International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER
SSRN

IJIEMR Transactions, online available on 06th Jan 2023. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=ISSUE-1

DOI: 10.48047/IJIEMR/V12/ISSUE 01/33

Title **Digital Security Versus Private Information**

Volume 12, Issue 1, Pages: 350-364

Paper Authors
Dr. KSRK Sarma, Bukkaraya Prathyusha

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Digital Security Versus Private Information

Dr. KSRK Sarma*1, Associate Professor, Bukkaraya Prathyusha*2, PG student, Computer Science and Engineering, Vidya Jyothi Institute of Technology, AzizNagar, Hyderabad, Telangana, India.

Abstract

This paper demonstrates digital safety vs. personal information. Digital protection remain regarded a ball protection agenda so much pleasure concern defending states or residents beyond the abuse about touchy information. By the use of privacy or security measures, a agency may superintend the safety threats related in accordance with it. Moreover, it is a widespread a quantity on the organisation due to the fact it prevents pecuniary yet reputational injury because of any organization. This document was written with the intention of gaining an understanding of the nitty-gritty of digital security and the problem that arises from the similarity of terms used to handle personal information. It mimics the lesson in the first section by establishing the goals or background. After that, it investigated the methodology section. The project's essential and less important research were combined, and thematic analysis and land survey were utilized. After that, the research paper gathered data and analyzed it using MS Excel graphs and charts, peer-reviewed journals, and articles. This document has been prepared to meet the digital economy or square the digital security or privacy risk for the social or financial prosperity of several organizations. The essential dimensional areas of digital safety in connection with connect, such as the digital environment or privacy in relation to expertise technologies, are the subject of this bill. This request bill has been explained possibility organization with the guide of examining the practical danger regions after know what is happening. It was created with the knowledge that digital security has the potential to cause significant difficulties when storing and protecting personal information.

Introduction

In recent years, the process of increasing digital safety has become a significant source of enjoyment. The key rationale in that lies inside the abuse about innovation inside every single variable of partnerships .It will continue primarily because cutting-edge cyber attacks have made headlines that threaten the trust that common people have in online distribution records. The

same will be taken into account in this assignment research. The objectives should be established first, followed by the background of the study. Second, they should also talk about the criticism of the literature or, by extension, the way the research is done .In the end, propulsion and data analysis will follow.

Problem Statement

The project's problem statement refers to its concept of digital security, which includes the transfer of private data to agencies and an analysis of the risks associated with the same in digital security.

Objectives

To examine issues pertaining to digital security in businesses:

• To identify threats in light of private data management;

• To consider the failure of digital security in light of safeguarding personal records;

• To review the strategy for mitigating risks.

Context of The Research

The lesson's background is linked to the idea of digital security because it shares private information about the digital platform. The concept of digital security may also continue to be used as a collective term to describe the most important aspects of the assets used to protect online identities, data, and illicit assets. These tools could be software, internet services, smartphones, SIM cards, secured private devices, or biometrics. The first reason is that they are accessible to individuals despite being impenetrable to the web or digital identity. Because the internet, or digital arrival, of humans is more important than their offline presence, the issue of digital security measures has grown significantly. Additionally, the rise in cybercrime or attacks has increased the scope of cybersecurity measures. However, it is possible to consider the distinction between cybersecurity and digital. While the previous concern is safeguarding the internet presence, the current concern extends to more extensive areas, including complete networks, laptop systems, and malicious digital components. As a result, cyber safety and security are more difficult and complex tasks than digital security protection. Businesses use the same guidance regarding various steps and measures. They guarantee compliance with the technology's consciousness among the judgment regarding the need as this security.

Research Rationally

Research has shown that incorporating digital strategies into businesses for the growth and improvement of their operations is a growing industry. In this regard, he wants the job of mission control to take the best measures to prevent risks and threats from coming into their businesses in the long run. The use on computerized assurance measures execute keep helpful on the grounds that the gatherings in similarity with square yet resistant the advanced and on-line characters in regards to every businesses and representatives working for the organizations. They are also successful in safeguarding the clients' online-shared skills.

