Global Scientific JOURNALS

GSJ: Volume 12, Issue 5, May 2024, Online: ISSN 2320-9186
www.globalscientificjournal.com

CYBER SECURITY CHALLENGES IN A SMART AND DIGITAL ECONOMY: A preliminary research overview of the emerging threats to data stored in information systems.

Dr. Ifeanyi Stanly Nwokoro – Senior Lecturer, Rhema University Nigeria – ifeanyinwokoro@gmail.com

Muhammad Qaim Aliyu Sambo – Principal Consultant, Five Stars ICT Ltd – qaeeemsambo@gmail.com

Ifeanyi Friday Eze – First Bank Nigeria – ifeanyieze50@gmail.com

Sanusi Yusuf Ahmed – Bank of Industry – ayusufsanusi@hotmail.com

Timothy Ola Akinfenwa – Osun State University – lordaikins@gmail.com

Zacciah Kwaku Adom-Oduro – University of Professional Studies Accra – okwadom@gmail.com

George Oshodin Osakpamwan – Addbeams Nig Ltd – osakpamwan.oshodin@gmail.com

Augustina N. Nwatu – Senior Technologist, Alex-Ekwueme Federal University – tenacious_nwatu@yahoo.com

ABSTRACT

IT security incidents have evolved over the past few decades from isolated information system attacks to deliberate, focused and complex cyber dangers at even national, institutional or individual level. Digital technology's interconnectedness has many advantages, but it also creates a number of new risks that have broad ramifications. Even though the phrases are sometimes used synonymously, information security and cyber security are not the same. The transition from information security to cyber security was covered in this study, primarily as a paradigm shift in the defense against persistent threats. While it was sufficient to undertake basic defense against "common" attacks in the information security era, organizations now need to develop clever, creative, and effective controls to identify and stop sophisticated and emerging cyber-attacks. Cyber security initiatives should now involve the entire organization, including participation from all staff members, rather than just IT departments or designated persons. Cyber security should be strategically connected with corporate strategy, just as digital technologies are. We have carried out preliminary research on the level of maturity of security measures in Nigerian large firms that are associated with vital or significant national infrastructure. We concluded that while basic protection works well, there is still space for improvement when it comes to implementing more sophisticated controls and pursuing a shared goal of comprehensive cyber security governance.

Keywords: Cyber Security, Cyber Threats, Smart Economy, Digital Transformations

1.0 INTRODUCTION

The term "digital economy" was introduced by Don Tapscott in 1995 in his book "The Digital Economy: Promise and Peril in the Age of Networked Intelligence." It encompasses emerging markets, products, and services that are built upon digital technologies as a fundamental business framework [1, 2]. The digital economy is built around the concurrent use and integration of several independently produced digital technologies that are accessible for usage. According to Bharadway [3], digital technologies are a fusion of information, computer, communication, and networking technologies. They argue that the advancement of cloud computing will bring out the next wave of digital technologies. This progress is fueled by significant improvements in the cost-effectiveness and performance of processing, storage, bandwidth, and software applications.

Emerging digital technologies, including cloud computing, drones, sensors, mobile technology, Internet of Things (IoT), augmented reality (AR), big data, cognitive technologies (AI), robotics, addictive manufacturing (3D printing), and others, have the capability to gather data from physical devices (such as sensor data on the condition of the device), swiftly distribute it using mobile technologies, store it in the cloud, analyze it in real-time using advanced analytics and big data, and seamlessly integrate products, services, and processes. If these technologies are used in conjunction with strategic goals and implemented in a coordinated and planned fashion, they have the potential to disrupt traditional business models [4].

Digital technologies, in contrast, have an external focus, connecting gadgets and offering excellent digital services to improve the consumer experience. IT initiatives, in contrast, have an internal emphasis and aim to align with existing business processes. A recent survey performed by Bonnet et al. [5] has shown that more than 90% of firm leaders in the United States and the United Kingdom anticipate that IT and technological innovations will play a more prominent strategic function in their overall business practices over the course of the next ten years. Leadership has prioritized digital transformation as a top item on their agenda. Nevertheless, these activities will subject them to an array of new risks, such as cyber security threats. Businesses are using cutting-edge digital technology to foster innovation, which is causing a change in the nature of IT security events. There is now a stronger focus on advanced and externally-targeted assaults, often referred to as cyber incidents.

