Vol. 3 issue 1, (2023) 270-285 https://doi.org/10.31181/jdaic10018122023g

The role of cyber security in advancing sustainable digitalization: Opportunities and challenges

Shankha Shubhra Goswami[1,*], Shouvik Sarkar[1], Krishna Kumar Gupta[1] and Surajit Mondal[1]

[1] Department of Mechnaical Engineering, Abacus Institute of Engineering and Management, Hooghly, India

* Correspondence: ssg.mech.official@gmail.com

Received 29 June 2023

Accepted for publication 10 December 2023

Published 18 December 2023

Abstract

Sustainable digitalization is a growing trend in which digital technology is used to promote environmental, social, and economic sustainability. Cyber threats can undermine sustainability efforts, resulting in economic and social disruptions. Therefore, it is important to consider cyber security as an integral component of sustainable digitalization. This paper explores the opportunities and challenges that arise from the integration of cyber security and sustainable digitalization. The paper argues that cyber security is critical to the advancement of sustainable digitalization and that both fields must be integrated to achieve their objectives. The paper examines the various risks associated with cyber security, such as privacy violations and data breaches, and highlights the need for flexible cyber security policies and regulations that can adapt to the rapidly changing digital landscape. Moreover, the paper recommends a multi-stakeholder approach to cyber security that takes into account the interests of all parties involved, including governments, businesses, and individuals. The paper provides a valuable resource for policymakers, researchers, and practitioners in the field of cyber security and sustainable development, helping them to navigate the complex challenges and opportunities of integrating cyber security into sustainable digitalization.

Keywords: Cyber security, Sustainable development, Data breaches, Digital infrastructure

1. Introduction

The use of digital technology has become more ubiquitous in everyday life, the importance of cyber security has grown significantly. Cyber security threats have evolved in sophistication and frequency, making it increasingly challenging to protect against them. Cyber security threats can range from basic phishing scams to advanced persistent threats that target critical infrastructure, such as power grids and financial systems. Cyber security incidents can result in significant economic and social disruptions, with the potential to cause widespread damage. The impact of cyber security threats has become more apparent in recent years, with high-profile data breaches and ransom ware attacks making headlines around the world (Almeida et al., 2020). Effective cyber security practices involve a range of strategies, including access control, encryption, and intrusion detection and prevention, and risk management. These strategies must be constantly reviewed and updated to keep pace with the rapidly evolving threat landscape. Cyber security is a complex and ever-evolving field, requiring collaboration and coordination among various stakeholders, including governments, businesses, and individuals. Overall, cyber security is critical to protecting digital assets and ensuring the safe and secure use of digital technology. It plays an essential role in safeguarding individual privacy, business continuity, and national security.

1.1. Need of cyber security

The need for cyber security arises due to several factors, including:

- Growing reliance on digital technology: With the increasing use of digital technology in everyday life, cyber security has become increasingly important to protect against cyber threats that can undermine the integrity, confidentiality, and availability of digital assets.
- Proliferation of cyber threats: Cyber threats have become more sophisticated, frequent, and widespread, making it challenging to protect against them.
- Protection of sensitive data: The protection of sensitive data, such as personal and financial information, is critical to safeguard against identity theft, fraud, and other forms of cybercrime.
- Business continuity: Cyber security is critical to maintaining business continuity, preventing disruptions to operations, and protecting against financial and reputational losses.
- Protecting intellectual property: Intellectual property, such as trade secrets and patents, is critical to the success of many businesses. Cyber security measures can help protect this intellectual property from theft and unauthorized use.
- Cyber security for remote work: With the increasing trend of remote work, cybersecurity has become even more critical. Employees working remotely can access sensitive company data from personal devices and networks.
- Protection of critical infrastructure: It can result in significant economic and social disruptions, and robust cyber security measures are essential to protect against these threats.
- Protection of privacy: Cyber security is critical to protecting individual privacy, especially in the age of big data. Cyber threats can compromise personal information, such as online activity and location data, resulting in violations of privacy.

The need for cyber security arises due to the increasing reliance on digital technology, the proliferation of cyber threats, the protection of sensitive data, business continuity, national security, compliance with regulations, protecting intellectual property, cyber security for remote work, protection of critical infrastructure, and the protection of privacy.

1.2. Sustainable digitalization

Sustainable digitalization refers to the use of digital technology in a manner that promotes sustainable development. It involves leveraging technology to drive economic growth, social development, and environmental protection while minimizing negative impacts. Sustainable digitalization recognizes the potential of digital technology to enable innovation, improve efficiency, and create new opportunities while addressing global challenges such as climate change, social inequality, and economic exclusion. Digitalization has become increasingly prevalent in all aspects of society, from government and business to education and healthcare. However, the rapid growth of digital technology has also resulted in negative impacts, such as increased energy consumption, e-waste, and cyber security risks (Salminen and Hossain, 2018). Sustainable digitalization seeks to address these challenges by promoting the responsible use of digital technology to achieve sustainable development. Sustainable digitalization involves a multi-stakeholder approach that includes governments, businesses, civil society organizations, and individuals. It requires the development of policies, regulations, and standards that promote sustainable digitalization while also ensuring the protection of human rights, privacy, and security. It also requires a focus on the environmental impact of digital technology and the development of sustainable digital infrastructure that supports energy efficiency and reduces waste. Sustainable digitalization is an essential aspect of sustainable development in the 21st century. It recognizes the potential of digital technology to drive positive change while also addressing the negative impacts of digitalization (Almeida et al., 2020). It requires collaboration and cooperation among various stakeholders to ensure that digital technology is used in a responsible and sustainable manner.

