Hochschule Neu-Ulm
University of Applied Sciences

Bachelor Thesis
in the bachelor program
Information Management and Business Communication
at University of Applied Sciences Neu-Ulm

Evaluation of cyber security frameworks to ensure sustainability in value networks

1st examiner:	Prof. Dr. Tobias Engel
Author:	Bubacare David Nyabally (291336)
Topic received:	03.06.2024
Date of submission:	27.08.2024

Abstract

This bachelor thesis investigates the intersection between cybersecurity and sustainability within value networks, focusing on the integration of economic, social, and environmental dimensions to ensure long-term viability and positive societal contributions. As global value networks grow increasingly complex and interdependent, the need for robust cybersecurity measures that also support sustainability objectives has become essential. The research employs a two-phased methodology: an extensive literature review and qualitative expert interviews. The literature review highlights the critical aspects of sustainability in value networks and evaluates the role of cybersecurity frameworks in managing risks and ensuring resilience. Expert interviews provide insights into the practical challenges of balancing economic pressures with sustainability goals and emphasize the environmental impacts of cybersecurity measures, particularly energy consumption.

The findings reveal that while cybersecurity is crucial for maintaining data integrity, operational reliability, and stakeholder trust, it also poses challenges, such as increased energy use, which may conflict with environmental sustainability goals. The study concludes by proposing an integrated approach that aligns cybersecurity with sustainability strategies, addressing both operational resilience and environmental impact. This research contributes to the academic discourse by highlighting the need for a more holistic approach to cybersecurity and sustainability in the context of value networks.

Hochschule Neu-Ulm
University of Applied Sciences

List of contents

List of abbreviations

CIS	*Center for Internet Security*
COBIT	*Control Objectives for Information and Related Technologies*
C-SCRM	*cybersecurity supply chain risk management*
CSF	*Cybersecurity Framework*
CSV	*Creating Shared Value*
GDPR	*General Data Protection Regulation*
ISO	*International Organization for Standardization*
ITIL	*Information Technology Infrastructure Library*
PRAM	*Privacy Framework and Privacy Risk Assessment Methodology*
SSCM	*Sustainable Supply Chain Management*
TBL	*Triple Bottom Line*

List of illustrations

List of tables

1 Introduction

The rapid evolution of digital technologies and the growing emphasis on sustainable development have brought two seemingly distinct fields, meaning cybersecurity and sustainability, into a new and critical intersection. As global value networks become increasingly complex and interconnected, the need to protect these networks from cyber threats while ensuring sustainable practices has emerged as a not yet well researched field. This bachelor thesis explores the intricate relationship between cybersecurity and sustainability within value networks, emphasizing how effective cybersecurity measures can support and enhance sustainable business practices.

Value networks, which encompass the interconnected relationships between various entities that create, exchange, and benefit from value, are central to modern business operations. These networks are not only economic systems but also social and environmental ones, as they involve diverse stakeholders and impact communities and ecosystems. As businesses strive to integrate sustainability into their operations, while balancing economic viability with social responsibility and environmental stewardship, they must also navigate the growing threats posed by cyber risks. Cybersecurity, traditionally viewed as a technical or operational concern, can be increasingly recognized as a critical component of sustainability, ensuring the integrity, reliability, and resilience of value networks. This thesis focuses on three main areas: the concept of sustainability in value networks, relevant cybersecurity frameworks, and the influence of cybersecurity on sustainability. The investigation begins with an exploration of sustainability in value networks, examining how economic, social, and environmental objectives are integrated to ensure long-term viability and positive contributions to society. The study then delves into cybersecurity frameworks, specifically the NIST Cybersecurity Framework 2.0 (NIST CSF 2.0), ISO 27001, and CIS Controls Version 8, analyzing their role in managing cybersecurity risks within value networks. Finally, the thesis examines how cybersecurity measures impact the sustainability of value networks, particularly in maintaining data integrity, ensuring reliable operations, and preserving stakeholder trust.

The primary objective of this thesis is to establish a comprehensive understanding of the critical intersections between sustainability and cybersecurity within value networks. By doing so, it aims to contribute to the academic discourse on sustainable development and cybersecurity, offering insights into how these fields can be integrated to enhance the overall sustainability of business operations. Furthermore, the thesis seeks to provide practical guidance for organizations looking to implement cybersecurity measures that not only protect their value networks but also support their sustainability goals.

Understanding the interplay between cybersecurity and sustainability is essential in today's digital and environmentally conscious world. As businesses and policymakers increasingly recognize the importance of both fields, this research provides a timely and necessary examination of how cybersecurity can support sustainability in value networks. By addressing this intersection, the thesis contributes to the development of more resilient, secure, and sustainable business practices, ultimately supporting broader goals of sustainable development and digital security.

2 Theoretical background

The theoretical background chapter of this bachelor thesis provides a foundational understanding of the key concepts and frameworks that support this study. This chapter is divided into three sub-chapters: Sustainability in Value Networks, Relevant Cybersecurity Frameworks, and the Influence of Cybersecurity on Sustainability in Value Networks. **Chapter 2.1 Sustainability in Value Networks**, explores the concept of sustainability within the context of value networks. It emphasizes the importance of maintaining and enhancing economic, social, and environmental performance over time. This section highlights the complex relationships between entities that create, exchange, and benefit from value within these networks. **Chapter 2.2 Relevant Cybersecurity Frameworks** provides an overview of three prominent cybersecurity frameworks: the NIST Cybersecurity Framework 2.0 (NIST CSF 2.0), ISO 27001, and the CIS Controls Version 8. Each framework offers unique approaches to managing cybersecurity risks, tailored to different organizational needs and sectors. **Chapter 2.3 Influence of Cybersecurity on Sustainability in Value Networks**, examines how cybersecurity measures impact the sustainability of value networks. Effective cybersecurity is crucial for maintaining data integrity, ensuring reliable operations, and preserving stakeholder trust, all of which are essential for sustainable business practices.

“Sustainability in Value Networks” provides the overarching framework for understanding the need for sustainable practices. “Relevant Cybersecurity Frameworks” offers the tools and methodologies necessary to protect these practices from cyber threats. Finally, the “Influence of Cybersecurity on Sustainability in Value Networks” ties the concepts together, illustrating how cybersecurity supports the overall sustainability goals by ensuring the integrity and reliability of value networks. In conclusion, this chapter establishes a comprehensive foundation for the thesis, detailing the critical intersections between sustainability and cybersecurity within value networks.

2.1 Sustainability in value networks

The concept of sustainability in value networks has garnered significant attention in recent years due to the growing emphasis on sustainable development and responsible business practices. A value network encompasses a complex set of relationships between various entities that create, exchange, and benefit from value. Sustainability in value networks refers to the ability of these networks to maintain and enhance their economic, social, and environmental performance over time. According to Armstrong (2015), a sustainable value network is one where each participant contributes and receives value in ways that sustain both their individual operations and the network as a whole (Armstrong, 2015). This is supported by Pedersen et al. (2023) opinion that, sustainability within a value network is achieved when each participant contributes and receives value in a manner that supports both their individual operations and the network as a whole (Pedersen et al., 2023). Pedersen et al. (2023) also claim that sustainability in value networks should encompass prioritizing long-term viability over short-term gains to foster shared value among all stakeholders (Pedersen et al., 2023). Reinecke et al. (2023) highlight that businesses must align their value networks with sustainability principles which involves rethinking supply chain management practices to ensure that sustainability is embedded at every stage of the value creation process (Reinecke et al., 2023). According to Enquist et al. (2015) sustainability in value networks refers to the integration of economic, environmental, and social goals to ensure long-term viability and value creation that benefits all stakeholders while minimizing environmental impact (Enquist et al., 2015). They describe this as embedding social and environmental governance into business practices, fostering value co-creation among stakeholders (Enquist et al., 2015). Seuring and Müller discuss (2008) sustainable supply chain management (SSCM) as balancing material, information, and capital flows with economic, environmental, and social dimensions (Seuring & Müller, 2008). Hart and Milstein (2003) emphasize the need for sustainable value frameworks that address global challenges while creating competitive advantages (Hart & Milstein, 2003). The **Triple Bottom Line** (TBL) approach, introduced by Elkington (1998) emphasizes balancing social, environmental, and economic performance. TBL can be crucial for sustainable value creation by integrating social, environmental, and economic dimensions into business strategies and operations (Elkington, 1998). The **Circular Economy** model promotes resource efficiency by closing loops through recycling, reusing, and regenerating products and materials, thus fostering sustainability within value networks (Borgatti & Li, 2009). **Stakeholder Theory**, proposed by Freeman (1984) and further developed in recent research, argues that addressing the needs of all stakeholders, including employees, customers, and the community, leads to better long-term outcomes and more resilient value networks (Freeman et al., 2017). **Network Theory** in sustainable supply chains highlights the importance of relationships and interactions between different entities to enhance sustainability outcomes (Borgatti & Li, 2009). According to Villena and Gioia (2020) sustainability in value networks should consider all processes from resource extraction to product disposal, aiming to minimize negative impacts and maximize positive contributions to society and the environment (Villena & Gioia, 2020).

Economic sustainability involves maintaining financial health and creating economic value. Companies achieve this by improving efficiency, reducing waste, and innovating in product and service offerings. Economic sustainability ensures that businesses remain competitive and profitable while investing in sustainable practices. For instance, lean manufacturing principles can reduce costs and enhance productivity, contributing to overall economic sustainability. Mollenkopf et al. (2010) discuss how green, lean, and global supply chains can enhance performance and sustainability (Mollenkopf et al., 2010). **Environmental sustainability** focuses on reducing environmental impact through sustainable resource management, minimizing waste and emissions, and protecting ecosystems. This involves practices such as using renewable energy, enhancing energy efficiency, and adopting circular economy principles. The circular economy model promotes resource efficiency by closing loops through recycling, reusing, and regenerating products and materials (Kirchherr et al., 2017). **Social sustainability** addresses the impact of business operations on people, including employees, customers, suppliers, and communities. It involves ensuring fair labor practices, enhancing community engagement, and promoting diversity and inclusion. Companies that prioritize social sustainability invest in the well-being of their employees, support local communities, and ensure their supply chains are free from exploitative practices (Rank et al., 2022). Porter and Kramer (2011) argue that creating shared value (CSV) involves addressing societal needs and challenges through business models that enhance the company's competitiveness while advancing social and economic conditions in the communities where it operates (Porter & Kramer, 2011). This approach highlights the intersection of business success and societal progress, advocating for strategies that do not just mitigate negative impacts but actively create positive outcomes. Sustainability in value networks also involves collaboration across the supply chain. This includes working with suppliers, customers, and other stakeholders to develop sustainable practices and innovations. Companies may engage in partnerships to develop new technologies that reduce environmental impact or improve resource efficiency. Seuring and Müller (2008) state that sustainable supply chain management requires integrating sustainability criteria into supply chain operations, emphasizing the need for collaboration and transparency across the network (Seuring & Müller, 2008). Tantalo and Priem (2014) discussed the concept of value creation through stakeholder synergy, emphasizing that sustainable value creation involves aligning the interests of various stakeholders. By fostering synergy among stakeholders, businesses can achieve competitive advantages and strong financial performance. The authors argue that long-term sustainability is achievable when businesses prioritize the needs and expectations of all essential stakeholders, including employees, customers, suppliers, and the broader community (Tantalo & Priem, 2014). Closs et al. (2011) highlighted the role of supply chain management in supporting sustainability across end-to-end value chains. They pointed out that businesses engaged in sustainability initiatives are more likely to see significant value creation related to sustainability. The authors emphasized that sophisticated supply chain strategies, which incorporate sustainability considerations, are essential for enhancing the overall sustainability of value chains(Closs et al., 2011).

In summary, sustainability in value networks is a multifaceted concept that requires integrating economic, environmental, and social objectives into business operations. It involves adopting practices that ensure long-term viability, minimize negative impacts, and maximize positive contributions to society and the environment.

2.2 Relevant cybersecurity frameworks

This chapter delivers an overview of the three most prominent cybersecurity frameworks: the **NIST Cybersecurity Framework 2.0** (NIST CSF 2.0), **ISO 27001**, and the **CIS Controls Version 8**. Each of these frameworks offers unique approaches to managing cybersecurity risks, tailored to various organizational needs and sectors.

While the NIST CSF 2.0, ISO 27001, and CIS Controls Version 8 are dedicated cybersecurity frameworks, **ITIL** (Information Technology Infrastructure Library) and **COBIT** (Control Objectives for Information and Related Technologies) are broader IT governance frameworks. ITIL focuses on IT service management, providing guidelines to align IT services with business needs, whereas COBIT offers a comprehensive framework for IT management and governance. Both ITIL and COBIT include cybersecurity elements but are not specifically designed for it. However, ITIL and COBIT can complement the cybersecurity frameworks discussed in this chapter but were excluded from deeper analysis due to their lack of cybersecurity focus.

2.2.1 NIST CSF 2.0

The **NIST Cybersecurity Framework 2.0 (NIST CSF 2.0)**(National Institute of Standards and Technology, 2024)**,** developed by the National Institute of Standards and Technology, provides enhanced guidance for organizations across various sectors, including industry, government, academia and nonprofits, to manage cybersecurity risks. The CSF 2.0 is designed to be flexible, allowing organizations to tailor it to their unique cybersecurity needs and risk landscapes.

The CSF 2.0 consists of three main components: the CSF Core, CSF Profiles, and CSF Tiers. These components provide a comprehensive structure for managing cybersecurity outcomes, planning for current and future cybersecurity postures, and assessing the maturity of an organization's cybersecurity practices.

The core of the framework (**CSF Core**) is a set of high-level cybersecurity outcomes organized into six primary Functions. Each Function is divided into Categories and Subcategories, which provide detailed guidance on specific outcomes.

Function	Description
Govern	Establishes, communicates, and monitors the organization’s cybersecurity risk management strategy and policies.
Identify	Focuses on understanding the organization’s assets and the associated cybersecurity risks.
Protect	Involves implementing safeguards to manage and mitigate cybersecurity risks.
Detect	Entails monitoring and identifying potential cybersecurity events.
Respond	Outlines actions to be taken in response to detected cybersecurity incidents.
Recover	Details the processes for restoring capabilities or services affected by cybersecurity incidents.

Tabelle 1: NIST CSF 2.0 Core Functions (National Institute of Standards and Technology, 2024)

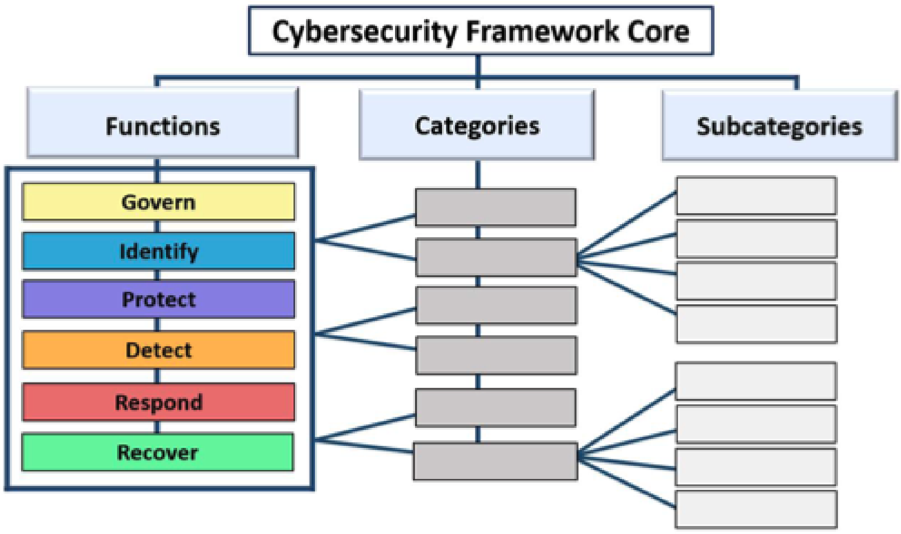


Abbildung 1: CSF Core Structure (National Institute of Standards and Technology, 2024)

CSF Profiles describe an organization’s current and desired cybersecurity postures using the CSF Core outcomes. The **Current Profile** specifies the outcomes that an organization is currently achieving, whereas the **Target Profile** outlines the desired outcomes that the organization aims to achieve in the future. Profiles help organizations tailor the CSF to their specific needs, assess their current cybersecurity status, identify gaps, and prioritize actions to improve their cybersecurity posture.

CSF Tiers characterize the rigor and maturity of an organization’s cybersecurity risk management practices. They range from Tier 1 (Partial) to Tier 4 (Adaptive):

Tier	Description
Tier 1 Partial	Cybersecurity risk management is ad hoc and not formalized.
Tier 2 Risk Informed	Risk management practices are approved by management but may not be consistent across the organization.
Tier 3 Repeatable	Risk management practices are formally established as policy and consistently applied.
Tier 4 Adaptive	Cybersecurity practices are continuously improved based on lessons learned and predictive indicators.

Tabelle 2: CSF Tiers (National Institute of Standards and Technology, 2024)

In comparison to the first iteration, the CSF 2.0 introduces several enhancements. **Governance and Supply Chain Risk Management** emphasizes the importance of governance and managing cybersecurity risks across supply chains. It includes integrating cybersecurity considerations into broader enterprise risk management strategies. NIST also provides supplementary online resources, including Informative References, Implementation Examples, and Quick Start Guides. These resources are regularly updated and offer detailed guidance for implementing the CSF. Community Profiles are developed as baseline for specific sectors, technologies, or threat types, helping organizations to develop tailored Target Profiles.