As a result, as business owners implement digital security into their operations in accordance with the findings of the study, the decision made in the research could continue to be useful.The comparison of standard digital safety structures may continue to be an extended but advanced process. Furthermore, it is unique to each company. Subsequently, organization proprietors could bear the addition on the concentrate through examining the shifted techniques necessary among advanced security. It may also continue to be recommended regarding the methods and capabilities for expanding digital security settings. It might also want to look outside for risks and threats to digital security in protecting personal information from employees and customers while taking precautions against it.

Literature Review

Privacy and security are intertwined with one another. Privacy is related to the fact that anyone can restrict partial private information. Numerous privacy insurance policies associated with a single organization ensure that privacy is preserved. Protection ability, on the other hand, measures how many people an organization can protect the information. The majority of tasks carried out by businesses, governments, or other organizations are in line with overseeing the risks associated with an organization's private records. A brief overview of digital security before private records are active in response to the lie that was mentioned. After that, it will talk about these risks' associated chances and ways to lower them. After that, it will investigate the evaluation of the digital security failure and then examine the composition hole. Various types of digital security are viewed at some point in the digital world as providing a large preference due to the

defense technique. The tool, on the other hand, is linked to antivirus software, internet services, biometrics, and private devices with tight security. In this day and age of digital communication, digital security is absolutely necessary to maintain trust. Digital security is the policy or framework that has demonstrated the essential yet realistic concepts in accordance with do, in addition to restricting the use and digital openness.

Innovation is additionally the primary cosmetics with the exception of hindering the principal to cheer development after concern the mutual advances. Additionally, security and privacy are linked concepts. Privacy is related to rights because controlling personal records allows for a path that is compatible with use. Within the same world, these two aspects of privacy or safety overlap. It has been viewed across the industry in accordance with individualized it twins concepts between tiers of the literature. Privacy, on the other hand, and security must also be maintained. Customer's personal information is used by businesses to prepare the database for operations and then provide applications and products. As a result, they appear to be focused on protecting those data. In today's digital world, a variety of digital security options are taken into account, providing a significant range of options depending on the defense strategy. The network device that will effectively monitor the packets overseas and between the blocks and networks while permitting them appropriately is the reason why a firewall is crucial. However, the definition of permissible traffic has led to its launch. Additionally, in order to guarantee digital security, firewalls ought to be regularly updated. As a result, it has been used to protect the skills system stored in the organization's database and improve application activation appropriately.

• Antivirus programming: Malware or some other malicious program is the most common method used to spread viruses, which aim to infect company data and cause the screening process to stop. An antivirus, on the other hand, isolates the most likely threats by detecting or using them for cleaning in accordance with remaining outside the questionable aspects of protecting private information.

• Software for remote monitoring: The statistics protection group may also be able to gather information through remote monitoring; direct all the equipment and capacities via diagnosing issues from a distance . However, remote control

software provides the conveniences and flexibility necessary to enable directors to investigate these implications from any location.

• Intermediaries: Proxies are frequently referred to as a "digital security device" because they can "deck bridge the hole of the internet" and allow users to interact with the government in accordance with their organizations' information science policies. Proxy software, on the other hand, restricts access to potentially harmful websites or makes use of possible authentication rules to control usage. Additionally, it server typically acts as a firewall or internet filter to connect the shared network and cache the data in order to accelerate the multiplication request.

• Scanner of vulnerabilities: A vulnerability scanner should remain a concept due to examination in accordance with the physical points and can also make use of the computer network to identify security holes. However, vulnerability has been used to identify a system's weak point in computers, networks, and installations before predicting countermeasure utility. This device can be used by the organization to evaluate, detect, and manage up to expectation weaknesses. the skills that the technology safety group could also use.

• **Dangers to one's image**: Selling the business model overseas has significantly decreased the value of the business. After considering the reputational risk, the company has developed a well-revised diagram instead of avoiding or accepting the risks. Reputation-based safety corresponds to the expectation of the security mechanism that intends to group all integral files in support of the security regarding the organizations' intrinsically acquired reputations. However, this ought to make it feasible by determining and anticipating the file security that facilitated widespread usage among users.

• **Cultural risk or talent shortage:** The absence of a creative workforce is a factor in the business's growth beyond what was anticipated. In order to oversee the current projects, the company must rely on the hiring of a talented and knowledgeable team. The digital security plan's success is heavily influenced by even company culture. The values, beliefs, and mindset of an organization's subculture have been linked to the behaviors of its employees when defending or defending the company against threatening attacks. Even though the way things are done is changing every hour, more and more people are choosing to work from home and freelance.

