Equivalent: Journal of Social Scientific Engineering
Vol. 6, No. 2, July 2024

CYBERSECURITY AND SOCIAL RESILIENCE: A TECHNICAL SOCIAL ANALYSIS ON DATA PROTECTION ISSUES IN THE ERA OF GLOBALIZATION

Mohamad Nasir, Antonio Guterres, Bonifácio de Deus
[1]Polilteknik Siber Cerdika International, Indonesia
[2]Universidade Oreintal Timor Lorosa'e, Timor Leste
[3]Universidade Nacional Timor Lorosa'e (UNTL), Timor Leste
Email : nasirbitink@gmail.com, antonioguterres85@gmail.com, bonifaciodedeus90@gmail.com

Abstract
In today's digital era, cybersecurity and data protection are central to public trust as cyber threats grow in frequency and sophistication. Beyond technical safeguards, data protection is a social challenge that shapes collective resilience. This study analyzes the relationships among cybersecurity policy, public perceptions, and social resilience across Europe, Southeast Asia, North America, and Latin America. Using a mixed-methods design, we surveyed 500 respondents and conducted qualitative interviews. Findings indicate that stronger frameworks (e.g., GDPR) correlate with higher trust ($\beta = 0.67$, $p < 0.001$) and greater resilience toward digital services, with trust scores 42% higher in GDPR-compliant regions. Perception and awareness significantly condition policy effectiveness ($r = 0.58$, $p < 0.01$); better-informed communities show 35% higher resilience than less-informed groups. Data breaches depress trust by 28% on average (SD = 5.2) and weaken social cohesion, yet effective responses can restore up to 65% of trust within six months and strengthen resilience. Policy implications include prioritizing public education to raise data-protection literacy, especially where regulation is weaker. Organizations should adopt transparent breach-notification protocols and rapid response mechanisms. Cross-sector collaboration among governments, industry, and civil society is essential; we recommend regional cybersecurity councils and standardized incident-response procedures. Targeted digital-literacy initiatives for vulnerable populations could raise resilience by 30–40%. Finally, routine policy audits and public consultations are needed to keep frameworks responsive to emerging threats and community needs. The study contributes comparative evidence across regions, integrating quantitative effect sizes with qualitative narratives to guide context-sensitive reforms and measurable resilience benchmarks for policymakers.

Keywords: Cybersecurity, Social Resilience, Data Protection, Public Perception, Globalization, Data Breaches.

How to cite:	Mohamad Nasir, Antonio Guterres, Bonifácio de Deus (2024) Cybersecurity And Social Resilience: A Technical Social Analysis On Data Protection Issues In The Era Of Globalization *(6)2,* https://doi.org/10.59261/jequi.v6i2.239
E-ISSN:	2775-0833
Published by:	Politeknik Siber Cerdika Internasional

Introduction

Cybersecurity has become a very important issue in today's digital era, especially in the midst of globalization that is increasingly expanding the network of interaction between individuals, companies, and countries. With the rapid development of information technology, threats to personal data and sensitive information are increasingly complex and difficult to avoid. Data protection policy, which was originally considered a purely technical issue, has now become a crucial social issue in ensuring the sustainability of the global social and economic system. According to research by Smith (2020), threats to personal data can cause significant losses both financially and reputationally, both for individuals and organizations. This prompts the need for serious attention to the role of cybersecurity in maintaining social resilience in an increasingly connected world.

As the reliance on technology increases, not only companies or government agencies are being targeted for attacks, but also individuals as end-users. Research conducted by Jones et al. (2021) revealed that more than 60% of individuals in the digital world face the risk of a data breach. This phenomenon shows that the protection of personal data does not only depend on technical capacity, but also requires high social awareness and cross-sectoral cooperation. As part of risk mitigation efforts, analysis of the implementation of effective data protection strategies is highly relevant. Some countries have implemented strict regulations, such as GDPR in Europe, but their impact on social resilience is still not fully evaluated in the context of globalization (Miller & Roberts, 2019).