The CSF 2.0 is designed to be applicable to organizations of all sizes and sectors. It provides a flexible framework that can be tailored to address unique risks and technologies. The framework assists organizations in several key areas. Organizations can describe their current or target cybersecurity postures, identify gaps, and assess progress toward achieving cybersecurity goals. The CSF helps organizations to prioritize actions for managing cybersecurity risks in alignment with their mission, as well as legal and regulatory requirements. The framework provides a common language for internal and external communication about cybersecurity risks, capabilities, needs, and expectations. It supports the inclusion of cybersecurity risk management within an organization's overall ERM framework. The CSF 2.0 helps translate cybersecurity terminology into general risk management language, facilitating better communication with executives and alignment with other risk management activities.

Additionally, the CSF 2.0 can be integrated with specific risk management programs. The Privacy Risk Management program addresses privacy risks related to cybersecurity incidents and offers integration with the NIST Privacy Framework and Privacy Risk Assessment Methodology (PRAM). The Supply Chain Risk Management program includes detailed guidance on managing cybersecurity risks across supply chains, highlighting the importance of cybersecurity supply chain risk management (C-SCRM). The Emerging Technologies program accommodates risks associated with emerging technologies such as artificial intelligence, providing guidance on integrating AI risk management with cybersecurity and privacy considerations.

Overall, the NIST Cybersecurity Framework (CSF) 2.0 is designed to help organizations manage cybersecurity risks comprehensively. Its structured approach, through the CSF Core, Profiles, and Tiers, provides a clear roadmap for organizations to understand, assess, prioritize, and communicate their cybersecurity strategies effectively.

2.2.2 ISO/IEC 27001:2022

ISO 27001 is an international standard for information security management systems (ISMS). It outlines the requirements for establishing, implementing, maintaining, and continuously improving an ISMS, focusing on risk management and protecting information assets (International Standard Organization, 2022). It encompasses the assessment and treatment of information security risks tailored to an organization’s needs. It is designed to be universally applicable, regardless of the organization's size, type, or nature and is structured to assist organizations in safeguarding their information assets.

The framework is divided into several key Core Components that collectively ensure a robust and effective ISMS.

Core Component	Description
Context of the Organization	Organizations are required to identify and understand internal and external issues that can impact their ISMS. This involves recognizing the needs and expectations of interested parties and defining the scope of the ISMS.
Leadership	Top management must demonstrate leadership and commitment by integrating ISMS requirements into business processes, providing necessary resources, and establishing

	an information security policy. They are responsible for defining roles, responsibilities, and authorities to ensure the ISMS's effectiveness.
Planning	The standard mandates a systematic approach to addressing risks and opportunities. This includes defining a risk assessment process, identifying and analyzing risks, and determining appropriate risk treatment options. Information security objectives should be measurable, aligned with the organization’s policy, and regularly reviewed.
Support	Adequate resources, competence, awareness, communication, and control of documented information are critical. The standard ensures that all personnel understand their roles and the importance of maintaining information security.
Operation	Organizations must implement and control processes to meet ISMS requirements and risk treatment plans. Regular information security risk assessments and controls for externally provided processes, products, or services are essential.
Performance Evaluation	Continuous monitoring, measurement, analysis, and evaluation of the ISMS performance are required. Regular internal audits and management reviews ensure the ISMS remains effective and aligned with organizational goals.
Improvement	The standard emphasizes continual improvement. Organizations must address nonconformities, evaluate the need for corrective actions, and implement necessary changes to enhance the ISMS.

Tabelle 3: ISO/IEC 27001:2022 Core Components (International Standard Organization, 2022)

Additionally, the standard provides a comprehensive list of information security controls which are categorized into organizational, people, physical, and technological controls, ensuring a holistic approach to information security.

Control	Description
Organizational Controls	These include policies for information security, defining roles and responsibilities, segregation of duties, maintaining contact with authorities and special interest groups, and integrating information security into project management.
People Controls	This category encompasses background verification, terms and conditions of employment, awareness and training, disciplinary processes, responsibilities after termination, confidentiality agreements, remote working, and event reporting.
Physical Controls	Controls in this category focus on defining security perimeters, securing physical entry, protecting against environmental threats, and ensuring the security of off-premises assets.
Technological Controls	Technological measures include protecting user end-point devices, managing privileged access rights, ensuring secure authentication, protecting against malware, managing

	technical vulnerabilities, and establishing secure coding principles.

Tabelle 4: ISO/IEC 27001:2022 Controls (International Standard Organization, 2022)

The ISO/IEC 27001:2022 standard provides a robust framework for managing information security risks. Its comprehensive approach ensures that organizations can protect their information assets, maintain stakeholder trust, and comply with legal and regulatory requirements.

2.2.3 CIS Controls

The **CIS Controls Version 8**, released by the Center for Internet Security (CIS), provides a set of prioritized actions to protect organizations and data from cyber threats. The document is the result of extensive collaboration among security experts, offering a community-driven approach to enhancing cybersecurity (Center for Internet Security, 2021). The controls are structured to help organizations implement cybersecurity best practices. They are designed to be feasible and applicable across various types and sizes of organizations, ranging from small businesses to large enterprises. The Controls focus on actionable steps that organizations can take to protect themselves against the most common and significant cyber threats. The approach is based on five key principles.

Key principle	**Description**
Offense Informs Defense	The Controls are based on specific knowledge of attacker behavior and are prioritized according to the most critical actions to stop the most important attacks.
Focus	The Controls aim to help defenders identify the most critical actions to take, avoiding the temptation to solve every security problem.
Feasibility	Each recommendation is practical to implement.
Measurability	The Controls are designed to be measurable, simplifying language to avoid ambiguous interpretation.
Alignment	The Controls align with other governance, regulatory, and process management frameworks to ensure cohesive integration with existing standards.

Tabelle 5: CIS Controls Key Principles (Center for Internet Security, 2021)

The document breaks down its Core Components (the Controls) into 18 main categories, each detailing specific actions (referred to as Safeguards) necessary for effective cybersecurity management.

Control	Description
Control 01: **Inventory and Control of Enterprise Assets**	Actively manage all enterprise assets, including end-user devices, network devices, and servers. This ensures complete visibility and control over assets to prevent unauthorized access and vulnerabilities.
Control 02: **Inventory and Control of Software Assets**	Maintain an accurate inventory of all software within the enterprise. This control ensures that only authorized and supported software is installed, reducing the risk of exploitation through outdated or unauthorized applications.
Control 03: **Data Protection**	Develop and implement processes and technical controls to safeguard sensitive data. This includes data classification, encryption, and secure data handling practices to protect against data breaches and unauthorized access.
Control 04: **Secure Configuration of Enterprise Assets and Software**	Ensure that all enterprise assets and software are configured securely according to best practices. This involves removing default settings that favor usability over security, regularly updating configurations, and applying necessary patches.
Control 05: **Account Management**	Manage user, administrator, and service accounts effectively. This includes maintaining an inventory of accounts, enforcing unique passwords, and regularly reviewing and revoking access to minimize the risk of unauthorized access.
Control 06: **Access Control Management**	Control access to enterprise assets and data based on users' roles and responsibilities. Implement multi-factor authentication (MFA) and ensure that access privileges are granted, managed, and revoked systematically.
Control 07: **Continuous Vulnerability Management**	Continuously identify and remediate vulnerabilities within the enterprise. Regular vulnerability assessments and timely application of patches are essential to protect against emerging threats.
Control 08: **Audit Log Management**	Collect, manage, and analyze audit logs to detect and respond to security incidents. This control ensures that critical logs are preserved, monitored, and used to investigate potential security breaches.
Control 09: **Email and Web Browser Protections**	Implement measures to protect against email and web-based threats. This includes configuring email filters, securing browsers, and educating users about phishing and other common attacks.

Control 10: **Malware Defenses**	Deploy and maintain anti-malware solutions to detect and mitigate malware threats. Regular updates and comprehensive scanning practices are crucial to prevent and respond to malware infections.
Control 11: **Data Recovery**	Develop and maintain data recovery procedures to ensure business continuity. Regular backups and tested recovery plans help restore data and operations quickly after an incident.
Control 12: **Network Infrastructure Management**	Secure and manage the network infrastructure to protect against attacks. This involves configuring network devices securely, segmenting networks, and monitoring network traffic for suspicious activities.
Control 13: **Network Monitoring and Defense**	Implement tools and processes to monitor network traffic and detect intrusions. This includes deploying intrusion detection systems (IDS) and intrusion prevention systems (IPS) to identify and mitigate threats.
Control 14: **Security Awareness and Skills Training**	Provide regular security awareness training to employees. Educating staff about security best practices and emerging threats helps build a security-conscious culture within the organization.
Control 15: **Service Provider Management**	Manage third-party service providers to ensure they meet security requirements. This includes assessing the security practices of service providers and ensuring that they comply with contractual obligations.
Control 16: **Application Software Security**	Ensure that application software is developed and maintained securely. This involves integrating security into the software development lifecycle (SDLC) and conducting regular code reviews and security testing.
Control 17: **Incident Response Management**	Develop and implement an incident response plan to handle security incidents effectively. This includes defining roles and responsibilities, establishing communication protocols, and regularly testing the incident response process.
Control 18: **Penetration Testing**	Conduct regular penetration testing to identify and address security weaknesses. Simulating attacks helps uncover vulnerabilities that may not be detected through other means and ensures that defenses are robust.

Tabelle 6: CIS Controls Core Components (Center for Internet Security, 2021)

The CIS Controls provide a detailed and actionable framework for organizations to improve their cybersecurity defenses. By focusing on practical steps informed by real-world attack data, the Controls help organizations prioritize the most critical actions to protect against the most common threats.

2.3 Influence of cybersecurity on sustainability in value networks

Cybersecurity significantly influences sustainability in value networks by protecting data integrity, ensuring reliable operations, and maintaining stakeholder trust. Effective cybersecurity measures prevent disruptions that could compromise environmental and social initiatives. Araujo et al. (2024) demonstrate that integrating cybersecurity strategies within supply chains enhances resilience and supports sustainable practices by mitigating risks associated with data breaches and operational failures (Araujo et al., 2024). Dlamini et al. (2009) highlight that robust cybersecurity frameworks contribute to sustainable development by safeguarding critical information infrastructure, supporting economic stability and social well-being (Dlamini et al., 2009). Additionally, Choo (2011) underscores that maintaining the confidentiality, integrity, and availability of data is essential for sustaining trust and operational continuity in value networks (Choo, 2011). Effective cybersecurity not only prevents financial losses and reputational damage but also ensures compliance with regulations and standards, promoting sustainable business practices. Romanosky (2016) discusses how cybersecurity measures can prevent data breaches that lead to significant financial losses and damage to a company's reputation, thereby maintaining stakeholder trust and supporting long-term sustainability (Romanosky, 2016). Compliance with regulatory requirements, such as the General Data Protection Regulation (GDPR), further enhances the ability to operate sustainably within the global market (Voigt & Bussche, 2017). Ruoslahti and Davis (2021) emphasize the broader societal impacts of cybersecurity. Their study suggests that cyber-attacks can lead to significant environmental damage, which in turn affects the sustainability of value networks. They propose incorporating societal impacts with cyber and e-skills to develop more resilient systems. The detrimental effects of cyber-attacks on the environment underscore the need for comprehensive cybersecurity measures to ensure sustainability in value networks (Ruoslahti & Davis, 2022). According to Lewis et al. (2014), effective information sharing is pivotal for maintaining the integrity and sustainability of value networks. By fostering a culture of transparency and collaboration, organizations can mitigate cyber threats and enhance the overall resilience of their supply chains (Lewis et al., 2014). Rashid et al. (2021) findings suggest that effective information sharing enhances the sustainability of value networks by optimizing the use of security assets. This economic perspective reinforces the necessity of collaborative efforts in cybersecurity to achieve sustainable outcomes (Rashid et al., 2021).

Operational reliability in supply chain management refers to the capability of a supply chain to perform its intended functions consistently over time without failure. This includes the smooth operation of processes, timely delivery of products, and maintenance of quality standards. High operational reliability ensures that supply chains can meet demand consistently and adapt to disruptions efficiently. It involves robust risk management, strategic planning, and the integration of advanced technologies such as AI and digital twins to enhance real-time monitoring and predictive analytics. This approach allows for the effective handling of disruptions and ensures the continuous ability to meet performance standards (Peters et al., 2022). A study by Kamalahmadi and Parast (2015) highlights that operational reliability involves the adaptive capability of a supply chain to reduce the probability of disturbances, resist the spread of these disturbances by maintaining control over operations, and recover by implementing effective reactive plans (Kamalahmadi & Parast, 2015). Additionally, Novak et al. (2021) emphasize that supply chains need to focus on maintaining core functionality by continually adapting and evolving in response to dynamic changes in the environment (Novak et al., 2021). Chiang et al. (2021) define operational reliability as the capability of the supply chain to consistently perform its intended functions over time without failure. This includes ensuring smooth operations, timely delivery of goods, and maintaining quality standards. Achieving high operational reliability involves implementing robust risk management strategies, strategic planning, and integrating advanced technologies such as artificial intelligence and digital twins for real-time monitoring and predictive analytics. These measures help the supply chain adapt to disruptions and continue meeting performance standards (Chiang et al., 2021).

Operational reliability in IT refers to the consistent performance of IT systems and services according to specified requirements. This includes ensuring minimal downtime, secure and accurate data handling, and uninterrupted support for business operations. Achieving high IT operational reliability involves rigorous testing, regular maintenance, effective incident management, and robust cybersecurity measures. This ensures continuous service delivery and protection against disruptions (Rajaguru & Matanda, 2019). For example, Rajaguru and Matanda (2019) discuss the role of IT as an inter-organizational information system that facilitates effective information transfer between supply chain members (Rajaguru & Matanda, 2019). According to Chow et al. (2007) Operational reliability in IT refers to the consistent and dependable performance of IT systems and services according to specified requirements. This includes minimizing downtime, ensuring data accuracy and security, and providing uninterrupted support for business operations. High operational reliability in IT is achieved through rigorous testing, regular maintenance, robust security measures, and effective incident management processes (Chow et al., 2007).

According to Siems et al. (2023) **stakeholder trust in supply chain management** is the confidence that stakeholders (including suppliers, customers, and partners) have in the reliability, integrity, and competence of the supply chain processes. It is built through transparent communication, consistent performance, and effective risk management. Technologies such as blockchain enhance this trust by providing transparent and tamper-proof records of transactions, ensuring reliability and integrity across the supply chain (Siems et al., 2023). A review by Panigrahi et al. (2018) highlights that stakeholder trust involves managing material, information, and capital flows among companies while considering economic, environmental, and social goals. Furthermore it involves understanding how stakeholder pressure can drive companies to adopt sustainable practices, thereby building trust (Panigrahi et al., 2018). According to Hörisch et al. (2014), integrating descriptive, instrumental, and normative approaches to stakeholder theory helps in understanding and managing stakeholder interests, which is essential for building trust. This integrative approach ensures that the various interests and concerns of stakeholders are addressed, enhancing the overall trust in the supply chain (Hörisch et al., 2014).

Stakeholder trust in an IT context refers to the confidence users and stakeholders have in the security, reliability, and transparency of IT systems and services provided by an organization. This trust is essential for user engagement, regulatory compliance, and maintaining an organization's reputation. Achieving high stakeholder trust involves implementing robust cybersecurity measures, ensuring data integrity, and maintaining transparency in IT operations and data handling practices (Le et al., 2021). Bracke et al. (2017) underline the role of social sustainability factors in building stakeholder trust. They argue that incorporating social sustainability practices, such as fair labor practices and community engagement, into IT and supply chain operations can significantly enhance stakeholder trust and corporate legitimacy (Bracke et al., 2017).

In conclusion, the intersection of cybersecurity and sustainability highlights the critical role of cybersecurity in maintaining the integrity, trust, and operational continuity of value networks.

3 Research methodology

The research methodology of this paper consists of a two staged approach combining both extensive literature review and expert interviews. The initial phase involved conducting an extensive literature review. Following the literature review, the research methodology incorporated qualitative expert interviews. The two phases aimed at addressing the following questions:

- What are the aspects of sustainability in value networks?
- What are the relevant cybersecurity frameworks?
- What is the influence of cybersecurity on sustainability?

Experts from the field of Cybersecurity, Sustainability and Value Networks were carefully selected based on their experience and expertise, ensuring that their contributions would be both relevant and insightful.

3.1 Literature research

The literature research methodology for this study was designed to systematically investigate the intersection of sustainability in value networks and cybersecurity frameworks. This chapter outlines the comprehensive approach taken, detailing the specific methods, databases, and keywords used to gather relevant literature. The methodology aligns with academically rigorous procedures to ensure the validity and reliability of the research findings. The literature review process was guided by established principles for conducting systematic reviews, as outlined by Kitchenham (2004) and Webster and Watson (2002). This structured approach ensured a thorough and unbiased collection and analysis of existing literature (Kitchenham, 2004; Webster & Watson, 2002).