1.3. Role of cyber security on sustainable digitalization

The integration of cyber security into sustainable digitalization is essential for promoting the responsible use of digital technology to achieve sustainable development goals. As digitalization becomes increasingly prevalent in all aspects of society, the risk of cyber threats also increases, making it imperative to prioritize cyber security in sustainable digitalization efforts (Saeed et al., 2023). Sustainable digitalization involves using digital technology to promote economic growth, social development, and environmental protection while minimizing negative impacts. Cyber security plays a vital role in this process, ensuring the protection of sensitive data, privacy, and critical infrastructure. Sustainable digitalization and cyber security are inherently linked, as the former relies on the latter to promote responsible and secure use of digital technology. It also involves the development of secure digital infrastructure, such as cloud-based services and blockchain Technology, that minimizes vulnerabilities and ensure data protection.

In addition, the integration of cyber security into sustainable digitalization requires a focus on the human factor, including cyber security awareness and education for individuals and organizations. It also requires a focus on the ethical considerations of digital technology, such as the responsible use of artificial intelligence and the development of ethical algorithms. It focuses on the development of resilient infrastructure, promoting sustainable industrialization, and fostering innovations, which require the integration of cyber security into digital infrastructure development. Cyber security is a fundamental component of sustainable digitalization that ensures the protection of digital assets and networks while promoting responsible and sustainable use of digital technology (Linkov et al., 2018). The integration of cyber security into sustainable digitalization efforts is essential for promoting sustainable development while minimizing the negative impacts of digital technology.

1.4. Significance of cyber security on sustainable digitalization

The significance of cyber security in sustainable digitalization cannot be overstated. The integration of cyber security into sustainable digitalization efforts is essential for promoting responsible and sustainable use of digital technology while ensuring the protection of digital assets, systems, and networks (Davidsson et al., 2016). Here are some key reasons why cyber security is significant in sustainable digitalization:

- Protection of digital assets: Cyber security ensures the protection of digital assets, such as sensitive data, intellectual property, and critical infrastructure. The loss or compromise of these assets can even threats to public safety.
- Promotion of trust: Cyber security promotes trust in digital technology, which is essential for its widespread adoption. Without trust, people may be hesitant to use digital technology, which can limit the potential benefits of sustainable digitalization.
- Mitigation of cyber threats: The integration of cyber security into sustainable digitalization efforts helps mitigate the risk of cyber threats such as malware, phishing, and ransom ware. This, in turn, promotes the stability and resilience of digital systems and networks.

- Advancement of sustainable development goals: The integration of cyber security into sustainable digitalization efforts is critical for the achievement of sustainable development goals, such as resilient infrastructure, social inclusion, and environmental protection. Cyber security ensures that digital technology is used in a responsible and sustainable manner while promoting economic, social, and environmental development.

So, the significance of cyber security in sustainable digitalization cannot be overstated. It plays a crucial role in ensuring the protection of digital assets, promoting trust, mitigating cyber threats, protecting privacy, and advancing sustainable development goals (Saeed et al., 2023). The integration of cyber security into sustainable digitalization efforts is essential for realizing the full potential of digital technology while minimizing its negative impacts.

1.5. Objectives of the present research

The objective of integrating cyber security into sustainable digitalization efforts is to ensure the protection of digital assets, systems, and networks while promoting responsible and sustainable use of digital technology. Here are some specific objectives of cyber security in sustainable digitalization:

- To mitigate the risk of cyber threats: The objective of cyber security is to mitigate the risk of cyber threats, such as phishing, malware, and ransom ware by implementing security controls, access controls, and incident response plans.
- To promote trust in digital technology: Cyber security aims to promote trust in digital technology by ensuring that it is used in a responsible and sustainable manner, and by providing transparency and accountability.
- To protect privacy: Cyber security aims to protect the privacy of individuals and organizations by ensuring that personal data is collected, processed, and stored securely and lawfully.
- Towards advance sustainable development goals: The objective of cyber security in sustainable digitalization is to promote the advancement of sustainable development goals, such as resilient infrastructure, social inclusion, and environmental protection, by ensuring that digital technology is used in a responsible and sustainable manner.

The objective of integrating cyber security into sustainable digitalization efforts is to ensure the protection of digital assets, promote trust in digital technology, protect privacy, and advance sustainable development goals. By achieving these objectives, sustainable digitalization can be realized while minimizing the negative impacts of digital technology.

2. Literature review

Cybersecurity has become an increasingly critical issue in today's digital age, with cyberattacks on the rise and becoming more sophisticated (Alshahrani et al., 2024). According to a study, the average cost of a data breach in 2019 was $3.92 million, representing a significant financial impact on organizations. This highlights the need for effective cybersecurity measures to protect digital assets and prevent costly data breaches. One key area of cybersecurity research is the development of machine learning and artificial intelligence (AI) techniques for detecting and mitigating cyber threats. For example, Sima et al. (2020) proposed a machine learning-based intrusion detection system that was able to detect cyberattacks with high accuracy. Similarly, Mondejar et al. (2021) developed an AI-based system for identifying and mitigating malware attacks. Another important aspect of cybersecurity is the role of human behavior in cybersecurity risk management. According to Bedi et al. (2018), individual behaviors, such as password practices and online behavior, play a significant role in cybersecurity risk. This suggests the importance of educating and training individuals on cybersecurity best practices to improve overall cybersecurity posture.

In addition to technical and behavioral aspects, cybersecurity is also influenced by legal and policy frameworks. For example, the European Union's General Data Protection Regulation (GDPR) has significant implications for how organizations collect, process, and store personal data, with potential fines for non-compliance. Similarly, the United States' Cybersecurity Information Sharing Act (CISA) provides a framework for sharing cybersecurity information between the government and private sector (Yevu et al., 2021). So, the literature suggests that effective cybersecurity measures are critical for protecting digital assets and preventing costly data breaches. This includes developing machine learning and AI techniques for detecting and mitigating cyber threats, addressing human behavior in cybersecurity risk management, and developing legal and policy frameworks to support cybersecurity efforts.