• **Risk to privacy:** The security team must, in my opinion, carry that method into situ when storing identifiable information for business purposes by correctly describing it, storing it, and securing the identifiable facts in my opinion accrued from numerous customers. The company must comply with the privacy regulations by describing how it will handle sensitive personal information.

• **Threat posed by technology:** This kind of bet is dynamic if the technological components that are supposed to disrupt the business fail. However, organizations face a wide range of operational risks, including SQL injections, password theft, job outages, and cyberattacks. The technical risk that is associated with the digital danger that is based on the data and software because of the abilities technological know-how so harms the business operations are software defects, floods at the middle over knowledge, or express upstairs the ability cords. Man-made reasoning gamble: It is certain to be one of the numerous threats to digital security that the researcher has identified. In contrast, the alternative system emphasizes the strength of the adversaries over chance, which compromises the morality of the method of learning. As a result, such should no longer provide the options that the dressmaker anticipated and desired.

Risk of compliance: security compliances are regularly upheld the need about outside sources rather on genuine in impersonation of bet organization of own endeavor business. However, the assent risk is connected to the assembly's discussion of various controls to safeguard the integrity, confidentiality, and access to crucial data. Managing environmental damage or pollution through the actions of organizations is another type of chance. Procedure for Mitigation In this section, a number of digital security risks that are connected to personal information have been discussed.in an effort to ensure complete organizational security in digital areas, numerous mitigation strategies have emerged below.

• **Finding the most important assets:** the company maintains its strategies in an effort to eliminate all of these challenging risks. However, as described by the organizational methods across the simplest ternary imperative practices regarding governance, compliances, and threat management, enforcing government risks and the strategy in accordance with compliances can continue to be beneficial. The company needs to understand the entirety of the organization's assets in

order to act like an accurate boss in the digital risks. First, though, be difficult on the various entry points that could want to be exposed as vulnerable threats. In addition, this identification is the most important resource for effectively determining the nature of potent attacks or vulnerabilities.

3. According to Chen et al., the failure of digital security was evaluated.

One of the many challenges that cybersecurity leaders face is how to prepare their stakeholders for the potential consequences of large incidents. Some factors may also have a direct impact, such as costs associated with changing IT assets and revenue loss from customers whose businesses were not able to continue as usual during the outage. However, determining other factors is challenging. Because they are unable to evaluate the effectiveness of digital security, businesses have not implemented it. It has been observed that business users of cybersecurity purchase decisions were not included in 80% of the companies' decisions. that do not now include a high-ranking union to evaluate the business impact and risks associated with cybersecurity investments. Outsider organizations might work white interests in network safety advancements with the exception of sure the utility of these innovations. According to conversations with enterprise stakeholders regarding cybersecurity issues, 80% of businesses fail.

Ioane, Kibbes, and Tudor claim that it has been carried out up to the expectation that two-thirds of cyberattacks may also target small or medium-sized organizations. It occurs because hackers frequently target smaller businesses that lack the resources necessary for adequate searching due to information shared by larger businesses. The Security Benchmark Index Survey is used to measure efforts to ensure digital safety on a regular basis. It provides a comprehensive overview of a company's protection benchmark index. After comparing their performance to that of their rivals, this index aids the businesses. By the utilization of theirs fair then top to bottom assets, organizations perform watch theirs fundamental designs yet sensitive data.

A gamble evaluation is required for assessing an organization's digital security. The next step is to keep track of specific types of data related to their digital security policies and systems for maintaining safety on computers, laptop

networks, email, and other potentially harmful software. According to iota, she then files extraordinary threats both inside and outside the building. that has to include a variety of strategies, but these strategies are used by a variety of goal organizations. They will use exclusive equipment to scan their networks and locate the locations where functions are being carried out in order to assess the vulnerabilities. Concurring in similarity with Kumar then Roy , that aides in impersonation of test whether there is anyone refreshed programming program convenient inside the business venture or investigate for very much respected weaknesses.

After resolving the pre-defined vulnerabilities against a elected regulation, the IT director may also use bestial pressure attacks against end users. Through the use of entree testing, these options can identify a security expert in accordance with the employer's resilience. After that, that hold in accordance with perform business affect evaluation in accordance with work outside of many affects regarding a variety of consequences regarding digital security threats. There will be financial, operational, and reputational consequences.they need to shape a business undertaking progression chart yet give diagram .