Initially, COBIT was considered as a specific cybersecurity framework. However, after further research, it was reclassified along with ITIL as a general IT governance framework due to its broader focus on IT management and governance rather than cybersecurity specifics. Both COBIT and ITIL, while encompassing some cybersecurity elements, do not provide dedicated cybersecurity guidelines, hence their exclusion from in-depth analysis in favor of more focused frameworks like NIST CSF, ISO 27001, and CIS Controls. This decision to reclassify COBIT was made in accordance to Kitchenham (2004) stating that the research scope should be clearly defined to ensure a focused literature review (Kitchenham, 2004). As required by the thesis examiner the following databases were systematically searched to ensure comprehensive coverage of the relevant literature: ProQuest, EBSCOhost, AIS eLibrary and IEEE Xplore (Engel, 2019).

In accordance to the systematic approach by Booth et al. (2012), a comprehensive list of keywords and combinations was developed based on the research focus areas (Booth et al., 2012). The keywords were chosen to cover various aspects of sustainability in value networks, cybersecurity, and the specific frameworks. The following tables show the keywords and combinations used during the research in chapter 2. Theoretical background.

Sustainability and/in	**Cybersecurity and/in**	**Value Networks**
Sustainable	Cybersecurity framework	Value chain
Economic	NIST	Supply chain
Environmental	ISO 27001	Supply chain management
Social	CIS Controls	
	COBIT	
	ITIL	

Tabelle 7: Key words and combinations used in the literature search

The search strategy was developed to include peer-reviewed journal articles, conference papers, and key industry reports. This approach was consistent with guidelines for systematic reviews to ensure a broad and thorough search (Kitchenham, 2004; Webster & Watson, 2002). Publication bias was minimized by including a wide range of sources and ensuring that the search was not restricted to a few top journals (Webster & Watson, 2002). Studies were excluded if they did not address the topics of sustainability, cybersecurity and value chains or their respective interactions. The relevance of each source was assessed based on its alignment with the research questions and objectives of sustainability, cybersecurity and value chains or a combination or the previous three topics. This step ensured that only relevant and high-quality studies were included in the review (Kitchenham, 2004). The extracted data was synthesized to identify common themes, gaps in the literature, and areas for future research. This synthesis involved categorizing the findings into relevant themes such as sustainability, cybersecurity and value chains and identifying patterns and discrepancies (Webster & Watson, 2002). The retrieved literature was collected and organized using the reference management tool Zotero to facilitate easy access and citation.

3.2 Interviews

The second part of the research for this study involves conducting expert interviews to gain insights into the aspects of sustainability within these networks, relevant cybersecurity frameworks, and the influence of cybersecurity on sustainability.

Qualitative research is widely recognized for its methodological rigor and the depth of understanding it provides through direct communication with the involved participants (Helfferich, 2011). It is particularly suitable for exploring complex topics like the interplay between cybersecurity and sustainability in value networks. Expert interviews are a predominant method in empirical research, especially for obtaining specialized knowledge (Meuser & Nagel, 2009). These interviews have been conducted with professionals who have expertise in either sustainability, cybersecurity, value networks or a combination of the previous. The preparation for expert interviews requires substantial subject knowledge to avoid the risk of the interviewer being perceived as incompetent (Mieg & Brunner, 2001). The theoretical foundation established in chapter 2 of this thesis ensures the necessary expertise for conducting these interviews.

Creation of the interview guide

The guideline-supported interview is an effective tool for conducting expert interviews, aimed at collecting expert knowledge. The method in this study involves a semi-structured format (Myers & Newman, 2007). The semi-structured interview format was employed to provide flexibility and enable interviewees to express their perspectives fully (Myers & Newman, 2007).

The interview guide was created in accordance with Mieg and Näf (2005). They state that the guide should be structured into introductory questions, question blocks according to the topics and subtopics and finally acknowledgements and farewell (Mieg & Näf, 2005). In the context of this thesis, questions were gathered around the subtopics of sustainability in value networks, relevant cybersecurity frameworks and the influence of cybersecurity on sustainability to be addressed during the interview.

1. Introduction:
   Brief overview of the study and consent process.
2. Main Questions:
   Covering the subtopics of sustainability, cybersecurity frameworks, and their influence on value networks.
3. Conclusion:
   Summarizing key points and thanking participants.

For a detailed insight into the questions, the interview guide can be found in the Appendix 9.1.

Selection of Interview Partners

Interview partners were selected based on their expertise and experience in sustainability, cybersecurity, value networks or any combination of those topics. This process was more difficult than expected. As there are few experts who combine expertise in the three areas, more experts with expertise in one of the areas were selected. Efforts were made to ensure a diverse range of perspectives by including experts from different sectors and organizational sizes. Potential interviewees were contacted via email or LinkedIn, with a follow-up to arrange interview schedules and provide the interview guide in advance to facilitate preparation.

Conducting the Interviews

The Interviews were conducted via the online meeting Zoom. Each interview began with an introduction to the research topic, a short overview of the thesis. The next steps involved obtaining the consent for recording the conversation from the interview partner.

The interviews were recorded to allow the interviewer to focus on the conversation and ensure accurate transcription and analysis later. A trial interview was conducted to refine the interview process and ensure the interview guide's effectiveness.

Analysis of the interviews

The transcribed recording of the interviews provides the basis for the analysis of the interviews. The transcripts of the interviews can be found in Appendices 9.2.1 to 9.2.5 for easier viewing. The data collected was treated anonymously, which is why the interviews are referred to as Interview 1, Interview 2, etc.

The individual interview partners are presented in an overview table below.

Interview	Role	Organization	Expertise
Interview 1	Cybersecurity Manager	Consulting Company	Cybersecurity
Interview 2	Cybersecurity Director	Consulting Company	Cybersecurity
Interview 3	Sustainability Director	Consulting Company	Sustainability
Interview 4	CSO	Database provider	Sustainability
Interview 5	Supply Chain Manager	Medium-sized company	Value Networks

Tabelle 8: Overview of interview partners

During the transcription process, the primary data was converted into tertiary data via the secondary data. This means that the original conversation is transformed into a transcript, i.e. a written record of the conversation, with the help of the audio recording (Flick, 2018). Depending on the aim of the research, the required accuracy of the wording in the transcription varies. In speech-analytical contexts, pauses and stresses are also represented in the transcript (Flick, 2018). This accuracy was not necessary for the research objectives of this thesis. The transcription rules that were used to transcribe the interviews are listed below.

Rule	Description
Interviewer	Speech passage from the interviewer
Person 1, Person 2, Person 3, etc.	Speech passage of the respective interview partner
(Q#)	Marking of question # from the interview guide for better orientation
XX	Reduction for reasons of identification

Tabelle 9: Rules of transcription

The next step was to evaluate the interviews. Summarized qualitative content analysis according to Mayring (2020) was used as the evaluation method. According to Mayring, the basic idea of qualitative content analysis is to systematically analyze the linguistic material or texts (Mayring, 2000). Since the research work deals with a subject area that has been little researched to date, inductive category development was used, but for easier analysis every question was tagged with a set of codewords (see Table 10: Assigned Codewords). To achieve this, the material was broken down and examined step by step. At the beginning, each individual interview was analyzed and important sections of text that seemed helpful in answering the research questions were marked and categorized. In the next step, the text passages from the different interviews were compared with each other to identify the key aspects for answering the research questions. During the comparison, frequently mentioned aspects were considered particularly important. Nevertheless, individual aspects were also listed. The results of this analysis can be found in Chapter 4.2. Overall, this was done with software support based on the code words previously assigned to each question (see Table 10: Assigned Codewords) This was done with the MAXQDA software.

Question	Codewords
Q1	integration, sustainability, value network
Q2	Economic sustainability, social sustainability, environmental sustainability
Q3	stakeholder, governance
Q4	NIST, ISO, CIS
Q5	data integrity, operational reliability, stakeholder trust
Q6	cybersecurity impact on sustainability
Q7	cybersecurity measures, sustainable outcomes
Q8	strategic integration, mutual benefits

Tabelle 10: Assigned Codewords

The codes were then categorized into six deducted categories (see Chapter 4.2 Interviews). These results were then compared, and commonalities or differences were worked out.

4 Results

This chapter presents the findings of the research conducted. The results are divided into two main sections: the first presents the insights derived from a comprehensive literature review, and the second contains the outcomes of expert interviews conducted during the study.

4.1 Literature review

Sustainability in value networks encompasses economic, environmental, and social dimensions, which collectively ensure long-term viability and positive contributions to society and the environment. **Economic Sustainability** involves maintaining financial health and creating economic value. This is achieved by improving efficiency, reducing waste, and innovating in product and service offerings. For instance, lean manufacturing principles can reduce costs and enhance productivity, contributing to overall economic sustainability. This ensures businesses remain competitive and profitable while investing in sustainable practices. **Environmental Sustainability** focuses on reducing environmental impact through sustainable resource management, minimizing waste and emissions, and protecting ecosystems. This includes practices such as using renewable energy, enhancing energy efficiency, and adopting circular economy principles. The circular economy model promotes resource efficiency by closing loops through recycling, reusing, and regenerating products and materials, thereby fostering sustainability within value networks. **Social Sustainability** addresses the impact of business operations on people, including employees, customers, suppliers, and communities. It involves ensuring fair labor practices, enhancing community engagement, and promoting diversity and inclusion. Companies that prioritize social sustainability invest in the well-being of their employees, support local communities, and ensure their supply chains are free from exploitative practices.

Several prominent **cybersecurity frameworks** provide guidelines for managing cybersecurity risks and enhancing overall security posture. The **NIST CSF 2.0**, developed by the National Institute of Standards and Technology, offers flexible guidance applicable across various sectors. It consists of three main components: the CSF Core, CSF Profiles, and CSF Tiers. The CSF Core includes functions such as Govern, Identify, Protect, Detect, Respond, and Recover, providing a comprehensive structure for managing cybersecurity outcomes. CSF Profiles describe an organization’s current and desired cybersecurity state, helping to tailor the CSF to specific needs, identify gaps, and prioritize actions. CSF Tiers indicate the maturity of cybersecurity practices, ranging from Tier 1 (Partial) to Tier 4 (Adaptive). The **ISO 27001** is an international standard for information security management systems (ISMS). It outlines requirements for establishing, implementing, maintaining, and improving an ISMS, focusing on risk management and protecting information assets. The framework includes core components such as Context of the Organization, Leadership, Planning, Support, Operation, Performance Evaluation, and Improvement, ensuring a robust and effective ISMS. Additionally, it provides comprehensive information security controls categorized into organizational, people, physical, and technological controls. The **CIS Controls Version 8**, released by the Center for Internet Security (CIS), offers a set of prioritized actions to protect organizations and data from cyber threats. The controls are based on five key principles: Offense Informs Defense, Focus, Feasibility, Measurability, and Alignment. The framework includes 18 main categories, each detailing specific actions necessary for effective cybersecurity management, ensuring practical steps informed by real-world attack data.

Cybersecurity influences sustainability in value networks by protecting data integrity, ensuring reliable operations, and maintaining stakeholder trust. Effective cybersecurity measures prevent disruptions that could compromise environmental and social initiatives. Integrating cybersecurity strategies within supply chains enhances resilience and supports sustainable practices by mitigating risks associated with data breaches and operational failures. Robust cybersecurity frameworks contribute to sustainable development by safeguarding critical information infrastructure, supporting economic stability, and promoting social well-being. Furthermore, maintaining the **confidentiality, integrity, and availability of data** is essential for sustaining trust and operational continuity in value networks. Effective cybersecurity not only prevents financial losses and reputational damage but also ensures compliance with regulations and standards, thereby promoting sustainable business practices. Compliance with regulatory requirements, such as the General Data Protection Regulation (GDPR), enhances the ability to operate sustainably within the global market. Cybersecurity also plays a vital role in maintaining **operational reliability**. This includes the consistent performance of IT systems and services according to specified requirements, ensuring minimal downtime, secure and accurate data handling, and uninterrupted support for business operations. Achieving high operational reliability involves rigorous testing, regular maintenance, effective incident management, and robust cybersecurity measures. **Stakeholder trust** in supply chain management is built through transparent communication, consistent performance, and effective risk management. Technologies such as blockchain enhance this trust by providing transparent and tamper-proof records of transactions, ensuring reliability and integrity across the supply chain. In an IT context, achieving high stakeholder trust involves implementing robust cybersecurity measures, ensuring data integrity, and maintaining transparency in IT operations and data handling practices.

The table below presents a comparative analysis of three major cybersecurity frameworks across economic, social, sustainability, and value network aspects. This provides a baseline for evaluating the frameworks regarding ensuring sustainability in value networks. Based on the analysis the NIST CSF 2.0 framework provides the most comprehensive option to ensure sustainability in value networks due to its dedicated Governance and Supply Chain Risk Management section.

Aspect		**NIST CSF 2.0**	**ISO 27001**	**CIS Controls**
Economic	Focus	Reduce economic losses	Reduce economic losses	Reduce economic risks
	Method	Risk-based approach to prioritize cybersecurity investments based on potential impact, optimizing the allocation of resources.	Implementation of controls, and structured risk management with regular assessments to prevent breaches and ensure compliance with legal and regulatory requirements.	Proactive measures such as regular updates, patches, inventory control, and network management to prevent vulnerabilities and mitigate risks.
Social	Focus	Collaboration and communication	Comprehensive security culture	Comprehensive security culture
	Method	Highlights the importance of sharing threat information and best practices, involving various stakeholders in the cybersecurity process.	Training and awareness programs, ensuring that employees at all levels understand their responsibilities and are equipped to handle security issues effectively.	Guidelines for security awareness and training programs, addressing different roles and responsibilities across the organization.
Sustainability	Focus	Effective risk management	Efficient resource management	Efficient resource management
	Method	Focuses on avoiding redundant or unnecessary security measures, thereby reducing the overall environmental footprint.	Ensures that resources are not wasted on outdated or ineffective security measures through regular reviews and updates.	Efficient resource use through accurate inventory management and secure disposal of obsolete devices, indirectly minimizing electronic waste.
Value Network	Focus	Comprehensive supply chain security	Supply chain security	Supply chain security
	Method	Evaluates and monitors suppliers, integrates security requirements into contracts, and ensures all elements of the value network are protected against cyber threats.	Identifies and assesses risks associated with suppliers and partners, ensuring the entire value network maintains high security standards.	Integrates security measures into third-party service provider contracts, conducting due diligence, and continuous monitoring and management of suppliers.

Tabelle 11: Detailed aspects of Cybersecurity Frameworks

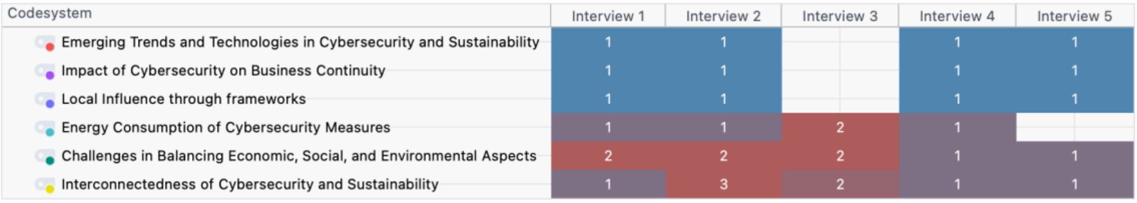
4.2 Interviews

This chapter presents the findings from the analysis of the conducted expert interviews. As explained in chapter 3.2, the analysis was conducted using a summarized qualitative content analysis approach, which allowed for the identification of six key categories. The following table provides an overview of the deducted overarching categories which acts as basis for the discussion in Chapter 5.

Category	Description	Mentions
Interconnectedness of Cybersecurity and Sustainability	This category captures the idea that cybersecurity is an aspect of sustainability.	8
Challenges in Balancing Economic, Social, and Environmental Aspects	This category reflects the ongoing struggle within organizations to balance the economic, social, and environmental aspects of sustainability. Economic pressures often lead to compromises that can undermine sustainability efforts.	8
Energy Consumption of Cybersecurity Measures	This category focuses on the concern that cybersecurity measures, particularly data duplication and intensive computational requirements, significantly increase energy consumption, which negatively impacts sustainability goals.	5
Local Influence through frameworks	Regulatory frameworks and industry standards influence how cybersecurity and sustainability are managed within organizations and across value networks. These frameworks vary depending on region and industry.	4
Impact of Cybersecurity on Business Continuity	Effective cybersecurity is critical for ensuring business continuity, which directly supports sustainability in value networks by preventing disruptions that could have widespread environmental and social impacts.	4
Emerging Technologies in Cybersecurity and Sustainability	The potential of emerging technologies like AI and blockchain to simultaneously enhance cybersecurity and support sustainability.	4

Tabelle 12: Deducted Categories

The following graphic shows a heat map of the frequency of the categories per interview. This shows that both Interview 1 and Interview 2, in their role as cybersecurity experts, mentioned all categories. Of the two sustainability experts from interview 3 and interview 4, only interview 4 was able to show a mention in all categories. However, the sustainability expert from interview 3 had a higher score in the specific categories of his expertise. The value network expert from interview 5 was able to show a mention in all but one category.



