JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Impact of Cyber Security in Business Environment Protection of Current Scenario

[1] Dr. V. SENTHILKUMAR, [2] Dr.K.G. SELVAN
[1]Associate Professor & Research Supervisor, [2]Head, Department of Commerce
Department of Commerce
[1]Vivekanandha College of Arts & Sciences for Women, (Autonomous)
Elayampalayam, Tiruchengode, Namakkal District, Tamilnadu
[2] Vivekanandha College of Arts & Sciences for Women, (Autonomous)
Elayampalayam, Tiruchengode, Namakkal District, Tamilnadu

Abstract: Cyber Security has been a major pillar for the Information Security framework to maintain the privacy and data consistency and integrity of customers especially when it comes to E-commerce domain. The platform needs high security intricate that affects the end user customers through everyday use of the commercial portal. 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 of business environment.

IndexTerms -Cyber Security, Business Cyber Attacks, Phishing, Cyber Crime, Network Security,

I. INTRODUCTION

In today's Internet-connected world where technologies underpin almost every facet of our society, cybersecurity and forensic specialists are increasingly dealing with wide ranging cyber threats in almost real-time conditions. The capability to detect, analyse, and defend against such threats in near real-time conditions is not possible without employment of threat intelligence, big data, and machine learning techniques.

"Cyber security" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction. 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 recentlysurfaced "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.

Objectives of the Study

- To pinpoint significant cybersecurity threats affecting Indian e-commerce business platforms.
- To suggest effective practices and preventive strategies utilized by e-commerce business enterprises.

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.

Challenges faced In Indian E-commerce:

- ❖ As companies increasingly rely on online platforms for transaction management, customer engagement, and data storage, they become attractive targets for cybercriminals who seek to exploit vulnerabilities for personal or financial gain. One of the most urgent cybersecurity threats is data breaches.
- ❖ 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

Cyber Threats to Business Organizations

The fact that we all live in a society that is centred 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.

Cyber-Attack Is an Electronic Attack on the Systems

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. These attacks may be carried out to undermine the targets' objectives and inflict damage within a competitive setting.

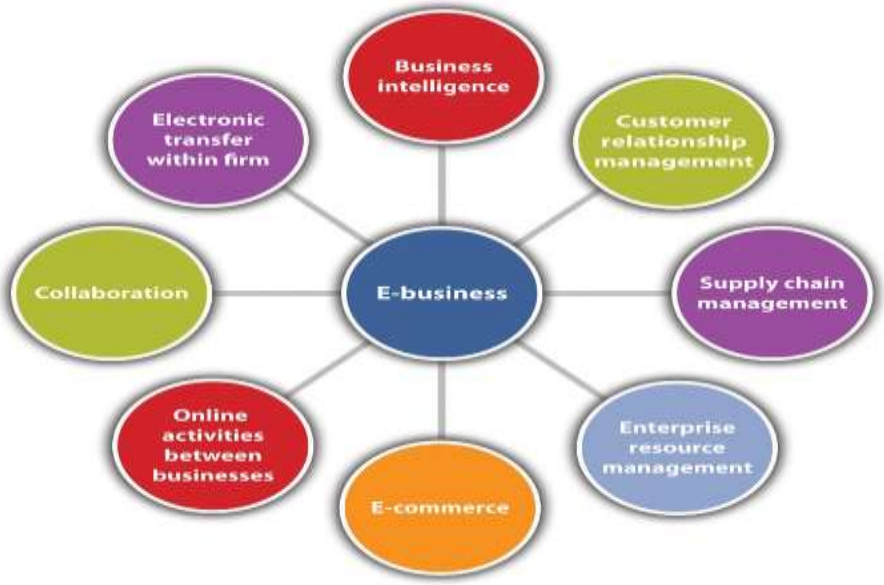
- **Protecting customer information**: Cybersecurity measures such as encryption and secure data storage help to protect sensitive customer information, such as credit card numbers, addresses, and other personal details, from cyber-attacks and fraud.
- **Ensuring secure transactions**: Cybersecurity measures such as two-factor authentication and fraud detection systems help to ensure that transactions are secure and legitimate, preventing fraudulent purchases and chargebacks.
- **Maintaining website availability**: Cybersecurity measures such as DDoS protection help to ensure that e-commerce websites are available and accessible to customers, even in the face of cyber-attacks that aim to disrupt or take down the website.
- **Preventing malware and cyber-attacks**: Cybersecurity measures such as anti-virus software and firewalls help to prevent malware and cyber-attacks that can compromise e-commerce websites, steal customer data, and cause other damage.

