The Role of Cyber security in a Digitalizing Economy: A Development Perspective

Chinyere Iheoma Erondu[1] and Udochukwu Iheanacho Erondu[2]
[1]Department of Sociology, University of Port Harcourt, Choba, Rivers State, Nigeria
[2]Department of Computer Science, Landmark University, Omu-Aran, Kwara State, Nigeria.

DOI: https://dx.doi.org/10.47772/IJRISS.2023.7011121
Received: 13 November 2023; Revised: 06 November 2023; Accepted: 10 November 2023; Published: 18 December 2023

ABSTRACT

A transforming economy undergoes several transformations including digitalization. The 21st-century economy must be driven on the wheels of digital technologies that cannot be wished away. This requires protecting vital information in the digital space with an increasing number of actual cyber-attacks and cyber frauds. The economy remains the base of any society and determines its level of development, any form of compromise in this institution spells doom for its various organizations or arms. There is a need to protect vital information which is key to development in any sector. Therefore, the paper interrogates the importance of securing cyberspace, especially in developing economies. Some prevalent cybersecurity threats include; malware that attacks information systems, information theft, and fraud in cyberspace. It becomes imperative that companies, organizations, individuals, and governments envisage security threats to their vital information and that of their clients and customers; and be proactive in adopting security measures and policies that will ensure the integrity of their information systems and reduce the cost of systems' compromise.

Keywords: Cybersecurity, Digitalization, Economy, Development

INTRODUCTION

The cyber-world is growing to include more and more parts of human organizations, and its importance is no longer hidden by our endless march toward progress. In recent years, the Internet has experienced phenomenal expansion by virtually every metric imaginable. The number of people who use the Internet rose from approximately 360 million in 2000 to nearly two billion by the end of 2010. At the beginning of 1998, fewer than 30 million hosts were connected to the Internet. By the middle of 2010, that number had climbed to approximately 770 million. This global network is estimated by the industry to assist or enable $10 trillion worth of Internet transactions every single year (Mbanaso & Dandaura, 2015). Economies are being pushed toward digital transformation by digitalization and company operations and processes are enhanced in the hopes of long-term gain and cost-optimization. To better serve their clients, several sectors of the economy, especially the corporate sector, are rapidly adopting digital technologies. However, because of the prevalence of technology, problems like cyber-attacks and cyber fraud are also on the rise, and businesses need to be cautious while responding to them. As a result, it is essential to consider the consequences of and mechanisms for cyber security (Ambastha et al., 2021).

In the present-day world, cybersecurity has emerged as a crucial element for ensuring national and global security. The efforts that were made to improve international security on a global scale pushed governments to keep looking for more effective strategies for negotiating peace and resolving conflicts (Stoessinger, 1963). The development of technology, the proliferation of the internet, and increased access to information have all contributed to both beneficial and harmful effects. One of the unintended consequences was a significant rise in the number of new "information" risks. At the tail end of the 1990s and well into the 2000s, there was an exponential rise in the number of computer-related incidents and threats that were

reported to authorities. A significant number of computer events involved the unauthorized disclosure of private information held by businesses operating in a wide variety of fields. Due to the dramatic rise in system vulnerabilities, it is now much simpler to carry out attacks on information systems. This has the effect of making cyberattacks more likely. Inadequate or non-existent information security measures were another contributing factor in the breach of security that allowed unauthorized access to confidential information. One of the most common reasons for unauthorized access and the exploitation of vulnerabilities is a failure to recognize potential dangers and take preventative measures against them (Tarte, 2003). Many companies have been very hesitant to embrace good information security policies to safeguard their firm and their customers' information. The individual parts that constitute information security are intended to deal with and lessen the impact of various threats to information. It is essential for the continued existence of the majority of businesses, as well as the economy as a whole, that information security be incorporated into corporate IT infrastructures, budgets, and strategies.

Since the late 1990s and well into the 2000s, one of the primary concerns of customers has been their right to personal privacy. Concern has been rising in recent years regarding the rising number of cases of reported identity theft and fraud. This rise can be directly attributed to the development and expansion of the Internet's influence in countries all over the world. Consumers have a responsibility to learn about the threats that could lead to these crimes as well as the part they play in preventing them. In addition, customers should exercise extreme caution before disclosing their personal information to businesses that give the impression of not adhering to the normal security standards designed to safeguard information.