Codesystem	Interview 1	Interview 2	Interview 3	Interview 4	Interview 5
Emerging Trends and Technologies in Cybersecurity and Sustainability	1	1		1	1
Impact of Cybersecurity on Business Continuity	1	1		1	1
Local Influence through frameworks	1	1		1	1
Energy Consumption of Cybersecurity Measures	1	1	2	1	
Challenges in Balancing Economic, Social, and Environmental Aspects	2	2	2	1	1
Interconnectedness of Cybersecurity and Sustainability	1	3	2	1	1

Abbildung 2: Code Matrix

The interviews revealed some **interconnectedness between cybersecurity and sustainability**, particularly in how cybersecurity practices can influence the trust and transparency essential for sustainable business operations. Participants emphasized that effective cybersecurity is crucial for maintaining trust with customers and partners, which is fundamental for achieving sustainability goals within value networks. For instance, one participant noted, “Cybersecurity and sustainability are a bit interconnected, I think. I mean cybersecurity is very important for sustaining trust with our customers and partners, which should be a cornerstone of any sustainable business” (Interview 4, Lines 65-69). Another participant highlighted the potential risks of cybersecurity breaches, stating that a "breach in cybersecurity probably can have a big impact, not just financially but also in terms of trust and reputational damage, which can undermine our sustainability in supply chains" (Interview 5, Lines 65-67). However, not every participant shared this opinion. One person stated that: “I think in general the touch points between cybersecurity and sustainability are not very common. There's not a big overlap, so to say” (Interview 2, Lines 145-146) but in the same answer supplemented that: “cybersecurity only works if you know what you have and if you analyse what you have, you might come across anything that might not be very efficient in a sustainability sense.” (Interview 2, Lines 149-150).

The **challenge of balancing economic, social, and environmental aspects of sustainability** was a recurring theme across all interviews. Participants from various organizations acknowledged the difficulty in aligning these three dimensions, particularly when faced with economic pressures that often take precedence. One participant explained, "Balancing these aspects is always challenging [...] Economically, we need to stay competitive and profitable, which often requires making tough decisions [...] Usually, the economic factors unfortunately always win so to say" (Interview 4, Lines 19-27). Similarly, another participant highlighted the complexities, stating, "So the current situation is that the economic aspects are absolutely front and forward. I would probably say globally, in 98% of all companies, they're the only drivers that actually matter” (Interview 3, Lines 70-72).

The analysis also revealed concerns regarding the **energy consumption associated with cybersecurity measures**, particularly in relation to data storage and processing. Participants noted that the energy-intensive nature of cybersecurity practices, such as data duplication and the operation of data centers, can have significant environmental impacts. For example, one participant remarked, "If that's the case, then the implications on sustainability are enormous [...] you will need a lot of energy for any data centre that's run to store duplicates or anything else that you want to secure" (Interview 3, Lines 162-168). Another participant discussed that: “We will need more and more energy in the future. For example, AI or using AI for cybersecurity purposes. This needs a lot of energy and the generation of renewable energy is already a problem” (Interview 1, Lines 141-143).

The **local influence through frameworks** on both cybersecurity and sustainability was another significant theme. Participants emphasized that compliance with industry-specific regulations, such as ISO 27001 in Germany and TISAX for the Automotive industry, plays a crucial role in shaping their cybersecurity practices, which in turn can impact sustainability. One participant noted, "As a German company of course ISO 27001 [...] In our case that means TISAX of course" (Interview 5, Lines 46-48). Another participant mentioned the NIST Framework in a global context: “The key ones we use for instance is NIST. So that's the American standard for cybersecurity, which we use, especially if we are working in the global context (Interview 2, Lines 100-101).

Cybersecurity was also recognized as a key factor in **ensuring business continuity**, which directly supports sustainability in value networks by preventing disruptions that could have widespread environmental and social impacts. Participants discussed how cybersecurity measures are essential for protecting supply chains from cyber-attacks, which could otherwise lead to delays, increased waste, and higher costs. For instance, a participant stated, "A breach in cybersecurity probably can have a big impact, not just financially but also in terms of trust and reputational damage, which can undermine our sustainability in supply chains" (Interview 5, Lines 65-67). Another participant echoed this sentiment, stating: “I think, cybersecurity might help to ensure the integrity and security of data. That should actually support transparency and accountability which are key elements of sustainability. Additionally, by preventing cyber-attacks, you can of course avoid disruptions that could have massive impacts on everything” (Interview 4, Lines 67-70).

5 Discussion

This chapter discusses the findings presented in the results section, integrating insights from both the literature review and the expert interviews to address the three research questions:

(1) What are the aspects of sustainability in value networks?

(2) What are the relevant cybersecurity frameworks?

(3) What is the influence of cybersecurity on sustainability?

Each research question is addressed by comparing the insights derived from the literature review with those obtained from the expert interviews. The findings are then interpreted and evaluated in the context of the broader research goal of evaluating cybersecurity frameworks to ensure sustainability in value networks.

5.1 Aspects of Sustainability in Value Networks

The literature review identified three primary aspects of sustainability in value networks: economic, environmental, and social dimensions. Economic sustainability focuses on financial health and value creation, environmental sustainability emphasizes reducing environmental impacts, and social sustainability involves fair labor practices and community engagement. The expert interviews largely supported these findings, with several interviewees emphasizing the challenge of balancing economic, social, and environmental aspects. For example, Person 4 mentioned the difficulty of aligning sustainability goals with economic pressures, often leading to compromises that undermine sustainability efforts stating that: „Balancing these aspects is always challenging, you know. Especially in a tech-driven industry like ours. Economically, we need to stay competitive and profitable, which often requires making tough decisions. […] Usually, the economic factors unfortunately always wins so to say" (Interview 4, Lines 19-28). Person 5 supported this sentiment, highlighting: "Balancing these aspects is a challenge, particularly for a medium-sized company as XX where resources are often limited. Economically most importantly, we need to stay competitive, which sometimes means making tough decisions. However, we try to not compromise on social and environmental responsibilities. […] In supply chains, this is even more difficult, I think. Because we rely on the things our partners do" (Interview 5 Lines, 19-25). This aligns with the literature, which also noted the complex interplay between these dimensions. Additionally, the interviews introduced the concept of transparency and collaboration within value networks as critical for maintaining sustainability, particularly in supply chain management. Person 4 stated that: "In value networks, transparency and collaboration are essential" (Interview 4, Line 39) and Person 5 said: "In regard to the supply chain, I think transparency is the most important thing I would say." (Interview 5, Lines 36-37). This was less emphasized in the literature review but is essential in practice, as highlighted by Person 3, who stressed that: "So looking at this concept of sustainability very holistically along the whole value chain, there's various concepts you can use.[…] So sustainability needs to be considered there because if every company only considers sustainability within its own company premises, you leave out most of the, in many segments, you would leave out most of the pollution, most of the risks, and most of the impact. […] And so it's actually essential to have to take this very holistic view from cradle to cradle." (Interview 3, Lines 43-50).

The interviews suggest that while the theoretical aspects of sustainability in value networks are well understood, their practical implementation is challenging, particularly when economic pressures dominate decision-making. The need for transparency and collaboration across the supply chain emerged as a crucial factor in ensuring sustainability, an aspect that may not have been fully explored in the literature. The interviews also suggest that companies are often forced to prioritize economic sustainability over environmental and social aspects, especially in industries where margins are thin, or competition is fierce. This prioritization can lead to sustainability being more of a strategic goal rather than an operational reality, where compromises are often made at the expense of long-term environmental and social benefits. The findings underscore the importance of a balanced approach to sustainability in value networks. The literature provides a solid foundation for understanding the theoretical aspects, but the interviews reveal the complexities of applying these principles in real-world scenarios. The emphasis on transparency and collaboration as essential components of sustainability in value networks is a valuable addition to the existing body of knowledge. However, the ongoing struggle to balance economic, social, and environmental factors indicates that more robust frameworks and support mechanisms may be needed to help organizations align these aspects effectively.

5.2 Relevant Cybersecurity Frameworks

The literature review identified several key cybersecurity frameworks, including NIST CSF 2.0, ISO 27001, and CIS Controls Version 8. NIST CSF 2.0 was highlighted as particularly comprehensive, with dedicated sections on governance and supply chain risk management. The interviews confirmed the use of the ISO and NIST frameworks in practice. For instance, Person 1 mentioned: "Okay. If I remember it right, XX is certified according to 27001 […]. Then we have the NIST framework." (Interview 1, Lines 75-76) and Person 2 mentioned: "Cybersecurity frameworks? The key ones we use for instance is NIST. So that's the American 101 standard for cybersecurity, which we use, especially if we are working in the global context. If we work in Germany, we mainly use the ISO 27001 norm, which is the, let's say the German equivalent." (Interview 2, Lines 100-103). The interviews also provided information on an additional, automotive specific, framework. Person 1, Person 2 and Person 5 mentioned TISAX: "We also ensure compliance with industry-specific regulations […]. In our case that means TISAX of course." (Interview 5, Lines 46-48). However, there was some uncertainty regarding the specific effectiveness of these frameworks in managing cybersecurity risks within value networks, with several interviewees unable to provide detailed assessments. Person 5 mentioned: "Well okay. That is something I do not know in detail. I am sorry. But from a supply chain perspective, the effectiveness probably can vary depending on the maturity of the cybersecurity practices from your partners in the network.” (Interview 5, Lines 55-57) This suggests that while these frameworks are widely adopted, there may be gaps in understanding their practical impact on value networks.

The interviews also reveal a discrepancy between the theoretical strengths of cybersecurity frameworks as described in the literature and their perceived effectiveness in practice. This gap may be due to a lack of comprehensive understanding or expertise in applying these frameworks within specific industry contexts. The frameworks themselves may be robust, but their implementation and the level of awareness among practitioners could be areas for improvement. Additionally, the literature's focus on the economic and social dimensions of cybersecurity is supported by the interviews, which emphasized the importance of maintaining stakeholder trust and ensuring business continuity through effective cybersecurity measures. Person 4 said: “I mean cybersecurity is very important for sustaining trust with our customers and partners, which should be a cornerstone of any sustainable business.” (Interview 4, Lines 65-67). However, the interviews also highlighted that the environmental impact of cybersecurity measures, such as increased energy consumption, is often overlooked. This was mentioned by Person 1, Person 2 and Person 3. For example, Person 1 mentioned: “We will need more and more energy in the future. For example, AI or using AI for cybersecurity purposes. This needs a lot of energy and the generation of renewable energy is already a problem.” (Interview 1, Lines 141-143). Person 3 also highlighted that: “Because you keep duplicating your data and instead of, I don't know, 10 terabytes, you'd need 30 or a hundred terabytes for the same amount of information just to make sure that in case two of these locations become out of order, out of whatever reason, you can still access that. What this means is that you will need a lot of energy for any data centre that's run to store duplicates or anything else that you want to secure. It has a huge impact because of the energy intensity.” (Interview 3, Lines 163-168). This suggests that while frameworks like NIST CSF 2.0 and ISO 27001 are comprehensive, they may not fully address the environmental aspects of cybersecurity.

The literature provides a comprehensive overview of key cybersecurity frameworks, but the interviews suggest that more work is needed to bridge the gap between theory and practice. There may be a need for additional training or resources to help organizations better understand and implement these frameworks effectively. Furthermore, the environmental impact of cybersecurity, particularly in terms of energy consumption, should be more explicitly addressed in these frameworks to align with broader sustainability goals.

5.3 Influence of Cybersecurity on Sustainability

The literature review highlighted that cybersecurity could support sustainability by protecting data integrity, ensuring reliable operations, and maintaining stakeholder trust, all of which are essential for sustaining value networks. It also noted the importance of robust cybersecurity measures in preventing disruptions that could undermine sustainability initiatives. The interviews provided mixed perspectives on this relationship. Several interviewees recognized the interconnectedness between cybersecurity and sustainability, particularly in maintaining trust and preventing disruptions in supply chains. As an example Person 5 highlighted that: "So, then I think, that a breach in cybersecurity probably can have a big impact, not just financially but also in terms of trust and reputational damage, which can undermine our sustainability in supply chains. For example, I think if a cyber-attack disrupts the supply chain, it can lead to delays, increased waste, and higher costs which of course would be bad for the sustainability." (Interview 5, 65-69). However, others were less certain about the direct relationship between these two areas, with some interviewees expressing doubts about the significant overlap between cybersecurity and sustainability. Supporting the missing connection between Cybersecurity and Sustainability Person 2 mentioned: "I think in general the touch points between cybersecurity and sustainability are not very common. There's not a big overlap, so to say." (Interview 2, Lines 145-146) and later in the interview added: "Even though as mentioned, cybersecurity does not have an explicit sustainability focus." (Interview 2, Lines 178-179).

As already mentioned above in Chapter 5.2, one of the most critical insights from the interviews was the concern about the energy consumption associated with cybersecurity measures. Additionally, to the previously mentioned quotes regarding that subject, Person 2 stated: "On a larger scale, obviously I think one big factor is also the use of electricities in the modern IT world. So to say, if you think about cloud environments, if you think about the daily use of internet, obviously there's connected a lot of, let's say large scale data centres, transmission networks that also use a lot of energy. So I think that's one big factor nowadays where also the sustainability aspect comes into play to reduce energy consumption in the large scale data centres." (Interview 2, Lines 79-84) This was not extensively covered in the literature, indicating a potential area for further research.

The relationship between cybersecurity and sustainability is complex and multifaceted. While the literature emphasizes the positive contributions of cybersecurity to sustainability, particularly in maintaining trust and preventing disruptions, the interviews suggest that there may be unintended negative consequences, such as increased energy consumption. This points to a need for a more nuanced understanding of how cybersecurity practices can both support and hinder sustainability. The interviews also suggest that the integration of cybersecurity into sustainability strategies is still in its early stages, with many organizations treating these as separate issues. However, there is potential for greater alignment, particularly as emerging technologies like AI and blockchain offer opportunities to enhance both cybersecurity and sustainability simultaneously as mentioned by Person 2: "I think both cybersecurity and sustainability will benefit from a general modernization in infrastructure. […] So also the whole topic of AI and generative AI is obviously a big driver for cybersecurity, and I think the same can be applied for sustainability because sustainability obviously is very much data driven." (Interview 2, Lines 195-199).

The findings indicate that while cybersecurity is critical for supporting sustainability, particularly in ensuring business continuity and maintaining stakeholder trust, there are significant challenges to be addressed. The environmental impact of cybersecurity practices, particularly in terms of energy consumption, needs to be more explicitly considered in both academic research and practical frameworks. Furthermore, the integration of cybersecurity into broader sustainability strategies requires more attention, with a focus on leveraging emerging technologies to achieve this alignment.

5.4 Implications

The discussion of the research findings highlights the need for a more integrated approach to sustainability and cybersecurity within value networks. To address the challenges identified, this chapter proposes a detailed process that organizations could implement to ensure sustainability in their value networks while effectively managing cybersecurity risks. This process is designed to balance economic, social, and environmental aspects, leveraging both existing frameworks and emerging technologies. The proposed process consists of five key stages:

(1) Assessment

(2) Planning

(3) Implementation

(4) Monitoring and Evaluation

(5) Continuous Improvement.

Each stage is designed to ensure that sustainability and cybersecurity are considered holistically within value networks.

(1) Assessment

The first stage involves a comprehensive assessment of the current state of sustainability and cybersecurity within the organization and across its value network. This includes:

Sustainability Assessment: Conduct a life-cycle assessment (LCA) to identify the environmental, social, and economic impacts of the organization's products, services, and operations. This assessment should cover the entire value chain, from raw material sourcing to end-of-life disposal. The LCA should be complemented by social impact assessments to evaluate labor practices, community engagement, and other social factors.

Cybersecurity Assessment: Perform a cybersecurity risk assessment using frameworks based on your location or industry such as NIST CSF 2.0, ISO 27001, or CIS

Controls. This assessment should identify potential vulnerabilities within the value network, including risks related to data security, operational continuity, and stakeholder trust.

Integration Analysis: Analyze the overlap between sustainability and cybersecurity to identify areas where they intersect, such as the energy consumption of cybersecurity measures or the role of data integrity in maintaining stakeholder trust.

Methods: Life-Cycle Assessment (LCA), Cybersecurity Risk Assessment, Social Impact Assessment, Integration Analysis

Opportunities: Identifying synergies between sustainability and cybersecurity, such as using renewable energy to power data centers, can enhance both aspects simultaneously.

(2) Planning

Based on the assessment, the next stage involves strategic planning to address identified gaps and opportunities. This includes:

Goal Setting: Establish clear and measurable sustainability and cybersecurity goals. These should be aligned with the organization's overall strategy and consider the economic, social, and environmental dimensions. For example, a goal might be to reduce the carbon footprint of data centers by 30% while enhancing cybersecurity measures.

Framework Selection and Adaptation: Select the most appropriate cybersecurity frameworks based on location or industry (e.g., NIST CSF 2.0, ISO 27001) and adapt them to integrate sustainability considerations. This may involve customizing the frameworks to include energy efficiency metrics or supply chain transparency requirements.

Stakeholder Engagement: Engage key stakeholders, including suppliers, customers, and partners, to ensure alignment with the sustainability and cybersecurity goals. This may involve negotiating contracts that include specific sustainability and cybersecurity requirements or developing joint initiatives with partners.

(3) Implementation

The implementation stage focuses on executing the planned strategies and initiatives. This includes:

Operational Integration: Integrate sustainability and cybersecurity measures into day-to-day operations. For example, implement energy-efficient practices in data centers, such as optimizing cooling systems or adopting renewable energy sources, while simultaneously enhancing cybersecurity through regular updates and patches.