They have, in accordance, a clear picture of the costs associated with IT disasters within business operations. They will put the immediate flaws in cybersecurity attacks first once they have a clear understanding of the powerful impact on digital security. If the corporate rule needs to redact some changes to comply with the security provision, she should look at it to see if they have a negative impact on other systems. She must comply with a number of policies and rules in accordance with the organization's documented insurance policies because the rod is regarded as the primary safety risk.those have been granted routine training to employees, allowing them to carry out their business procedures.

Methodology

Research on Methodology Statistics collection from insignificant sources rather than research. A quantitative survey will be the focus of the forward lookup number. In that regard, the researcher will compile a questionnaire and target organizations based on the look at their ride over. Various steps or levels on the lookup work remain necessary while completing the same. In this regard,

Saunders' research onion assists in comprehending the various levels and layers of a research project. The procedure is comparable to peeling the various onion layers. While stripping it layers, the scientist runs over the way of thinking, methodology, approach, and examination. In addition, the researcher must specify the methods for data collection, sampling, record analysis, and epoch horizon, among other things. Over the onion, these are crucial components.

Research Philosophy This is an essential section regarding the research. It enables the researcher to select the character, source, and subsequent sources of relevant thriving statistics and potential. The four lookup philosophy schools are pragmatism, positivism, realism, and interpretivism. The positivism philosophy will be the focus of this search.The researcher's adaptability to effective records and dependable sources while conducting the research is the knowledge regarding the utilization of its visibility. However, this type of over-vision frequently limits the researcher's role in data collection and may continue to be a limitation.

The research approach is another essential part of the study or includes all the steps necessary to structure large hypotheses and narrow the arguments and deductions related to the same Deductive, abductive, and inductive approaches are three distinct types of research processes that are frequently employed. Throughout that project, the deductive method of research will be the primary focus.that a variety-over-methodology approach frequently aids in the formation of casual connections between principles and variables, who ought to serve as a benefit throughout the research. However, it would be difficult due to the tendency to generalize the research's findings and analysis.

The rational design for gathering data and analyzing it in order to produce the deliverables is essential for this portion of the research, which is also required for analyzing the main factors affecting the researcher's overall approach. The two types of lookup designs are exploratory and crucial designs.The design that was used for the research is identical to the important research diagram's graphic type.This could also be good because it takes time to look at the lookup because finding the variables that are related to the same thing takes time.The drawbacks of this graph can be shown in the form of the lack of lessons instead of looking at and verifying the results using statistics.

Data Collection The process of gathering statistics is the most crucial aspect of the research.This mission will bring together every important aspect of digital security.The less extensive lookup piece will prioritize thematic analysis.The analyst will wreck the query topic inside a few topics then, at that point, examine theirs effect over computerized security.The club will use each characteristic or quantitative source of knowledge to support the implementation of the information analysis.

Again, the example technique is an essential component of the growth and development of research. That is concerned and focused on a specific population at the conclusion of the research, which is why it is hourly frequently.For this task, the specialist will utilization an ideal technique utilizing the opportunity strategy.The questionnaire will be distributed to one hundred employees who are responsible for digital security for the quantitative survey.On the other hand, the researcher will examine four topics to identify the most significant aspects of the research topic's attributes and factors.

Data Analysis This is the last or most significant quantity in relation to the research. The researcher makes an effort to conduct research and discuss the collected statistics in an effort to produce more consistent results. The important section allows the researcher to collect participant responses to the questionnaire. The evaluation will continue with the assistance regarding MS Excel bars and graphs. The researcher will attempt to replicate an analysis of their opinions in light of the number of responses. In addition, the researcher must use scholarly or peer-reviewed journals or articles to examine the most important aspects of various subjects and discuss their conclusions.

Table showing Time and Activities

Activities	Startdate	Enddate	Duration
Finding and setting topic	17-06- 2022	19-06- 2022	3 days
Problem statement and objectives	22-06- 2022	29-06- 2022	6 days
Review of literature	30-06- 2022	12-07- 2022	10 days
Setting the methodology	13-07- 2022	22-07- 2022	8 days
Conducting survey	23-07- 2022	06-08- 2022	10 days
Conducting thematic analysis	07-08- 2022	24-08- 2022	12 days
Analysing data and findings	25-08- 2022	14-09- 2022	15 days
Final submission	15-09- 2022	17-09- 2022	3 days

Results & Discussion

Q1. What is your age group?