2.1. Past literatures on sustainable digitalization

Sustainable digitalization refers to the use of digital technologies to support sustainable development goals, such as reducing greenhouse gas emissions, improving resource efficiency, and promoting social inclusion. According to recent report, digitalization could reduce global energy consumption by up to 10% by 2030, while also enabling the integration of more renewable energy sources into the grid (Najaf et al., 2021). One key area of research in sustainable digitalization is the use of smart city technologies to improve urban sustainability. For example, the implementation of smart energy management systems can reduce energy consumption in buildings and public lighting, while the use of smart transportation systems can improve traffic flow and reduce emissions. Similarly, the use of digital technologies for waste management can improve resource efficiency and reduce waste generation. Another important aspect of sustainable digitalization is the need to address the digital divide and ensure equal access to digital technologies. This suggests the need to promote digital inclusion and ensure that digital technologies are accessible to all.

In addition to technical and social aspects, sustainable digitalization is also influenced by legal and policy frameworks. For example, statistics includes measures to promote sustainable digitalization, such as improving the eco-design of digital products and promoting the use of digital technologies for resource efficiency. Sustainable digitalization has the potential to support sustainable development goals and improve resource efficiency, but requires attention to technical, social, and legal aspects (Baidya et al., 2021). This includes the use of smart city technologies for urban sustainability, addressing the digital divide and promoting digital inclusion, and developing legal and policy frameworks to support sustainable digitalization efforts.

2.2. Previous studies addressing the impact of cyber security on sustainable digitalization

The growing use of digital technologies in sustainable development efforts has raised concerns about cyber security risks. Cyber security threats can undermine the reliability and resilience of digital systems, potentially causing significant economic and social harm. Therefore, ensuring cyber security is a crucial aspect of sustainable digitalization. One area of research in cyber security and sustainable digitalization is the development of secure and resilient infrastructure. For example, the use of blockchain technology can enhance the security of digital transactions and improve supply chain management in sustainable development efforts (Agrawal et al., 2022). Similarly, the implementation of secure cloud computing can enhance data security and privacy, which is important for sustainable digitalization efforts in areas such as healthcare and environmental monitoring. Another important aspect of cyber security in sustainable digitalization is the need for risk assessment and management.

According to a report, cyber security risks should be systematically assessed and managed as part of sustainable development efforts. This includes identifying and mitigating potential vulnerabilities in digital systems, as well as developing effective incident response plans. In addition to technical measures, cyber security in sustainable digitalization also requires attention to legal and policy frameworks. Similarly, sustainable development ensures that cyber security measures respect human rights and do not contribute to social harm (Branca et al., 2020). Cyber security is an essential aspect of sustainable digitalization efforts, and requires attention to technical, social, legal, and policy aspects. This includes the development of secure and resilient infrastructure, risk assessment and management, and the development of legal and policy frameworks to support cyber security efforts.

2.3. Novel applications of cyber security

Cybersecurity has always been an important aspect of the digital world, but with the increasing focus on sustainable digitalization, new challenges and opportunities have emerged. Here are some novelties in cyber security related to sustainable digitalization:

- Green cybersecurity: With the growing concern over the environmental impact of technology, green cybersecurity has become a priority for sustainable digitalization. This involves developing cybersecurity solutions that are energy-efficient and have a minimal carbon footprint.
- Cybersecurity for smart cities: As cities become more connected and digitized, the need for robust cybersecurity measures becomes critical. Sustainable digitalization requires cities to prioritize cybersecurity in their smart city initiatives.
- Cybersecurity for renewable energy: As renewable energy becomes more prevalent, the need for cybersecurity measures to protect these systems from cyber attacks increases. Sustainable digitalization requires the development of strong cybersecurity measures to protect renewable energy systems.
- Cybersecurity for sustainable supply chains: Sustainable supply chains are becoming increasingly important as consumers demand environmentally friendly products. Cybersecurity is essential in ensuring that these supply chains are secure and sustainable.

Sustainable digitalization requires a holistic approach to cybersecurity that takes into account the environmental impact of technology and ensures that cybersecurity measures are sustainable and effective.

2.4. Existing research gaps

Despite the increasing importance of sustainable digitalization and cybersecurity, there are several research gaps in this field. Here are some potential research gaps related to cyber security and sustainable digitalization:

- Lack of frameworks: There is a lack of established frameworks for integrating cybersecurity and sustainable digitalization (Çelik et al., 2022). Researchers can explore the development of a comprehensive framework that addresses the unique challenges and opportunities of sustainable digitalization.
- Limited research on green cybersecurity: Although green cybersecurity is gaining attention, there is limited research on its implementation and effectiveness. Researchers can investigate the best practices for green cybersecurity and explore the potential benefits and challenges of this approach.
- Inadequate cybersecurity measures for smart cities: Smart cities are vulnerable to cyber attacks, but there is a lack of effective cybersecurity measures to protect these systems. Researchers can explore the development of robust cybersecurity measures for smart cities and investigate the challenges of implementing these measures.
- Limited understanding of cybersecurity for renewable energy: Renewable energy systems are susceptible to cyber attacks, but there is a limited understanding of the unique challenges and opportunities of cybersecurity for renewable energy (Akram et al., 2022). Researchers can investigate the development of cybersecurity measures for renewable energy systems and explore the potential benefits of this approach.
- Insufficient attention to sustainable cybersecurity in supply chains: While sustainable supply chains are gaining importance, there is limited attention to sustainable cybersecurity in these systems. Researchers can

explore the development of sustainable cybersecurity measures for supply chains and investigate the challenges and opportunities of implementing these measures.