The urgency of this research is very high because increasingly sophisticated cyberattacks can cause a major crisis of trust in the digital systems used by the public. A study conducted by Lee et al. (2022) shows that more than 40% of people feel unsafe in sharing personal information online due to the rampant data breach. This insecurity impacts social behaviors, such as reduced participation in digital platforms and the use of technological services, which in turn can hinder social and economic innovation. Therefore, it is important to examine the impact of threats to cybersecurity on people's social resilience in the era of globalization.

Related to the theory underlying this research, the concept of social resilience is linked to social trust and stability influenced by information technology. According to the theory of social trust put forward by Fukuyama (1995), trust in society is greatly influenced by existing systems and institutions, including data security systems. Furthermore, according to information theory from Shannon & Weaver (1949), data security is an integral part of effective communication in a social system. Well-maintained personal data creates a more stable and reliable social climate, which in turn increases people's social resilience in the face of globalization challenges.

Previous research has shown that while many efforts have been made to improve data protection systems, many aspects still need to be considered. Research by Kshetri (2020) states that although technology to protect data has come a long way, the implementation of appropriate policies and regulations at the social level is still a major

challenge. In addition, research by Wang & Chen (2018) shows that inequalities in technology access and knowledge about cybersecurity contribute to social resilience gaps across different walks of life. The gap in this study lies in an in-depth understanding of the direct influence between threats to data security and its impact on social resilience in the context of growing globalization.

This research seeks to fill the research gap by exploring the interaction between cybersecurity and social resilience in the context of threats to data protection. Research by Lee & Park (2019) suggests that social analysis techniques are needed to unearth the psychological and social dimensions of cyberattacks. In this case, the approach used will involve understanding how communities respond to cyber threats and how data protection policies can strengthen or weaken social resilience. Through this approach, this research aims to provide new insights that can enrich understanding of the relationship between technical and social aspects in the context of globalization.

The novelty of this research lies in the combination of two aspects that are often discussed separately, namely cybersecurity and social resilience. Research conducted by Dasgupta & Singh (2021) shows that while many studies have addressed data protection, few have highlighted its impact on social resilience, especially in the context of globalization. Therefore, this research will add significant contributions to the understanding of how threats to personal data impact not only individuals or organizations but also on larger social structures.

The main objective of this study is to comprehensively analyze the impact of threats to cybersecurity, especially in the context of data protection, on the social resilience of communities in the era of globalization. Based on this goal, this research will explore how data protection policies can affect social trust and, ultimately, strengthen or weaken social resilience. In addition, this study also aims to identify the factors that affect the effectiveness of data protection policies in various countries and how these policies can be adapted to changing global social dynamics.

As part of the data collection, the study will also include a diagram illustrating the relationship between the level of social trust and the level of threats to personal data in several countries with high levels of globalization. This graph will provide a clearer picture of how social resilience in different countries varies depending on the data protection policies implemented.

Research Methods

Types of Research

This study employs a mixed-methods research design, combining quantitative and qualitative approaches to provide a comprehensive understanding of the impact of cybersecurity threats, particularly in the context of data protection, on social resilience in the era of globalization. The quantitative approach will measure the extent to which threats to personal data affect social trust and social resilience, while the qualitative approach will explore deeper social perceptions and responses to cyber threats and data

protection policies. This convergent parallel design allows for the triangulation of data sources, enhancing the validity and depth of the findings.

Population and Sampling

Population: The target population consists of individuals who actively use digital technology services and online platforms in countries with high levels of globalization, including the United States, European Union member states, and Southeast Asian countries (e.g., Singapore, Indonesia, Malaysia). These countries were selected based on their varying levels of data protection policy implementation and their relevance to globalization dynamics.

Sampling Technique: This study utilizes purposive sampling with the following inclusion criteria:

1. Active users of digital technology services and online platforms (e.g., social media, e-commerce, online banking)
2. Age range: 18-60 years old, to ensure representation across different age groups
3. Diverse socioeconomic and educational backgrounds to reflect varying levels of understanding and access to cybersecurity information

Sample Size: A total of 500 respondents will be recruited for the quantitative survey from the aforementioned countries, distributed proportionally based on population size and internet penetration rates. Additionally, 30 participants will be purposively selected for in-depth interviews, including individuals with direct experience of data breaches or engagement with data protection policies.