For information security to be successful in the present and future economy, it will require the participation of all its stakeholders and the cooperation of those players. It is necessary to have standards and rules in place to offer the appropriate guidance for successfully securing information

Digital Economy

The term "digital economy" is used to describe new forms of business, as well as new markets, products, and services, particularly those that are predicated on the use of digital technologies as an essential component of core corporate infrastructure. The concept of a digital economy relies on the merging and concurrent use of various digital technologies that have been created separately and are now available for utilization. It is also possible to define it as a combination of information, computing, communication, and connectivity technologies. One can argue that exponential advancements in the price/performance capability of computing, storage, bandwidth, and software applications are moving to the next generation of digital technologies to be supplied through cloud computing (Spremić et al., 2018). The rise of digitization and digital business brings a plethora of opportunities for the rapid development of new capabilities and gaining a competitive edge. The digital economy offers the convenience of 24/7 services accessible from the comfort of a customer's bedroom. According to a study conducted in 2017, over 42% of businesses globally were conducted online (Choi, 2017). Leveraging digital solutions and new technologies can potentially overcome major development challenges and contribute to achieving universal access to all business services. Businesses need to keep up with the digital revolution to maintain their competitive edge and ensure their sustainability in the market. The use of big data and digital systems, accessible via the internet and various IT devices, may put at risk the company's ability to maintain its confidentiality. Dispute-related cyberattacks have become the primary threat to businesses and typically come with associated financial implications. There has been a recent uptick in the number of businesses all over the world that have begun to implement artificial intelligence into their daily operations. This is because AI assists businesses in lowering their operating costs, increasing their productivity, and providing the best possible service to their clients (Moşteanu, 2020). Economies have benefited not only from access to new markets but also from the free flow of information that has been made possible by advancements in information technology and the Internet. Businesses can thrive in the new economy, thanks to the accessibility of timely information and the

free exchange of that knowledge. With the help of this information, businesses can improve their decision-making processes and provide more individualized goods and services to the market to satisfy the requirements of specific customers. According to a statement made by James Chessen, a chief economist for the American Bankers Association, "Information Technology has significantly altered how business is conducted in the modern era." Businesses can better regulate their inputs and inventories, as well as experience cheaper expenses associated with advertising and marketing when they have greater access to information (Tarte, 2003).

What is Cybersecurity?

The issue of "cybersecurity" has been the focus of both academic and popular works of writing, the majority of which have taken a singular point of view about the subject matter. The term is employed in a very general sense, and its definitions are quite fluid, dependent on context, frequently subjective, and, at times, uninformative. There is a dearth of published materials that clarify what the phrase "really means" and how it should be understood in a variety of settings. The lack of a concise, generally acceptable definition that captures the multidimensionality of cybersecurity may impede technological and scientific advances. This is because the lack of a definition reinforces the predominantly technical view of cybersecurity, while also separating disciplines that should be working together to resolve complex cybersecurity challenges. For instance, there is a wide range of technical solutions that can be utilized to support cybersecurity. However, these solutions are not sufficient to solve the problem on their own. There are numerous examples and a significant body of scholarly work that demonstrate the challenges related to organizational, economic, social, political, and other human dimensions that are inextricably tied to cybersecurity efforts (Craigen, et al., 2014).

Protecting computer systems, computer networks, and computer programs from being attacked digitally is a technique known as cybersecurity. These types of intrusions typically have one of three goals in mind: gaining access to sensitive information, modifying or destroying that information, extorting money from users in the form of ransomware, or disrupting normal corporate activities.

It can also be defined as the collection of technologies, procedures, practices, responses, and mitigation mechanisms meant to protect networks, computers, programs, and data against attack, damage, or unauthorized access to preserve confidentiality, integrity, and availability (Public Safety Canada, 2014).

In 2014, after an in-depth survey on various definitions of cybersecurity, Craigen, et al., came up with a near-perfect definition and they defined cybersecurity as the organization and collection of resources, processes, and structures that are used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure and de facto property rights. This can happen when de jure property rights are not aligned with de facto property rights.

Economy

The economy stands as the cornerstone of human society, underpinning the very essence of our existence. It orchestrates the orchestration of resources, the production of essential goods and services, and their subsequent consumption, thus safeguarding our continuous survival. This intricate institution juggles an array of activities crucial to the advancement and progress of nations. The decisions forged within this institution hold the key to human welfare, a fact that underscores its prominence in Marxian analysis.

Marx, recognizing the dynamic nature of the economy, positioned it as the superstructure upon which other social institutions are erected. Over the decades, the economic landscape has undergone transformative shifts and continues to evolve. The infusion of various digital technologies into the operations of post-industrial societies attests to this reality. Developing economies are rapidly closing the gap with their more

advanced counterparts in adopting digital tools to manage their economies. Remarkably, even in rural areas, digital technologies are reshaping the landscape of everyday business operations.

This evolution underscores the pressing need for rigorous cybersecurity measures to safeguard cyberspace. Ensuring its security is not only vital for reaping the full benefits of digital technology but also for averting potential losses stemming from cyberattacks, threats, and fraudulent activities.

