Mastering the Survival of the Fittest: How Digital Technologies Can Help Organizations to Succeed throughout the Evolution of Cybersecurity

Dissertation

zur Erlangung des Grades eines Doktors der Wirtschaftswissenschaft

der Rechts- und Wirtschaftswissenschaftlichen Fakultät

der Universität Bayreuth

Vorgelegt

von

Florian Lennart Weiß

aus

Hamburg

Dekan:	Prof. Dr. Claas Christian Germelmann
Erstberichterstatter:	Prof. Dr. Nils Urbach
Zweitberichterstatter:	Prof. Dr. Maximilian Röglinger
Tag der mündlichen Prüfung:	23.06.2026

You don't get results by focusing on results. You get results by focusing on the habits and behaviors that produce results.

Mike Hawkins

Abstract

In the course of digitalization and digital transformation, organizations have fundamentally changed in terms of their business models, organizational structures, processes, and the technologies employed. This has significant implications for their cybersecurity, which must evolve from primarily focusing on maximum security to developing proactive and resilient solutions. To explore how digital technologies can help organizations navigate this fundamental development in cybersecurity, this dissertation utilizes evolution theory as a theoretical lens. Specifically, three research goals (RGs) are defined and aim to investigate, firstly, which particular developments impact organizations' cybersecurity, secondly, what new requirements arise as a consequence, and thirdly, how digital solutions must be designed to meet these new requirements. In order to achieve these research goals, this dissertation is structured cumulatively, comprising six essays, with two essays dedicated to each RG. To achieve RG1, Essay 1 offers insights into architectural IT changes using modern bond markets as a case study, while Essay 2 details how virtual 3D environments could lead to best possible athlete performances in digital sports. To fulfill RG2, Essay 3 examines the new organizational requirements emerging from increased utilization of cloud technologies from an organizational theory perspective. This is complemented by Essay 4, which explores the energy market, illustrating how cybersecurity solutions have transformed from highly centralized to increasingly decentralized structures along the entire value chain. To complete RG3, Essay 5 builds upon the insights of the previous RGs, introducing an artifact for conducting automated cloud security audits. The dissertation concludes with Essay 6, which presents another technical artifact for prioritizing cybersecurity controls, aimed at organizations with limited cybersecurity resources.

Keywords: Cybersecurity, Evolution theory, Information systems, Design Science, Empirical research.

Copyright Statement

The following sections are partly comprised of content from the research papers included in this thesis. To improve the readability of the text, I omit the standard labeling of these citations.

Acknowledgments

This dissertation is the result of four years of intensive work, supported by many colleagues, friends, and family members.

First, I sincerely thank my supervisor, Prof. Dr. Nils Urbach, for his constant support, open-mindedness, and for giving me the freedom to shape my research topics. Special thanks go to Dr. Tobias Guggenberger for his tireless guidance and assistance in numerous projects. His commitment was invaluable, especially over the past two years.

I am also grateful to my early academic mentors who inspired me to pursue a doctorate: Prof. Dr. Paul Weiß, Dr. Marlies Weiß-Jennrich, and Dr. Bärbel Weiß. My first position in academic research at TU Berlin laid the foundation for my academic journey. Thank you very much to Prof. Dr. Christian von Hirschhausen, Dr. Ben Wealer, and Petra Haase for your support and for the opportunities you have given me to get involved into research.

My deepest thanks go to my colleagues at the FIM Research Center for Information Management and Fraunhofer FIT for creating an inspiring and motivating environment for this work.

Above all, I owe heartfelt gratitude to my family and friends for their unwavering support across all stages and locations from Hamburg, Berlin, Bayreuth, to Munich. A special mention goes to my partner Larissa, whose encouragement and support was indispensable throughout this journey.

Finally, I thank all external experts from academia and various industries who contributed through interviews, feedback rounds, and (conceptual) discussions.