Goals of Cyber Security in E-commerce

- **Preventing unauthorized access:** Cybersecurity measures such as access controls and authentication mechanisms are implemented to prevent unauthorized access to e-commerce systems and data.
- **Protecting sensitive information**: Encryption techniques and secure communication protocols are used to protect sensitive information, such as credit card details, from being intercepted or stolen.
- **Maintaining system availability**: Cybersecurity measures such as firewalls and intrusion detection systems are implemented to ensure that e-commerce systems remain available and functional, even in the face of cyber-attacks.
- **Preventing fraud**: Cybersecurity measures such as fraud detection algorithms and transaction monitoring systems are implemented to prevent fraudulent activities, such as identity theft and payment fraud.
- **Ensuring compliance**: E-commerce businesses must comply with various regulations and standards, such as the Payment Card Industry Data Security Standard (PCI DSS), which outlines the minimum-security requirements for handling credit card information. Cyber security measures are implemented to ensure compliance with these regulations and standards.

E- BUSINESS

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.



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.

Integrity

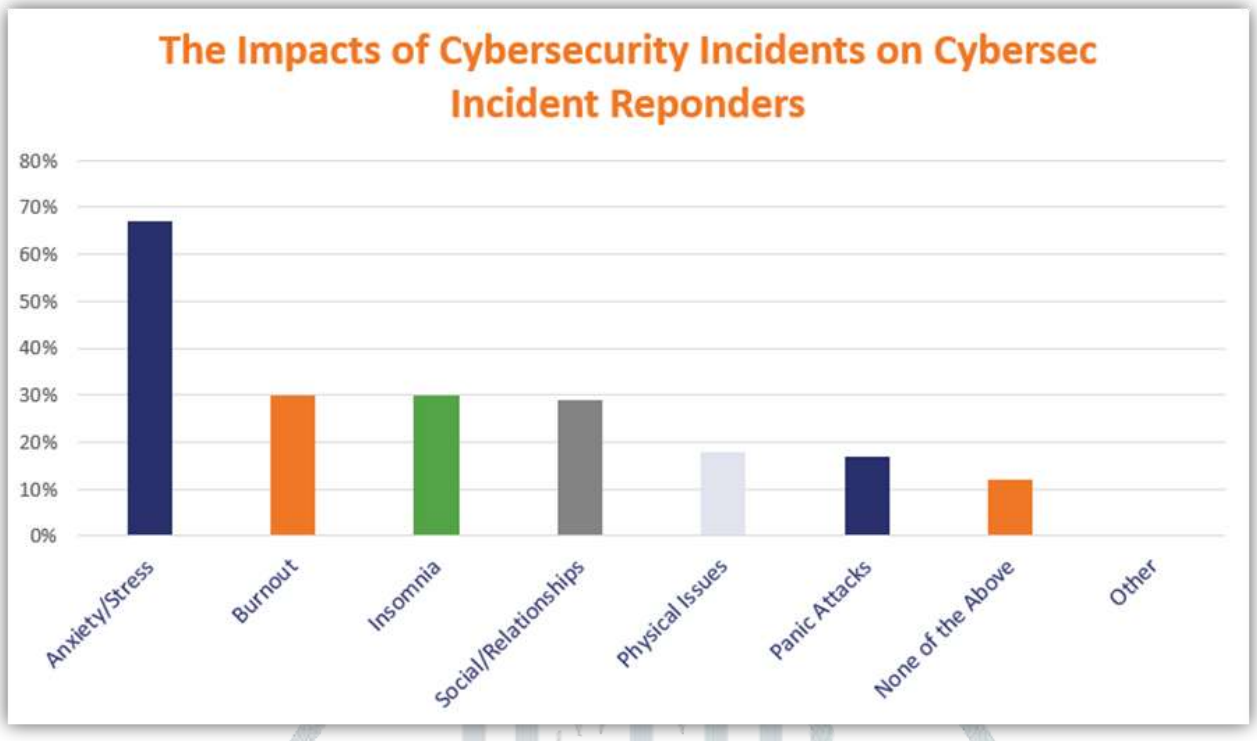
Integrity refers to the state of not having communications and messages intentionally corrupted or changed in any way. Integrity is the reliability of data throughout its lifespan while retaining both the external and internal consistency of the data. It refers to the process of safeguarding data against 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.

Availability

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.

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.



Cyber Security

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"

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.

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.

- 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 centre 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:

- **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.
- **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.
- **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.
- **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.
- **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
- **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.

  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.

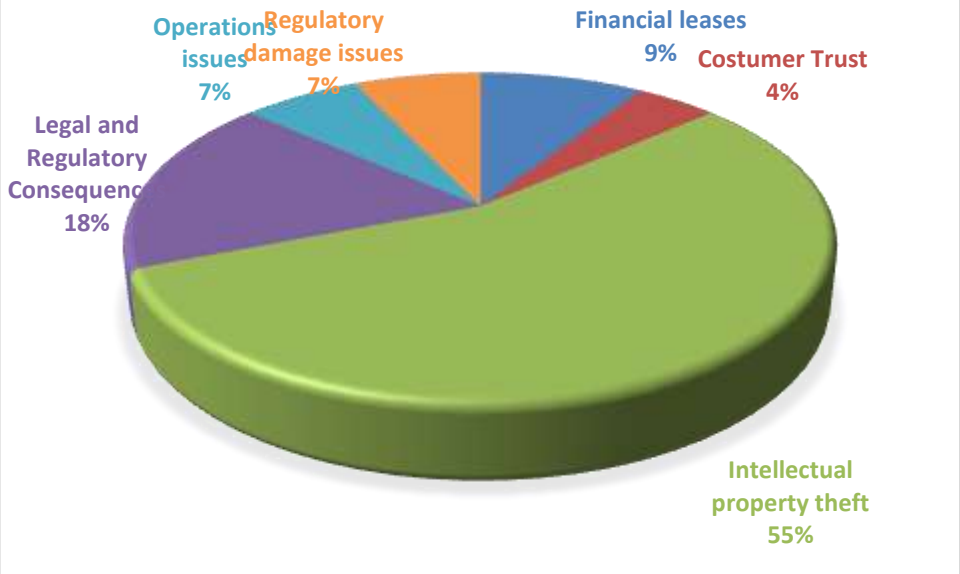
Financial Loss: Businesses that fall victim to cybercrime often have to bear the hefty expenses involved with fixing damage to information technology systems, lost productivity, and legal fees. This can result in a major financial loss for the company. It does not include the amount of money you would 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.
- **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.