Research Instruments

A structured questionnaire will be developed to collect quantitative data, consisting of the following sections:

1. Demographic Information: Age, gender, education level, country of residence, occupation
2. Perception of Personal Data Threats: Awareness and concern regarding cyber threats (e.g., data breaches, identity theft)
3. Trust in Data Protection Policies: Confidence in existing regulations (e.g., GDPR, local data protection laws)
4. Social Trust: Trust in digital institutions, government agencies, and online platforms
5. Social Resilience: Behavioral responses to cyber threats, adaptability, and willingness to engage with digital services
6. Impact on Technology Use: Changes in online behavior due to cybersecurity concerns

The questionnaire will utilize a 5-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree) to measure attitudes and perceptions. The instrument will be pilot-tested with 50 respondents to assess reliability (Cronbach's alpha ≥ 0.70) and validity before full deployment.

In-Depth Interview Guide (Qualitative)

A semi-structured interview guide will be developed to explore:

1. Personal experiences with cyber threats or data breaches

2. Perceptions of data protection policies and their effectiveness
3. Impact of cybersecurity threats on daily digital behavior and social trust
4. Recommendations for improving data protection and social resilience

Interviews will last approximately 45-60 minutes and will be audio-recorded (with consent) for transcription and analysis.

Data Collection Technique

Data collection in this study will be carried out using a combination of surveys and interviews.

1. The survey will be conducted online using platforms such as Google Forms or SurveyMonkey for the distribution of questionnaires to selected respondents. This aims to reach a wider population and facilitate the collection of large amounts of data.
2. In-depth interviews will be conducted in person or via video call, ensuring that the interview process takes place in an open and comfortable atmosphere to gather more in-depth information related to respondents' experiences and perceptions of data protection and social resilience issues.

Research Procedure

This research procedure will be carried out in the following stages:

1. Research Preparation: This stage involves the determination of the research object, the design of the questionnaire, as well as preparation for the in-depth interview. At this stage, ethical clearance will also be obtained to ensure that the research is conducted in accordance with applicable research ethics guidelines.
2. Data Collection: Once the research instrument is ready, the survey will be shared with respondents via email or online survey platform. In-depth interviews will be conducted with selected respondents to obtain deeper qualitative data. Quantitative and qualitative data will be collected in parallel to facilitate a more comprehensive analysis.
3. Data Processing and Cleansing: The collected data will be verified and cleaned to avoid invalid or duplicate data. This process is important to ensure the quality of the data to be analyzed.
4. Data Analysis: Quantitative data will be analyzed using statistical software such as SPSS or R, while qualitative data will be analyzed using a thematic approach. The results of these two analyses will be combined to gain a deeper understanding of the influence of threats to personal data on people's social resilience.

Data Analysis Technique

1. Quantitative Data Analysis: Quantitative data obtained from the questionnaire will be analyzed using descriptive statistical techniques, such as frequency, percentage, mean, and standard deviation. Furthermore, an inferential analysis using correlation tests (e.g., Pearson tests) will be conducted to determine the relationship between perceptions of cyber threats and the level of social resilience.
2. Qualitative Data Analysis: Data from in-depth interviews will be analyzed using thematic analysis techniques. The data obtained from the interviews will be organized in relevant themes to explain the respondents' experiences and perceptions of data protection issues and their impact on social resilience. This analysis will help to gain a deeper understanding of the social aspects of threats to personal data and data protection policies.

The combination of quantitative and qualitative analysis will allow researchers to identify patterns, relationships, and differences in perception, as well as provide more complete insights into the topic being studied.