Florian Lennart Weiß
Bayreuth, April 2026

List of Abbreviations

AI	Artificial Intelligence
CAS	Complex Adaptive System
CIS	Center for Internet Security
DO	Design Objective
DP	Design Principle
DSO	Distribution System Operator
DSR	Design Science Research
EU	European Union
Fintech	Financial Technology
HMD	Head-Mounted Display
IaaS	Infrastructure as a Service
IS	Information System
ISM	Information Security Measure
IT	Information Technology
MR	Meta Requirement
MVP	Minimum Viable Product
NIS2	Network and Information Security 2 (Directive)
OS	Operating System
OT	Operational Technology
PaaS	Platform as a Service
RG	Research Goal
SaaS	Software as a Service
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SME	Small or Medium Enterprise
TAC	Transaction Costs
TSO	Transmission System Operator
VHB PMR	VHB Publication Media Ranking
VM	Virtual Machine
VR	Virtual Reality
ZTA	Zero Trust Architecture

Table of Contents

Introduction to Mastering the Survival of the Fittest: How Digital Technologies Can Help Organizations to Succeed Throughout the Evolution of Cybersecurity

Abstract

The overarching goal of this dissertation is to support organizations in mastering the "survival of the fittest" throughout the evolution of cybersecurity. By employing evolution theory as a theoretical lens, three research goals were defined, which are addressed in two essays each. This introduction is structured as follows: After this dissertation's goals and relevance are motivated in Section 1, a review of the technical and conceptual foundations of cybersecurity follows in Section 2. Afterwards, Section 3 presents the three research goals defined that constitute the fundamental framework for the six essays included in this dissertation. Subsequently, Section 4 details the research methodologies used to explore the research questions, before Section 5 summarizes the findings of each essay. The introduction ends with a discussion of the overarching insights, an acknowledgment of the study's limitations, and potential directions for future research in Section 6.

Keywords: Cybersecurity, Evolution theory, Information systems, Design Science, Empirical research.

Table of Contents – Introduction

1 Motivation

The world has undergone significant change over the past decades. Until today and over the course of several industrial revolutions, many industries and the organizations operating within them have evolved from traditional businesses to digitally transformed entities (Berawi et al., 2020; Sermpezis et al., 2024). By employing a variety of digital technologies, resulting in highly interconnected systems and actors, the technology landscape has become significantly more dynamic and complex (Schneier & Vance, 2025).

In the wake of digital transformation, companies today find themselves in a fundamentally changed business environment, which also poses new demands on companies to ensure their long-term success. In biological evolution theory, this concept is referred to as "survival of the fittest," which implies that organisms must adapt to their respective external environments by changing their characteristics and consolidating them genetically (e.g., through plastic mutations) (Darwin, 1859). Notably, such changes can originate from the organisms themselves and prevail, or a change in the environment can induce it (Laland et al., 2014).

Just as biological organisms must evolve in order to survive in the long term, industries and organizations must evolve in order to remain successful beyond industrial revolutions, too (Ruse, 1975). This also applies to the evolution of cybersecurity in modern organizations throughout digital transformation. In the past, digital networks were physically separated, the technologies used were straightforward, and development cycles were longer (Buck et al., 2021). Under these circumstances, the goal was always to achieve maximum security, proactively avoiding risks and responding appropriately to unforeseen events (Bitzer et al., 2023; Knudtson, 2021). Examples of this include the "castle and moat model," in which networks are protected against external threats with firewalls and it is assumed that only trustworthy actors and systems reside inside the network (Rose et al., 2020). In an environment where complexities were manageable and security perimeters were clearly separated, these approaches worked well.

However, these conditions no longer apply to modern digital technology landscapes, whereas especially three trends are particularly influencing the evolution of cybersecurity leading to new requirements organizations have to fulfill (Tzavara & Vassiliadis, 2024).

The first important trend to highlight is *decentralization*. With the advent of the internet, technologies such as cloud and edge computing have become well established, meaning that assets that were once physically separated from the rest of the world are now distributed beyond network boundaries (Buck et al., 2021; Cuervo-Cazurra et al., 2020; Nurse et al., 2021). This applies not only to information technologies (IT) such as data storage and processing, but also to operational technologies (OT) such as industrial plant control systems (Buck et al., 2023). The protection of assets can therefore no longer be achieved, along clearly defined network perimeters only (He et al., 2022; Rose et al., 2020).