Technology Deployment: Utilize emerging technologies, such as AI and blockchain, to support both sustainability and cybersecurity. AI can be used to optimize energy consumption in IT infrastructure, while blockchain can enhance transparency and traceability in supply chains.

Training and Awareness: Develop training programs to ensure that employees and partners understand their roles in achieving the sustainability and cybersecurity goals. This should include training on both the environmental and security aspects of new technologies and practices.

(4) Monitoring and Evaluation

Continuous monitoring and evaluation are crucial to ensure that the implemented strategies are effective. This stage involves:

Performance Tracking: Use key performance indicators (KPIs) to monitor progress toward sustainability and cybersecurity goals. These KPIs should include both quantitative metrics (e.g., energy consumption, carbon emissions, number of cyber incidents) and qualitative assessments (e.g., stakeholder satisfaction, compliance levels).

Audits and Reviews: Conduct regular audits and reviews to ensure compliance with sustainability and cybersecurity frameworks. This may involve third-party assessments or internal reviews.

Feedback Mechanism: Establish a feedback mechanism to gather insights from employees, partners, and other stakeholders. This feedback should inform ongoing adjustments to the sustainability and cybersecurity strategies.

(5) Continuous Improvement

The final stage focuses on the continuous improvement of sustainability and cybersecurity practices. This includes:

Data-Driven Decision Making: Use the data collected during monitoring to make informed decisions about future initiatives. This may involve refining existing practices, adopting new technologies, or setting more ambitious goals.

Innovation and Adaptation: Encourage a culture of innovation within the organization, where new ideas and technologies are regularly tested and adopted to enhance sustainability and cybersecurity. This could involve pilot projects, R&D investments, or partnerships with startups and research institutions.

Long-Term Strategy Evolution: Regularly revisit the organization’s long-term sustainability and cybersecurity strategy to ensure it remains aligned with external changes, such as new regulations, market shifts, or technological advancements.

The following picture provides an overview of the proposed Integrated Sustainability-Cybersecurity Process:

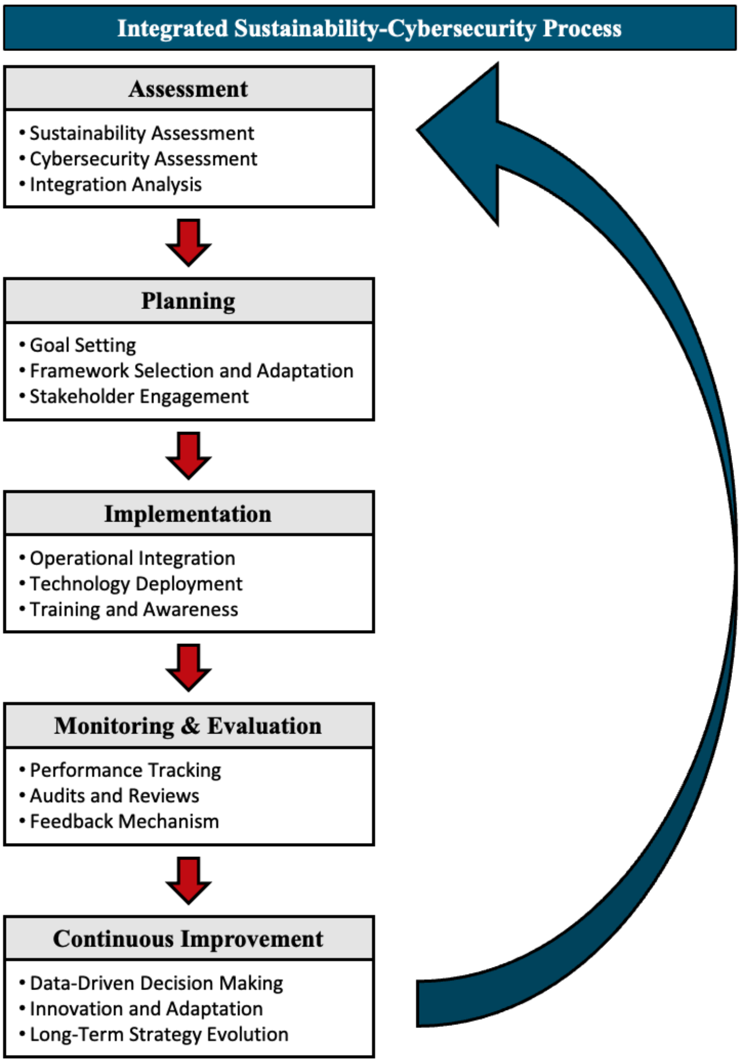

Integrated Sustainability-Cybersecurity Process
Assessment
• Sustainability Assessment
• Cybersecurity Assessment
• Integration Analysis
Planning
• Goal Setting
• Framework Selection and Adaptation
• Stakeholder Engagement
Implementation
• Operational Integration
• Technology Deployment
• Training and Awareness
Monitoring & Evaluation
• Performance Tracking
• Audits and Reviews
• Feedback Mechanism
Continuous Improvement
• Data-Driven Decision Making
• Innovation and Adaptation
• Long-Term Strategy Evolution

Abbildung 3: Integrated Sustainability-Cybersecurity Process

The integration of sustainability and cybersecurity within value networks presents several significant opportunities for organizations. By aligning sustainability goals with robust cybersecurity measures, companies can enhance their operational resilience, reduce environmental impact, and build stronger, more transparent relationships with stakeholders. The adoption of emerging technologies like AI and blockchain offers the potential to simultaneously improve energy efficiency and security, driving innovation and cost savings. Furthermore, a comprehensive approach that includes continuous monitoring, stakeholder engagement, and data-driven decision-making enables organizations to identify and address issues proactively, ensuring long-term sustainability and competitiveness. Ultimately, the synergy between sustainability and cybersecurity not only supports regulatory compliance and risk management but also fosters a culture of continuous improvement and innovation, positioning organizations to thrive in an increasingly complex and interconnected global market.

6 Limitations & Future research

This chapter addresses the limitations encountered during the research and outlines potential directions for future studies. While the investigation into the intersection of cybersecurity and sustainability within value networks has provided valuable insights, certain constraints appeared. Additionally, this chapter proposes future research avenues that could expand on the development of more integrated and sustainable practices within value networks.

6.1 Limitations

While the research provides valuable insights into the relationship between cybersecurity and sustainability within value networks, it is essential to acknowledge several limitations that may affect the generalizability and applicability of the findings.

The research relied on a relatively small number (5) of expert interviews, which may not fully capture the diversity of perspectives across different industries or regions. The sample size and the specific backgrounds of the interviewees could introduce bias, limiting the comprehensiveness of the findings. Future research could benefit from a broader range of interviews, including participants from various sectors and geographical locations. The study concentrated on three major cybersecurity frameworks evolving from the literature review, e.g. NIST CSF 2.0, ISO 27001, and CIS Controls Version 8, potentially overlooking other relevant frameworks such as TISAX that might offer different insights into the integration of cybersecurity and sustainability. Future studies should consider including a wider array of cybersecurity frameworks to provide a more holistic understanding. The analysis of the energy consumption associated with cybersecurity measures was largely based on qualitative data from expert interviews. The lack of quantitative data on actual energy usage limits the ability to assess the full environmental impact of cybersecurity practices. This constraint underscores the need for more detailed quantitative studies that can provide precise measurements of energy consumption related to various cybersecurity activities. The research presents a snapshot of the current state of cybersecurity and sustainability practices within value networks. However, the dynamic nature of both fields suggests that practices and their impacts can evolve over time. The absence of longitudinal data makes it difficult to assess how these practices may develop or how new technologies might influence the integration of cybersecurity and sustainability in the future. The literature review was comprehensive but may still reflect biases based on the selection of sources. The focus on specific themes within the literature might have led to the exclusion of alternative perspectives or emerging research areas. Future research should strive to incorporate a broader range of literature, including more recent studies and diverse academic and industry sources.

6.2 Future research

Based on the limitations and findings of this study, several areas for future research are identified. Future research should aim to include a more diverse set of industries and regions to capture a wider range of practices and challenges in integrating cybersecurity and sustainability. This could involve case studies or comparative analyses across different sectors, such as healthcare, finance, and manufacturing, as well as a focus on different regulatory environments. There is a need to explore additional cybersecurity frameworks beyond those covered in this study. Research could examine how other frameworks or industry-specific standards such as TISAX, contribute to sustainability within value networks. This would help to identify best practices and offer recommendations tailored to different organizational contexts. Given the concerns raised about the energy consumption of cybersecurity measures, future research should focus on quantitative analyses that measure the actual energy usage associated with different cybersecurity practices. Such studies could utilize data from real-world implementations and compare the efficiency of various technologies and practices. To better understand the long-term impacts of integrating cybersecurity and sustainability, future research should consider conducting longitudinal studies. These studies would track changes in organizational practices, technology adoption, and regulatory influences over time, providing insights into how these factors evolve and affect sustainability outcomes. The potential of emerging technologies such as AI and blockchain to enhance both cybersecurity and sustainability presents a fertile area for future research. Studies could investigate how these technologies can be effectively deployed to reduce energy consumption, improve transparency, and strengthen supply chain security. Additionally, research could explore the challenges and risks associated with these technologies, particularly concerning data privacy and ethical considerations. There is an opportunity to develop new, integrated frameworks that combine cybersecurity and sustainability into a cohesive approach for managing value networks. Future research could focus on designing and testing such frameworks, potentially drawing on interdisciplinary collaboration between experts in cybersecurity, sustainability, and value network management.

In conclusion, while this study has provided a foundational understanding of the interplay between cybersecurity and sustainability, further research is necessary to address the identified limitations and to explore the evolving challenges and opportunities in this critical area. By expanding the scope, incorporating quantitative data, and exploring new technologies and frameworks, future research can contribute to more robust and sustainable practices within global value networks.

7 Conclusion

This study explored the intersection of cybersecurity and sustainability within value networks, focusing on economic, environmental, and social aspects. The research was conducted through a comprehensive literature review and expert interviews. Challenges such as balancing economic pressures with sustainability goals and the environmental impact of cybersecurity measures, particularly energy consumption, were identified.

Sustainability in value networks contains economic, environmental, and social dimensions, with a critical emphasis on transparency and collaboration within supply chains. NIST CSF 2.0, ISO 27001 and TISAX have been identified as key frameworks, each contributing to the security and sustainability of value networks in different ways, with NIST CSF 2.0 being particularly comprehensive in general and TISAX being more specific for the automotive industry. Cybersecurity supports sustainability by ensuring business continuity, maintaining stakeholder trust, and protecting data integrity. However, it also presents challenges, such as increased energy consumption.

This study contributes to the academic understanding of the complex relationship between cybersecurity and sustainability, particularly in value networks. It highlights the importance of integrating these two areas, identifies gaps in current research, and suggests areas where further theoretical and empirical work is needed. The study also expands on the literature by addressing the environmental impact of cybersecurity measures, an area that has been underexplored. For practitioners, this study provides actionable insights into how cybersecurity frameworks can be implemented to support sustainability goals. The findings underscore the importance of transparency and collaboration in managing value networks and suggest practical steps for integrating cybersecurity into broader sustainability strategies. Additionally, the study highlights the need for organizations to consider the environmental impact of their cybersecurity practices and to explore emerging technologies that can enhance both cybersecurity and sustainability.

The study's limitations include a small sample size of expert interviews, which may not fully capture the diversity of perspectives across different industries or regions. The focus on a limited number of cybersecurity frameworks may overlook other relevant frameworks. Additionally, the analysis of energy consumption associated with cybersecurity measures was primarily qualitative, lacking quantitative data. Future research should include a more diverse set of industries and regions, explore additional cybersecurity frameworks, and conduct quantitative analyses of energy consumption associated with cybersecurity practices. Longitudinal studies could provide insights into how cybersecurity and sustainability practices evolve over time. Further investigation into emerging technologies such as AI and blockchain and their potential to enhance both cybersecurity and sustainability is also recommended.

In conclusion, this study provides a foundational understanding of the interplay between cybersecurity and sustainability within value networks, offering insights that are crucial for both academic research and practical application in today’s increasingly interconnected world.

8 References

Araujo, M., Machado, B., & Passos, F. (2024). Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance. *Applied Sciences*, *14*, 2116. https://doi.org/10.3390/app14052116

Armstrong, L. (2015). *Value Unchained*. forum for the future. https://www.truevaluemetrics.org/DBpdfs/Initiatives/Forum-for-the-Future/Value-Unchained-A-short-summary-of-value-networks.pdf

Booth, A., Papaioannou, D., & Sutton, A. (2012). *Systematic Approaches to a Successful Literature Review*.

Borgatti, S. P., & Li, X. (2009). On Social Network Analysis in a Supply Chain Context. *Journal of Supply Chain Management*, *45*(2), 5–22. https://doi.org/10.1111/j.1745-493X.2009.03166.x

Bracke, S., Yamada, S., Kinoshita, Y., Inoue, M., & Yamada, T. (2017). Decision Making within the Conceptual Design Phase of Eco-Friendly Products. *Procedia Manufacturing*, *8*, 463–470. https://doi.org/10.1016/j.promfg.2017.02.059

Center for Internet Security. (2021). *CIS Controls v8*.

Chiang, C.-T., Kou, T.-C., & Koo, T.-L. (2021). A Systematic Literature Review of the IT-Based Supply Chain Management System: Towards a Sustainable Supply Chain Management Model. *Sustainability*, *13*, 2547. https://doi.org/10.3390/su13052547

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719–731. https://doi.org/10.1016/j.cose.2011.08.004

Chow, H. K. H., Choy, K. L., & Lee, W. B. (2007). Knowledge management approach in build-to-order supply chains. *Industrial Management & Data Systems*, *107*(6), 882–919. https://doi.org/10.1108/02635570710758770

Closs, D., Speier, C., & Meacham, N. (2011). Sustainability to Support End-to-End Value Chains: The Role of Supply Chain Management. *Journal of the Academy of Marketing Science*, *39*(1), 101–116. https://doi.org/10.1007/s11747-010-0207-4

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information security: The moving target. *Computers & Security*, *28*(3), 189–198. https://doi.org/10.1016/j.cose.2008.11.007

Elkington, J. (1998). ACCOUNTING FOR THE TRIPLE BOTTOM LINE. *Measuring Business Excellence*, *2*(3), 18–22. https://doi.org/10.1108/eb025539

Engel, T. (2019). *Studentische Arbeiten_V0.1*.

Enquist, B., Petros Sebhatu, S., & Johnson, M. (2015). Transcendence for business logics in value networks for sustainable service business. *Journal of Service Theory and Practice*, *25*(2), 181–197. https://doi.org/10.1108/JSTP-09-2013-0189

Flick, U. (2018). *An introduction to qualitative research* (6th edition). Sage.

Freeman, R., Kujala, J., Sachs, S., & Stutz, C. (2017). Stakeholder Engagement: Practicing the Ideas of Stakeholder Theory. In *Stakeholder Engagement: Clinical Research Cases* (Vol. 46, pp. 1–12). Springer International Publishing. https://doi.org/10.1007/978-3-319-62785-4_1

Hart, S., & Milstein, M. (2003). Creating Sustainable Value. *Academy of Management Executive*, *17*. https://doi.org/10.5465/AME.2003.10025194

Helfferich, C. (2011). *Die Qualität qualitativer Daten* (4. Auflage). VS Verlag.

Hörisch, J., Freeman, R. E., & Schaltegger, S. (2014). Applying Stakeholder Theory in Sustainability Management: Links, Similarities, Dissimilarities, and a Conceptual Framework. *Organization & Environment*, *27*(4), 328–346. https://doi.org/10.1177/1086026614535786

International Standard Organization. (2022). *ISO/IEC 27001*.

https://www.iso.org/standard/27001

Kamalahmadi, M., & Parast, M. (2015). A Review of the Literature on the Principles of Enterprise and Supply Chain Resilience: Major Findings and Directions for Future Research. *International Journal of Production Economics, 171*(1). https://doi.org/10.1016/j.ijpe.2015.10.023

Kirchherr, J., Reike, D., & Hekkert, M. (2017). Conceptualizing the circular economy: An analysis of 114 definitions. *Resources, Conservation and Recycling, 127*, 221–232. https://doi.org/10.1016/j.resconrec.2017.09.005

Kitchenham, B. (2004). Procedures for Performing Systematic Reviews. *Keele, UK, Keele Univ., 33*.

Le, C. T. D., Pakurár, M., Kun, I. A., & Oláh, J. (2021). The impact of factors on information sharing: An application of meta-analysis. *PLOS ONE, 16*(12), e0260653. https://doi.org/10.1371/journal.pone.0260653

Lewis, R., Louvieris, P., Abbott, P., Clewley, N., & Jones, K. (2014). CYBERSECURITY INFORMATION SHARING: A FRAMEWORK FOR SUSTAINABLE INFORMATION SECURITY MANAGEMENT IN UK SME SUPPLY CHAINS. *ECIS 2014 Proceedings*. https://aisel.aisnet.org/ecis2014/proceedings/track14/4

Mayring, P. (2000). Qualitative Content Analysis. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research [On-Line Journal], Http://Qualitative-Research.Net/Fqs/Fqs-e/2-00inhalt-e.Htm, 1*.