It seems that many people still mistakenly consider information systems (IS) and the underlying IT and digital technologies as a distinct entity within a business, resulting in a separate perception of risk, control, and security. However, the nature of IS security incidents and associated risks has undergone significant changes in recent decades. A decade or two ago, a security incident in the field of information systems could have resulted in minor technical problems. However, in today's advanced and intentional cyber-attacks, these incidents have the capability to cause extensive damage, incur substantial direct and indirect expenses, and harm a company's competitive standing and strategic objectives [6].

According to a study conducted by PricewaterhouseCoopers, companies that had cyber security events incurred an average loss of 2.1% of their overall worth. On average, each incident resulted in a loss of approximately 1.6 billion USD. Due to the interconnectedness of digital technology, cyber security breaches may cause significant harm to both enterprises and people, including phishing attempts and identity theft. In addition, these occurrences may also present dangers at the national, regional, and municipal levels, such as assaults sponsored by governments, organized criminal organizations, and the exploitation of weaknesses in "intelligent" equipment to get unauthorized entry to data, control systems, or vital national infrastructure.

Back in the past, namely fifteen years ago, when the focus was on "information security," the occurrence of this was less probable. According to a recent World Economic Forum report [8], one of the top five most significant threats the world is currently facing is a significant cyber security compromise. The threat's scope is predicted to increase significantly [9]; by 2025, the expected global cost of cyber security breaches would quadruple from the 2020 figure which is estimated to be US$18 trillion.

This article will present an overview of the changing nature of security events, starting with common assaults and IT incidents that occur inside an organization's IT system, and progressing to more complex and emerging cyber attacks that target the organization from external sources in the digital world. We will discuss the differences between cyber and information security, as well as tactics for protecting against persistent online attacks. In order to effectively regulate cyber events, it is necessary to adopt a more complete approach due to their targeted nature, advanced techniques, and difficulty in detection and prevention [10]. The primary objective of cyber security management is to strategically design and implement essential safeguards against common assaults, while also using innovative, discerning, and advanced security protocols to detect and mitigate more intricate and evolving threats.

2.0 CYBER SECURITY VERSUS INFORMATION SECURITY

The interconnectivity of various digital technologies and critical infrastructure systems has led to the emergence of much new vulnerability that might have extensive and major implications. Cyber security is a component of information security, since the term "cyber" is often used in a wide manner, mostly due to the growing intricacy of digital information in the modern day [11]. Cyber security focuses largely on addressing deliberate, advanced, and challenging to identify or control types of attacks, breaches, or incidents. Cyber security extends beyond the mere safeguarding of cyberspace. Additionally, it entails protecting those who use it and whatever resources they own that may potentially be obtained via it [12]. Cyber security, as defined by ISACA [13], is the act of safeguarding information assets from possible attacks that may target data processed, stored, and sent via networked information systems. Cyber security is the field that deals with creating and executing strategies to safeguard persons and businesses against deliberate assaults, breaches, incidents, and their subsequent outcomes.

Over the last fifteen years, several challenges have arose that impact the transition from information security to cyber security. These issues involve an increase in internal risks, including incidents of internal information leaks, unauthorized access to data, and intentional attacks that come from within emerging technologies, particularly digital technologies that are focused on external connectivity and allow ongoing interaction between different devices (such as cloud computing, sensors, and the Internet of Things). These technologies have increased the susceptibility to viruses and data breaches from external sources. According to ISACA [14], the total cost of a single data breach, which includes both direct and indirect losses, exceeded 5.5 million USD. However, according to Ponemon Institute [15], the direct costs of a data breach in 2023 were predicted to be 3.62 million USD. The volume of data being sent across interconnected systems is increasing exponentially, with the quantity of data doubling every 20 months. Similarly, the amount of data stored on mobile devices is also doubling on an annual basis [16].

Cyber security events may cause significant harm at several levels, such as individual, institutional, organizational, corporate, and national. They may lead to secondary effects such as legal responsibilities, compromised privacy, identity theft, regulatory fines, damage to reputation, and negative public opinion, as well as immediate financial and other losses (such as downtime, inability to carry out corporate operations, and data breaches). Many organizations still lack effective methods to tackle this, as shown by studies [17], [18], and [19]. For instance, Charlie Müller and Chris Valasek broke into a Jeep Cherokee in July 2015 while the driver was on the highway. Every modern car has an infotainment system, and due to vulnerabilities in this system, hackers have been able to remotely take control of the vehicle while seated on their sofa or using a smart phone. The 1.4 million automobile recall, repairs, customer complaints, reputational issues, legal requirements, etc., were discussed in the epilogue [20].