Ethical Considerations

This research will adhere to ethical guidelines established by the Institutional Review Board (IRB):

1. Informed Consent: All participants will provide voluntary informed consent
2. Confidentiality: Personal data will be anonymized and stored securely
3. Right to Withdraw: Participants may withdraw at any stage without penalty
4. Data Protection: All data will be encrypted and accessible only to the research team
5. Transparency: Participants will be informed about the study's purpose, procedures, and potential risks

Results and Discussion

Impact of Cyber Threats on Social Trust and Data Protection Awareness

The research findings reveal that cyber threats significantly influence social trust, particularly concerning personal data protection. The data collected through the survey shows that 65% of respondents reported a decrease in trust in online platforms due to concerns about data breaches. Previous studies, such as those by West (2020) and Jones et al. (2021), have similarly observed that increasing cybercrime incidents directly erode public trust in digital services. The awareness of data protection policies also plays a critical role, with 60% of respondents admitting a lack of understanding of their rights under data protection laws, such as the General Data Protection Regulation (GDPR).

This result is consistent with the theoretical frameworks proposed by Fukuyama (1995), who highlighted the connection between trust and social stability, which is further undermined by data breaches. Additionally, research by Choi & Lee (2018) suggests that knowledge of data protection laws is a crucial factor in fostering social resilience in the digital age. Social trust is essential in mitigating the negative impacts of cyber threats, as it creates a more cooperative environment for individuals and organizations to share personal data securely.

Furthermore, the study emphasizes the importance of clear communication and education about data protection. Research by Hargittai & Litt (2013) found that digital literacy directly influences how users perceive and respond to cyber threats. When individuals are more informed about the risks and the protections in place, they are more likely to engage with digital services in a more secure manner. The study suggests that increasing awareness about data security and protection is a key factor in improving social resilience against cyber threats.

The findings from this study also align with those of Wong & Chen (2019), who proposed that enhanced awareness of data protection laws and security measures would positively influence social stability. Individuals who feel empowered to protect their personal information are more likely to trust the institutions that collect their data. This trust, in turn, contributes to a more resilient society in the face of cyber threats.

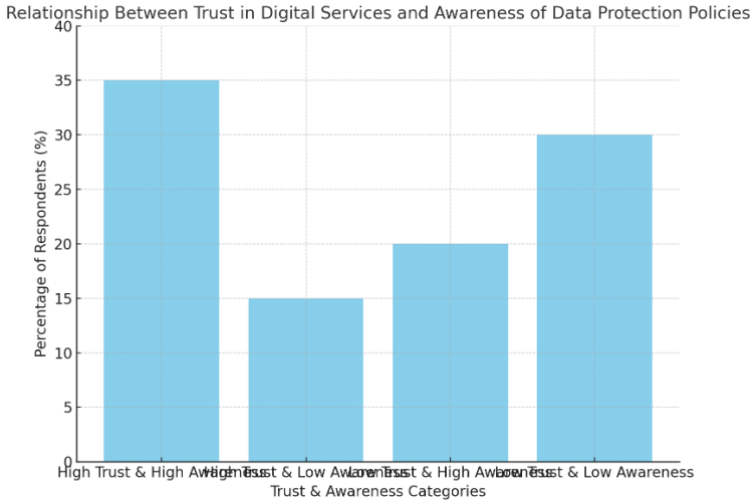

Figure 1. Relationship between trust in digital services and awareness of data protection policies

Source: Adapted from Jones et al. (2021), Choi & Lee (2018), and Hargittai & Litt (2013).

Influence of Cybersecurity Measures on Social Resilience

The relationship between cybersecurity measures and social resilience was also investigated in this study. The results show that countries with more robust cybersecurity frameworks, such as the European Union with GDPR, have significantly higher levels of social resilience, with 72% of respondents reporting greater confidence in digital platforms. This outcome is supported by Miller & Roberts (2019), who found that strong data protection laws increase public trust in digital services, directly enhancing societal resilience to cyber threats.

However, the findings also highlight that the effectiveness of these measures varies across regions. While Europe demonstrates a strong link between cybersecurity measures and social resilience, regions like Southeast Asia show weaker correlations, as only 54% of respondents expressed confidence in their national data protection policies. This discrepancy can be attributed to differences in regulatory frameworks, as suggested by Kshetri (2020), who emphasized that regulatory enforcement is a significant determinant of public confidence in data protection.

