Decision: Jurnal Administrasi Publik
https://journal.unpas.ac.id/index.php/decision

E-ISSN: 2656-4939, P-ISSN: 2655-884X
Vol. 6, No. 1, Maret 2024

Information Security and Privacy: Networking Challenges Policy in the Digital World

Olena Derevianko
Public Administration,National University of Food Technologies, Ukraina

Abstract

Information security and privacy issues are growing more difficult in the quickly evolving digital era. This article examines the critical role of policy networks in tackling these issues. We provide a thorough understanding of information security, digital privacy, and the legislative complexities that surround digital regulations. The primary focus is on modern information security risks such as malware, ransomware, and identity theft, as well as how policy networks can be used to coordinate solutions. Regulatory complexity, inter-agency collaboration, and stakeholder involvement are among the issues addressed. Case studies and lessons from policy implementation provide specific insights into the effectiveness of policy network activities. The conclusion highlights major results and practical implications for improving digital information security and privacy, with a focus on interagency collaboration and raising awareness. This study adds to our understanding of the critical role of policy networks in addressing the dynamics of information security and privacy in the digital age.

Keywords : Information Security, Policy Networks, Digital Privacy

Article Info

Corresponding Author:
Olena Derevianko
(olena@gmail.com)

Received: 15-01-2024
Revised: 28-02-2024
Accepted: 05-03-2024
Published: 16-03-2024

1. Introduction

In recent decades, we have seen the tremendous advancement of information technology, which has fundamentally altered the social, economic, and political scene. Communication, connectivity, and information availability have all improved dramatically as a result of the digital revolution. The internet, social media platforms, and other technological developments have changed the way we work, communicate, and connect with our surroundings. However, as technology advanced, new challenges arose in terms of information security and privacy in the digital world. Information security and privacy are two key components of data management and online activity. The advancement of information technology has many advantages, but it also opens the door to a variety of threats that can hurt individuals, businesses, and even entire countries. Malware attacks, data theft, and communication interception are all genuine threats that internet users throughout the world confront. Furthermore, privacy concerns are growing, with the potential of identity theft and personal privacy violations becoming more prevalent. This task becomes more challenging as assault patterns evolve and technology capabilities advance. As a result, it is critical that we thoroughly comprehend the dynamics of information security and privacy in this digital age. In this scenario, policy networks appear as a viable answer to the dilemma. As these dangers and difficulties grow, the formation of policy networks becomes more critical. A policy network is a collection of legislation, conventions, and interagency collaborations designed to preserve information security and privacy. In an era where the physical and digital worlds are becoming increasingly intertwined, the success of policy networks is critical to reducing risks and preserving common interests. The issues of managing information security and privacy in the digital environment are complicated and ever-changing. New dangers develop on a regular basis, necessitating the use of innovative and adaptable security policy and practice methods. Furthermore, inter-institutional cooperation and the involvement of relevant parties are critical in addressing this obstacle. Critical challenges that arise include how to design effective policies, deal with rapid technology developments, and secure the long-term viability of policy networks in the face of environmental change. This study attempts to provide a thorough understanding of the dynamics of information security and privacy in the digital age. The research also focuses on the importance of policy networks in addressing this dilemma. It is hoped that by better understanding the interactions between information security, privacy, and policy networks, effective and long-term solutions to maintain the integrity of information systems and protect individual privacy rights can be developed, emphasizing an inclusive and collaborative approach to managing complex interactions and dynamics involving many stakeholders (Ilhami, 2023a).

This study is highly significant in the context of an increasingly digitally connected society. It is believed that the research findings would help to shape regulations, information security practices, and preventive actions for privacy. Furthermore, a greater understanding of the role of policy networks might aid in developing frameworks that are more effective and responsive to emerging threats. With this approach, this research contributes positively to efforts to preserve information security, maintain privacy, and enhance policy structures in today's digital world, which is always changing. It is intended that by thoroughly comprehending the issues encountered and potential solutions that might be adopted, this research will provide helpful guidance to enterprises, governments, and the general public in dealing with the complexities of information security and privacy in the digital era.

2. Method

Research technique is a framework that guides researchers in collecting, analyzing, and interpreting data to answer research questions. In the context of this publication, the study methodology will help describe the technique taken to investigate information security and privacy issues, as well as the role of policy networks in addressing them in the digital world.