A huge cyber catastrophe occurred in Sweden in July 2017.The incident included the disclosure of confidential information of a country, a significant global dispute, a violation of very classified material stored in a cloud computing system, a peril to national security, a governmental turmoil, and the resignation of ministers [9]. In June 2017, more than 100 flights departing from London airports were cancelled as a consequence of a disruption in British Airways' information system. This incident amounted to a direct financial loss estimated at 114 million EUR. The WannaCry virus struck numerous services around the globe in May 2017: the National Health Service in the United Kingdom; Renault halted output at some of its French facilities; Deutsche Bahn experienced issues displaying train lines at train stops; Maersk experienced extremely challenging container traffic globally among others [9].

A cursory examination of the given instances and case studies indicates that these cyber-threats are not random occurrences, but rather are meticulously orchestrated and directed towards accomplishing a well-defined objective. In addition to its numerous advantages, the idea of a "digital economy" raises a number of issues, particularly in the field of cyber security. This is primarily because everyone can become the target of a cyber-attack; individuals, businesses of all kinds, organizations functioning in any industry, states, etc. The 'life cycle' of cyber events is meticulously designed and comprises the key stages [21];

- Sniffing, investigating and vulnerability assessment,
- Evaluation of vulnerabilities found and test attack preparation,
- Experiential or test cyber-attack by evaluating test attack outcomes, learning about security measures that ought to identify and avert the attack,
- Improvements in cyber-attacks,
- The upcoming test attack,
- A significant, well-planned attack with a clear goal.

Hence, it can be deduced that the primary goal of the management of computer security is to strategically devise and implement sophisticated and intelligent security measures that are both effective and efficient in combating prevalent, cutting-edge, and emerging data threats in information systems driven by technological advances.

3.0 MANAGING CYBER SECURITY THROUGH THE APPLICATION OF SUFFICIENT CONTROLS: A preliminary study's conclusions

The key developments in cyber security in the year 2023 were as follows, per the ENISA [8] Threat Landscape Report:

- An increase in the complexity and sophistication of harmful operations in cyberspace.
- Malevolent infrastructures keep evolving toward customizable, multipurpose features like anonymization.
- Cybercrime is becoming a lucrative endeavor for threat actors, especially cybercriminals.
- State-sponsored actors are very prevalent hostile entities in the digital realm.
- Cyber-war is increasingly and finally becoming a reality.

The primary threats seen in 2023 included malware, web-based and web-application assaults, ransomware, phishing, spam, botnets, denial of service, insider threats, and physical manipulation, damage, theft, or loss of equipment [21]. However, inadequate cyber security skills and information system management are to blame for cyber mishaps rather than any sort of "accident" or "bad luck." Numerous embedded IT controls are present in every information system, allowing for uninterrupted, precise, dependable, and efficient operation. Organizations that adopt more effective basic and sophisticated controls, capable of identifying and thwarting cyber threats, are less vulnerable to cyber risks and will experience lower levels of risk.

Consequently, it is critical to continuously assess the efficacy of security policies in order to effectively manage cyber threats [22]. ISACA [13] reports that organizations with robust controls have the potential to prevent 97% of cyber-attacks. Security controls are put in place to detect and prevent undesired processes, events, or data in information systems, including misuse, incorrect data, inefficiencies, flawed algorithms, or faulty inputs. They also address external threats like attacks, data corruption during transmission, natural disasters, and so on.

4.0 METHODOLOGY AND SAMPLE FOR THE RESEARCH

We would like to look into the control mechanisms that are in place to reduce the cyber dangers that enterprises connected to vital or crucial national infrastructure may face, as we have learnt from prior research findings. National infrastructure, abbreviated as NI, encompasses the intricate delivery and support systems that are crucial for the functioning of essential services on a wide scale inside a country [23]. These services include banking organizations, electricity control networks, telecommunication service providers, public transportation providers, military assistance, and other broadly accessible services. Still, not every national infrastructure is considered a "critical" national infrastructure (abbreviated CNI). The term "Critical National Infrastructure" (CNI) in Nigeria refers to systems and assets, both physical and virtual that is crucial to the country's national security, public health or safety, and national economic security. The inability or destruction of these CNI would have a severe and debilitating impact on these aspects of Nigeria.