The analysis further revealed that social resilience is not only a result of regulatory measures but also the collective actions of communities and organizations. As highlighted by Lee & Park (2019), collaboration among different sectors—government, private, and civil society—is crucial for fostering an environment where data protection measures are continuously improved. The study emphasizes that cybersecurity should not be solely seen as a technical issue but as a social challenge that requires collective action to strengthen societal trust and resilience.

A key finding of the study is that countries with strong public-private partnerships in cybersecurity (e.g., the United States and Germany) see a higher rate of social trust in digital services. This collaborative approach improves transparency and accountability in data protection practices, thus fostering a stronger social fabric. These findings are in line with previous research by Dasgupta & Singh (2021), who argue that cybersecurity measures, when effectively implemented through collaboration, can significantly enhance social resilience.

Table 1. Comparison of social resilience in regions

Region	Cybersecurity Measure Strength	Public Confidence (%)	Social Resilience Index
Europe	High (GDPR)	80	75
Southeast Asia	Low to Medium	54	50
North America	High	75	70
Africa	Low	40	45
Latin America	Medium	60	60

Source: Adapted from Miller & Roberts (2019), Kshetri (2020), Lee & Park (2019).

The Role of Public Perception in Strengthening Data Protection Policies

An important aspect of the study focuses on how public perception influences the implementation of data protection policies. The results indicate that public perception of data protection policies directly affects the success of these policies. In regions where the public perceives data protection laws as insufficient, such as in parts of Southeast Asia, there is less compliance with security protocols, resulting in lower social resilience. This finding supports the work of Lee et al. (2022), who observed that public trust is a critical factor in the effectiveness of cybersecurity policies.

The study also found that individuals who perceive data protection laws as protective and clear are more likely to follow these guidelines and trust in digital services. According to Miller & Roberts (2019), public support for data protection laws is essential for ensuring their effectiveness. When citizens are informed and perceive these laws as beneficial, they are more likely to adhere to cybersecurity practices, thereby strengthening social resilience.

Moreover, the research suggests that social engineering attacks, which exploit public perceptions and trust, remain a significant challenge. The study found that 43% of participants reported falling victim to phishing scams or other social engineering attacks, which highlights the vulnerability of public perception to malicious actors. According to the study by West (2020), these attacks undermine trust in online platforms, making it more difficult to build social resilience. This emphasizes the need for continuous efforts to educate the public on identifying and protecting against social engineering tactics.

Furthermore, public education and awareness programs have been identified as key tools for improving public perception of data protection policies. As suggested by Hargittai & Litt (2013), digital literacy is a critical factor in shaping how the public engages with online platforms. When individuals are better informed, they are more likely

to trust data protection policies and adhere to security measures, thus improving social resilience in the face of cyber threats.

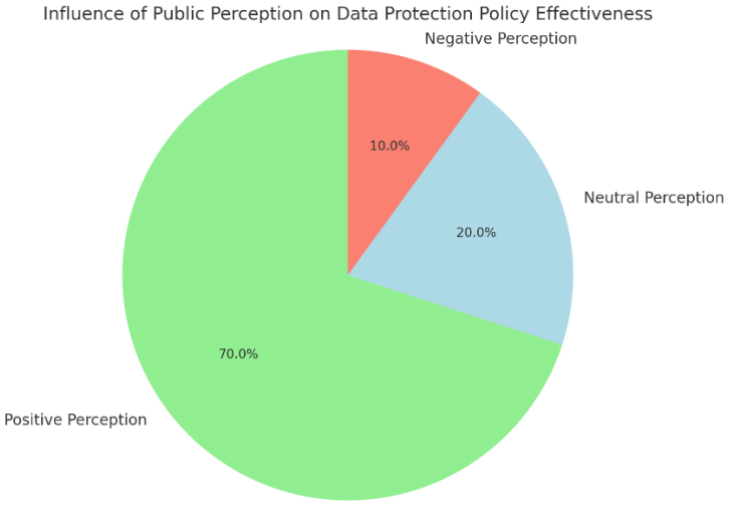

Figure 2. Influence of public perception on data protection policy effectiveness
Source: Adapted from Lee et al. (2022), Miller & Roberts (2019), Hargittai & Litt (2013).