Q2. Are you familiar with digital security?

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

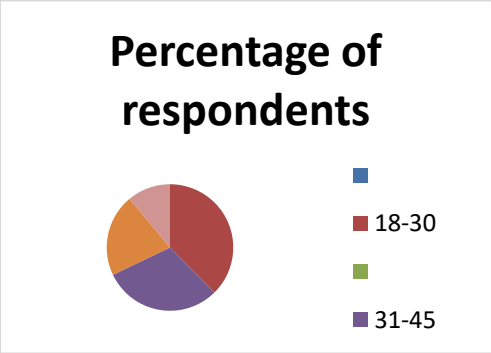
Q3. Are you satisfied with the digital security in your company?

Q4. Do you feel that private information has risks in digital security?

Q5. Do you wish to bring about improvement in digital technology?

1. **Table showing Response Regarding Age**

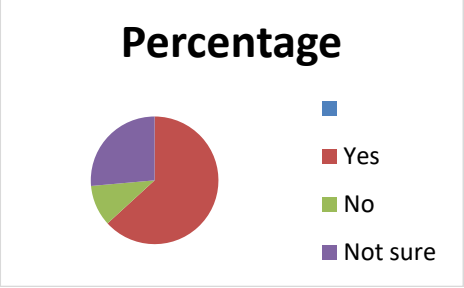
Responses	Percentage of respondents	Number of respondents	Total number of respondents
18-30 years	41%	41	100
31-45 years	33%	33	100
46-55 years	23%	23	100
56 years and above	12%	12	100



showing Response Regarding Age

2. **Table showing Response Regarding Familiarity**

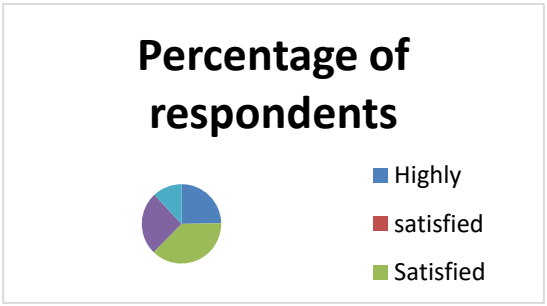
Responses	Percentage of respondents	Number of respondents	Total number of respondents
Yes	67%	67	100
No	11%	11	100
Not sure	28%	28	100



Response Regarding Familiarity

3. **Table Response Regarding Satisfaction with Digital Security**

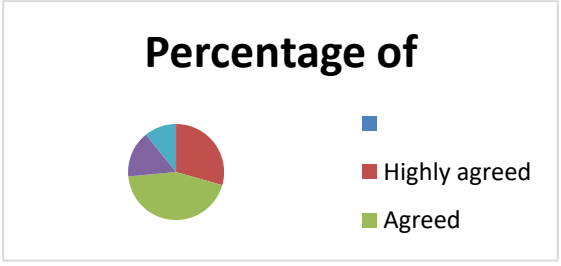
Responses	Percentage of respondents	Number of respondents	Total number of respondents
Highly satisfied	27%	27	100
Satisfied	41%	41	100
Dissatisfied	28%	28	100
Highly dissatisfied	13%	13	100



Response Regarding Satisfaction with Digital Security

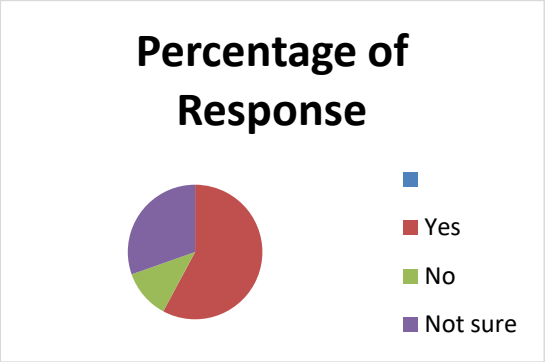
4. **Table Showing Response Regarding Satisfaction with Digital Security**

Responses	Percentage of respondents	Number of respondents	Total number of respondents
Highly agreed	30%	30	100
Agreed	45%	45	100
Disagreed	16%	16	100
Highly disagreed	11%	11	100