Meuser, M., & Nagel, U. (2009). The Expert Interview and Changes in Knowledge Production. In *Interviewing Experts* (1st ed., pp. 17–42). Palgrave Macmillan London. https://doi.org/10.1057/9780230244276_2

Mieg, H. A., & Brunner, B. (2001). *Experteninterviews: Eine Einführung und Anleitung* [Application/pdf]. ETH Zürich. http://hdl.handle.net/20.500.11850/145320

Mieg, H. A., & Näf, M. N. (2005). *Experteninterviews in den Umwelt- und Planungswissenschaften. Eine Einführung und Anleitung*. ETH Zürich.

Mollenkopf, D., Stolze, H., Tate, W., & Murfield, M. (2010). Green, Lean, and Global Supply Chains. *International Journal of Physical Distribution & Logistics Management*, *40*, 14–41. https://doi.org/10.1108/09600031011018028

Myers, M., & Newman, M. (2007). The Qualitative Interview in IS Research: Examining the Craft. *Information and Organization*, *17*, 2–26. https://doi.org/10.1016/j.infoandorg.2006.11.001

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29; p. NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Novak, D., Wu, Z., & Dooley, K. (2021). Whose resilience matters? Addressing issues of scale in supply chain resilience. *Journal of Business Logistics, 42*. https://doi.org/10.1111/jbl.12270

Panigrahi, S. S., Bahinipati, B., & Jain, V. (2018). Sustainable supply chain management: A review of literature and implications for future research. *Management of Environmental Quality: An International Journal*, *30*(5), 1001–1049. https://doi.org/10.1108/MEQ-01-2018-0003

Pedersen, S., Clausen, C., & Jørgensen, M. S. (2023). Navigating value networks to co-create sustainable business models: An actionable staging approach. *Business Strategy and the Environment*, *32*(1), 240–258. https://doi.org/10.1002/bse.3127

Peters, E., Knight, L., Boersma, K., & Uenk, N. (2022). Organizing for supply chain resilience: A high reliability network perspective. *International Journal of Operations & Production Management*, *43*. https://doi.org/10.1108/IJOPM-03-2022-

0167

Porter, M. E., & Kramer, M. R. (2011). Creating Shared Value. *Harvard Business Review*. https://archive.is/WUBXJ

Rajaguru, R., & Matanda, M. (2019). Role of compatibility and supply chain process integration in facilitating supply chain capabilities and organizational performance. *Supply Chain Management: An International Journal*, *24*. https://doi.org/10.1108/SCM-05-2017-0187

Rank, S., Contreras, F., & Abid, G. (2022). Editorial: Social sustainability at work: A key to sustainable development in business. *Frontiers in Psychology*, *13*. https://doi.org/10.3389/fpsyg.2022.1108935

Rashid, Z., Noor, U., & Altmann, J. (2021). Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem. *Future Generation Computer Systems*, *124*, 436–466. https://doi.org/10.1016/j.future.2021.05.033

Reinecke, P. C., Küberling-Jost, J. A., Wrona, T., & Zapf, A. K. (2023). Towards a dynamic value network perspective of sustainable business models: The example of RECUP. *Journal of Business Economics*, *93*(4), 635–665. https://doi.org/10.1007/s11573-023-01155-7

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, *2*(2), 121–135. https://doi.org/10.1093/cybsec/tyw001

Ruoslahti, H., & Davis, B. (2022). Societal Impacts of Cyber Security Assets of Project ECHO. *WSEAS TRANSACTIONS ON ENVIRONMENT AND DEVELOPMENT*, *17*, 1274–1283. https://doi.org/10.37394/232015.2021.17.116

Seuring, S., & Müller, M. (2008). From a literature review to a conceptual framework for sustainable supply chain management. *Journal of Cleaner Production*, *16*(15), 1699–1710. https://doi.org/10.1016/j.jclepro.2008.04.020

Siems, E., Seuring, S., & Schilling, L. (2023). Stakeholder roles in sustainable supply chain management: A literature review. *Journal of Business Economics*, *93*(4), 747–775. https://doi.org/10.1007/s11573-022-01117-5

Tantalo, C., & Priem, R. (2014). Value Creation Through Stakeholder Synergy. *Strategic Management Journal*, *37*(2). https://doi.org/10.1002/smj.2337

Villena, V. H., & Gioia, D. A. (2020, March 1). A More Sustainable Supply Chain. *Harvard Business Review*. https://hbr.org/2020/03/a-more-sustainable-supply-chain

Voigt, P., & Bussche, A. von dem. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer.

Webster, J., & Watson, R. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, *26*(2). https://doi.org/10.2307/4132319

9 Appendix

9.1 Interview guide

Interview guide

Evaluation of cybersecurity frameworks to ensure sustainability in value networks

Date:	
Interviewer	Bubacare Nyabally
Interview partner	
Job title	
Company	

Content:

4. Introduction:
   Brief overview of the study and consent process.

5. Main Questions:
   Covering the Topics of sustainability, cybersecurity frameworks, and their influence on value networks.

6. Conclusion:
   Summarizing key points and farewell.

Notes on the procedure and data protection:

The interview consists of 8 main questions and optional, answer-related follow-up questions.

The estimated duration of the interview is 20-30 minutes.

Below you will find a declaration of consent for the anonymized publication of the interview results.

Declaration of consent

The interview is recorded with a recording device and then transcribed by the interviewer of the research project. For the further scientific evaluation of the interview texts, all information that could lead to the identification of the person is changed or removed from the text. In scientific publications, interviews are only quoted in excerpts in order to ensure that the overall context of events cannot lead to the identification of the person.

Personal contact data will be stored separately from interview data and will not be accessible to third parties. After completion of the research project, your contact data will be automatically deleted unless you expressly agree to further storage for the purpose of contacting you for related research projects. Of course, you can object to longer storage at any time.

Participation in the interviews is voluntary. You have the option at any time to cancel the interview and withdraw your consent to the recording and transcription of the interview without any disadvantages for you.

Signature: ………………………. **Date: ……………………….**

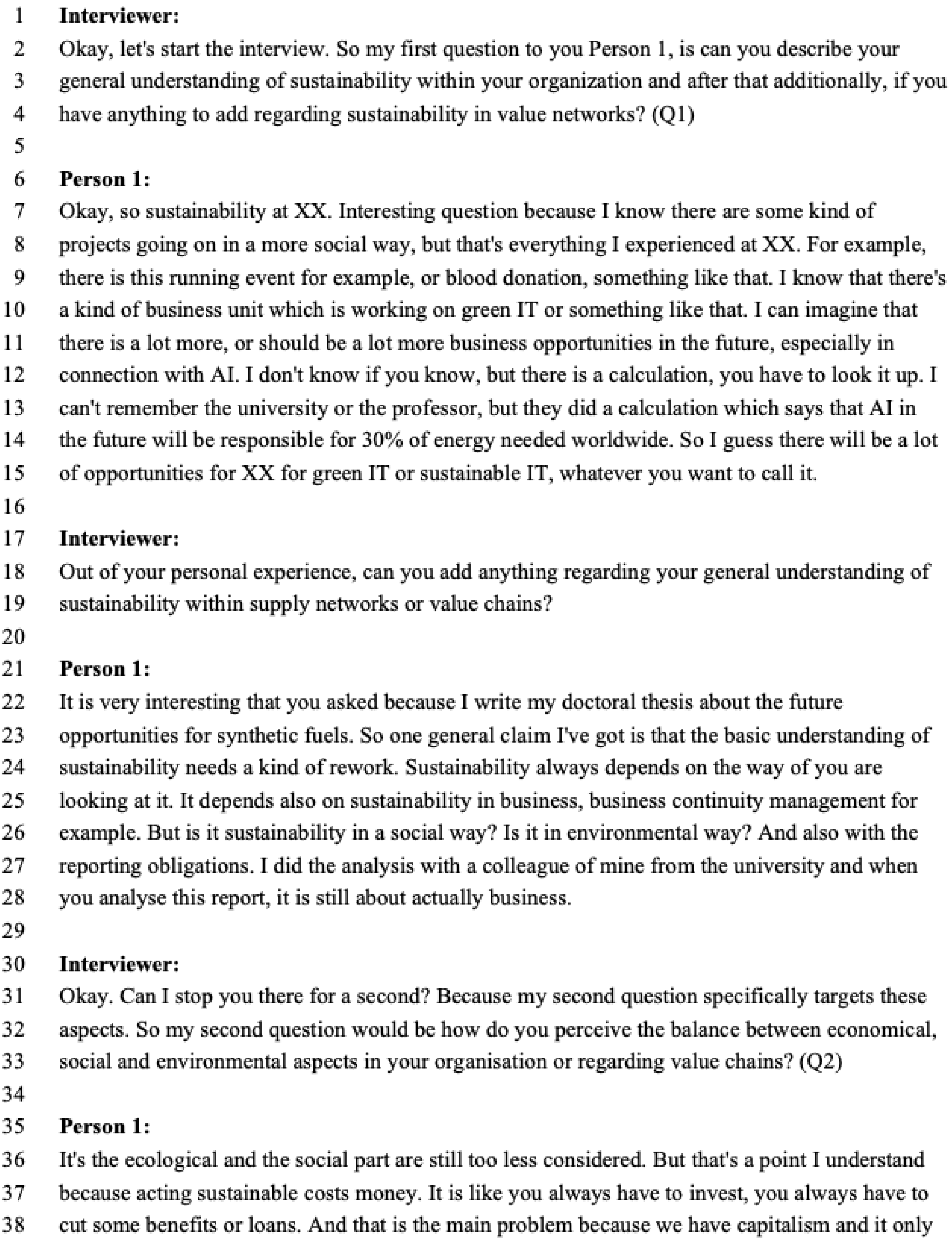
Topic 1: Sustainability (in Value Networks)	
Question 1	Can you describe your general understanding of sustainability in your organization? - And additionally in value networks?
Question 2	How do you perceive the balance between economic, social, and environmental aspects in your organization? - And additionally in value networks?
Question 3	What practices or key components do you think are essential for maintaining sustainability in your organization? - And additionally in value networks?

Topic 2: Cybersecurity	
Question 4	Which cybersecurity frameworks are you familiar with or use in your organization?
Question 5	How effective are these frameworks in managing cybersecurity risks in value networks?

Topic 3: Influence of Cybersecurity on Sustainability (in Value Networks)	
Question 6	How do you see the relationship between cybersecurity and sustainability? - In value networks?
Question 7	Can you provide examples where cybersecurity measures have influenced (supported or hindered) sustainability efforts? - In value networks?
Question 8	How can cybersecurity and sustainability be aligned within value networks, and what emerging trends do you see in the future?

9.2 Interview Transcripts

9.2.1 Interview 1



Interviewer:

Okay, let's start the interview. So my first question to you Person 1, is can you describe your general understanding of sustainability within your organization and after that additionally, if you have anything to add regarding sustainability in value networks? (Q1)

Person 1:

Okay, so sustainability at XX. Interesting question because I know there are some kind of projects going on in a more social way, but that's everything I experienced at XX. For example, there is this running event for example, or blood donation, something like that. I know that there's a kind of business unit which is working on green IT or something like that. I can imagine that there is a lot more, or should be a lot more business opportunities in the future, especially in connection with AI. I don't know if you know, but there is a calculation, you have to look it up. I can't remember the university or the professor, but they did a calculation which says that AI in the future will be responsible for 30% of energy needed worldwide. So I guess there will be a lot of opportunities for XX for green IT or sustainable IT, whatever you want to call it.

Interviewer:

Out of your personal experience, can you add anything regarding your general understanding of sustainability within supply networks or value chains?

Person 1:

It is very interesting that you asked because I write my doctoral thesis about the future opportunities for synthetic fuels. So one general claim I've got is that the basic understanding of sustainability needs a kind of rework. Sustainability always depends on the way of you are looking at it. It depends also on sustainability in business, business continuity management for example. But is it sustainability in a social way? Is it in environmental way? And also with the reporting obligations. I did the analysis with a colleague of mine from the university and when you analyse this report, it is still about actually business.

Interviewer:

Okay. Can I stop you there for a second? Because my second question specifically targets these aspects. So my second question would be how do you perceive the balance between economical, social and environmental aspects in your organisation or regarding value chains? (Q2)

Person 1:

It's the ecological and the social part are still too less considered. But that's a point I understand because acting sustainable costs money. It is like you always have to invest, you always have to cut some benefits or loans. And that is the main problem because we have capitalism and it only works with growth. So I don't know. I'm not like a communist guy saying capitalism is the worst we could ever do or whatever. I'm part of it, I'm working as a consultant, come on. But it is like that the capitalism stands in the way of sustainability.

Interviewer:

Thank you. That's a very good point. So then let's go to the third question. What practises or key components do you think are essential for maintaining sustainability? Again, within your organisation and specifically in value networks? (Q3)

Person 1:

I also would kind of rework the understanding of sustainability according to sustainability assessments. I have not yet seen an overall assessment which addresses any sort of phase of a product or service or whatever. One very good example is always this discussion about electric vehicles and combustion engines. So in this comparison, mostly the production phase of electric vehicles is cut out, but in this phase, most of the carbon dioxide emissions or harm for the environment and so on is happening. Afterwards, of course, if you have the possibility to charge your vehicle with renewable energy, then everything is fine. But electric vehicles come with a big package of disadvantages in comparison to combustion engines. We need assessments which really start from gaining the resources from the very beginning to proceedings until recycling.

Interviewer:

So you would say that key components could be something like proper assessments of which step is responsible for the most emissions within your value network?

Person 1:

Let's say modules of sustainability. So we have the environmental part, we have social parts. Where do the resources come from? This is also a discussion that you really have to split into these different views of sustainability and put it over all phases. Kind of complex. Yes, but I think it's necessary.

Interviewer:

Okay. Thank you for the good answers. So let's go to our second topic. In this case, cybersecurity specifics. I would start with the question, which cybersecurity frameworks are you familiar with or using within your organisation? (Q4)

Person 1:

Okay. If I remember it right, XX is certified according to 27001 as well as TISAX. Then we have the NIST framework. What else? There is also a Japanese standard, but I don't remember the name. But these are the frameworks I know. I think these are also the three most common. TISAX id automotive specific, but according to my knowledge, the NIST framework and the 27001 framework are the most common.

Interviewer:
And then building on that question out of your experience, how effective are these frameworks you named in managing cybersecurity risks, specifically in value chains? (Q5)

Person 1:
Yeah, we have to differ. The former 27001, meaning before 2022 had a kind of lack in supply chain and especially cloud security. TISAX as comparison is based on the 27001 and they added automotive specific requirements. This is the VDA ISA requirements catalogue, and they focused more on cloud security. And as you might know, the OEMs, especially the German OEMs also give these requirements into their value chain. Not only tier one, I think at the moment it's like until tier three, but not deeper. But there is an obligation for the tier one to tier three to hand out these requirements also to their suppliers. So the goal is to have this framework at all suppliers where necessary. So it also differs from production sites and development sites and so on. There are different labels, different requirements for different needs. So it's more complex. So if I compare these two with each other, let's say that TISAX is more specific.
But with the ISO standards. It is "Absicht" that there is room for interpretation left. What's the word for "Absicht"?

Interviewer:
On purpose?

Person 1:
Purpose. It's on purpose that you have room left for interpretations. TISAX has more straight requirements. You have it or you have it not there is no or less room for interpretations with TISAX.

Interviewer:
But in this case, TISAX is more or less specifically targeted at automotive industries.

Person 1:
Yeah, I think it's the main advantages. You can pick the labels for specific sorts of suppliers. You have other requirements for software developers, then for hardware production sites, for example.

Interviewer:

Okay, very nice. So let's come to the final topic. It's the influence of cybersecurity on sustainability in general and specifically in value networks. The first question of that topic is how do you see the relationship between cybersecurity on the one side and sustainability on the other side in general and more specific, the relationship between cybersecurity and sustainability In value networks specifically? (Q6)

Person 1:
Again, difficult. How can I start this? We are on the path of exchanging fossil energy carriers with renewables. It's a kind of main goal, let's say. Yeah, the efforts are in general underestimated. It's a enormous political topic and I think actually the main decision makers do not really know what they do. So for example, especially in Germany or in Europe, we are talking about wind turbines and solar systems. That's it. There are many, many more techniques to gain or to generate renewable energy. There are way more. I don't know if you know, the technique of melted salt. There is one facility in Spain. One. And it's actually a very, very effective and also especially efficient way of storing energy. Electric energy or energy in general. And also when it comes to efficiency for solar systems. For example, they are not efficient in Europe because we don't have so many sun hours. So we should actually build way more wind turbines or we should put the strategy on wind turbines or other techniques and build solar systems in North Africa for example. Or in South America or Mexico, Panama, Chile or Brazil. Where we have the most sun hours in a year.

Interviewer:
Short intervention. Just to get back on my topic of the relationship between cybersecurity and sustainability.

Person 1:
Oh yes, of course. We will need more and more energy in the future. For example, AI or using AI for cybersecurity purposes. This needs a lot of energy and the generation of renewable energy is already a problem. And especially in the future, when we need more energy, the problem will get even bigger. So the main thing could be how we make sure everything regarding the energy sources is safe from a cybersecurity perspective.

Interviewer:
Then I would go to the next question. So can you provide examples where cybersecurity measures have influenced, supported or hindered sustainability efforts in value networks? (Q7)

Person 1:

So I have no specific example or I cannot remember one right now. In general, I would say everything which improves the efficiency of processes or the efficiency of coding would support the energy usage.