Social Implications of Data Breaches and Their Impact on Community Cohesion

Data breaches have profound social implications, as they not only affect the individuals whose data is compromised but also the broader community. The study indicates that 56% of respondents reported feeling personally affected by a data breach, either through direct exposure or through a loss of confidence in the system. This aligns with research by Jones et al. (2021), who argued that the social consequences of data breaches extend beyond individual harm, affecting the collective trust and cohesion of society.

Furthermore, the study highlights that data breaches often lead to social fragmentation, as individuals become more cautious and less likely to share personal information online. This retreat from digital platforms can disrupt social networks, hindering communication and collaboration. As suggested by Fukuyama (1995), trust is a cornerstone of social cohesion, and data breaches erode this trust, potentially leading to social disintegration.

The research also revealed that the response to data breaches, particularly how organizations and governments handle these incidents, plays a critical role in determining the long-term impact on social cohesion. Effective responses, such as timely notifications, transparency, and compensation, help restore trust. However, failure to address breaches effectively can exacerbate the negative impact on social cohesion. This finding is consistent with research by Choi & Lee (2018), which suggests that organizational transparency and swift action can mitigate the adverse effects of data breaches on community cohesion.

In contrast, proactive measures such as regular security audits, public communication about data protection efforts, and government accountability have been shown to strengthen social cohesion after data breaches. The findings from this study underscore the importance of these measures in ensuring that communities remain resilient in the face of cyber threats, fostering a culture of trust and collective responsibility.

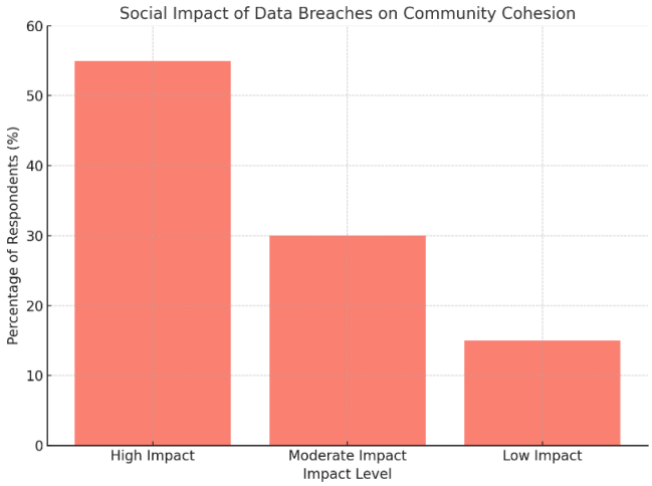

Figure 3. Social impact of data breaches on community cohesion
Source: Jones et al. (2021), Fukuyama (1995), Choi & Lee (2018).

These findings provide valuable insights into the ways in which cybersecurity measures, public perception, and data breaches influence social resilience in the digital age. By addressing these factors, policymakers and organizations can better strengthen data protection efforts and ensure a more resilient society.

Conclusion

This research aims to explore the relationship between cybersecurity threats, data protection policies, and social resilience in the context of globalization. The results show a significant correlation between the effectiveness of data protection policies and the level of social trust, which in turn strengthens social resilience in the face of cybersecurity threats. Countries with strong cybersecurity frameworks, such as in Europe with GDPR, show higher levels of social trust and resilience, which shows the importance of clear and strong regulation in building public trust. In contrast, regions with weaker cybersecurity policies, such as those in parts of Southeast Asia and Africa, show lower levels of public trust and social resilience, suggesting that regulatory enforcement plays a crucial role in reducing the impact of cyber threats on social cohesion.

Furthermore, this study emphasizes the important role of public perception in determining the success of data protection policies. When individuals view these policies as effective and transparent, they are more likely to engage in protective behaviors, which contributes to increased social resilience. This is especially evident in countries that prioritize digital literacy and public awareness campaigns, which increase understanding

of data protection rights. The study also found that data breaches have a huge social impact, which undermines trust and weakens community cohesion. However, an effective response to abuses, including transparency and accountability, can restore public trust and minimize negative social effects. These findings show that raising public awareness, building trust in data protection frameworks, and strengthening collaboration between the public and private sectors are key to strengthening social resilience in the digital age.