Development implications of cybersecurity

Development conceptions are diverse and many, shaped by the multifaceted nature of the phenomenon and the perspectives of various authors and philosophers in the realm of development discourse. From this vantage point, the authors perceive development as an ongoing process that encompasses improvements in all aspects of society, with the overarching goal of enhancing the quality of life for individuals. This extends to economic well-being, political stability, education, healthcare, the judiciary, and even religious aspects.

In alignment with this view, Thomas (2010) posits that development is a multi-dimensional process involving substantial changes in social structures, public attitudes, and national institutions. It also entails accelerating economic growth, reducing inequality, and eradicating poverty. Sen (1999) expands this perspective by emphasizing that development equates to freedom from various constraints, enabling individuals to enjoy greater well-being and autonomy in their life choices.

Todaro and Smith (2004) as cited in Thomas (2010) describe development as the sustained elevation of an entire society and its social system toward a better and more humane life. In this context, it becomes evident that cybersecurity plays a pivotal role in sustainable development. As we intensify the digitalization of the economy, akin to more advanced nations, it is imperative to prioritize the security of information systems within institutions, particularly in the face of escalating cyber threats.

Compromised cyber security is, without a doubt, the swiftest way to impede the development process, given the substantial losses it often incurs. In the banking sector, substantial financial losses have been incurred due to cyberattacks on financial institutions. Cybercriminals continually seek ways to breach information systems, acquire account holder information, and employ it for nefarious purposes, including fraud. Academic institutions have also fallen victim to data breaches, where hackers unlawfully access the personal information of both staff and students for fraudulent activities.

Instances such as the compromise of the Integrated Personnel Payment Information System (IPPIS) salary payment platform for Federal Government employees in Nigeria underscore the magnitude of the problem, resulting in significant financial losses to scammers. The recent suspicion of compromised cyberspace at the Independent National Electoral Commission (INEC) of Nigeria serves as a stark reminder of the severe consequences such abuses can bring about.

Despite the potential for significant losses, the digitization of the economy must be encouraged, albeit with the necessary precautions to ensure cyber security. In a digitally driven society, all sectors are affected, as information is vital to their functioning. Therefore, securing information systems is paramount, particularly in the context of numerous existing threats and challenges in many developing economies worldwide. Any cyber security threat is an additional burden requiring immediate attention.

When critical information is compromised in any sphere of society, it not only reflects underlying fundamental issues that challenge societal values but also has far-reaching effects that transcend boundaries. For instance, in Nigeria's recent presidential election in 2023, allegations of compromised cyberspace at the Independent National Electoral Commission (INEC) have raised questions about the accuracy of the election results. This has led to widespread protests, legal battles, and increased societal tension, impacting

both time and resources. Furthermore, compromised cyber security has affected various institutions, including educational bodies like the Joint Admission and Matriculation Board (JAMB), West African Examination Council (WAEC), and National Examination Council Organization, undermining the integrity of these institutions.

Addressing these cyber security challenges is crucial for the sustainable development of nations. The following sections will explore potential solutions and strategies to mitigate these issues and ensure the safe and secure progression of society in the digital age.

RELATED WORKS

The value of the cybercrime sector reached a record high of 450 billion US dollars in 2016. According to some records, the annual cost of cybercrime around the globe has reached 575 billion USD. The combined amount lost as a result of cybercrime in the world's four leading economies (the United States, China, Japan, and Germany) reached a staggering USD 200 billion. In the context of cybercrime, a loss is not limited to the actual damages that have been incurred as a result of an attack; rather, it also includes recovery and opportunity costs (Morgan, 2020). According to a study conducted in Italy (Teoh & Mahmood, 2018), the amount of money lost due to cybercrime was 875 million US dollars, while the cost of recovery and opportunity lost was 8.5 billion US dollars. On the other hand, there are research results that conflict with one another, which question the idea that the cost of events is approximately equal to its annual investment in IT security. According to the findings of the study, the costs are broken down into first- and third-party losses. The reputation of a corporation, its goodwill, and its stock values are all negatively impacted by cybercrime.

Cyber threats pose a significant danger to all levels of society, including the government, organizations, and individuals. There is a concerning lack of skilled professionals and academic programs that can develop and generate these professionals. This shortfall is alarming. This is seen as a crisis in human capital by several countries, notably the United States and New Zealand. In this article, we analyze the severity of the issue as well as its many different facets. In this study, an examination of data collected on cyber-attacks by a research center specializing in cyber security is presented, along with the proposal of some practical solutions and the elaboration of several cases originating from New Zealand. The report presents its findings by drawing inferences from a comparison of the data gathered on New Zealand and Japan (Fourie et al., 2014).

In this day and age of constant cyberattacks, Dr. Catherine Mulligan (2017), a Research Fellow in the Department of Innovation and Entrepreneurship who also holds a joint appointment in the Department of Computing, discusses the importance of cybersecurity that is both effective and manageable.