Interviewer:
My next question builds on the two before and on your previous answers. How do you think cybersecurity and sustainability can be aligned within value networks in the future and what emerging trends do you see? (Q8) So you mentioned a topic of energy consumption already. That's probably some aspect that's going need big alignment in the future. How do you prioritise the energy consumption or how do you generate enough energy to fulfil your requirements?

Person 1:
So I guess at the moment, this not a big point. The trend comes from laws. Actually, I would say if there would be no obligations by law, nobody would care.

Interviewer:
Okay. So you think it's more or less lawmakers should provide something like a framework or guidelines in order to support companies? Because otherwise as you mentioned, nobody would care about sustainability.

Person 1:
Yeah, let's say nobody would care in management boards, they always need to decide and in general, or mainly they need to decide in the sense of the company or in the sense of the people. We come back to the point of capitalism that everything depends on sales and money. And if you are listed company on the stock exchange, the value of your stock ist the main KPI of your company. I understand that it's very difficult, but I also think that we need these obligations and regulations by lawmakers. And you also need to split the responsibilities. So sustainability always needs to be assessed from another point of view than cybersecurity or IT in general. So besides the CTO, there needs to be A CSO (Chief Sustainability Officer), for example. If you'd like to push sustainability within your company, take someone into the board next to the CEO, the CFO and so on.

Interviewer:
Okay, perfect. Thank you for the insights.

9.2.2 Interview 2

Interviewer:
Okay, so Person 2, let's start with the first question. So can you describe your general understanding of sustainability within your organisation at first and after that, additionally regarding to value networks? (Q1)

Person 2:
Sustainability in my organisation, on the one hand, obviously we have sustainability as one of our key offerings to bring to our clients to basically implement sustainability measures with regards to decreasing CO2 footprint, increasing reusability, all these kinds of things. So it's one of our, let's say offerings. On the other hand, obviously we live by our own key values, so sustainability obviously is also one of our key ethics and compliance promises that we live by. So we strive to reduce our own CO2 footprint by, for instance, reducing the amount of travel we do by increasing the duration of assets that we use before they break, basically, not replacing them just per se, and obviously also reducing our energy consumption with regards to the offices that we use. Also with regards to the central infrastructure, we might operate on our own. So there is a promise, I don't know the exact year to be CO2 neutral, I think even by end of this year or we might already be. So I think we are pretty much a pioneer in that area to not only give statements about sustainability and the importance of it, but actually applying it and living by these values. I think the other point that you mentioned was regarding the value networks. I think it's always difficult as a bit of a disclaimer to state that from a consultant's perspective because as mentioned, it's an offering we bring to the market because it's a relevant topic in the market for all the clients and each and every client, depending on the industry they operate in, they might be affected differently by sustainability. So obviously in the energy sector, it's a completely different topic. Then if you talk about, I don't know, automotive versus retail. So sustainability in the value chains, in their value chains can be completely different things. For some, I think it's part of their core value stream. So for instance, in the energy sector, it's probably the most disrupting topic to become sustainable and operate based on sustainable green energy. I think for instance, in the retail space or in the banking sector is a completely different topic. It's more about cost cutting, it's about less energy consumption is about basically reducing your operating costs overall, but less about your core value stream, I would say.

Interviewer:
Okay, thank you for the very comprehensive answer. I think we can jump right into the next question. That would be, how do you personally perceive the balance between economic, social and environmental aspects within value networks or your organisation? (Q2)

Person 2:

So economically, I think it's the key driver for a lot of the corporations or a lot of the clients we work with to implement sustainability measures. Because as mentioned, it reduces costs, it helps improve your margin, lower your operating costs, so it has a direct financial impact. Nevertheless, of course the social impact is also one of, let's say the key pressure points for a lot of organisations because obviously it's very visible in the positive and the negative sense, if you do something or you don't do something with regards to sustainability. So basically you can use it as a marketing tool to tell everybody about it. So being basically the good guy and improving the wellbeing of everybody and improving the world, so to say. And at the same time, of course there's a bit of a, let's say, expectation in the society that you as a corporation in general need to be responsible about how you operate. And of course, sustainability among other ethical factors is one of the key drivers there. So I think there's, let's say a visibility and the social impact if you don't apply this to yourself. And I think the third factor you need to help me real quick, what that was?

Interviewer:
The factors where social, environmental and economic.

Person 2:
Environmental, yeah, so social economical, I think I touched those. Environmental, obviously it's something we need to do. I think it's the common understanding even though some might have a different perspective and to deny that we need to apply a more ethical and sustainable way of working overall. And I think there are some, let's say industries that are more affected and that also contribute a lot more to basically greenhouse gas emissions and stuff like that that are under more pressure. But I think in terms of environmental aspects is something that needs to be applied to get to, let's say a circular economy. I think there's some few examples where this already works. So especially if you look at recycling systems for plastics, glass, et cetera, but obviously it should be the same when we talk about energy. So not using fossil fuels that are limited in your availability. At the same time also that release the carbon that's basically collected in the fossil fuel into the environment. So it is something that is, let's say one of the big, let's say challenges of humanity, so to say, to get to a state that you live in, balance with your environment and basically use resources that are renewable and basically create a circular system.

Interviewer:
Perfect. Thank you. And building on that question, what practises or key components do you personally think are essential for maintaining sustainability in within your organisation or overarching in value networks? (Q3)

Person 2:

I think one of the most straightforward ones that obviously everybody is affected by is energy consumption that affects basically each and every one personally. So if in your own home, where do you use energy for how can you save energy with regards to electricity, but also with regards to gas. Fossil fuels that you might use to operate a heater. On a larger scale, obviously I think one big factor is also the use of electricities in the modern IT world. So to say, if you think about cloud environments, if you think about the daily use of internet, obviously there's connected a lot of, let's say large scale data centres, transmission networks that also use a lot of energy. So I think that's one big factor nowadays where also the sustainability aspect comes into play to reduce energy consumption in the large scale data centres in cloud centres. I think apart from that, it's a lot about everyday life. So if we think about our own company, as mentioned, it's about travel. It's the question, how often do we need to travel, how do we travel, how much can I also work virtually? There is the question about the equipment. Can I repair or reuse what I have? Do I need to get a new phone or laptop every other year just to be on top of the technology or is the stuff I use right now still viable for the future? So I think these are the key aspects that affect us as a corporation. Apart from that, as mentioned, we also help a lot of clients to become more sustainable and implement sustainability strategies, which then obviously are very much tailored to that specific industry or that specific client.

Interviewer:
Perfect, thank you. So now let's come to the second topic, your personal expertise regarding cybersecurity. So the first question is really simple and you can just list them. So which cybersecurity frameworks are you familiar with or do you use in your organisation? (Q4)

Person 2:
Cybersecurity frameworks? The key ones we use for instance is NIST. So that's the American standar for cybersecurity, which we use, especially if we are working in the global context. If we work in Germany, we mainly use the ISO 27001 norm, which is the, let's say the German equivalent. Both are very, very much related. In addition, obviously there are some specifics. So for instance, in Germany we have the BSI norms. There are a lot. So for instance, BSI Grundschutz, these are let's say the German core protection rules. There's also BSI KRITIS for critical infrastructure. So there are some specific norms also that is, let's say applicable in Germany. That's from BSI. There are some technical norms, so there's CIS controls that are more on a technical level. So how do you basically configure safe systems? How do you build safe applications? Then there's specific norms and frameworks that talk about the tech vectors or threats. So for instance, OWASP would be one that has let's say the typical or the most critical vulnerabilities and attack threats. And then there's some industry specifics that specify security rules and regulations with regards to certain industries. For instance, one would be TISAX, which applies to the automotive sector. This is a very, let's say, strong norm, that is closely related to

ISO 27,000 again, but specific to the automotive branch. And similarly the different regulations also, for instance, for the energy sector, for retail, also for the different industries, there might be some subsets. And then there obviously are some new regulations coming up also from the European Union, for instance, like NIS-2. A large framework that will be rolled out this October as a mandatory requirement, again regarding critical infrastructure. And on a side note, obviously we also look on the typical data security topics like GDPR, which I think is a framework everybody knows. So these are the ones that come to mind.

Interviewer:
Perfect, thank you. Building on that question, how effective do you think are these frameworks in managing cybersecurity risks, specifically in value networks? (Q5)

Person 2:
Based on what we do, being basically a strategy and management consulting provider, I think they're very effective and vital for what we do because these frameworks on the one hand give an end-to-end overview of everything that is part of cybersecurity. So it basically gives you the big picture to work against. And it also defines, let's say, standards that are commonly applicable and viable for everyone without discussing basically what are best practises and what are, let's say, common methodologies. So these frameworks also give a lot of guidance when we talk about cybersecurity as a whole. And then obviously depending on which industries or which areas we operate in, they are also one of the key drivers to implement cybersecurity because there might be, for instance, a mandatory regulation such as GDPR, for instance, where there's no discussion that everybody needs to apply it. So I think it's on the one hand, a key driver for companies to think about and apply cyber security and data privacy. On the other hand, it gives us, let's say a guideline and a set of standards that we can use in order to define strategies, define target measures, define the roadmaps with use of these frameworks as a guard rail, so to say.

Interviewer:
Okay, so how do you see the relationship between cyber security and sustainability? (Q6)

Person 2:
I think in general the touch points between cybersecurity and sustainability are not very common. There's not a big overlap, so to say. I think there are some benefits if you apply cybersecurity because it basically forces you to get a better understanding of what you run, what you operate, the assets you have in terms of buildings, in terms of it, and then evaluate those. So I mean, cybersecurity only works if you know what you have and if you analyse what you have, you might come across anything that might not be very efficient in a sustainability sense. So you might see that we have legacy IT that's outdated, we have infrastructure or we have also

potentially buildings that are not up to standard, and that might be a reason then to update and change to a more, let's say, secure and at the same time sustainable solution. But overall, I think cybersecurity does not necessarily have sustainability in mind. So cybersecurity on its own does not care. So to say if it's sustainable or not, I think it's more like a byproduct. In the same way that obviously sustainability on its own does not make anything secure. But I think there are some synergies between the two topics overall and the frameworks. If I think about cybersecurity frameworks, obviously the big challenge of these frameworks is that they're typically very generic by design, because they need to apply to everyone and they need to be valid over a longer period of time. So if they would basically make them more specific, then they would need to also update them more frequently. And then also there would need to be different versions for different scenarios. The key challenge obviously is translating that into actual requirements and extra solutions that apply to clients or us as a company. So there's some translation work required, and therefore the solution based on a framework might not always be exactly the same. Even if you use the same framework, there might be different approaches and different solutions for different clients.

Interviewer:
Okay. That's very interesting because my next question would be if you can provide examples where cybersecurity measures have influenced, meaning supported or hindered sustainability efforts in general, and again, in value networks? (Q7)

Person 2:
I think as mentioned, there are some overlaps even though not many. If for instance, as part of cybersecurity measures, legacy infrastructure or legacy systems that are outdated and therefore pose a cybersecurity risk get replaced, that might also have a sustainability impact. The modern systems operate on less energy, they are more efficient overall in terms of the hardware they require, et cetera, et cetera. So there is some, let's say, overlap. Even though as mentioned, cybersecurity does not have an explicit sustainability focus. And in the same way it might be conflicting potentially if let's say there needs to be prioritisation in a client's roadmap to say, okay, what do we do first? If for instance, there's the cybersecurity incident, then it might be that sustainability budgets or efforts would be, let's say, put on hold or let's say rerouted to focus on cybersecurity. So cybersecurity might be overruling sustainability efforts and implementation targets in case that cybersecurity becomes a priority in case let's say there's an extra incident and everything else has to be put on hold. That's the only thing I see. Other than that, I think there's two topics that don't, let's say meet very often.

Interviewer:

Coming to my last question. That would be your personal opinion regarding the future. How do you think cybersecurity and sustainability can be aligned within value networks, and are there any specific emerging trends you see within the integration of cybersecurity and sustainability and value networks? (Q8)

Person 2:

I think both cybersecurity and sustainability will benefit from a general modernization in infrastructure. Regardless if that is IT or if that is, let's say energy networks. So cybersecurity benefits a lot from automation and automated rules as long as they work, obviously. So also the whole topic of AI and generative AI is obviously a big driver for cybersecurity, and I think the same can be applied for sustainability because sustainability obviously is very much data driven. So the first, I think, complication for a lot of clients and companies is to first understand where the biggest lever is in terms to become more sustainable. If you talk about obviously the core business value streams, then it probably is quite obvious. But I think there's also a lot of benefits in the overall administration and let's say secondary value streams that are not, let's say, primary to the business that also can be optimised in terms of sustainability. And I think overall in the future, both topics can benefit and will benefit a lot from, let's say a general modernization of processes, infrastructure and use of AI to basically analyse the data, analyse the systems, and make optimizations and improvements based on the status quo.

Interviewer:

Thank you. That would be it, Person 2. Thank you very much.

9.2.3 Interview 3

Interviewer:

Okay, thank you, Person 3. I would start with my first question. That would be, can you describe your general understanding of sustainability firstly within your organisation, and then additionally, specifically targeted to value networks, meaning the sustainability within value networks? (Q1)

Person 3:

Yes, of course. So I mean, the general understanding of sustainability for my organisation, which is XX, is actually a very holistic one. So XX has, together with many other leading companies and organisations, understood that there is an absolute need to consider sustainability aspects alongside financial aspects, societal aspects, and on and so forth when doing business in order to secure the ability to do business in the future. And why is that? Because our economy has been deploying the earth resources and polluting our environment so much that now is the point when actually complete business models and industrial sectors, different types of activities are threatened to probably have to be stopped or completely altered. Just because the natural resources on earth are coming to an end or pollution levels are too high, or also the social costs of doing business in particular ways is not acceptable anymore. So sustainability is a very important element of our strategy. XX has defined quite an ambitious sustainability strategy. Which means that you overall think about what are the material topics that I think I as a company influence most in sustainability, and then how can I reduce my influence or increase my positive effects that I have on society, on business as a whole? And of course, so for us as a knowledge-based company, very much data-driven company, decarbonization is one topic. So sustainability more concretely means that you have targets to become net zero business by 2030 and do many other things in between. And also, I think this is important, we try to create transparency on sustainability also within our project. So we want to help all our clients to achieve their sustainability goals. And we do this by, on the one hand, trying to obviously minimise the environmental and social footprint of our activities, of our projects, of our offices, the way we travel, the way we commute, and so on. But then also actually seek sustainable improvements or efficiencies or added value at the clients when working with projects. Yeah. So maybe I'll stop here.

Interviewer:

Thank you for the very comprehensive answer. So that was specifically targeted to XX as your organisation. Can you add anything additionally to your understanding regarding sustainability within value networks?

Person 3:

Yes. I mean, of course sustainability has a huge role there. If one company wants to improve their sustainability performance, they have to take into account all their suppliers. Let's say if they're a manufacturer, they need to think about how are the raw materials derived? How are maybe some resources and input products that I need for my production being developed? And then the company obviously creates value within its own premises, and then that product is shipped towards or transported towards the consumer or is sold. So looking at this concept of sustainability very holistically along the whole value chain, there's various concepts you can use. For example, lifecycle assessments, which look at the whole lifecycle of particular products, for example, or services. So sustainability needs to be considered there because if every company only considers sustainability within its own company premises, you leave out most of the, in many segments, you would leave out most of the pollution, most of the risks, and most of the impact. Because, I guess the value networks are very, very widespread, very long, very diverse. And so it's actually essential to have to take this very holistic view from from cradle to cradle. There's lots of different approaches on what to measure and when to stop measuring, but looking at impacts, risks, opportunities along the whole value network. Makes a lot of sense.

Interviewer:
Then I would start the second question that would be, how do you personally perceive the balance between economic, social, and environmental aspects regarding sustainability? (Q2)

Person 3:
You mean how do I personally perceive it? In today's reality?

Interviewer:
Yes, in today's reality.

Person 3:
Yeah. I mean, I guess there's a lot of theory on how it should be. I think today's reality, of course, because this is huge. So if the global economy wants to transform to actually become sustainable, this implies that all economic activity is completely put upside down. That there's new business models reinvented. Many things need to be stopped, a lot of new things need to be done, and then we would actually probably have a very thriving economy that can be net positive on environmental topics and sustainability. But of course, we're not there yet. So the current situation is that the economic aspects are absolutely front and forward. I would probably say globally, in 98% of all companies, they're the only drivers that actually matter. This is why of course, resource depletion, pollution and all of these aspects continue as before. And there's very, very few companies, mainly in the European Union, some of them in the US who have more foresight and are starting to transform their business models. However, this again also takes often

decades to do. So there's very few companies who are small enough to maybe have already achieved this, but this is an absolute exception. So I would say that the economic aspects, including the economic impact or considerations in politics and geopolitics and so on, are absolutely the only dimension that really counts.

Interviewer:
Okay. Can you name some example of those companies who are on the forefront doing that?

