lasting effect on your company.

Malware

An attacker using malware will inject malicious software into a target system or network that is unaware of the attack to cause damage, disrupt operations, or obtain unauthorized access to steal sensitive information, banking data, and passwords.

Email attachments and websites that have been compromised can be vectors for the distribution of malware such as viruses, worms, and Trojan horses.

Malware, after it has been installed on a computer, sets itself up to steal personal data, such as passwords and financial data, and in the most extreme circumstances, it may even take control of your entire system.

Phishing

This danger takes the form of a social engineering assault, in which the perpetrator poses as a member of the target organization to deceive its employees and customers into divulging confidential information. What's worse is that research indicated that a resounding 54% of global MSPs feel that phishing attacks are the biggest cyber security concern for enterprises and the major delivery mechanism for ransomware attacks. This information comes from a poll that was conducted worldwide. These assaults can be difficult to notice, and they involve urgent requests for personal information such as usernames and passwords. These requests might come in the form of emails, texts, or other kinds of contact, and they are sent by impersonators of respected businesses.

Ransomware

Ransomware is a type of malicious software that infiltrates a target machine and encrypts the user's files. The attacker will then demand a sizable ransom in exchange for the decryption key, which will let the company regain access to its encrypted data. It is a sophisticated form of attack in which the offender poses as a reliable organization and delivers a message to stakeholders by email, text messages, or direct messaging on social media that contain a link to a malicious website. The payload infects the target system when an employee clicks on the link without being aware of what it leads to. [16] Once it has infected the system, it can carry out a variety of harmful activities, including encrypting files, stealing sensitive data, reproducing itself across other computers on the network, and even deleting data completely. It can do substantial harm to the company's reputation, as well as its operational and financial health, which nearly always re-

sults in a loss of consumer trust.

Potential Consequences of Cyber Attacks

Cybercrime can have a devastating effect on enterprises, resulting in monetary losses, the cessation of operations, shifts in business practices, legal responsibilities, reputational damages, and the theft or compromise of intellectual property.

Financial Loss

Businesses that fall victim to cybercrime often have to bear the hefty expenses involved with fixing damage to information technology systems, lost productivity, and legal fees. This can result in a major financial loss for the company. It does not include the amount of money you would have to spend to restore the reputation of your company, reclaim market share, and win back the trust of your customers. These losses may soon build up, which can have a significant impact on the bottom line of the organization.

Operational Stoppage

An operational standstill can also be the consequence of a cyber assault, which has a significant impact on the ability of a corporation to function. If the information technology systems of a company are breached, it is conceivable that the company will be unable to continue operations until the issue is located and fixed.

Change in Practices

A modification in corporate procedures may be necessary after a cyber attack in certain circumstances. For instance, if a firm discovers that its customer data has been infiltrated, it may be necessary for the organization to create more stringent data protection procedures to prevent such assaults.

Legal Liabilities

As a result of cyber assaults, companies may potentially be held legally liable for damages. Companies may be responsible for damages to customers and other parties harmed by an attack, depending on the sort of attack that was carried out and the data that was stolen or otherwise compromised. These potential legal liabilities might cost the company millions of dollars, thus they must be avoided at all costs.

Reputational Damage

Damage to a company's reputation is one of the most important repercussions that might result from a cyber assault. Imagine that the customer information of a company has been stolen. In this scenario, it may lead to a loss of trust among consumers and other stakeholders, which may have long-term repercussions for the reputation, market position, and profitability of the organization. Numerous companies that have been victimized by cybercrime frequently discover that it is quite difficult to get back their former reputation.