The definition of CNI, according to the UK Government, is any physical or electronic infrastructure asset that is critical to the integrity and continuous provision of the basic services that the country depends on and whose loss or compromise could result in fatalities or serious economic or social repercussions [24]. While CNI is more concerned with occurrences that seriously impair public safety and security, NI places more attention on events that have a broad influence on national security. As a result, CNI is a subgroup of all the structures that collectively make up NI for a nation. The majority of nations start by developing their cyber security plans in an effort to safeguard their online spaces [2]. These tactics typically provide some instructions on how to apply cyber security concerns in every institution that is part of the NI or CNI. The influence of cyber security proceedings on NI or CNI remains unmeasured. Furthermore, it is yet unknown what cyber security measures the companies connected to NI or CNI are taking.

This article presents the results of our initial investigation into the cyber security management practices of major Nigerian corporations, specifically those affiliated with critical national infrastructure (CNI) or significant national infrastructure (NI). We carefully looked into the controls that are in place to reduce cyber threats and their effectiveness, as there were no previous studies of this kind. In order to gather broad information on cyber security issues, we first design a survey questionnaire in order to satisfy the research purpose. The questionnaire is consistent with studies that we have discussed earlier [18] [11] [14]. Cyber security professionals, research experts with worldwide credentials in the field, tested it to boost research validity. After that, we focused only on five carefully chosen businesses, and we eventually conducted a number of thorough, in-depth interviews with those in charge of cyber security. Two separate researchers chose and examined the transcripts of the interviews.

Five sizable Nigerian businesses, with an average of 2.707 workers and annual revenue of 500 billion NGN, comprise the sample for our study. Given that it includes nearly all enterprises of that size in the nation that are either NI or CNI-related, we may consider this sample to be representative in that regard. While we hope to perform a separate, more in-depth study on a much bigger sample in the future, spanning numerous industries and organizations of all sizes, we will use this example for preliminary research in this paper. Table 1 displays the sampled companies' profiles.

Table1: List of all sampled companies that are related to Critical National Infrastructure

Profile of sampled companies	
Average number of employees Average income	100,000 1 Trillion Naira
Industry profile	
Financial industry (banks) Telecommunication Food and agriculture	3 (60%) 1 (20%) 1 (20%)
Responsibility for IT/Cyber Security Risk Assessment	

Board member	1
C-suite executive level	1
CISO	1
Cyber security advisor	2

Every company in the sample has a designated employee in charge of cyber security: one of them immediately report to the CEO, one of them is a board member, two have an independent cyber security advisor, and one has a CISO (Chief Information Security Officer) who directly report to the CEO and supervisory board. They all routinely assess the efficacy of the security procedures and provide the top executive levels with reports on cyber security. Nearly every company in the sample is required to abide by national or international cyber security standards. The majority of them allocate about 1% of their overall revenue to cyber security, and they all have important internal policies in place regarding cyber security or IT security. We may also draw the conclusion that important organizational controls are successful and efficient since C-suite level administrators are knowledgeable about cyber dangers and frequent IT safety audits are conducted.

However, even though some of the establishments in our model have included cyber safety in their organization's strategies, C-suite level interest in these matters is limited because they continue to believe that cyber security is the exclusive domain of IT units or designated individuals (CISO and similar). Accordingly, organizations should involve more staff in the topic of cyber security, have a more ambitious goal for managing cyber security, and develop a more comprehensive and integrated cyber security vision. Cyber safety is still not a fundamental component of company stratagem or philosophy.

Table 2 indicates that the average threat grade is quite low (ranging from 2.22 to 3.22 on a 1–5), which may indicate that the sampled organizations either overestimate the threat posed by cyber-attacks or have high confidence in the effectiveness and maturity of their control mechanisms. This is not the case in this instance, mostly because our sample consists of businesses that are not as concerned with digital transformation challenges as they are with key national infrastructure. The ISACA record on the State of Cyber security 2023 [14], found that Internet of Things (IoTs) is displacing mobile as the emergent sphere of attention. Since these studies are barely similar, our results could be helpful as a starting point for understanding different cyber safety concerns.