It is becoming increasingly obvious that the world needs more advanced cybersecurity that can also be easily managed as the rate of digitalization continues to rise. Since 2010, one of the top four threats to UK national security has been identified as cyber-attacks. In light of recent happenings, such as a string of company hackings and the possibility of interference with the election in the United States, it appears that this kind of activity is only going to increase. In the same way that digital disruption has opened the door to a wealth of new opportunities for the development of business models, it has also made it possible for new forms of aggression to be launched against corporations, cities, and even nations (Jang-Jaccard & Nepal, 2014)

It is important to note that problems with security are not just caused by malevolent threats like criminals, so-called "hacktivists," and hostile nation governments. A vital component of assuring the security of systems is making certain that the code performs as it was designed to. Incorrectly written code can result in flaws in smart city systems, which have the potential to result in catastrophic industrial accidents or even the

loss of human lives. The importance of cyber security to the digital economy cannot be overstated. Without it, some of the most fundamental pillars of our economic system, such as our ability to trust the data and information that are provided to us by our banks and enterprises, as well as the dependability of the sources that we use to obtain our news, would be called to question.

In 2013, the President of the United States signed an executive order that was intended to assist in protecting the key infrastructure of the country against cyberattacks. As part of his directive, he instructed the National Institute of Standards and Technology (NIST) to create a framework that would serve as a reliable source for information security best practices. It's important to note that participation in the framework is completely optional. It won't be easy to motivate businesses to go along with it. Will frameworks like the one that the NIST has advocated truly cause companies to implement better security controls? If not, then why not? (Foreign Policy Cyber Security Executive Order 13636, n.d.). This study investigated the nature and costs of cyberattacks, and it also tried to determine whether or not there are financial incentives for businesses to strengthen their security protocols and cut the likelihood of being targeted by hackers. To be more specific, a sample of over 12,000 different types of security breaches was taken. First, the researchers conducted an investigation into the nature of these security breaches (such as causes and types of information compromised). The next step was to analyze the number of data breaches and lawsuits filed, sector by sector, to determine the sectors that bear the highest financial burden as a result of cyberattacks. After that, they compared these expenses to those of other industries' bad debts and fraudulent activity. The findings indicate that public concerns regarding the rising frequency of data breaches and legal actions may be exaggerated in comparison to the very little financial impact that these occurrences have on businesses that are affected by them. The public's concerns about the rising number of data breaches and legal actions are at odds with the findings of their study as stated in their research report, which demonstrate a significantly reduced monetary impact on businesses that are affected by such occurrences. Furthermore, it was stated that the cost of an average cyber event in their sample is less than $200,000 (which is around the same as the company's yearly budget for IT security) and that this only accounts for 0.4% of their expected annual revenues (Romanosky, 2016).

In the 21st century, a severe obstacle to the operations of businesses has emerged in the form of data breaches. Organizations leave themselves vulnerable to potential cyber threats due to a lack of awareness of cybersecurity. As a result, the purpose of this research was to determine the many facets of capacities related to cybersecurity awareness. The findings of the study, which were based on the dynamic capabilities framework, showed that personnel capabilities (knowledge, attitude, and learning), management capabilities (training, culture, and strategic orientation), and infrastructure capabilities (technology and data governance) are three thematic dimensions that can be used to address challenges related to cybersecurity awareness (Akter et al., 2022).

The dynamic nature of the relationship that exists between businesses and their clientele today is what drives home the importance of fostering digital trust between the two parties. The rate at which customers are becoming connected to internet businesses today is increasing at a rapid pace, and the speed at which internet businesses are becoming faster and more conventional globally has provided internet-based businesses with the best possible opportunities in the field of e-commerce. The commercial operations that currently take place online will, in the not-too-distant future, constitute the overwhelming majority of those in developing countries. However, for these kinds of online businesses to thrive and advance, consumer loyalty is required. This can be accomplished through the development of digital trust, which gives customers more confidence in the services and business partners they work with while reducing the associated risks (Shalhoub & Al Qasimi, 2010).

In the 21st century, one of the most current topics of worry for national and global security is cybersecurity. [Cybersecurity] At the individual, enterprise, and national, levels, as well as at the international level, it is an

essential component of security in both the public and private sectors. (Mat et al., 2019) carried out a study and they opined that Malaysia is one of the economies that are undergoing an economic transition towards digital activities as the current economy in these rising economies shifts. A safe and secure online environment is fundamental to effective cybersecurity and is required for the development of a thriving digital economy. The purpose of this study was to investigate the role that ensuring a safe and secure online environment, often known as cybersecurity, plays in fostering a digital economy in Malaysia by creating a trusted legal framework for businesses and their customers. The problem at hand is the potential for exposure to danger in cyberspace, which translates to the fact that there are actual dangers to information security. The research was conducted using a qualitative approach to the gathering and analysis of data. The data were analyzed using content analysis, and thematic analytical interpretations were utilized during the process. The data were gathered from both primary and secondary sources. According to the findings of the research study, the level of cybersecurity in Malaysia is good and suffers from than in other countries. Nevertheless, there are still threats and vulnerabilities that could have an impact on digital trust and digital business. As a result, it is proposed that the rules on digital trust and cybersecurity should be harmonized, and public awareness should be reinforced, to reduce the risk as much as possible and to be ready for anything that may occur in the future.