1. study Design: This study design takes a mixed approach. This methodology combines qualitative and quantitative methodologies to explore information security and privacy concerns, as well as the function of policy networks in the digital age. To get a thorough understanding of the perspectives of policymakers, information security specialists, and digital privacy practitioners, qualitative methodologies will be used, including document analysis and literature reviews. Meanwhile, quantitative methodologies will be used, with questionnaires distributed online to responders from several linked areas. This design combines document analysis, literature review, and online questionnaires to enable the integration of qualitative and quantitative data. This allows researchers to gain a full understanding of the difficulties and solutions associated with information security and privacy. (Sobry and Hadisaputra, 2020).
2. Data Types and Sources: The research will include both qualitative and quantitative data. Document analysis will be used to obtain qualitative data, such as pertinent information security policies and digital privacy practices. In addition, qualitative data sources will include literature reviews to better understand the viewpoints of policy stakeholders, information security specialists, and digital privacy practitioners. On the other hand, quantitative data will be collected by administering questionnaires to respondents in order to assess their perceptions and comprehension of information security and privacy.
3. Data Collection Technique: This study's data collection technique will include both document analysis and online questionnaires. Document analysis will be performed on information security and privacy rules, reports, and literature. To obtain quantitative data, questionnaires will be given online to responders from diverse sectors. It is believed that the combination of these methodologies would provide a comprehensive picture of policy makers' perspectives and experiences with information security and privacy issues. This method will enable balanced data analysis from both qualitative and quantitative perspectives without requiring direct interviews (Sobry & Hadisaputra, 2020).
4. Data Analysis:. Data will be analyzed using a combination of qualitative and quantitative methods. Thematic analysis will discover major patterns and conclusions in qualitative data from in-depth interviews and organize them into main themes and sub-themes. Meanwhile, descriptive analysis describes the frequency distribution of quantitative data from questionnaires, and inferential analysis tests hypotheses and identifies correlations between variables. The combination of these

two methodologies is projected to provide a thorough understanding of information security and privacy challenges, as well as the efficacy of policy network responses to these issues.

5. Validity and Reliability: Validity and reliability are important principles for determining research quality. Validity assesses how well a research instrument measures what it is designed to measure. To assure validity, this study employs questionnaire and interview procedures that have been carefully designed to address relevant aspects of information security and privacy. Meanwhile, reliability measures the instrument's capacity to generate consistent results. The questionnaire's internal reliability coefficient will be calculated to assess its reliability. This study attempts to give accurate and reliable results by putting validity and reliability first. This methodology, which combines qualitative and quantitative approaches, is designed to provide a comprehensive and in-depth understanding of the difficulties of information security and privacy, as well as the success of policy networks in dealing with them in the digital age.

3. Results and Discussion

Information Security Challenges in the Digital World: Threats and Mitigation Strategies 9 World Economic Forum (2018). The Future of Cybersecurity and Digital Trust: Scenarios for the Cybersecurity Landscape in 2022. Retrieved from http://www3.weforum.org/docs/WEF_Shaping_Th In today's ever-expanding digital age, information security has emerged as a vital issue that must be addressed. Threats to information security become more sophisticated and diverse as technology advances. This essay will look at the main problems to information security in the digital era, identify potential dangers, and examine effective mitigation techniques. Threats To Information Security

1) Malware and Virus Attacks. Malware and virus attacks are among the most common risks. Malware can take different forms, including viruses, worms, trojans, and ransomware. These attacks can damage, destroy, or steal data, causing harm to both companies and individuals.
2) Ransomware Attacks. Ransomware attacks have become a growing danger. In this assault, hackers encrypt the victim's data and demand a ransom for the decryption key. These attacks are not only financially damaging, but can also harm customer reputation and confidence.
3) Privacy Threats Individual privacy is under increasing threat, particularly from identity theft and communication interception. Stolen personal information might be exploited for criminal purposes, and communication interceptions can endanger both personal and professional lives.
4) Regulatory non-compliance The intricacy of information security regulations might present a challenge in and of itself. Many firms struggle to understand and comply with all applicable requirements, resulting in security holes that can be exploited.