Table 2: Cyber Threats

Serious cyber-threats (from 1 to 5 with 1 being the minimum and 5 the maximum)	
Employees behaviours	3.22
Disruptive technologies (Internet of Things, Mobile AdHoc Networks, Cloud Computing)	3.00
Cyber criminals	2.78
Organizational Complexity (Culture, Awareness & Policies)	2.56
Compliance with Standards and Regulations	2.22
What is the probability that these dangers will materialize?	
Mobile devices loss	3.67
Attacks in form of phishing	3.11
Attacks in form of Malware	3.00
Social engineering	2.44
Breach of Dana	2.33
Attacks coming from External (DDoS, SQL injection, etc)	2.11
Attacks coming from Internal	2.00

Finally, our respondents have rated the actions used to reduce these threats as well developed and efficient, with average scores ranging from 4.22 to 4.33 on a scale of 1 to 5. The organizational controls get a rating of 4.22, the physical controls also receive a grade of 4.22, and the technical controls receive a rating of 4.33. Based on our research participants' feedback, the primary concerns regarding IT/cyber security are as follows: employees' insufficient understanding of cyber security matters (rated at 2.89 on a scale of 1-5); inadequate education (2.89); employees' lack of skills that are technical and business competencies (2.22); the absence of qualified experts (2.22); and ineffective preventive and detective controls (1.89).

The ENISA 2023 study [18] identified ransomware, phishing, spam, denial of service attacks, malware, web-based and web application assaults, botnets, inner circle dangers, and physical damage/theft/manipulation/loss of equipment as the primary hazards in 2023. Table 3 illustrates the high level of confidence shown by our respondents regarding the ability of security controls to identify and avert significant cyber threats. This is an essential aspect for any organization, particularly those pertaining to vital national infrastructure.

Table 3: Cyber Threat Controls' effectiveness

How successful are the measures in place to identify and stop cyber threats? (1 lowest, 5 maximum, on a scale of 1 to 5)?	
Web base attacks	4.22
Malware	4.22
Internal fraud	3.89
Internal attacks	3.78
Identity theft	3.44
Data breach	3.33
Loss of mobile devices	3.22

5.0 Discussion

The majority of organizations across all industries, commerce, and government sectors rely heavily on their information systems (IS) and would swiftly collapse if the technology (ideally IT, or information technology, plus more recently, innovative digital technologies) that powers their operations ever stopped [21]. Cyber safety seems to be primarily handled by IT departments, even though the nature of IS safety occurrences and related risks have evolved considerably over the past few decades. These occurrences have transitioned from isolated instances in the age of information security to intricate cyber-attacks that capitalize on weaknesses in linked systems in the era of cyber security.

Apart from routine IT incidents that can be controlled by fundamental security measures, modern cyber-attacks are sophisticated and constantly evolving, necessitating the implementation of clever, creative, and effective controls to identify and stop them. We provided an introduction of digital technology and discussed how the transition from information to cyber security challenges is being influenced by its outward focus and interconnecting aspects. We debated the distinctions between these two terms, which are frequently used synonymously, and came to the conclusion that the primary goal of cyber security is to develop and put into place intelligent, sophisticated, yet functional controls that will shield people and businesses from deliberate, sophisticated attacks, breaches, incidents, and their aftermath.

Lastly, we have carried out an initial investigation of the cyber security management practices of major Nigerian corporations connected to critical national infrastructure (CNI) or significant national infrastructure (NI). Our particular focus was in determining the level of maturity and efficacy of basic and forward-thinking safeguards to reduce cyber dangers. The basis of our research consisted of a survey questionnaire, which was then supplemented by in-depth interviews conducted with IT and cyber security experts. The selection of these five organizations for our study is significant due to their representation across diverse sectors, their average workforce size of 2.707 individuals, substantial financial resources, and their involvement in providing vital national infrastructure (NI) or critical national infrastructure (CNI).

The majority of the studied organizations allocate around 1% of their entire revenue to cyber security. Additionally, they all have significant internal rules and provide frequent updates on cyber dangers to their C-suite executives, mainly via monthly or quarterly reports. Given that cyber security personnel report directly to CEOs, it may be inferred that crucial organizational safeguards are effectively operating. Nevertheless, even with increased awareness, cyber security issues remain a crucial component of company strategy and culture.

Our study indicates that top-level executives, often known as C-suite executives, maintain the belief that cyber security is the primary accountability of IT units or designated professionals such as CISOs. Given this information, firms should adopt a more holistic and cohesive strategy to managing cyber security. Every employee, as well as everyone involved in the organization's ecosystem, should be accountable for cyber security [4]. It is evident that the sampled companies are not keeping up with the latest and most sophisticated measures.