Fintech technologies and the transformation of digital systems have become the most widely used words in the past decade, and they have a direct impact on the organizational structure and design of any firm. The business process is altered as a result of the reorganization of the values. The study emphasizes that for organizational structures to remain competitive and achieve market longevity, they need to keep up with the digital transformation and implement new security systems to face exposure to cyberattacks. This is one of the main points that the study makes. It is related to the adoption of innovation and the adoption of digital changes into organizational culture and the redesign of an organization's structure that the safeguarding of data (such as financial and client information), the improvement of performance, and the survival of institutions is related to. The purpose of the article is to demonstrate how digital transformation and the adoption of new technologies have changed the approach that is taken toward the requirements of jobs on a global level. Specifically, the article focused on how the organizational structure can be improved to better deal with actual challenges, such as cyberattacks. The author rethinks an organizational structure by taking into account the difficulties posed by new technologies and the introduction of new functions to demonstrate the importance of making changes to the business process. To mitigate the potential for operational hazards, the change that has been suggested for the redesign of the organizational structure is centered on striking a balance between the distinctiveness and integration among the specialized divisions (Mosteanu, 2020).

Cybersecurity incidents related to information technology have undergone a significant transformation over the past few decades. Previously, these incidents were isolated attacks on information systems. However, nowadays, they are planned, targeted, and highly sophisticated cyber threats at the individual, institutional, or even national level. While digital technologies offer various benefits, they also introduce a range of new risks that have severe consequences. Even though these terms are sometimes used interchangeably, cyber security and information security are not the same thing. (Spremić, 2018) in an article titled "Cyber security challenges in a digital economy", This article explored the transition from information security to cyber security, primarily as a shift in the paradigm of how protection should be approached against continuing threats. During the era of information security, it was sufficient for organizations to conduct basic protection against "common" attacks. However, during the era of cyber security, organizations are required to implement controls that are smart, innovative, and efficient to detect and prevent advanced and emerging cyber-attacks. It is no longer acceptable for IT departments or appointed persons (Chief Information Security Officers (CISOs) to bear the entire responsibility for cyber security activities. Instead, these activities should be institution-wide efforts in which all employees participate. In the same way that the strategic alignment of digital technologies with company strategy is being done, the same should be done with cyber security. The researchers carried out some preliminary studies to determine the degree to which

security measures at large firms in Croatia are developed about significant or vital aspects of the nation's infrastructure. They concluded that fundamental protection is effective; however, there is still potential for development in establishing a collective aspiration toward holistic cybersecurity governance and employing more advanced controls.

The era of the "digital age" brings about rapid changes that can be seen in various aspects such as connectivity, integration, supply chain management, models, and others. As a direct consequence of this, security is a very lucrative business. Securing vital information, operations, and the consumer profile goes beyond the four walls of physical security. It is necessary, as a result, to reconsider the meaning of the term "security" and to strengthen the resistance of technological systems. Both information technology (IT) infrastructures and electrical systems are part of the electric power system. These systems include cyberspace, people, physical systems, and money. There are three main categories of risks: physical, internal, and external, and cyber dangers can come from any direction. Dealing with cybercrime and cyberattacks directed at the energy sector presents significant issues in and of themselves. These dangers can only be minimized; they cannot be removed entirely. Threat mitigation incurs costs in terms of both money and effort, as well as downtime and economic and psychological implications on the sector as a whole. These effects have the potential to harm both corporate performance and national economies. The purpose of this study is to draw attention to the numerous security threats posed to the energy infrastructure and the consequential effects on the economy. The study not only analyzes economics but also proposes a mechanism and highlights the importance of global security coordination to decrease the likelihood of attacks. (Venkatachary, 2017).

MATERIALS AND METHODS

Research in previously published works formed the basis for this article. The researchers gathered material from a wide variety of published sources, including scholarly journal articles, international reports, textbooks, recent developments in relevant industries, and emerging patterns in markets. After the literature had been collected, the researchers went through them to decide which ones were relevant to the topic at hand to finalize the representative literature (Teoh & Mahmood, 2018). The selected works of literature were evaluated for their relevance based on criteria like purpose, authority, efficacy, and reliability. Since the problems relating to cybersecurity are timely and always evolving, the writings on the subject need to be up to date for them to be relevant. In this investigation, reputable papers, journal articles, and news articles on technological developments were used. It offers an analysis of the most recent procedures and advancements in the field of cybersecurity.