Mitigation Strategy

1) Strong Network Security. Building good network security is an important step in combating malware and virus attacks. This entails deploying firewalls, intrusion detection, and regular software updates to close security gaps that hackers may exploit.
2) Effective data recovery. An effective data recovery method can mitigate the effects of a ransomware attack.
3) Performing regular data backups and maintaining duplicates in a separate location is a critical step in restoring operations following an assault.
4) Improved user awareness and training. Awareness of information security issues must be raised at all levels of the company. Training users on typical hacking strategies, such as phishing, can help prevent user-initiated attacks.
5) Data Encryption Data encryption is an excellent method for protecting privacy. Encryption can help safeguard stored data as well as data that moves between devices or networks, ensuring that information remains confidential.
6) Monitoring and Early detection. An effective security monitoring system detects unusual behavior and responds quickly to threats. Real-time monitoring enables firms to discover and respond to risks as soon as they arise.

7) Collaboration with External Parties and Policy Networks. Creating policy networks that incorporate engagement with third parties, such as security and government agencies, can help firms acquire a broader perspective and assist more effective threat responses.
8) Regulatory Compliance. Maintaining compliance with current standards is a critical step toward reducing legal risks and ensuring sufficient data protection. This includes a thorough understanding of regulations and the implementation of suitable procedures. Information security concerns in the digital age necessitate a comprehensive solution that incorporates technology, training, and policy. Organizations must respond quickly and effectively to threats that are always evolving11.

In this dynamic digital environment, organizations may better safeguard their data, retain privacy, and meet information security problems by using the correct mitigation methods. Policy Network Challenges Policy networks play an important role in tackling information security and privacy issues in the digital era. However, as the digital environment becomes more complicated and dynamic, new issues emerge, necessitating mature techniques and ways to tackle them.

1) Regulatory Complexity. The complexity of legislation governing information security and privacy is one of the most significant difficulties that policy networks face. The 11 EU Cybersecurity Agencies' varying and evolving regulations (2020). Threat Landscape Report 2020: European Union Agency for Cybersecurity. Various government departments and regulatory entities can be challenging to combine smoothly. This generates ambiguities and legal gaps that might be exploited by malevolent actors. Furthermore, inconsistencies between regulations and their implementation frequently develop, hampering policy efforts to offer effective protection. To achieve a consistent and efficient legal environment, institutions must work together better to synchronize and align legislation (Ditia Saputra et al., 2023).
2) Interagency Coordination Inter-agency coordination is another key difficulty. The ability of institutions involved in policy networks to collaborate is critical to their success in resolving information security and privacy challenges. Even within a single country, techniques and priorities are frequently inconsistent (Ilhami, 2023a). A lack of adequate communication systems among agencies might impede the quick transmission of information and response to developing risks. As a result, there is a need for initiatives to increase coordination, such as frequent meetings or joint security information centers, where multiple organizations can share intelligence and coordinate actions (Martomo, 2020).
3) Participation of Related Parties Another problem is the involvement of a diverse set of stakeholders, including the commercial sector, civil society, and educational institutions. Successful information security and privacy regulations necessitate active cooperation from these diverse groups. However, because of competing interests and limited resources, this involvement is not always straightforward to accomplish. Concerns regarding company secrecy, for example, and the desire to retain competitiveness may limit private sector participation. As a result, incentives and restrictions must be in place to encourage participation, such as tax breaks or long-term corporate benefits.
4) Limited resources. Limited resources, both in terms of cash and experience, pose a significant challenge for policy networks. Implementing information security and privacy regulations necessitates significant investments in training, technology, and skilled individuals. However, many government agencies and organizations may face budgetary limits or trouble obtaining suitable employees. To address these difficulties, institutions and sectors may need to work together to share resources and information. Furthermore, attempts to enhance capacity through continual training and education can help address human resource shortages.

The Importance of Policy Networks in Overcoming Challenges. Information security and privacy in the digital environment are becoming increasingly complex and difficult, necessitating the involvement of policy networks in the development of successful solutions. This section will go into detail on the role of policy networks in helping enterprises and governments overcome the issues of protecting information security and privacy.