Cyber Risk and Types of Cyberattacks

The term "operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems" is one approach to explain cyber risk. Cyber risk, in compared to the other risk categories that are covered by insurance, contains

features that are comparable to property risk and liability risk, in addition to catastrophic risk and operational risk. These similarities come from the fact that cyber risk is a relatively new type of risk. On the one hand, first parties, also known as the target, as well as third parties, also known as a counterpart to the target, may be affected by cyber risk. Losses that are sustained as a result of cyber risk, on the other hand, are often modest and unconnected; nonetheless, they may also occur seldom yet have a large impact ("blackout scenario"). According to the explanation provided in the definition of cyber events, the term "cyber risk" does not necessarily have to be synonymous with "cyber attacks." For instance, software updates or natural disasters may contribute to the crystallisation of cyber risk through the disruption of corporate operations without any nefarious intent on the part of the actor. [17] [18] Businesses run the risk of having their availability, integrity, and confidentiality of their information compromised as a result of cyber attacks since these are the three aspects of information security that are considered to be of the utmost importance. It is possible for there to be a breach of confidentiality if sensitive information about an organization is divulged to third parties in any way, including through a data breach. When the systems are utilized dishonestly, as is the case with fraud, this can lead to problems with the integrity of the organization. In conclusion, but certainly not least, issues with availability might result in disruptions to corporate operations. The following are some of the ways in which various types of cyber attacks have unique ramifications for the targets of such attacks: However, the ramifications of data breaches take longer to manifest, and they materialize in the form of reputational damages in addition to legal expenditures. Fraud results in direct monetary losses, whereas data breaches take longer. Interruptions to business operations make it difficult for companies to function, which results in revenue being lost. When it comes to the financial system, business interruptions are more likely to have direct short-term contagion effects than fraud or data breach, both of which tend to have an effect in the short-term on only the firm that is being targeted. In general, the danger of a loss of confidence following cyber-attacks might be considerable for the financial sector, given the reliance of financial institutions on the faith of their clients. In particular, the risk could be high for banks. [19]

Compromised Intellectual Property

Attacks conducted over the internet can potentially result in the theft of intellectual property from a corporation. It may contain important trade secrets, data on customers, and unique technology, all of which are difficult to recover or replace and may incur a high cost.

Recommendations to the E-Business Stakeholders and the Government [20]

- E-Businesses are more dependent on this kind of information due to the restriction on resources available to invest in research into areas such as these themselves, and the government should implement clear mechanisms that support Internet security. The government should also be supported for at-

tempting to offer advice to companies for a minimal charge, as E-Businesses are more dependent on this type of information. Because SMEs do not share the same features as bigger organizations, this must also have some influence on the advice that is provided.

- The information technology staff has a responsibility to raise awareness of cybercrime and assist all E-Business stakeholders in comprehending the nature of cybercrime.
- It is the responsibility of all parties involved in e-business to raise awareness about what truly constitutes an e-business from a safety standpoint.
- The government's information technology sector ought to raise knowledge about the many resources that are available to e-businesses to strengthen security.
- The thought process of e-business should be more heavily centered on proactive rather than reactive actions. Many e-businesses do not believe that they are at any significant risk, and as a result, they do not take the matter as seriously as they should. Their way of thinking is predicated on responding to situations as they arise rather than anticipating and preventing them.

4. Conclusion

In this piece, we discuss a big problem known as cybercrime, which affects the majority of countries across the world at present and will continue to do so in the years to come. This issue will continue to be a challenge for many nations throughout the world. Within the confines of our conversation, we dove into the world of cybercrime and attempted to throw some light on the formidable problem that is cybersecurity. It appears that most countries will have difficulties and struggle mightily to get beyond this obstacle. Instead, researchers are putting numerous defenses into operation intending to minimize or limit the harmful consequences that cyber attacks have. Cybercrime can only exist in societies that either do not have any laws or where the necessary government institutions are either incompetent or insufficient in their implementation of the laws that are on the books. Those who are charged with the enforcement of applicable laws, such as law enforcement officers and other stakeholders, are strongly encouraged to observe the highest ethical standards as a result. However, there is a strong notion that if individuals who commit cybercrime can be recognized and punished, it would further diminish the desire to do cybercrime, and we should be on our way to creating the necessary trusts in e-commerce and indeed the internet. This idea is supported by several studies that have been conducted in recent years. This is an essential action that has to be carried out before we will be able to proceed in any meaningful way.