CONCLUSION

An analysis of the information gathered shows that cyber threats and attacks are real and manifest. They come in various forms capable of compromising the integrity of information systems and thereby causing huge losses to victims, individuals, and corporate entities. The development implications are adverse and make efforts to improve production and service delivery using digital technologies futile. Cyber insecurity can lead to financial losses, stagnation, and loss of opportunities in economic development and progress in other spheres of society. Incorporating security in cyberspace is vital to forestalling compromises, ensuring the protection of confidential information and the right to privacy, preventing fraud, and maintaining the general integrity of systems of information anywhere found. This way, the gains of applying digital technology to economic development will fully be harnessed.

In this study, the importance of cybersecurity is highlighted in the context of our increasingly digital world. It discusses several key findings and emphasizes the significance of cybersecurity for various aspects of society, including economic development. The study highlights the expanding digital world, underlining the

rapid growth of the Internet and its significant role in facilitating trillions of dollars in annual transactions. It emphasizes the economic transformation driven by digitalization and the adoption of digital technologies across various sectors. With this digital progress, the text points out the increasing challenges posed by cyber threats, including cyberattacks and cyber fraud. In this context, the importance of understanding the consequences of cyberattacks and implementing robust cybersecurity measures is paramount.

Furthermore, the study stresses the critical role of cybersecurity in ensuring both national and global security in our present world. It acknowledges the positive and negative impacts of technology proliferation and emphasizes the rise in "information" risks. With the digital economy on the rise, the study underscores the opportunities it offers and the importance of businesses embracing digital solutions to remain competitive.

The study distinguishes between information security and cybersecurity and highlights the need for smart and efficient security measures to address advanced cyber threats. It also underscores the significance of cybersecurity awareness, involving employees, management, and infrastructure capabilities to tackle cybersecurity challenges effectively.

Also, this study highlights the importance of fostering digital trust in customer-business relationships and its role in reducing risks and ensuring customer loyalty. It connects cybersecurity to development, emphasizing that compromised cybersecurity can hinder the development process, especially in sectors like finance and education.

Finally, the study suggests the need for global security coordination to minimize threats and attacks on critical infrastructures while recognizing the reality that such threats cannot be entirely eliminated. Overall, the study underscores the vital importance of cybersecurity in our increasingly digital world.

RECOMMENDATIONS

The following recommendations are suggested based on the findings of this study according to the order of priority:

Increase Awareness and Education: Develop comprehensive cybersecurity awareness programs and educational initiatives targeting individuals, businesses, and organizations. This would help in promoting a culture of cybersecurity and ensuring that people are equipped with the knowledge and skills to identify, prevent, and respond to cyber threats. Comprehensive cybersecurity awareness programs should encompass a variety of strategies and resources to effectively educate and empower individuals, businesses, and organizations. Here are some key components that such programs might include:

- **Cybersecurity Training Workshops**: Offer hands-on workshops and training sessions covering essential cybersecurity topics. These workshops can range from basic cybersecurity hygiene for beginners to advanced training for IT professionals.
- **Online Learning Platforms**: Develop online courses, webinars, and e-learning modules that are easily accessible to a broad audience. These can cover topics such as password management, email security, safe browsing, and more.
- **Awareness Campaigns**: Launch public awareness campaigns that focus on the importance of cybersecurity. These campaigns can use various media channels, including social media, websites, and traditional advertising.
- **Cyber Hygiene Best Practices**: Provide clear and concise guidelines on fundamental cyber hygiene practices, such as regularly updating software, using strong passwords, and enabling two-factor authentication.
- **Security Toolkits:** Offer toolkits and resources that individuals and organizations can use to assess

their cybersecurity readiness. These toolkits can include checklists, assessment tools, and guidelines for improving security.

- **Threat Alerts and Updates**: Keep participants informed about the latest cybersecurity threats and vulnerabilities. Provide regular updates on emerging threats, scams, and techniques used by cybercriminals.
- **Implement Effective Security Measures**: Establish robust cybersecurity measures suiting an organization, including the adoption of advanced security technologies, regular security audits, and penetration testing. This would help in protecting information systems, networks, and data from cyber threats. Here are some specific security measures and technologies that organizations should consider implementing:
- **Firewalls:** Deploy both network and host-based firewalls to monitor and filter incoming and outgoing network traffic. Next-generation firewalls offer advanced threat detection and intrusion prevention capabilities.
- **Antivirus and Anti-Malware Software**: Use up-to-date antivirus and anti-malware solutions to detect and remove malicious software, including viruses, worms, and spyware.
- **Intrusion Detection and Prevention Systems (IDPS)**: Employ IDPS to monitor network and system activities for suspicious behavior and automatically respond to potential threats.
- **Data Encryption**: Encrypt sensitive data both at rest and in transit using strong encryption algorithms. This includes using HTTPS for web traffic and encrypting files and databases.
- **Multi-Factor Authentication (MFA):** Require MFA for accessing critical systems and accounts. MFA adds an extra layer of security by confirming users' identities through multiple authentication methods.