Furthermore, as a result of technological advances, new digital technologies are being introduced every day, significantly increasing the *diversity* of the technology landscape as a second essential trend to note (Bennett & Robertson, 2019; Schneier & Vance, 2025). Generally, all digital technologies employed have specific characteristics in terms of their technical implementation, operational properties, and, as a result, risk profiles (Hasan et al., 2023; Rekeraho et al., 2024). As the diversity of digital technologies used increases, so does the number of opportunities for unintended behavior and sources of error, as well as potential targets for attack (Lewis & Wang, 2019; Torkura et al., 2019). As a consequence, organizations have to implement several types of measures to assess and actively manage their newly introduced risks, to avoid, e.g., loss of confidential data or downtimes (Buck et al., 2023).

A third substantial trend affecting cybersecurity is the shift towards *fast-paced* environments. In this regard, another result of (technological) progress is the sharp increase and continuous rise in the frequency of development and release cycles (Y. Zhang et al., 2021). Consequently, manual checks cannot keep pace with either the speed or the volume of assets that need to be protected (Salnitri et al., 2014). Digital technologies are therefore needed to provide support through automation and prioritization, reducing the workload of those in charge and ensuring that they can concentrate on the most important tasks (Bécue et al., 2021).

Consequently, the overarching goals of cybersecurity have changed fundamentally (Rinehart & Shortridge, 2020; Taha, 2023). It is now widely agreed that “there is no such thing as 100% cybersecurity” (Weppler, 2017, p. 118). Because both unintentional errors (e.g., due to incorrect user behavior) and intentional damage (e.g., due to insider or external attacks) can no longer be prevented entirely, other objectives, such as

resilience, have gained in importance and have become central components of regulatory requirements (Bitzer et al., 2023; Directive (EU) 2022/2555, 2022; Executive Office of the President, 2024).

To master these evolutionary challenges, digital technologies can support organizations in numerous ways and therefore play an essential role in ensuring resilience and cybersecurity, thus enabling them to survive within the new business environment (Strobel et al., 2023). For example, digital technologies make important contributions to enhancing the effectiveness and efficiency of vulnerability prevention, information system monitoring, and the detection of and response to cybersecurity incidents (Bécue et al., 2021; Kopanaki, 2022). However, it is not only the correct choice of technology that is crucial for success, but also the organizational structure and the adoption of and anchoring within respective processes (Annarelli et al., 2020; Soomro et al., 2016). Research must therefore not only focus on the potential of digital technologies in ensuring future-proof cybersecurity, but also examine how they can be optimally implemented and used (Abdullayeva, 2023).

In the literature, strategies and measures in this context are primarily discussed in a fragmented manner (i.e., often industry- or application-specific and either operational or strategic) (Wenye Wang & Lu, 2013). In addition, important developments are often discussed simultaneously, e.g., being summarized under the term “complexity,” without sufficiently shedding light on the individual causes or individual factors that lead to an overall increase in complexity (Schneier & Vance, 2025). Although the body of knowledge available today already includes various approaches to solving numerous challenges incurred by the continuously evolving field of cybersecurity, there is often a lack of overarching structuring of strategic and operational developments to effectively address the new requirements resulting from digital transformation. Evolution theory, as well as its various applications, especially in the economic sciences, provides a useful theoretical lens for the integrated analysis of both evolution-driving factors and the solutions developed to resolve them.

With this dissertation, I aim to contribute to this discourse by taking a holistic yet differentiated approach. Hence, I start by exploring which factors precisely influence the evolution of cybersecurity and in which ways. Additionally, I am building upon this to determine which new requirements arise for organizations to survive under these changed conditions. Finally, I develop specific solutions addressing these identified

new requirements for particularly representative use cases and contribute to the available knowledge through the experiences and insights gained from designing to (practically) testing them. To achieve these ambitions, I define the following overarching research goal:

Supporting organizations to master the survival of the fittest throughout the evolution of cybersecurity

In this context, this dissertation aims to advance the discourse in Information Systems (IS) research on the evolution of cybersecurity. By addressing a range of both specific and multifaceted research questions across six essays, I examine the three dimensions of evolution. Thus, this dissertation contributes a distinguished and end-to-end analysis of, first, the evolution's origins, second, their implications, including necessary changes for organizations, and third, possible IS artifacts enabling the fulfillment of these new requirements.