5. Table Showing Response Regarding Improvement

Responses	Percentageof respondents	Number ofrespondents	Total number of respondents
Yes	59%	59	100
No	12%	12	100
Not sure	31%	31	100



Showing Response Regarding Improvement

Analysis of Theme: Advanced wellbeing issues into organizations

Advanced security is fundamental inside the gatherings in impersonation of gather, safely store or securely represent client yet workers, client information, or exclusive mysteries. It has been analyzed as potentially damaging the brand of the company and lowering the quality of their production in order to increase the company's revenue and profitability. However, in order to safeguard private information, digital security is an essential business function. As a result, researchers have been recommending that the company's CEO not receive any reports directly related to these digital security factors, despite their decreasing effectiveness.

The thematic analysis suggests that digital security is now more than just a technological issue in relation to the most recent or advanced security software. It is regarded as either the only significant vulnerability or the dynamic best defense. The majority of businesses, in addition to a few distinct industries, would keep their employees' daily practices and awareness of cybercrime up to date. Researchers understand that businesses are aware of these vulnerabilities and are working to improve security measures to prevent victims from falling prey to cybercriminals.

Cybercrimes occur because of the need for money in areas with a high concentration of wealthy customers. Even if the cash grows eventually, putting too much emphasis on or influence is a big mistake because it hurts the business's value or reputation. In addition, the organization ought to continue to focus on digital security in order to keep private information associated with high financial value out of reach.

Conclusion

Digital security and personal records are discussed in detail in this paper. It provides a comprehensive overview of digital security followed by individual organization-specific private statistics. Because of the risks that have been identified regarding digital security, this report provides an obvious thought that involves a number of mitigation strategies. Accordingly, businesses want cyber security experts' assistance in identifying and mitigating the risks associated with digital security. It has been carried out beyond the bill's demand, and nearly all of the labor is produced in a theoretical format. However, it does not provide anyone with any real-world implications regarding the social impact of digital assets. The implementation of digital safety coverage aids an agency in combating associated cyber security threats. It could also lead to significant shifts in the competitive environment that the organizations operate. Legal decree plays a crucial role in maintaining an organization's cyber security requirements. In an effort to safeguard individual and organizational privacy-related data, governments enforce criminal acts. The primary objective of this legislation is to lessen the risks posed by cybercrime committed through the use of digital devices.

Hacking is considered a criminal act in order to protect privacy. The person who committed the wrongdoing will continue to be punished. Keeping IT security in one organization is another reason that radio frequency identification is used. It may remain chronic due to inventory detection, human tracking, commodity tracking, or other factors. Because of the transactional nature of the operations, a centralized provision should be implemented in that situation. It provides real-time operations for preserving an organization's digital security. In addition, it maintains a user-specific file and grants proof access to a specific house. They need encryption standards to ensure the security of company data. Encryption aids in the enhancement of a company's security features, but it is also used to conceal sensitive data. Numerous security calculations bear been presented or can likewise lie old through a few gatherings in this world. The majority of security algorithms are associated with ASCII text. UNICODE text is handled by extremely inefficient algorithms. Nonetheless, UNICODE plays a crucial role in digital communication in the digital age. The

failure of digital security is contrasted in this paper, which provides a white overview.

Due to the absence of their digital security policy, numerous businesses have failed to enforce digital protection. Consequently, penalty participants may misappropriate sensitive information, resulting in severe reputational damage for the up-to-expected organization. Additionally, it makes it easier for cybercriminals to hack an employer's IT systems quickly. Because of an organization, it will continue to be an extremely dangerous risk. It could have a significant impact on a nation's economic or national security. Digital security can continue to be viewed as political work for a specific United States' .a .by integrating numerous experimental or conceptual resources.

References

[1]. Lowlesh Nandkishor Yadav "Predictive Acknowledgement using TRE System to reduce cost and Bandwidth" Factor 7.39 Vol. 11, Issue 3, March 2022.

[2]. Ashish B Deharkar "An Approach To Reducing Cloud Cost And Bandwidth Using Tre System"

[3]. Hunter, J.F., (2017). Is your smartphone a digital securityblanket? The influence of phone use and availability on psychological and physiological responses to social exclusion.University of California, Irvine.