There is a need for more research on the integration of cybersecurity and sustainable digitalization. Addressing these research gaps can help to develop effective cybersecurity measures that are sustainable, resilient, and able to address the challenges of the digital age.

3. Sources of cyber security sustainable digitization

Cyber security and sustainable digitization are two critical areas that are intertwined (Yenugula et al., 2023). Here are some sources that can help promote cyber security in the context of sustainable digitization:

3.1. Sustainable digitization standards

Standards such as ISO 14001 and ISO 50001 provide guidelines for sustainability in digitization efforts, which can help organizations, make informed decisions about how to implement their digital transformation initiatives (Ahmad et al., 2021). Developing sustainable digitization standards that promote cyber security in the context of sustainable digitization requires a comprehensive approach. Here are some steps to consider:

- Define sustainability goals: Start by defining the sustainability goals for the organization's digitization efforts. This should include environmental, social, and economic goals.
- Identify digital assets: Identify all digital assets, including hardware, software, data, and network infrastructure. This includes both internal and external assets.
- Conduct a sustainability assessment: Identify the environmental impact of each digital asset, including energy consumption, carbon emissions, and waste production. This should include an assessment of the life cycle of each asset.
- Develop sustainability standards: Develop sustainability standards that promote sustainable digitization. This should include energy-efficient hardware and software, renewable energy sources, and responsible waste management practices.
- Implement sustainability standards: Implement the sustainability standards across the organization's digital infrastructure. This should be done in a phased approach, starting with high-impact areas and then moving on to lower-impact areas.
- Monitor and evaluate: Monitor the effectiveness of the sustainability standards and evaluate the overall sustainability and cyber security posture of the organization on a regular basis. This should include regular assessments of the environmental impact of the organization's digitization efforts and regular cyber security assessments.
- Employee training and awareness: Train employees on the sustainability standards and make them aware of the organization's policies and procedures. This should be an ongoing process, with regular refresher training.

These steps can help to develop sustainable digitization standards that promote cyber security in the context of sustainable digitization.

3.2. Risk assessments

Conducting regular risk assessments can help organizations develop effective risk mitigation strategies. Making risk assessments for cyber security in the context of sustainable digitization requires a comprehensive approach (Chauhan et al., 2022). Here are some steps to consider:

- Identify digital assets: Start by identifying all digital assets, including hardware, software, data, and network infrastructure. This includes both internal and external assets.

- Define the scope of the assessment: Define the scope of the assessment, including the time frame and the specific areas of the organization's digital infrastructure that will be assessed.
- Analyze the impact: This should include an assessment of the environmental, social, and economic impact of each threat.
- Assess the risk: Assess the overall risk for each identified threat based on the likelihood and potential impact. This should include an assessment of the overall risk to the organization's sustainability goals.
- Implement risk mitigation strategies: It should be implemented across the organization's digital infrastructure. This should be done in a phased approach, starting with high-risk areas and then moving on to lower-risk areas.
- Monitor and evaluate: Monitor the effectiveness of the risk mitigation strategies and evaluate the overall cyber security and sustainability posture of the organization on a regular basis. This should include regular vulnerability assessments and penetration testing.

In the context of sustainable digitization, risk assessments should address vulnerabilities and improve sustainability outcomes.

3.3. Employee training and awareness

Employee training and awareness is an essential part of promoting cyber security in the context of sustainable digitization (Balogun et al., 2020). Here are some steps to consider:

- Identify training needs: Start by identifying the training needs of employees. This should include training on sustainable digitization practices and cyber security best practices.
- Make training mandatory: Make cyber security training mandatory for all employees, regardless of their job function through variety of training methods, such as online training modules, in-person training sessions, and simulations.
- Reinforce training: Reinforce cyber security training on a regular basis, such as through regular refresher training and awareness campaigns.
- Incorporate sustainability training: Incorporate training on sustainable digitization practices into the cyber security training. This ensures that employees are aware of the organization's sustainability goals and how they can contribute to those goals.
- Encourage reporting: Encourage employees to report any cyber security incidents or suspicious activity. This helps the organization to respond quickly to any potential threats.
- Measure effectiveness: Measure the effectiveness of the training and awareness program. This can be done through employee surveys, assessments of employee behavior, and monitoring of cyber security incidents.

By following these steps, organizations can develop an effective employee training and awareness program that promotes cyber security in the context of sustainable digitization.

3.4. Encryption and data protection

Encrypting sensitive data and protecting it with strong passwords can help prevent unauthorized access and data breaches (Onyango and Ondiek, 2021). Encryption and data protection are critical components of cyber security in the context of sustainable digitization. Here are some steps to consider:

- Develop an encryption strategy: Develop an encryption strategy that will help to determine what needs to be encrypted and protected. This should include the type of encryption to be used, the key management strategy, and the encryption algorithms.
- Implement encryption controls: Implement encryption controls across the organization's digital infrastructure. This should include all data protection controls are in place and functioning properly.

- Develop data protection policies: Develop policies and procedures that outline how sensitive data is to be handled, stored, and transmitted. This should include guidelines for data retention, access control, and incident response.
- Train employees: Train employees on the importance of encryption and data protection, as well as on the policies and procedures that govern the handling of sensitive data.

Organizations can develop an effective encryption and data protection strategy that promotes cyber security in the context of sustainable digitization. It is important to note that encryption and data protection should improve sustainability outcomes.