The remainder of this introduction is organized as follows: It begins with an overview of the technical and conceptual foundations of cybersecurity. This is followed by the presentation of three Research Goals (RGs), which serve as a unifying framework for the six essays comprising this dissertation. Subsequently, the research methods employed to investigate the corresponding research questions are outlined, and a summary of the key findings from each essay is provided. The introduction concludes with a discussion of the overarching insights, a consideration of the study's limitations, and an outline of avenues for future research. The six essays are presented in the chapters that follow this introduction.

The findings presented in the essays are the outcome of collaborative research conducted with co-authors. Consequently, the plural pronoun "we" is used when referring to the content of these essays in the following sections. For the sake of improved readability, I have deliberately omitted the standard citation labels typically used to indicate co-authorship.

2 Theoretical Background

2.1 Introduction to Cybersecurity

In IS literature, various terms, approaches, and instruments exist to protect (digital) assets against vulnerabilities and their intentional or unintentional exploitation. In this regard, the term "asset" refers to any kind of resource worth protecting, whether they are entirely digital (such as information in databases or text documents) or have interfaces with physical systems (i.e., cyber-physical systems like control units for filtration systems or voltage regulators). "Vulnerabilities" describe the potential threats to these assets (e.g., publicly accessible confidential information online or over the internet, accessible control units of wind turbines). In general, organizations only suffer from damage through the actual "exploitation" of a vulnerability, e.g., by an external attacker (Bayuk, 2013). Furthermore, the literature differentiates between intentional and unintentional exploitation of vulnerabilities, as each may require different mitigation strategies (Diesch et al., 2020). Instruments and measures employed to reduce risks by mitigating vulnerabilities are called "controls". Today, risk assessments and evaluations are regularly conducted to decide which controls should be implemented to either prevent the exploitation of identified vulnerabilities or to eliminate vulnerabilities completely. IS scholars have agreed that completely eliminating any potential vulnerability is not optimal for companies if the expected damage does not exceed the costs for vulnerability elimination. At the operational level, potential damage scenarios are multiplied by their probabilities of occurrence to determine risk values, which are then used to make decisions about whether to avoid or accept these risks (Bayuk, 2013). Thus, such approaches are often referred to as risk-based, as the purpose of cybersecurity functions usually aims at minimizing losses rather than generating additional income (Diesch et al., 2020).

Until today, decision-makers and cybersecurity professionals have historically struggled to secure sufficient budgets, personnel, and equipment for ensuring sufficient cybersecurity as a consequence of their risk-minimizing rather than income-generating nature (Soomro et al., 2016). In daily routines, some organizations have even developed negative perceptions of cybersecurity functions, viewing them as opponents rather than supporters who are rather consuming than increasing company resources. In recent decades, this perception has significantly changed in many organizations due to

the dramatic increase in successful cyberattacks on businesses. With production lines being forced to stop, sustained reputational damage experienced, and even several bankruptcies observed, the role of cybersecurity in companies has grown significantly in importance (Boakye et al., 2024). Today, especially in highly digitalized or digitally transformed organizations, cybersecurity has become a crucial prerequisite for future viability and success. In the subsequent subsection, these developments will be further explored.

However, before being able to analyze the evolution of cybersecurity, it is vital to define the term cybersecurity and understand that there are multiple dimensions, perspectives, and underlying philosophies that must be distinguished both generally and specifically. The most prevalent overarching terms in the literature aiming towards the protection of (digital) assets are "information security", "information and communication technology security", and "cybersecurity" (R. von Solms & van Niekerk, 2013). To illustrate the differences between these terms, it is important to differentiate which dimensions and factors are respectively considered to protect which kinds of assets. On one hand, there is the digital dimension, which includes, e.g., digital networks, storage units, actors (both human and machine-based), and the physical dimension, which involves, e.g., hardware, analog data carriers (like printed documents), people, and relevant environmental factors (like temperature, humidity, or vibrations). While information security focuses on (both digital and analog) information as well as the digital technologies employed, information and communication technology security exclusively targets the security of technical components. In contrast, cybersecurity aims to protect not only technical components and information but also any tangible assets (e.g., functioning critical infrastructures) and intangible assets (e.g., not being discriminated or exploited on the internet) belonging to people and societies (R. von Solms & van Niekerk, 2013). Due to this broader perspective in cybersecurity, including both people and digital technologies, i.e., the core subjects of IS research, I chose cybersecurity as the subject for investigation in my dissertation. Figure 1 illustrates the similarities and differences between the three terms.