Conflicts of Interest

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

References

[1] Jain, A.K., *et al.* (2021) Biometric Recognition: Challenges in Forensics. http://biometrics.cse.msu.edu

[2] Bank of England (2017) Systemic Risk Survey Results—2017 H2. London. https://www.bankofengland.co.uk/systemic-risk-survey/2017/2017-h2

[3] Bholat, D., Hansen, S., Santos, P. and Schonhardt-Bailey, C. (2015) Text Mining for Central Banks. Centre for Central Banking Studies. https://doi.org/10.2139/ssrn.2624811

[4] Cashell, B., Jackson, W.D., Jickling, M. and Webel, B. (2004) The Economic Impact of Cyber Attacks (April), Congressional Research Service Web Report. https://sgp.fas.org/crs/misc/RL32331.pdf

[5] Fifthen, K. (2013) Internet Denial of Service Attacks and the Federal Response, https://cdt.org/wp-content/uploads/security/000229judiciary.shtml

[6] World, E. (2022) Business Leaders Warn of Cybercrime Threat to Internet Development.

[7] M. Butler (2017) Effective Global Regulation in Capital Markets. *Speech at the ICI Conference*, London, 5 December 2017. https://www.fca.org.uk/news/speeches/effective-global-regulation-capital-markets

[8] Clarke, A. and Hancock, J. (2012) Payment System Design and Participant Operational Disruptions. *Journal of Financial Market Infrastructures*, **2**, 1-25. https://doi.org/10.21314/JFMI.2013.023

[9] Franklin, I. (2001) A Can of Worms. *Computer Fraud & Security*, **2001**, 12-13. https://doi.org/10.1016/S1361-3723(01)01218-0

[10] Gengler, G. (2017) Paypal's Anti-Fraud Team, *Computer Fraud & Security*, **2002**, 5. https://doi.org/10.1016/S1361-3723(02)00311-1

[11] Glaser, M. and Haene, P. (2007) Simulation of Participant-Level Operational Disruption in Swiss Interbank Clearing: Significant Systemic Effects and Implications of Participants' Behavior. *Payment and Settlement Simulations Seminar*, Helsinki, 28 August 2007. https://www.suomenpankki.fi/globalassets/en/financial-stability/payment-and-settlement-system-simulator/events/2007_06_glaser_member-level-disruption-in-sic.pdf

[12] G.A., de Oliveira Alves, L.F.R., da Costa Carmo and A.C.R.D., de Almeida (2006) Enterprise Security Governance: A Practical Guide to Implement and Control Information Security Governance (ISG) *The First IEEE/IFIP International Workshop on Business-Driven IT Management*, Vancouver, 3-7 April 2006, 71-80.

[13] Harris, G. (2016) Compsec 2016: Watching the Threat from without Science Direct, Queen Elizabeth II Centre, London, 19.

[14] Holm, H., Sommested, T., Ekstedt, M. and Nordstrom, L. (2013) CySeMol: A Tool for Cyber Security Analysis of Enterprises. *The 22nd International Conference and Exhibition on Electricity Distribution*, Stockholm, 10-13 June 2013. https://doi.org/10.1049/cp.2013.1077

[15] Joel Kayode Theophilus (2006) The Nigerian Police Cyber Crime Containment Prospects. West African Chief of Police Conference Abuja.

[16] Kopp, E., Kaffenberger, L. and Wilson, C. (2017) Cyber Risk, Market Failures, and Financial Stability. IMF Working Paper No. 2017/185. https://doi.org/10.5089/9781484313787.001

[17] Mark Brown, Director for Advisory Risk & Information Security at Ernst & Young. Enterprise Security Architecture. *Computer Weekly*.

[18] Menezes, A.J., van Oorschot, P.C. and Vanstone, S.A. (1996) Handbook of Applied Cryptography. CRC Press, Boca Raton. http://www.cacr.math.uwaterloo.ca/hac

[19] Miller, A. (2015) More than Half of IT Managers Are Ignorant of Rising Cybercrime Threat.

[20] von Solms, R. and van Niekerk, J. (2013) From Information Security to Cyber Security. *Computers & Security*, **38**, 97-102. https://doi.org/10.1016/j.cose.2013.04.004