Invest in Research and Development: Government and private sectors should allocate resources for research and development in the field of cybersecurity. Promote innovation in developing new technologies, tools, and methodologies to combat emerging cyber threats effectively. Here are some ways governments and the private sector can incentivize and support cybersecurity research and development:

- **Grants and Scholarships**: Establish grant programs and scholarships to support cybersecurity research at universities and research institutions. These financial incentives can encourage students and researchers to pursue cybersecurity-related projects
- **Research Grants**: Provide research grants to cybersecurity experts, startups, and established companies to fund innovative projects. Government agencies, private foundations, and industry associations can offer these grants.
- **Tax Credits and Incentives**: Governments can introduce tax credits or financial incentives for private sector organizations that invest in cybersecurity research and development. These incentives can offset some of the costs associated with R&D efforts.
- **Collaborative Research Centers**: Establish collaborative research centers where government agencies, private sector organizations, and academic institutions work together on cybersecurity projects. These centers can facilitate knowledge sharing and joint research efforts.
- **Curriculum Development**: Work with universities to incorporate cybersecurity into their curricula, ensuring that students receive up-to-date training and knowledge in the field.
- **Transfer Mechanisms**: Establish mechanisms for transferring cybersecurity research outcomes from academic and government research institutions to the private sector, allowing for practical implementation.
- **Collaborate Globally**: Engage in international partnerships and collaborations to share resources, expertise, and research findings in the global fight against cyber threats.

Foster Collaboration and Information Sharing: Encourage collaboration and information sharing among stakeholders, including government agencies, private sector organizations, and cybersecurity experts. This

would facilitate the exchange of intelligence, best practices, and emerging threat insights, leading to more effective cybersecurity strategies. Here are some ways to facilitate collaboration between stakeholders:

- **Information Sharing and Analysis Centers (ISACs):** ISACs are industry-specific organizations that allow private sector entities to share threat intelligence, best practices, and cybersecurity information within their respective industries. Different sectors, such as finance, healthcare, and energy, have their own ISACs.
- **Government-Private Sector Partnerships**: Governments can establish partnerships with private sector organizations, creating platforms for sharing threat information. In the United States, for example, the Department of Homeland Security (DHS) collaborates with private sector entities through programs like the Enhanced Cybersecurity Services (ECS) initiative.
- **Cybersecurity Conferences and Workshops:** Participating in or hosting cybersecurity events, conferences, and workshops can bring together experts, government agencies, and private sector representatives to discuss emerging threats and best practices. Examples include the RSA Conference and DEFCON.
- **Threat Intelligence Sharing Platforms:** Consider using threat intelligence sharing platforms and services like the Cyber Information Sharing and Collaboration Program (CISCP) or Information Sharing and Analysis Organizations (ISAOs) that allow organizations to share and receive real-time threat information.
- **Public-Private Initiatives**: Explore public-private initiatives and partnerships that encourage collaboration. These initiatives can include joint cybersecurity exercises, threat information-sharing initiatives, and industry-specific task forces.
- **Cybersecurity Information Sharing Portals**: Governments and industry groups can develop dedicated online portals where organizations can share threat intelligence and access up-to-date information on emerging threats.
- **Cross-Industry Information Sharing**: Encourage information sharing not only within specific industries but also across industries to gain a broader perspective on emerging threats and vulnerabilities.

Strengthen Legal and Regulatory Frameworks: Enhance existing laws and regulations relating to cybersecurity to address the evolving nature of cyber threats. This includes promoting international cooperation in prosecuting cybercriminals, ensuring adequate punishment for cyber offenses, and protecting victims' rights.

Enhance Incident Response and Recovery Capabilities: Establish robust incident response and recovery mechanisms to minimize the impact of cyber-attacks. This includes developing incident response plans, conducting regular simulations and exercises, and establishing partnerships with cybersecurity incident response teams. To establish robust incident response and recovery mechanisms, organizations should create dedicated Incident Response Teams (IRT) composed of trained members from various fields. They should develop detailed response plans, conduct regular exercises, and define clear communication protocols for both internal and external stakeholders. Additionally, maintaining thorough incident documentation, collaborating with external IRTs, and continuously improving the response process are essential. Investment in advanced security technologies, data backups, and legal compliance is crucial. Lastly, establishing clear incident reporting mechanisms helps identify and assess incidents promptly. These measures collectively enable organizations to effectively manage cyber incidents and enhance their overall cybersecurity posture.