3.5. Security testing and vulnerability assessments

Regular security testing and vulnerability assessments can help organizations identify weaknesses in their digital infrastructure and take proactive measures to address them (Ghobakhloo, 2020). Security testing and vulnerability assessments are crucial components of cyber security in the context of sustainable digitization. Here are some steps to consider:

- Develop a testing plan: Develop a plan for testing the security of these assets. This should include vulnerability assessments, penetration testing, and other forms of security testing.
- Test regularly: Test the organization's digital assets on a regular basis, such as quarterly or annually. This ensures that the organization is continually identifying and addressing vulnerabilities.
- Use automated tools: Use automated security testing tools to increase the efficiency and effectiveness of security testing.
- Develop a remediation plan: Develop a plan for remediating vulnerabilities, including timelines and resources required.
- Test remediation: Test the effectiveness of remediation efforts to ensure that vulnerabilities have been successfully addressed.
- Incorporate sustainability testing: Incorporate sustainability testing into security testing and vulnerability assessments (Tseng et al., 2021). This ensures that the organization's sustainability goals are being met and that sustainable practices are being maintained.

It can help to develop an effective security testing and vulnerability assessment program that promotes cyber security in the context of sustainable digitization.

3.6. Incident response planning

Incident response planning is an important component of cyber security in the context of sustainable digitization. Here are some steps to consider:

- Establish incident response teams: Establish incident response teams that are responsible for implementing the incident reaction strategy. This should embrace both technical and non-technical staff, as well as external partners as needed.
- Integrate sustainability considerations: Integrate sustainability considerations into the incident response plan. This includes considering the environmental impact of incident response activities and developing sustainable recovery strategies.
- Develop communication plans: Develop communication plans that outline how the organization will communicate with internal and external stakeholders in the event of an incident. This includes communication with customers, suppliers, and other partners.

It is important to note that incident response planning should identify potential cyberattacks and up to date with emerging threats and sustainability goals (Brunila et al., 2021).

Therefore, a combination of these sources can help organizations promote sustainable digitization while also ensuring that their digital infrastructure remains secure.

4. Potential threats caused by cyber security sustainable digitization

While sustainable digitization can bring many benefits to organizations, it can also introduce potential threats that can impact cyber security (Ayerbe et al., 2022). Some of the potential threats caused by cyber security sustainable digitization include.

- Cyber attacks: Sustainable digitization relies on the use of technology, which can be vulnerable to cyber attacks such as malware, phishing, and ransom ware. These attacks can compromise the security of an organization's digital assets, leading to data breaches, financial loss, and reputational damage.
- Supply chain vulnerabilities: Sustainable digitization involves working with suppliers and partners who may have their own vulnerabilities (Sethy et al., 2023). These vulnerabilities can be exploited by attackers to gain access to an organization's digital assets.
- Insider threats: Sustainable digitization can increase the risk of insider threats, such as employees or contractors with privileged access to digital assets intentionally or accidentally exposing or compromising data.
- Environmental impact: Sustainable digitization can also have negative environmental impacts, such as increased energy consumption, e-waste generation, and carbon emissions.
- Regulatory compliance: Sustainable digitization can require organizations to comply with new regulations and standards related to data protection, privacy, and sustainability, which can be complex and time-consuming.
- Data privacy: Sustainable digitization can lead to the collection and use of large amounts of personal data, which can raise concerns around data privacy and compliance with data protection regulations.

It is important for organizations to be aware of these potential threats and take appropriate measures to address them, such as implementing robust security measures, training employees, and regularly conducting risk assessments and vulnerability testing.

5. Role of sustainability in promoting cyber security sustainable digitization

Sustainability can play an important role in promoting cyber security sustainable digitization by providing a framework for responsible and ethical use of technology (Goswami and Behera, 2023). Here are some ways in which sustainability can promote cyber security sustainable digitization.

5.1. Environmental impact

Sustainable digitization can help to reduce e-waste and minimizing carbon emissions by reducing the energy consumption and physical footprint of digital infrastructure (Ahmad et al., 2022). Here are some ways in which environmental impact can be addressed to promote sustainable digitization:

- E-waste reduction: The disposal of e-waste is a major environmental issue. Sustainable digitization can promote e-waste reduction by promoting the reuse and recycling of digital devices and components.
- Green data centers: The design and construction of green data centers can significantly reduce the environmental impact of digital infrastructure. This can be achieved by using energy-efficient cooling systems, renewable energy sources, and green building materials.
- Virtualization: Virtualization technology can help to reduce the physical footprint of digital infrastructure, reducing the energy consumption and environmental impact of digital technology.
- Remote work: Remote work can significantly reduce the environmental impact of digital technology by reducing the need for commuting and travel.

By addressing the environmental impact of digital technology, sustainable digitization can help to promote a more responsible and sustainable approach to cyber security (Elsisi et al., 2021). By promoting energy efficiency, renewable energy, e-waste reduction, green data centers, virtualization, and remote work, organizations can significantly reduce the environmental impact of digital technology while ensuring that they are effectively protecting their digital assets.

5.2. Ethical use of technology

Sustainability can promote the ethical use of technology by promoting privacy, data protection, and responsible use of digital assets. This can help to reduce the risk of cyber attacks by ensuring that digital assets are used in a responsible and ethical manner. The ethical use of technology is another important aspect that needs to be considered when promoting cyber security sustainable digitization (Ichimura et al., 2022). Here are some ways in which ethical use of technology can promote sustainable digitization:

- Privacy protection: Ensuring that personal and sensitive data is protected and only used for its intended purpose is essential to promoting the ethical use of technology.
- Data protection: Modification or destruction is essential to promote the ethical use of technology, which can be accomplished by strong access controls, authentication mechanisms, and data backup and recovery processes.
- Responsible use of digital assets: Promoting responsible use of digital assets is essential to promoting the ethical use of technology. Acceptable use policies can help to achieve these and provides training to the employees to ensure that they are aware of their responsibilities when using digital assets.
- Cyber security awareness: Measures of cyber security threats are essential in promoting the ethical use of technology. This can be achieved by providing regular cyber security training and awareness programs.
- Compliance with ethical standards: Ensuring that all digital activities comply with ethical standards and regulations is essential to promoting the ethical use of technology.