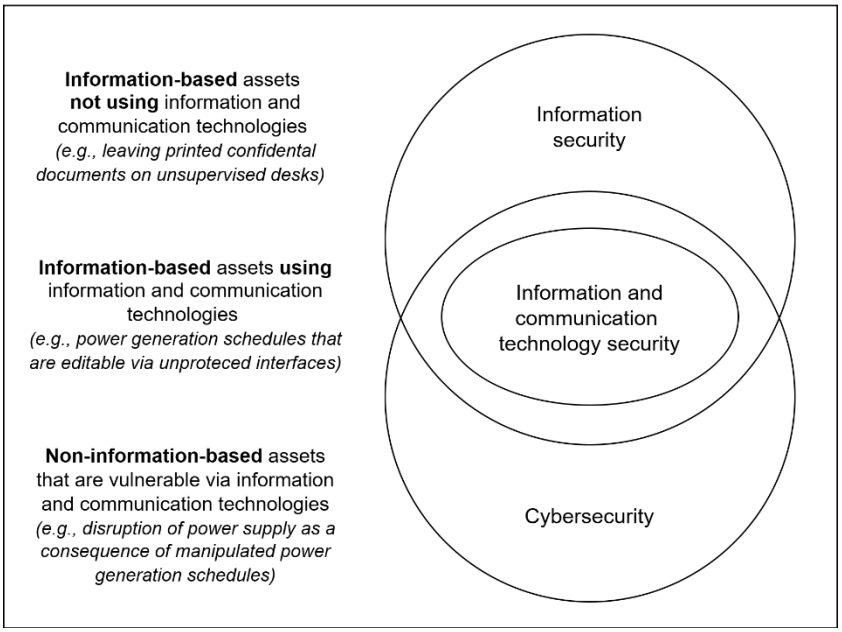

Figure 1: Differentiation of information and communication technology security, information security, and cybersecurity based on R. von Solms and van Niekerk (2013)

2.2 Evolution of Cybersecurity

Until today, digital technologies have led to various improvements by transforming the everyday operations of organizations. Companies are increasingly digitalizing their processes to increase efficiency, enhance customer experiences, and secure competitive advantages (Berawi et al., 2020; Bresciani et al., 2021; Meier, 2017). This digitization involves adopting a range of technologies, such as AI, IoT, and big data analytics (Bresciani et al., 2021; Feroz et al., 2021). However, these technological advancements and shifts in business practices have also led to evolving security threats (Mishra & Gochhait, 2023; Weiyu Wang & Siau, 2019).

In this context, several key developments are emerging. One significant shift affecting security is the increasing decentralization and diversity of digital technologies (Bacis et al., 2020; Nguyen Duc & Chirumamilla, 2019). Remote work, whose adoption was significantly accelerated throughout the COVID-19 pandemic, has spread workforces across different locations, with employees now accessing corporate networks from various environments using multiple devices and technologies (Nurse et al., 2021). Also, businesses are operating on a global scale, with complex supply chains and international collaborations that require technical interfaces (Cuervo-Cazurra et al., 2020). Furthermore, the convergence of physical and digital components has considerably

expanded the attack surface of IS, making them vulnerable to both physical and digital remote attacks (Rekeraho et al., 2024). The increasing number and diversity of digital technologies, along with the multiple actors involved in deploying them, introduce additional risks, thereby heightening the vulnerability even more (Hasan et al., 2023).

Another trend is the continuous development and enhancement of digital solutions to maintain and elevate their value (Beach et al., 2019; Nagel et al., 2012; Welsh & Benkhelifa, 2020), leading to rapid changes in code, sometimes happening within minutes (Y. Zhang et al., 2021). Especially widely adopted cloud architectures involve numerous components, interaction patterns, and services, often exceeding human comprehension of the system and its behavior (Mouratidis et al., 2020; L. Tang et al., 2023).

This overall substantially increasing complexity redefines the security landscape, creating new demands (Schneier & Vance, 2025). As a consequence, traditional controls have been found to be inadequate to ensure sufficient protection levels within these decentral, diverse, and fast-paced environments (Rinehart & Shortridge, 2020). Simultaneously, cyber-attacks have become more sophisticated and frequent, requiring even more robust measures (Abrahams et al., 2024). Advancements in AI, for instance, facilitate high-level, automated attacks (Bécue et al., 2021). Consequently, cybersecurity has emerged as a critical concern requiring active attention and innovative approaches (Furrer, 2022).