Foster International Cooperation: Collaborate with international organizations, governments, and industry forums to address global cybersecurity challenges. This includes sharing threat intelligence, harmonizing cybersecurity standards, and promoting international norms and agreements. To foster international cooperation, governments can take a lead role by facilitating diplomatic efforts, negotiations,

and the establishment of international agreements and norms. They should actively share threat intelligence and cooperate with international law enforcement agencies to combat cyber threats.

Private sector organizations can contribute by actively participating in industry forums and working groups focused on cybersecurity. They should collaborate in sharing threat intelligence and best practices, while also ensuring their own systems adhere to international cybersecurity standards

Industry forums play a vital role in bringing stakeholders together. They can provide a platform for discussions, promote the sharing of best practices, and encourage the development of common standards. These forums facilitate dialogue and coordination among governments, organizations, and experts to address global cybersecurity challenges effectively. In this way, each stakeholder plays a distinct role in fostering international cooperation, contributing to a more secure cyberspace.

By implementing these recommendations, the study can contribute to strengthening cybersecurity measures and mitigating the adverse effects of cyber threats on individuals, businesses, and society as a whole, this will impact positively the development status of developing economies.

REFERENCES

1. Akter, S., Uddin, M. R., Sajib, S., Lee, W. J. T., Michael, K., & Hossain, M. A. (2022). Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. Annals of Operations Research, 1-26.
2. Ambastha, A., Desai, K., Patil, P., Chavan, O., Dodia, H., Jhawar, S., &Parihar, M. (2021, September). Implication of Cyber Security in a Digital Economy: Learning from Corporate Sector with Special Reference to BFSI. In The International Conference On Global Economic Revolutions (pp. 543-552). Springer, Cham.
3. C. (2018, February 21). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybercrime Magazine. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
4. Choi, K. (2017). 99 Facts on the Future of Business in the Digital Economy 2017. Retrieved at https://www.slideshare.net/sap/99-facts-onthe-future-of-business-in-the-digital-economy-2017).
5. Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review, 4(10).
6. Fourie, L., Pang, S., Kingston, T., Hettema, H., Watters, P., &Sarrafzadeh, H. (2014). The global cyber security workforce: an ongoing human capital crisis.
7. Foreign Policy Cyber Security Executive Order 13636. (n.d.). The White House. https://obamawhitehouse.archives.gov/node/298406
8. Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of computer and system sciences, 80(5), 973-993.
9. Karake-Shalhoub, Z., & Al Qasimi, L. (2010). Cyber law and cyber security in developing and emerging economies. Edward Elgar Publishing.
10. Mat, B., Pero, S., Wahid, R., &Sule, B. (2019). Cybersecurity and digital economy in Malaysia: Trusted law for customer and enterprise protection. International Journal of Innovative Technology and Exploring Engineering, 8(3), 214-220.
11. Mbanaso, U. M., & Dandaura, E. S. (2015). The cyberspace: Redefining a new world. IOSR Journal of Computer Engineering, 17(3), 17-24.
12. Moşteanu, N. R. (2020). Challenges for organizational structure and design as a result of digitalization and cybersecurity. The Business & Management Review, 11(1), 278-286.
13. Mulligan, C. (2017). Cybersecurity: the cornerstone of the digital economy. Imperial College Business School London.
14. Public Safety Canada. 2014. Terminology Bulletin 281: Emergency Management Vocabulary. Ottawa: Translation Bureau, Government of Canada. http://www.bt-tb.tpsgc-

pwgsc.gc.ca/publications/documents/urgence-emerge…
15. Romanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), 121-135.
16. Sen, A. (1999). Development As Freedom. Anchor Books.
17. Spremić, M., & Šimunic, A. (2018, July). Cyber security challenges in the digital economy. In Proceedings of the World Congress on Engineering (Vol. 1, pp. 341-346). Hong Kong, China: International Association of Engineers.
18. Stoessinger, J. G. (1963). Discord and Collaboration: Essays on International Politics. By Arnold Wolfers. (Baltimore: The Johns Hopkins Press, 1962. Pp. xvii, 283. $6.00.). American Political Science Review, 57(2), 451-452.
19. Tarte, J. (2003). The Need for Information Security in Today's Economy. Accessed May 5, 2003.
20. Teoh, C. S., & Mahmood, A. K. (2018). Cybersecurity workforce development for the digital economy. The Educational Review, USA, 2(1), 136-146.
21. Thomas, A. N. (2010). The Praxis of Development and Underdevelopment. Ethiope Publishing Corporations.
22. Venkatachary, S. K., Prasad, J., & Samikannu, R. (2017). Economic impacts of cyber security in the energy sector: A review. International Journal of Energy Economics and Policy, 7(5), 250.