By promoting the ethical use of technology, organizations can ensure that their digital activities are carried out in a responsible and sustainable manner (D'Adamo et al., 2021). This can help to reduce the risk of cyber attacks and protect personal data while ensuring that organizations are able to effectively leverage digital technology to achieve their goals.

5.3. Resilient digital infrastructure

Sustainable digitization can promote resilient digital infrastructure that is designed to withstand cyber attacks and other disruptions (Irmak et al., 2023). This can be achieved by promoting the use of redundancy, backups, and disaster recovery measures. Resilient digital infrastructure is essential to promoting cyber security sustainable digitization. Here are some ways in which resilient digital infrastructure can be promoted:

- Redundancy: Ensuring that digital infrastructure is redundant can help to ensure that critical services are available and can be achieved by redundant servers, storage devices, and networking equipment.
- Backup and recovery: Ensuring regular back up or other disruption is essential in promoting resilient digital infrastructure. This can be achieved by implementing regular data backup and recovery processes. Outlining of a plan for disaster recovery is essential to promote resilient digital infrastructure. This can be achieved by developing a comprehensive disaster recovery plan that includes processes for restoring digital infrastructure and testing the plan
- Continuous monitoring: Implementing continuous monitoring of digital infrastructure can alert administrators to potential threats or disruptions.

- Rapid response: Ensuring that digital infrastructure can be quickly and effectively respond to disruption is essential in promoting resilient digital infrastructure. This can be achieved by implementing incident response plans that outline how cyber threats will be responded.

By promoting resilient digital infrastructure, organizations can ensure that their digital assets are protected from cyber attacks and other disruptions while ensuring that they are able to leverage digital technology to achieve their goals.

5.4. Innovation and collaboration

Sustainability can promote innovation and collaboration in the development of cyber security sustainable digitization solutions. This can be achieved by promoting the use of open standards and collaborative approaches to developing sustainable digitization solutions (Klimburg-Witjes and Wentland, 2021). Innovation and collaboration are key to promoting cyber security sustainable digitization. Here are some ways in which innovation and collaboration can be promoted:

- Research and development: Investing in research and development of new cyber security technologies and techniques can help to promote innovation in the field of cyber security. This can be achieved by collaborating with academic institutions and other organizations to fund research and development projects.
- Collaboration with industry partners: Collaborating with industry partners can help to promote innovation by forming partnerships with other organizations to share information and expertise.
- Information sharing: Sharing information about cyber threats and vulnerabilities can help to promote collaboration and innovation in the field of cyber security. This can be achieved by participating in information sharing networks and forums.
- Open source software: It can help to promote innovation in the field of cyber security. This can be achieved by providing regular cyber security training and education programs.

By promoting innovation and collaboration, organizations can stay ahead of the constantly evolving cyber security landscape while ensuring that their digital assets are protected from cyber threats (MacPherson et al., 2022). This can help to promote sustainable digitization by ensuring that organizations are able to effectively leverage digital technology to achieve their goals.

5.5. Corporate responsibility

Sustainability can promote corporate responsibility by encouraging organizations to take responsibility for the impact of their digital activities on the environment, society, and the economy (Sengan et al., 2020). This can be achieved by promoting the use of sustainable business practices, ethical standards, and responsible governance. Corporate responsibility plays a crucial role in promoting cyber security sustainable digitization. Here are some ways in which corporate responsibility can be promoted:

- Data protection: Organizations have a responsibility to protect the data using data encryption, access controls, and regular data backups.
- Cyber security awareness: Organizations have a responsibility to educate their employees and other stakeholders about cyber security risks and best practices. This can be achieved by providing regular cyber security training and education programs.
- Transparency: Organizations have a responsibility to be transparent about their cyber security practices and the measures they have in place to protect their digital assets. This can be achieved by regularly communicating with stakeholders about cyber security risks and the measures that are being taken to mitigate those risks.

By promoting corporate responsibility, it can help in sustainable digitization by building trust and confidence in digital technology and the organizations that use it. So, sustainability can provide a holistic framework for promoting cyber security sustainable digitization that addresses not only the technical aspects of cyber security, but also the social, environmental, and economic impacts of digital technology (Litvinenko, 2020). By promoting sustainability in the design, development, and use of digital technology, organizations can ensure that they are promoting a responsible and ethical approach to digital transformation.

6. Conclusion

Cyber security is an essential aspect of sustainable digitization, and it plays a crucial role in ensuring that the digital ecosystem remains secure and resilient. As the world continues to embrace digital transformation, there is a growing need to ensure that adequate measures are put in place to safeguard the digital infrastructure against cyber threats. The research paper has shown that sustainable digitization requires a proactive approach towards cyber security, which involves identifying potential threats, implementing appropriate security controls, and continuously monitoring and assessing the security posture of the digital ecosystem. This approach requires collaboration and coordination between different stakeholders, including governments, businesses, and individuals. Furthermore, the paper has highlighted some of the key challenges and emerging trends in cyber security, such as the rise of ransom ware attacks and the increasing adoption of artificial intelligence and machine learning in cyber security. Addressing these challenges will require a combination of technical expertise, policy frameworks, and awareness-raising initiatives. Sustainable digitization is not only about creating a digital ecosystem that is efficient, reliable, and accessible, but also one that is secure and resilient. As such, cyber security should be an integral part of any digital transformation strategy, and efforts should be made to ensure that cyber security is given the attention and resources it deserves.