In this context, understanding why traditional measures fall short is crucial. Historically, security approaches prioritized creating maximally secure systems (Knudtson, 2021; Rinehart & Shortridge, 2020), employing preventive and reactive measures to protect an organization's assets. While preventive measures focus on identifying and mitigating potential threats before they materialize (Baskerville et al., 2014), such as through regular threat analyses and ethical hacking (Bishop, 2007), reactive measures, like incident response management, tackle security breaches after they occur, minimizing damage and facilitating recovery (Bitzer et al., 2023).

Despite playing a critical role in cybersecurity, traditional measures are insufficient against the rising number and diversity of cyber threats (Shinde & Ansurkar, 2023). As system complexities grow, failures become inevitable (Bitzer et al., 2023). In this regard, literature acknowledges that "there is no such thing as 100 percent security" (Weppler, 2017, p. 118), and cybersecurity must also ensure resilience, enabling

systems to handle faults and incidents that are assumed inevitable in modern systems (Ross et al., 2021; Safitra et al., 2023).

Another major issue of traditional controls is their inadequate integration into organizational processes. Conducted late in development, these measures at least complicate vulnerability resolution, as fundamental flaws are hard to resolve shortly before planned release (Muñoz et al., 2018). Basically, the widely adopted techno-centric approach fails to address cybersecurity's socio-technical nature, neglecting organizational factors such as processes and structures (Christine & Thinyane, 2022). Thus, cybersecurity controls must be employed in early development stages, too, to identify and address vulnerabilities proactively as soon as possible (Abdullayeva, 2023).

Consequently, organizations must adapt their cybersecurity strategies. It has been found that those embracing resilience and proactive approaches are more likely to sustain operations and recover from cyber incidents (Tzavara & Vassiliadis, 2024). As the shift towards resilience and proactive cybersecurity caught the attention of both politics and industry (e.g., Directive (EU) 2022/2555, 2022 (2022), NIST (2024)), also academic literature has addressed various evolutionary aspects, from meta-studies to distinct strategic measures and considerations (Saeed et al., 2023; Schneier & Vance, 2025). In this regard, a strategic vision illustrating the necessary structural and procedural adaptations organizations need, harmonizing efforts to ensure sufficient cybersecurity in the long term, was found to be fundamental. As a prerequisite, organizations need a comprehensive overview to develop future-proof cybersecurity strategies, addressing both technical and organizational factors (Whitten & Kayworth, 2010).

Finally, developing solutions for identified problems and methods for evaluating and selecting various approaches is vital. However, multiple solutions may be applicable to achieve similar targets but vary in protection goal prioritization, costs incurred, or risk mitigation effectiveness. Organizations must, thus, trade off these solutions to its risk profile, desired security level, and (economic) constraints (Diesch et al., 2020).

2.3 Evolution Theory

In his work, Charles Darwin focused on the evolution of biological organisms. He concluded that every species faces "struggles," as otherwise they would reproduce endlessly and overtake other life forms (Darwin, 1859). In contrast, these struggles might

cause certain life forms to stop reproducing and eventually become extinct if these struggles are not sufficiently addressed. From this, Darwin (1859) inferred that there must be specific characteristics enabling organisms to overcome their struggles. As these characteristics evolve over generations, potentially enhancing or diminishing survival chances, he described retaining beneficial characteristics and discarding disadvantageous ones as "natural selection" resulting from the "survival of the fittest". Generally, this process can stem from multiple origins. Firstly, a particularly advantageous variation of an organism might emerge throughout the development of generations and eventually dominate in a given environment. Secondly, a change in the environment might lead to a variation in behaviors that solidify genetically, or a previously less advantageous variation of characteristics might become beneficial under new conditions and thus succeed (Laland et al., 2014).