1) Inter-agency coordination and collaboration. One of the most important parts of policy networking is strengthening inter-agency coordination and collaboration. Information security concerns

frequently entail multidisciplinary components, necessitating efficient collaboration among agencies. Good coordination can enable a timely and accurate sharing of information, allowing for more efficient responses to developing threats. In this context, a thorough examination of the implementation of policy networks in the public sector can provide real insights into how coordination and collaboration processes are structured. Case study data and findings can help uncover success factors and impediments to improving policy network effectiveness.

2) Adaptive Policy Development Policy networks must be able to keep up with technological advances and new assault strategies. Thus, adopting adaptive policies is critical in overcoming information security concerns. Data analysis from a series of security incidents can be used to update and reinforce current policies (Marisa & Atika, 2022). Adaptive policy formulation must also incorporate stakeholders such as the private sector, research institutes, and civil society. Open communication among stakeholders can provide a solid platform for developing more relevant and effective policies.
3) Increased awareness and education. The success of policy networks is partly dependent on the amount of awareness and understanding shared by all parties. Regular training programs can help individuals enhance their abilities and awareness of information security. Furthermore, public awareness initiatives can alert people about the security and privacy dangers they face. End-user knowledge can help to lower the risk of attacks caused by insecure activities.
4) Implementation of Latest Security Technology The policy network must include plans for deploying the most recent security technology. Successfully countering information security threats frequently requires the use of modern technologies such as artificial intelligence, behavioral analysis, and early detection. Integrating these technologies into policy frameworks can enhance attack detection and response time (Pakarti et al., 2023). Implementing security technologies necessitates continual risk evaluation. Case studies on security technology implementation in unique businesses can shed light on the obstacles and benefits of using current technologies.
5) Network Performance Evaluation Policy Evaluation of the performance of policy networks is a crucial stage in determining the success of the actions done. Performance metrics may include threat reaction time, attack prevention success rate, and resource allocation efficiency. The evaluation results can then be used to improve and optimize the policy network. Regular evaluation is required to guarantee that the adopted policies remain relevant and effective in the face of the ever changing information security environment.
6) Involvement of stakeholders. A effective policy network also involves active participation from a variety of stakeholders, including the commercial sector, non-governmental groups, and academic institutes. This involvement may include participation in policy forums, the development of industry safety standards, and contributions to collective safeguards. Verizon's 12 policy network aims to encourage engagement. (2021). Database Breach Investigations Report (DBIR). Verizon Communications can organize monthly meetings, workshops, and conferences to explore common information security challenges. Close partnership with the private sector can help enhance the flow of information and resources (Pakarti et al., 2023).

Policy networks play an important role in addressing information security and privacy issues in the digital era. Maintaining information integrity and security requires good coordination, adaptive policies, greater awareness, adoption of cutting-edge security technology, performance measurement, and the involvement of connected parties.12. Policy networks, when approached holistically and responsively, can lay a solid foundation for preserving information security and privacy in an ever-changing digital environment. Understanding these elements is critical for ensuring that policymaking is fair, inclusive, and responsive to society's changing needs. (Ilhami, 2023A).

4. Conclusion

In the conclusion section, this study was successful in thoroughly presenting and assessing the issues of information security and privacy in the digital era, as well as the critical role of policy networks in addressing them. Some of the key results that can be taken away include: 1. Main concerns: According to this research, information security and privacy concerns in the digital world are becoming more complex, particularly with the emergence of new attacks such as malware, ransomware, and identity theft. These dangers necessitate significant efforts to ensure data integrity and confidentiality. 2. Role of Policy Networks: Policy networks play a significant role in overcoming these obstacles. Effective agency coordination and collaboration, adaptive policy creation, awareness raising, and the use of cutting-edge security technology are all critical components of creating a safe and clean digital environment. 3. Inter-agency cooperation: Inter-agency cooperation is seen as an essential component of policy networks. To respond to rapid advancements in information security and privacy, governments, the private sector, and civil society must work together to build comprehensive and effective policies. 4. Education and knowledge: Raising public knowledge of information security and privacy risks is critical. Policy networks can play an important role in promoting this project by educating the public, corporate leaders, and other stakeholders. 5. Use of Cutting-Edge Technology: Using cutting-edge security technology is crucial to ensuring information security and privacy. To respond to increasing attacks and threats, policy networks must promote and support the incorporation of cutting-edge technologies. It is intended that by gaining a thorough understanding of these dynamics, the findings of this study can help to design more effective and responsive information security policies and procedures in the digital environment. As a result, this conclusion serves as the foundation for the subsequent phases in developing a safe, dependable, and trustworthy digital ecosystem.