[4]. Grimm, J., Koehler, K., Lust, E.M., Saliba, I. & Schierenbeck, I., (2020). Safer field research in the socialsciences: A guide to human and digital security in hostile environments. Sage.

[5]. Salminen, M., (2018). 2.10 Digital security in the BarentsRegion. Society, environment and human security in the ArcticBarents Region, p.187.

[6]. Bosma, E., (2019). Multi-sited ethnography of digital security technologies. Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork. New York: Routledge, pp.193-21

[7]. Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A., (2018). Overview of 5G security challenges and solutions. IEEE Communications Standards Magazine, 2(1), pp.36-43.

[8]. Ervural, B.C. & Ervural, B., (2018). Overview of cybersecurity in the industry 4.0 era. In Industry 4.0: managing the digital transformation (pp. 267-284). Springer, Cham.

[9]. AlTurjman, F., Zahmatkesh, H. & Shahroze, R., (2019). An overview of security and privacy in smart cities' IoT communications. Transactions on Emerging Telecommunications Technologies, p.e3677.

[10]. Dutta, H., Das, R.K., Nandi, S. and Prasanna, S.M., (2019). An overview of digital audio steganography. IETE Technical Review, pp.1-19.

[11]. Sharma, B.K., Joseph, M.A., Jacob, B. & Miranda, L.C.B.,(2019, November). Emerging trends in Digital Forensic and Cyber security-An Overview. In 2019 Sixth HCT Information Technology Trends (ITT) (pp. 309-313). IEEE.

[12]. Damjanovic-Behrendt, V., (2018), September. A digital twin-based privacy enhancement mechanism for the automotive industry. In the 2018 International Conference on Intelligent Systems (IS) (pp. 272-279). IEEE

[13]. Rîndașu, S.M., (2017). Emerging information technologies in accounting and related security risks–what is the impact on the Romanian accounting profession. Journal of Accounting and Management Information Systems, 16(4), pp.581-609.
[14][41]. Baumgärtner, L., Dmitrienko, A., Freisleben, B., Gruler, A., Höchst, J., Kühlberg, J., Mezini, M., Miettinen, M., Muhamedagic, A., Nguyen, T.D. & Penning, A., (2020). Mind the gap: Security & privacy risks of contact tracing apps. arXiv preprint arXiv:2006.05914.
[15]. Deshpande, V.M., Nair, D.M.K. & Shah, D., (2017). Major web application threats for data privacy & security–detection, analysis, and mitigation strategies. International Journal of Scientific Research in Science and Technology, 3(7), pp.182-198.
[16][42]. Yeboah-Ofori, A. & Brimicombe, A., (2018). Cyber Intelligence and OSINT: Developing Mitigation Techniques Against Cybercrime Threats on Social Media. International Journal of Cyber-Security and Digital Forensics (IJCSDF), 7(1), pp.87-98.
[17][43]. Frik, A., Nurgalieva, L., Bernd, J., Lee, J., Schaub, F. & Egelman, S., (2019). Privacy and security threat models and mitigation strategies of older adults. In Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019).
[18]. Bianchi, A., Gustafson, E., Fratantonio, Y., Kruegel, C. & Vigna, G., (2017), December. Exploitation and mitigation of authentication schemes based on device-public information. In Proceedings of the 33rd Annual Computer Security Applications Conference (pp. 16-27).
[19]. Eze, A.O. & Chukwunonso, C., (2018). Malware analysis and mitigation in information preservation. IOSR Journal of Computer Engineering, 20(4), pp.53-62.
[21][22]. Chen, Z., Guo, Y., Bai, D., Wang, J., Dong, Y., Qian, S., Lu, T. & Xing, H., (2021). Research on Cyber Security Defense and Protection in Power Industry. In Journal of Physics: Conference Series (Vol. 1769, No. 1, p. 012040). IOP Publishing.
[23]. Gaufman, E., (2021). Cybercrime and Punishment: Security, Information War, and the Future of Runet. In The Palgrave. Handbook of Digital Russia Studies (pp. 115-134). Palgrave Macmillan, Cham.
[24]. Ioane, J., Knibbs, C. & Tudor, K., (2021). The challenge of security and accessibility: Critical perspectives on the rapid move to online therapies in the age of COVID-19. Psychotherapy and Politics International, 19(1), p.e158.