6.1. Practical implications

Practical implications for cyber security sustainable digitization include:

- Establishing a comprehensive security strategy: Managers can utilize this strategy to prevent and detect emerging threats. It also helps in recovery of data and changing business needs.
- Continuous monitoring and testing: Organizations should continuously monitor their networks and systems for any security incidents or vulnerabilities.
- Collaboration and information sharing: Organizations should collaborate with other organizations and share information on threats and vulnerabilities to stay up-to-date with emerging threats. This can involve participating in industry groups, attending conferences, and sharing threat intelligence.
- Regulatory compliance: Organizations should comply with relevant regulatory standards and guidelines to ensure that they are following best practices in terms of cyber security.

The practical implications of cyber security sustainable digitization should focus on providing concrete recommendations that can be implemented by organizations to improve their cyber security posture and ensure sustainable digitization.

6.2. Limitations

Limitations on cyber security sustainable digitization include:

- Human error: Even with the best cyber security practices in place, human error can still lead to security breaches. For example, employees may accidentally click on phishing emails or use weak passwords.
- Limited resources: Some organizations may have limited resources to invest in cyber security technology or to hire dedicated cyber security personnel. This can make it challenging to implement and maintain effective cyber security measures.

- Difficulty in measuring the effectiveness of cyber security measures: It can be difficult to measure the effectiveness of cyber security measures, as there may be no clear way to quantify the impact of these measures on reducing risk.
- Complexity of systems: As organizations digitize more of their operations, their systems become increasingly complex, which can make it more difficult to implement effective cyber security measures.
- Lack of standardization: There is currently a lack of standardization in cyber security practices, which can make it challenging for organizations to know which practices to follow or which technologies to implement.
- Insider threats: Insider threats, such as employees intentionally leaking confidential information or introducing malware, can be difficult to detect and prevent.

These limitations highlight the need for organizations to remain vigilant and to continually assess and adapt their cyber security measures to address evolving threats and changing business needs.

6.3. Future scope

The future scope of cyber security sustainable digitization includes:

- Quantum computing: Quantum computing has the potential to break current encryption algorithms, which means that new encryption technologies will need to be developed to ensure secure communication and data storage.
- Block chain technology: Block chain technology can be used to provide secure and tamper-proof data storage and transfer, which can help to address cyber security concerns.
- Cyber security regulations and standards: Governments and regulatory bodies are increasingly focusing on cyber security, and new regulations and standards are likely to be introduced in the future to address cyber security concerns.

The future scope of cyber security sustainable digitization will require ongoing innovation and investment in new technologies and practices to address emerging threats and ensure the secure digitization of business operations.

Acknowledgements

We extend our heartfelt gratitude to all those who played a pivotal role in the completion of this research article. We also acknowledge the support and resources provided by Abacus Institute of Engineering and Management, Mogra, which enabled us to conduct this research smoothly. We are grateful to our colleagues and peers who offered valuable discussions and constructive criticism, enriching our perspectives and enhancing the rigor of our work.

References

Agrawal, R., Wankhede, V. A., Kumar, A., Upadhyay, A., & Garza-Reyes, J. A. (2022). Nexus of circular economy and sustainable business performance in the era of digitalization. International Journal of Productivity and Performance Management, 71(3), 748-774.

Ahmad, T., Madonski, R., Zhang, D., Huang, C., & Mujeeb, A. (2022). Data-driven probabilistic machine learning in sustainable smart energy/smart energy systems: Key developments, challenges, and future research opportunities in the context of smart grid paradigm. Renewable and Sustainable Energy Reviews, 160, 112128.

Ahmad, T., Zhang, D., Huang, C., Zhang, H., Dai, N., Song, Y., & Chen, H. (2021). Artificial intelligence in sustainable energy industry: Status Quo, challenges and opportunities. Journal of Cleaner Production, 289, 125834.

Akram, S. V., Malik, P. K., Singh, R., Gehlot, A., Juyal, A., Ghafoor, K. Z., & Shrestha, S. (2022). Implementation of digitalized technologies for fashion industry 4.0: Opportunities and challenges. Scientific Programming, 2022, 7523246.

Almeida, F., Santos, J. D., & Monteiro, J. A. (2020). The challenges and opportunities in the digitalization of companies in a post-COVID-19 World. IEEE Engineering Management Review, 48(3), 97-103.

Alshahrani, R., Yenugula, M., Algethami, H., Alharbi, F., Goswami, S. S., Naveed, Q. N., Lasisi, A., Islam, S., Khan, N. A., & Zahmatkesh, S. (2024). Establishing the fuzzy integrated hybrid MCDM framework to identify the key barriers to implementing artificial intelligence-enabled sustainable cloud system in an IT industry. Expert Systems with Applications, 258, 121732.

Ayerbe, E., Berecibar, M., Clark, S., Franco, A. A., & Ruhland, J. (2022). Digitalization of battery manufacturing: current status, challenges, and opportunities. Advanced Energy Materials, 12(17), 2102696.

Baidya, S., Potdar, V., Ray, P. P., & Nandi, C. (2021). Reviewing the opportunities, challenges, and future directions for the digitalization of energy. Energy Research & Social Science, 81, 102243.

Balogun, A. L., Marks, D., Sharma, R., Shekhar, H., Balmes, C., Maheng, D., Arshad, A., & Salehi, P. (2020). Assessing the potentials of digitalization as a tool for climate change adaptation and sustainable development in urban centres. Sustainable Cities and Society, 53, 101888.

Bedi, G., Venayagamoorthy, G. K., Singh, R., Brooks, R. R., & Wang, K. C. (2018). Review of Internet of Things (IoT) in electric power and energy systems. IEEE Internet of Things Journal, 5(2), 847-870.

Branca, T. A., Fornai, B., Colla, V., Murri, M. M., Streppa, E., & Schröder, A. J. (2020). The challenge of digitalization in the steel sector. Metals, 10(2), 288.