References

Acemoglu, D., & Robinson, J. A. (2012). Why nations fail: The origins of power, prosperity, and poverty. Crown Business.

Aulia, A. F., Asbari, M., & Wulandari, S. A. (2024). Independent Curriculum: Teacher problems in implementing information technology in the learning process. Journal of Information Systems and Management, 03(02), 65–70.

Cavoukian, A., & Tapscott, D. (1997). Who knows: Protecting your privacy in a networked world. McGraw-Hill.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security: Exploring a fuzzy set preference programming approach. Information Systems Journal, 16(3), 245-266.

Ditia Saputra, D., Ayu Pramesty, L., & Farah Munifah, N. (2023). Privacy violations in police investigative reality programs in Indonesia: Threats, policies, and the need for reform. JCIC: CIC Journal of the Institute for Social Research and Consulting, 5(1), 29–38. https://doi.org/10.51486/jbo.v5i1.85

EU Agency for Cybersecurity. (2020). Threat landscape report 2020. European Union Agency for Cybersecurity.

European Union Agency for Cybersecurity (ENISA). (2020). Threat landscape for 5G networks. Retrieved from https://www.enisa.europa.eu/publications/threat-landscape-for-5g-networks

Ilhami, R. (2023a). Policy network actors as units of public policy analysis. Journal of Social Science and Communication (Ju-SoSAK), 1, 103–111.

Ilhami, R. (2023b). Policy network management in tourism sector policy. 3(02), 199–207.

Khasanah, C. U., Mursidi, M. A., Mahardika, A. T., & Akbara Surakarta, P. (2023). Analyze privacy and security features as an effort to mitigate hacking on social media. IJM: Indonesian Journal of Multidisciplinary, 1, 1385–1394. https://journal.csspublishing/index.php/ijm

Lambanon, J. E., Waha, C. J. J., & Kalalo, M. E. (2023). Juridical studies on misuse of personal data in online loan services are linked to the right to privacy in Indonesia. 3, 718–727.

Marisa, D., & Atika. (2022). The role of blockchain technology in security in data privacy. Journal of Computer Science, Economics and Management (JIKEM), 3(1), 129–138.

Martomo, Y. P. (2020). Contribution of political communication in building a coalition network for formulating liquor policy in the City of Surakarta. Journal of Communication Science PROGRESSIO, I(I). http://ejournal.unsa.ac.id/index.php/progressio/article/view/386

NIST. (2018). NIST Cybersecurity Framework (CSF) Version 1.1. National Institute of Standards and Technology.

Nur, S., Rahmawati, E., Hasanah, M., Rohmah, A., Adytia, R., Pratama, P., Anshori, I., Management, P., Economics, F., & Business, D. (2023). Privacy and ethics in digital human resource management. Journal of Management Research and Research Innovation, 1(6), 1–23. https://doi.org/10.61132/lokawati.v1i6.328

Nurazkia, N., Dian, H., & Ari, R. (2023). Policy networks in developing tourist villages (Study in Santanamekar Village, Cisayong District, Tasikmalaya Regency. Economia Journal, 17(1), 34–48.

Pakarti, M. H. A., Farid, D., Hendriana, H., Saepullah, U., & Sucipto, I. (2023). The influence of technological developments on privacy protection in civil law. Sultan Adam: Journal of Law and Social Affairs, 1(1), 204–212.

Schneier, B. (2015). Data and Goliath: The hidden battles to collect your data and control your world. W. W. Norton & Company.

Silva, A. L. R. da. (2004). Introdução às relações internacionais: temas, atores e visões. Revista Brasileira de Política Internacional, 47(1), 191–194. https://doi.org/10.1590/s0034-73292004000100012

Sobry, M., & Hadisaputra, P. (2020). Qualitative research: Explaining what and how to practically write and conduct qualitative research correctly from A to Z.

World Economic Forum. (2018). Shaping the future of cybersecurity and digital trust: Scenarios for the cybersecurity landscape in 2022. Retrieved from http://www3.weforum.org/docs/WEF_Shaping_the_Future_of_Cybersecurity_and_Digital_Trust_scenarios_2018.pdf