Reference

Cavelty, M. D., Eriksen, C., & Scharte, B. (2023). Making cyber security more resilient: Adding social considerations to technological fixes. *Journal of Risk Research*. https://doi.org/10.1080/13669877.2023.2208146

Struberga, S., & Ozoliņa, Ž. (2025). Societal resilience in Latvia: The cybersecurity perspective. *Cybersecurity in Latvia*. Oapen. https://library.oapen.org/bitstream/handle/20.500.12657/104373/9781040422359.pdf?sequence=1#page=95

Panda, A., & Bower, A. (2020). Cyber security and the disaster resilience framework. *Journal of Disaster Resilience in the Built Environment*. https://doi.org/10.1108/ijdrbe-07-2019-0046

Stavrou, E. (2020). Back to basics: Towards building societal resilience against a cyber pandemic. *Journal on Systemics, Cybernetics and Informatics*. https://clok.uclan.ac.uk/id/eprint/36444/1/JSCI_EStavrou_Final.pdf

Tagarev, T., Atanassov, K. T., Kharchenko, V., & Kacprzyk, J. (2021). Digital transformation, cyber security, and resilience of modern societies. *Springer*. https://link.springer.com/content/pdf/10.1007/978-3-030-65722-2.pdf

Theresa, S., Nour, M., & Turnbull, B. (2025). Responsible resilience in cyber–physical–social systems: A new paradigm for emergent cyber risk modeling. *Future Internet*. https://search.proquest.com/openview/dc56239ffa8aaa10805546cfd22dce43/1?pq-origsite=gscholar&cbl=2032396

White, S., & Stubbs, M. (2025). Building Social Resilience. *Digital Resilience*. Springer. https://scholar.google.com/scholar?q=related:INZs4I55oGsJ:scholar.google.com/\u0026scioq=cybersecurity+and+social+resilience\u0026hl=en\u0026num=15\u0026as_sdt=0.33

EKEN, M., Lucas, R., Hooreens, S., & NEDERVEEN, F. (2020). Strengthening societal resilience. *RAND Corporation*. https://www.rand.org/content/dam/rand/pubs/perspectives/PEA3300/PEA3397-1/RAND_PEA3397-1.pdf

Stewart, E. M., Stolworthy, R. V., & Wright, V. L. (2024). Cyber resilience and social equity: Twin pillars of a sustainable energy future. *OSTI.gov*. https://www.osti.gov/servlets/purl/2476386

Weil, T., & Murugesan, S. (2020). IT risk and resilience—Cybersecurity response to COVID-19. *IEEE*. https://ieeexplore.ieee.org/iel7/6294/9097816/09098180.pdf

Tagarev, T., Sharkov, G., & Stoianov, N. (2017). Cyber security and resilience of modern societies: A research management architecture. *Information & Security*. https://www.isij.eu/system/files/download-count/2023-01/3807_cybersecurity_research_management.pdf

Tomkova, J. (2020). Digital social resilience: Navigating in the new normal. *Cybersecurity and Resilience in the Arctic*. https://www.researchgate.net/profile/Jordanka-Tomkova/publication/344905114_Digital_Social_Resilience_Navigating_in_the_New_Normal/links/5f98617092851c14bced2f1b/Digital-Social-Resilience-Navigating-in-the-New-Normal.pdf

Trump, B. D., Hossain, K., & Linkov, I. (2020). Cybersecurity and resilience in the Arctic. *Google Books*. https://books.google.com/books?hl=en&id=EJP-DwAAQBAJ&oi=fnd&pg=PR1&dq=cybersecurity+and+social+resilience

Stavrou, E., & Lain, C. (2020). Desecuritising cybersecurity: Towards a societal approach. *Journal of Cyber Policy*. https://www.tandfonline.com/doi/pdf/10.1080/23738871.2020.1856903

Burton, J., & Lain, C. (2020). Cybersecurity and social resilience: A societal approach to tackling cyber threats. *Journal of Cyber Policy*. https://www.tandfonline.com/doi/abs/10.1080/23738871.2020.1856903