On a scale of 1 to 5, our respondents rate the effectiveness of measures put in place to minimize frequent cyber threats as extremely high (4.22 average for organizational controls and 4.33 for technological controls). However, major cyber security issues receive relatively low grades. The factors contributing to these concerns are as follows: workers' limited comprehension of cyber security matters (rated at 2.89 on a scale of 1-5); insufficient training and education (2.89); employees' deficiency in technical abilities and business competences (2.22); a shortage of qualified specialists (2.22); and inefficient measures for prevention and detection (1.89). This suggests that the organizations being sampled may either have an excessive level of confidence in the efficacy and efficiency of their procedures in mitigating cyber threats, or they may underestimate their importance.

6.0 Conclusion

This exploratory research has limitations, despite the fact that the paper adds to the body of knowledge already in existence. The sample itself was modest (five enterprises), but representative, as our focus was on large Nigerian companies involved in significant or vital national infrastructure. The research findings are not comparable to many other surveys and cannot be broadly applied to a single industry, but they may serve as a reference for future investigations. Our long-term goal is to apply these first results to a considerably wider sample size, a variety of industries, and organizations of all sizes in order to carry out an independent, more in-depth study.

REFERENCES

[1] Amoroso, E.G. (2010). Cyber attacks: Protecting national infrastructure, Bh, Elsevier.

[2] Atoum I, Otoom A., Abu Ali A. (2014). A holistic cyber security implementation framework, Information Management & Computer Security Vol. 22 No. 3, 2014 pp. 251-264.

[3] Bharadwaj, A., El Sawy, O., Pavlou, P.A., Venkatraman, N., (2013). Digital business strategy: toward a next generation of insights, *MIS Quarterly* Vol. 37, No. 2, pp 471-482.

[4] Spremić, M. (2023). Governing Digital Technology – how Mature IT Governance can help in Digital Transformation?. *International Journal of Economics and Management Systems,* **2**, 214-223.

[5] Bonnet, D., Ferraris, P., Westerman, G. and McAfee, A., (2012). Talking 'bout a Revolution, *Digital Transformation Review* Vol 2, No 1., pp. 17-33.

[6] Cybersecurity Ventures (2023): Cybercrime Report 2023 Edition.

[7] PricewaterhouseCoopers (2015). Global State of Information Security, http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/key-findings.html

[8] World Economics Forum (2023). Global Risk Report 2023.

[9] Cheng, Y., Groysberg, B. (2017). Why Boards Aren't Dealing with Cyber-threats, Harvard Business Review, https://hbr.org/2017/02/why-boards-arent-dealing-with-cyberthreats.

[10] Spremić, M. (2013). Holistic approach to governing information system security, Lecture Notes in Engineering and Computer Science, Volume 2 LNECS, 2013, Pages 1242-1247.

[11] ISACA (2015). Global Cyber Security Status Report, ISACA, Rolling Meadows, Illinois, USA.

[12] Von Solms, B. (2006). "Information security – the fourth wave", Computers & Security, Vol.25 No.3 pp165-8.

[13] ISACA (2012). Extracting Value from Information Chaos: Why Good Governance Makes Good Sense, CobiT 5, ISACA, Rolling Meadows, Illinois,USA.

[14] ISACA (2023). State of Cyber Security 2023, ISACA, Rolling Meadows, Illinois, USA.

[15] The Ponemon Institute (2023). Cost of Data Breach Study, June 2023.

[16] Spremić, M. (2018). Enterprise information system in digital economy, College of Basic and Applied Science, Rhema University Aba.

[17] EY (2023). Global Information Security Survey, December 2023.

[18] European Union Agency for Network and Information Security - ENISA (2018). Threat Landscape Report 2023, January, 2024.

[19] Executive Order no. 13636 (2013). Improving Critical Infrastructure Cyber security, DCPD-201300091, 2013.

[20] Klahr, R., Shah, J.N., Sheriffs, P, et. al (2017). Cyber Security Breaches Survey 2017, UK Department for Media, Culture and Sport, https://www.gov.uk/government/publications/cyber-security-breaches-survey-2017

[21] International Telecommunication Union – ITU (2023). Global Cyber Security Index, December 2023.

[22] Tapscott D., *The Digital Economy: Promise and Peril in the Age of Networked Intelligence*, McGraw-Hill, 1995.

[23] Siponen, M.T., Oinas-Kukkonen, H. (2007). "A review of information security issues and respective research contributions", The Database for Advances in Information Systems, Vol.38 No.1 pp 60-81.

[24] UK Cabinet Office (2010). Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards, March 2010

[24] Werlinger, R., Hawkey, K., Beznosov, K. (2009). "An integrated view of human, organizational, and technological challenges of IT security management", Information Management & Computer Security, Vol. 17 Iss: 1, pp.4 – 19.