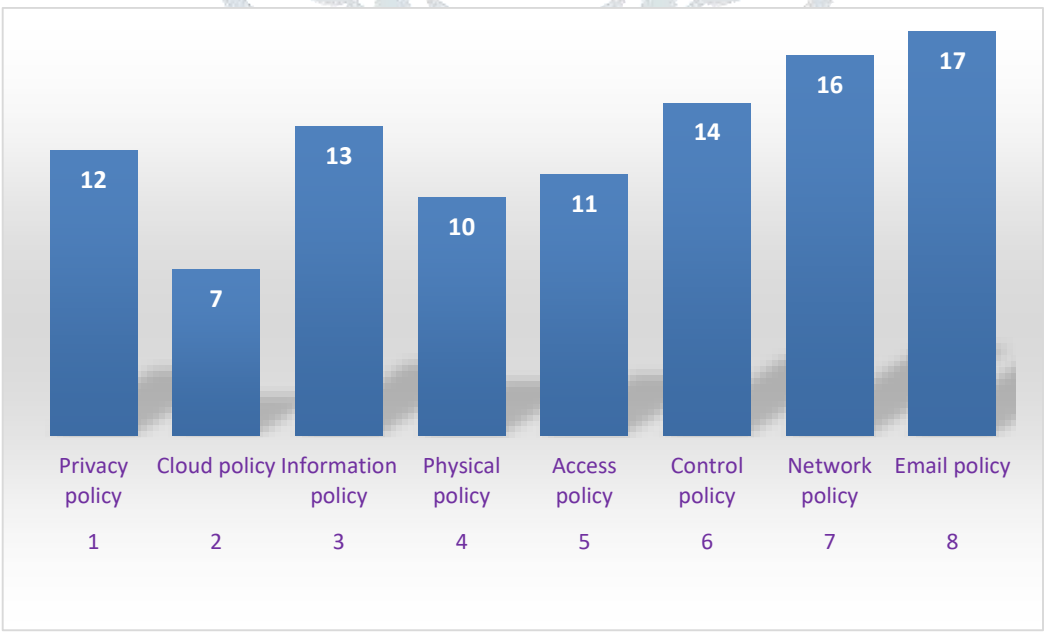
CYBER SECURITY IMPACT LEVEL

Factors	Percentages
Financial leases	18
Costumer Trust	9
Intellectual property theft	111
Legal and Regulatory Consequences	35
Operations issues	13
Regulatory damage issues	14



CYBER SECURITY POLICY LEVEL:

S.No	Cyber security policy	Percentage level
1	Privacy policy	12
2	Cloud policy	7
3	Information policy	13
4	Physical policy	10
5	Access policy	11
6	Control policy	14
7	Network policy	16
8	Email policy	17



RECOMMENTATIONS

- 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 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.

- **Prevention:** Implementing security measures to prevent unauthorized access or breaches.
- **Detection:** Identifying potential threats and vulnerabilities in a system.
- **Response:** Taking necessary actions to mitigate the impact of a security incident.

CONCLUSION

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 defences 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.

REFERENCES

- Jain, A.K., et al. (2021) Biometric Recognition: Challenges in Forensics. http://biometrics.cse.msu.edu.
- Bank of England (2017) Systemic Risk Survey Results—2017 H2. London. https://www.bankofengland.co.uk/systemic-risk-survey/2017/2017-h2
- Clarke, A. and Hancock, J. (2022) Payment System Design and Participant Operational Disruptions. Journal of Financial Market Infrastructures, 2, 1-25. https://doi.org/10.21314/JFMI.2022.023
- Harris, G. (2022) Compsec 2022: Watching the Threat from without Science Direct, Queen Elizabeth II Centre, London, 19
- Joel Kayode Theophilus (2021) The Nigerian Police Cyber Crime Containment Prospects. West African Chief of Police Conference Abuja.
- Von Solms, R. and van Niekerk, J. (2024) From Information Security to Cyber Security. Computers & Security, 38, 97-102. https://doi.org/10.1016/j.cose.2013.04.004