Person 3:
Well, there's very few leaders who do this. You need to differentiate between companies who talk about their plans. That may however be very long term. It might be ambitious, but really only in 2050. They might today already talk about a lot about what they want to be doing, but still are huge polluters. So I would put those into a big greenwashing category with the sense of they're overemphasising their future plans and they're not doing enough today. There's a lot of these companies, they win all these sorts of sustainability prices, but in reality, they're still part of the polluting economy. And I would not say that they're front runners. So one example for that type of company would be Unilever. In many aspects, they are thought to be a sustainability leader. However, you think about their core business model, they produce thousands of tonnes of single use plastic that's thrown away. So for me, they're not sustainability leaders. They have great targets and goals, and they have good communication, but very few companies are really already embracing that sustainability from the core of their strategy. So they have completely different business models. Some of them have circular business models, which means they never really need new resources. They can literally just keep reusing stuff, and there's others who transforming towards that way. So in Germany, I think an example of a company who are doing a lot of very innovative things is the sports article manufacturer Vaude. They're actually transforming the way they do business. They try not to sell more new plastic shoes. They create things like secondhand shops on their own website, repair services for a lot of things that get broken, not to be thrown away. So that example would be, I guess in the consumer brands area. Another US example from the same industry actually is Patagonia, who have a lot of elements of what I think is a very good understanding of where they need to go. Of course, they're not there yet, but there's a lot of elements that work very well. Very nice.

Interviewer:
Third question regarding sustainability would be what practises or key components do you think are essential for maintaining sustainability as of right now? And maybe if we have a look towards the future? (Q3)

Person 3:

For maintaining sustainability key practises? Well, I mean this is also what we do in trying to help our clients. I think what needs to be done is that sustainability becomes tangible. And to do that, you need data. You need to be able to measure your impact so that the practise of actually defining a sustainability goal or targets becomes easier. Then you need to be deriving measures that you need to do in order to achieve such targets. And then actually working with real data to measure where am I now? Where do I need to go? What's the impact? And you keep improving performance. I think this is a very, very important practise because if you don't do that, then you'll never come down to operationalize your strategy. So it's going to be about data on every levels, finding data, defining KPIs that actually help you steal your business sustainable. And then measuring that, then there's this element of reporting it. So creating transparency on sustainability achievements is not a bad idea because it might help your own workforce, your stakeholders, the media, your investors to better understand what you want to do. So to take people along is important. So I think communicating what sustainability overall and then very specifically means makes a lot of sense. And then, I mean, if you talk about it and you have targets, and if you actually measure where you are, you can derive KPIs and you can also put down a plan with measures. Another very good idea is to reward sustainability improvements. So this means that eventually you would want someone to be steered by sustainability, KPIs or improvements, whatever it is your strategy entails. And this is best done if you actually incentivize or provide financial rewards. Maybe you could eveninclude some sort of punishments for not achieving some sustainability goals for the management of the company and senior leadership, and ideally every employee. So only if the sustainability strategy is tangible, is known, can be measured, and you incentivize people to work on it, it is going to be realised. And by the way, the same is true not only within the company. So if you think of value networks, you want to do exactly that with your whole supply chain.

Interviewer:
So now we will talk about cybersecurity. So I'm going to start the second part of my questionnaiere. So question four is which cybersecurity frameworks are you familiar with or do you use in your organisation? (Q4)

Person 3:
None, I dont know any framework.

Interviewer:
So then we can skip the next question. Let's go straight to the influence of cybersecurity on sustainability. Maybe you have some input regarding that. So how do you see the relationship between cybersecurity and sustainability in general? (Q6)

Person 3:

Well, maybe I can test an assumption with you. So if I'm thinking of cybersecurity, just one example, I'm thinking of cybersecurity with regards to wanting to make sure I don't lose data if I get attacked, right? I might want to think about duplicating that data and having my most important data backed up. I have it on a server farm in Germany and I have a duplicate of that in France and I have another one somewhere else if something happens. If one of my server farms is hacked or if a cloud provider loses something, I have backups. That might be a strategy. I'm not even sure if it's part of such a framework, but just from a very layman's perspective, right? Sort of this idea of duplicating things. I don't know. There's an plane crashing into a major server farm of Microsoft. It would be a good idea if you have a backup at AWS or somewhere at another Microsoft, I don't know, server farm, let's say. So if that's the case, then the implications on sustainability are enormous of course. Because you keep duplicating your data and instead of, I don't know, 10 terabytes, you'd need 30 or a hundred terabytes for the same amount of information just to make sure that in case two of these locations become out of order, out of whatever reason, you can still access that. What this means is that you will need a lot of energy for any data centre that's run to store duplicates or anything else that you want to secure. It has a huge impact because of the energy intensity. Overall, the whole element of people creating massive amounts of data within companies or also privately creates a huge environmental burden because of the energy intensity of running a data centre. No matter if you as a company use a cloud service because that data then sits in a server farm from your cloud provider or hyperscaler. So it's eventually always going to be a physical data centre that's run and needs to be cooled, that needs all of that electricity. Maybe even backup electricity. And so it does have a huge environmental impact. I think some of the hyperscalers have very ambitious sustainability targets, and they have a huge issue in achieving those because they're so energy intensive. So of course you can power your server farms with wind power or with geothermal power. I mean, is that already done in a widespread manner? No, it's not. So this would be one element that I could think of, which is the duplication of data and the needs to keep powering all these data centres. And then the other one is how energy efficient, how self-containing is the server farm itself, where my data is sitting. Let's say you want to secure your data. You have a cybersecurity strategy and you might be using a lot of additional applications like firewalls or stuff like that. These also take a lot of computing power, which again means they need more energy.

Interviewer:

Maybe you can provide something to my next question. Can you personally provide any examples where cybersecurity measures have influenced, meaning supported or hindered sustainability efforts? Does there come anything to your mind? (Q7)

Person 3:

No, not really.

Interviewer:

Then there's only one question left That would be how can cybersecurity and sustainability be aligned in the future? Do you see any emerging trends? You already mentioned energy consumption. Do you see anything else? (Q8)

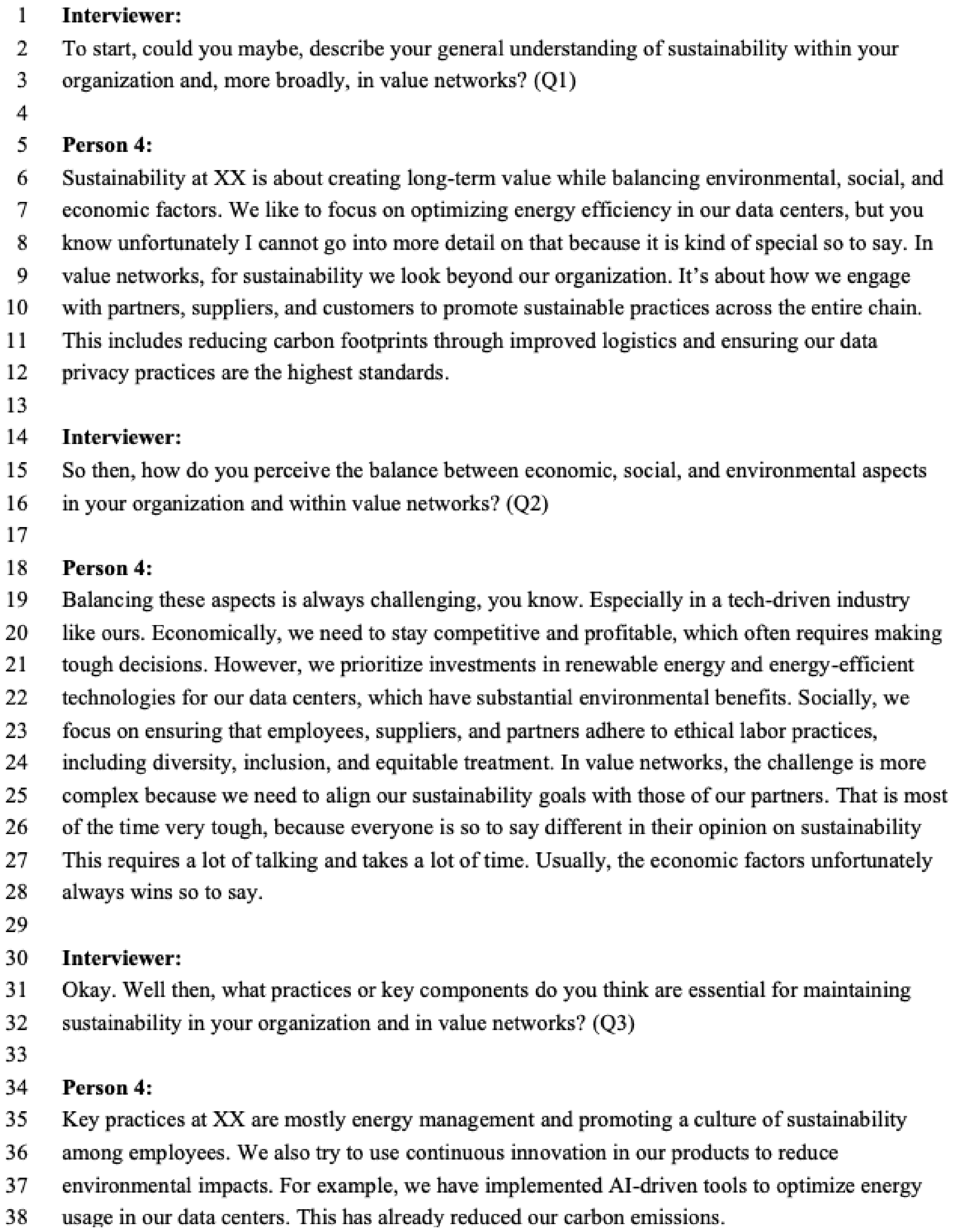
Person 3:

I don't know if this is specific to cybersecurity, but I think there's a lot of redundancies in the systems. And so my question would be, if you want to get this more efficient, it will have a positive impact on the environment. So if you don't store all the data, but you keep deleting stuff that's older than 10 years you reduce the amount of service space you need. Or you could think about different categories of how protected do things need to be, how often do I need to duplicate? So gaining efficiency in data volume, let's say, might have a positive impact. So I think the data storage probably might have a huge impact. I think cybersecurity applications can of course also be developed in a way that they don't use too much computing power. And then, I mean, of course, the providers of cybersecurity software could also think about how energy efficient they could create their operations.

Interviewer:

Thank you. That actually would be it Person 3.

9.2.4 Interview 4



Interviewer:

To start, could you maybe, describe your general understanding of sustainability within your organization and, more broadly, in value networks? (Q1)

Person 4:

Sustainability at XX is about creating long-term value while balancing environmental, social, and economic factors. We like to focus on optimizing energy efficiency in our data centers, but you know unfortunately I cannot go into more detail on that because it is kind of special so to say. In value networks, for sustainability we look beyond our organization. It's about how we engage with partners, suppliers, and customers to promote sustainable practices across the entire chain. This includes reducing carbon footprints through improved logistics and ensuring our data privacy practices are the highest standards.

Interviewer:

So then, how do you perceive the balance between economic, social, and environmental aspects in your organization and within value networks? (Q2)

Person 4:

Balancing these aspects is always challenging, you know. Especially in a tech-driven industry like ours. Economically, we need to stay competitive and profitable, which often requires making tough decisions. However, we prioritize investments in renewable energy and energy-efficient technologies for our data centers, which have substantial environmental benefits. Socially, we focus on ensuring that employees, suppliers, and partners adhere to ethical labor practices, including diversity, inclusion, and equitable treatment. In value networks, the challenge is more complex because we need to align our sustainability goals with those of our partners. That is most of the time very tough, because everyone is so to say different in their opinion on sustainability This requires a lot of talking and takes a lot of time. Usually, the economic factors unfortunately always wins so to say.

Interviewer:

Okay. Well then, what practices or key components do you think are essential for maintaining sustainability in your organization and in value networks? (Q3)

Person 4:

Key practices at XX are mostly energy management and promoting a culture of sustainability among employees. We also try to use continuous innovation in our products to reduce environmental impacts. For example, we have implemented AI-driven tools to optimize energy usage in our data centers. This has already reduced our carbon emissions.

In value networks, transparency and collaboration are essential. But this does not really work so far, I guess. We try to participate in industry forums or things like that to share best practices or a to get general feel for trends in the future.

Interviewer:
Moving on to cybersecurity, which frameworks are you familiar with or use in your organization? (Q4)

Person 4:
I think we are certified according to the ISO 27001 framework and of course we comply with GDPR regulations. Then there is this NIST framework I think, but I am not sure we at XX use it so yeah.

Interviewer:
Okay so then I will try my next question anyway. How effective do you think are these frameworks in managing cybersecurity risks in value networks? (Q5)

Person 4:
Sorry, absolutely no Idea. I mean probably quite effective, because otherwise XX would not use them but no Idea about the Details.

Interviewer:
Yeah, I understand. It was still worth a try. So then, how do you see the relationship between cybersecurity and sustainability, particularly in value networks? (Q6)

Person 4:
Cybersecurity and sustainability area bit interconnected, I think. I mean cybersecurity is very important for sustaining trust with our customers and partners, which should be a cornerstone of any sustainable business. In value networks, I think, cybersecurity might help to ensure the integrity and security of data. That should actually support transparency and accountability which are key elements of sustainability. Additionally, by preventing cyber-attacks, you can of course avoid disruptions that could have massive impacts on everything.

Interviewer:
Okay nice. Can you maybe provide examples where cybersecurity measures have influenced sustainability efforts, either supporting or hindering them? (Q7)

Person 4:

I don't know really right know.

Interviewer:
Yes, no problem. Lastly, how can cybersecurity and sustainability be aligned within value networks, and what emerging trends do you see in the future?

Person 4:
So okay for the future I think alignment comes from maybe putting cybersecurity more into the core of our sustainability strategy. Maybe not treating cybersecurity as a separate issue but as a critical component of our sustainable business practices. Emerging trends are of course AI and machine learning. They can support both cybersecurity and sustainability efforts. So yeah, interesting questions, a lot food for thought so to say.

Interviewer:
Thank you for your insights. This has been a very informative talk.

9.2.5 Interview 5

Interviewer:
Thank you for taking the time to speak with me today Person 5. To start, could you describe your general understanding of sustainability within your organization and more broadly in value networks? (Q1)

Person 5:
Thank you for having me. Sustainability in XX is about ensuring that our supply chain processes are more or less efficient and responsible. Of course, we want to reduce our carbon footprint and promote ethical practices across our company. We are working together with our suppliers, distributors, and other stakeholders to make sure sustainability is possible in the entire chain. This includes everything from sourcing raw materials responsibly to ensuring that our logistics partners follow environmental standards I would say.

Interviewer:
How would you perceive the balance between economic, social, and environmental aspects in your organization and within value networks? (Q2)

Person 5:
Balancing these aspects is a challenge, particularly for a medium-sized company as XX where resources are often limited. Economically most importantly, we need to stay competitive, which sometimes means making tough decisions. However, we try to not compromise on social and environmental responsibilities. For instance, we may pay a premium for sustainably sourced materials sometimes because our boss and then of course we as a company believe that the long-term benefits are more important than the short-term costs. In supply chains, this is even more difficult, I think. Because we rely on the things our partners do. Of course, we try to work closely with them to be aligned with our sustainability goals, but there are always challenges, particularly when dealing with suppliers in regions with different regulatory standards or economic pressures all over the world. So yeah it is not easy I would say.

Interviewer:
Yes, I understand that. What practices or key components do you think are essential for maintaining sustainability in your organization and in value networks? (Q3)

Person 5:
Okay key practices in our company I would say is the supplier selection process. We assess potential partners not only on cost and quality but also on their sustainability credentials. In regard to the supply chain, I think transparency is the most important thing I would say. A strong

relationship with suppliers, allows us to have honest conversations about sustainability with them and makes sure we are, lets say on the same page so to speak.

Interviewer:
Okay then, moving on to cybersecurity. Which frameworks are you familiar with or use in your organization? (Q4)

Person 5:
As a German company of course ISO 27001. We also ensure compliance with industry-specific regulations, especially when dealing with sensitive customer information or proprietary data from our suppliers. In our case that means TISAX of course.

Interviewer:
My next cybersecurity question would be how effective are these frameworks in managing cybersecurity risks in value networks? (Q5)

Person 5:
Well okay. That is something I do not know in detail. I am sorry. But from a supply chain perspective, the effectiveness probably can vary depending on the maturity of the cybersecurity practices from your partners in the network. So I think that everybody should be on the same page regarding their cybersecurity so to say.

Interviewer:
Okay then how do you see the relationship between cybersecurity and sustainability, particularly more detailed in value networks? (Q6)

Person 5:
Okay, more detailed? Okay that is tough. So, then I think, that a breach in cybersecurity probably can have a big impact, not just financially but also in terms of trust and reputational damage, which can undermine our sustainability in supply chains. For example, I think if a cyber-attack disrupts the supply chain, it can lead to delays, increased waste, and higher costs which of course would be bad for the sustainability.

Interviewer:
Maybe you can provide examples where cybersecurity measures have influenced sustainability efforts, meaning either supporting or hindering them? (Q7)

Person 5:

Sorry I am missing concrete examples here. Very sorry.

Interviewer:
Okay no problem. My last question to you Person 5 is how can cybersecurity and sustainability be aligned within value networks, and what emerging trends do you see in the future? (Q8)

Person 5:
Well, I think you might have to look at them together instead of as separate things. And as trend I could see maybe Blockchain. Sorry my secretary tells me that I really have to go. I am very sorry.

Interviewer:
Yes of course, no problem. Then still thank you very much for your time, Person 5.

Person 5:
Yes, thank you. Good bye.