Brunila, O. P., Kunnaala-Hyrkki, V., & Inkinen, T. (2021). Hindrances in port digitalization? Identifying problems in adoption and implementation. European Transport Research Review, 13, 1-10.

Çelik, D., Meral, M. E., & Waseem, M. (2022). Investigation and analysis of effective approaches, opportunities, bottlenecks and future potential capabilities for digitalization of energy systems and sustainable development goals. Electric Power Systems Research, 211, 108251.

Chauhan, C., Parida, V., & Dhir, A. (2022). Linking circular economy and digitalisation technologies: A systematic literature review of past achievements and future promises. Technological Forecasting and Social Change, 177, 121508.

D’Adamo, I., González-Sánchez, R., Medina-Salgado, M. S., & Settembre-Blundo, D. (2021). E-commerce calls for cyber-security and sustainability: How european citizens look for a trusted online environment. Sustainability, 13(12), 6752.

Davidsson, P., Hajinasab, B., Holmgren, J., Jevinger, Å., & Persson, J. A. (2016). The fourth wave of digitalization and public transport: Opportunities and challenges. Sustainability, 8(12), 1248.

Elsisi, M., Tran, M. Q., Mahmoud, K., Mansour, D. E. A., Lehtonen, M., & Darwish, M. M. (2021). Towards secured online monitoring for digitalized GIS against cyber-attacks based on IoT and machine learning. IEEE Access, 9, 78415-78427.

Ghobakhloo, M. (2020). Industry 4.0, digitization, and opportunities for sustainability. Journal of cleaner production, 252, 119869.

Goswami, S. S., & Behera, D. K. (2023). An Overview of Multiple Criteria Decision Making Techniques in the Selection of Best Laptop Model. Advances in Systems Science and Applications, 23(2), 11-23.

Ichimura, Y., Dalaklis, D., Kitada, M., & Christodoulou, A. (2022). Shipping in the era of digitalization: Mapping the future strategic plans of major maritime commercial actors. Digital Business, 2(1), 100022.

Irmak, E., Kabalci, E., & Kabalci, Y. (2023). Digital Transformation of Microgrids: A Review of Design, Operation, Optimization, and Cybersecurity. Energies, 16(12), 4590.

Klimburg-Witjes, N., & Wentland, A. (2021). Hacking humans? Social Engineering and the construction of the "deficient user" in cybersecurity discourses. Science, Technology, & Human Values, 46(6), 1316-1339.

Linkov, I., Trump, B. D., Poinsatte-Jones, K., & Florin, M. V. (2018). Governance strategies for a sustainable digital world. Sustainability, 10(2), 440.

Litvinenko, V. S. (2020). Digital economy as a factor in the technological development of the mineral sector. Natural Resources Research, 29(3), 1521-1541.

MacPherson, J., Voglhuber-Slavinsky, A., Olbrisch, M., Schöbel, P., Dönitz, E., Mouratiadou, I., & Helming, K. (2022). Future agricultural systems and the role of digitalization for achieving sustainability goals. A review. Agronomy for Sustainable Development, 42(4), 70.

Mondejar, M. E., Avtar, R., Diaz, H. L. B., Dubey, R. K., Esteban, J., Gómez-Morales, A., Hallam, B., Mbungu, M. T., Okolo, C. C., Prasad, K. A., She, Q., & Garcia-Segura, S. (2021). Digitalization to achieve sustainable development goals: Steps towards a Smart Green Planet. Science of the Total Environment, 794, 148539.

Najaf, K., Mostafiz, M. I., & Najaf, R. (2021). Fintech firms and banks sustainability: why cybersecurity risk matters?. International Journal of Financial Engineering, 8(02), 2150019.

Onyango, G., & Ondiek, J. O. (2021). Digitalization and integration of sustainable development goals (SGDs) in public organizations in Kenya. Public Organization Review, 21(3), 511-526.

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. Sensors, 23(15), 6666.

Salminen, M., & Hossain, K. (2018). Digitalisation and human security dimensions in cybersecurity: An appraisal for the European High North. Polar Record, 54(2), 108-118.

Sengan, S., Subramaniyaswamy, V., Nair, S. K., Indragandhi, V., Manikandan, J., & Ravi, L. (2020). Enhancing cyber–physical systems with hybrid smart city cyber security architecture for secure public data-smart network. Future generation computer systems, 112, 724-737.

Sethy, N. K., Yenugula, M., Goswami, S. S., Bhola, A., & Behera, D. K. (2023). Selection of Ideal IoT Based Overhead Conductor for Optimizing the Performance of a Small Hydropower Project. Journal of nano- and electronic physics, 15(4), 04006.

Sima, V., Gheorghe, I. G., Subić, J., & Nancu, D. (2020). Influences of the industry 4.0 revolution on the human capital development and consumer behavior: A systematic review. Sustainability, 12(10), 4035.

Tseng, M. L., Tran, T. P. T., Ha, H. M., Bui, T. D., & Lim, M. K. (2021). Sustainable industrial and operation engineering trends and challenges Toward Industry 4.0: A data driven analysis. Journal of Industrial and Production Engineering, 38(8), 581-598.

Yenugula, M., Goswami, S. S., Kaliappan, S., Saravanakumar, R., Alasiry, A., Marzougui, M., AlMohimeed, A., & Elaraby, A. (2023). Analyzing the Critical Parameters for Implementing Sustainable AI Cloud System in an IT Industry Using AHP-ISM-MICMAC Integrated Hybrid MCDM Model. Mathematics, 11(15), 3367.

Yevu, S. K., Yu, A. T. W., & Darko, A. (2021). Digitalization of construction supply chain and procurement in the built environment: Emerging technologies and opportunities for sustainable processes. Journal of Cleaner Production, 322, 129093.