Until today, Darwin's work is considered one of the most significant scientific contributions and has influenced fields beyond biology. For instance, his work has been adopted by economics, where consensus emerged regarding marginal efficiency increases being the driver for economic change, and economic progress being equivalent to evolution (van den Bergh & Gowdy, 2000). Additionally, neo-classical economists like Schumpeter (1949) further developed Darwin's survival of the fittest into the well-known principle of "creative destruction". Overall, evolutionary thought holds as much significance in economics as it does in biology, for multiple reasons. Firstly, since the eighteenth century, economic systems have undergone rapid transformation, exhibiting patterns of qualitative, structural, and irreversible changes, challenging the concept of stable growth paths suggested by multiple theories. Secondly, economic systems possess an extensive capacity for sustained learning and adaptation across various levels, from individuals and households to organizations, sectors, and even globally. Thirdly, evolution is reflected in the economy's horizontal structure, encompassing science, technology, markets, and culture (Nelson, 1995; van den Bergh & Gowdy, 2000).

While concepts like coevolution (Johnson et al., 2016), evolutionary game theory (Ba et al., 2000), and evolutionary psychology (Kock, 2009) have emerged in IS literature, IS scholars have, to the best of my knowledge, only indirectly adopted Darwin's evolution theory concepts regarding the survival of the fittest to IS research. Yet, it seems plausible that economic principles influenced by evolution theory would apply to IS,

analogously, as the goals of growth and long-term success effectively drive the development, choice, and use of digital technologies in organizations, too (Bacon, 1992).

As highlighted earlier, the technology landscape, organizational vulnerabilities, and threat environments have radically changed. Consequently, some general approaches, e.g., business-based language between budget managers and security professionals (Tran & Jøsang, 2023), and specific controls, e.g., penetration testing, have proven effective, while others are either replaced or present new challenges (e.g., cloud security auditing). In Darwin's terms, companies face existential struggles, necessitating adaptation for survival. Since cybersecurity incidents can quickly become existential threats, particularly if a manufacturing company's production is halted or critical infrastructures, like health services or energy and food supply, are disrupted (Boakye et al., 2024). In my dissertation, I utilize evolution theory as a framework to analyze, first, which changes lead to such existential struggles, and second, what the implications for organizational cybersecurity are. Third, I present solutions to support organizations to master the survival of the fittest throughout the evolution of cybersecurity.

3 Derivation of Research Gaps and Research Goals

To achieve my overarching RG, I have defined the following three research goals based on Darwin's evolution theory:

(RG1) *Identify the environmental changes that necessitate an adaptation of cybersecurity for modern organizations*

(RG2) *Determine the requirements that arise from these changes to effectively and efficiently adapt cybersecurity in modern organizations*

(RG3) *Develop digital solutions that support the adaptation of cybersecurity in modern organizations to meet the identified requirements*

To achieve the research goals, each of them was addressed within two essays. To fulfill RG1, it was necessary to develop a deep understanding of the key developments at various levels concerning the digitalization and digital transformation of organizations. For this purpose, I conducted comprehensive investigations into the respective issues and potential analyses for possible solutions, as well as developed corresponding prototypes. For achieving RG2, I conducted several studies to analyze the socio-technical implications of these changes, highlighting both the current state of implementation and areas that still leave room for improvement. Building on these insights, I developed specific solutions for both operational and strategic challenges as part of fulfilling RG3. It can be summarized that the individual RGs build upon each other, thus facilitating a holistic understanding of the evolution of cybersecurity. However, achieving each RG rigorously also required a nuanced and in-depth exploration of the respective knowledge and the development of innovative solutions that incorporate both socio-technical and economic perspectives.

3.1 RG1: Identify the Environmental Changes that Necessitate an Adaptation of Cybersecurity for Modern Organizations

To achieve RG1, I focused on the central developments related to digital transformation in Essay 1 and Essay 2. To correctly identify the relevant new requirements for cybersecurity in RG2, we first examined in RG1 exemplary structural changes at the overarching market architecture level (Essay 1) as well as those resulting from the transformation of work towards immersive virtual working spaces (Essay 2).

For the investigation of fundamental changes in market structures, we concentrated

on the transformation of today's corporate bond markets. This case is particularly suitable because the corporate bond market in the United States alone accounted for USD 10 trillion in 2020 (International Capital Market Association, 2020), playing a crucial role in both funding companies and offering diverse investment prospects for investors. Moreover, the growing significance of this market has led to the establishment of numerous players and processes within the corporate bond market, demanding smooth interactions, significant coordination efforts, and information maintenance. These intricate structures involve various institutional intermediaries, such as clearing and settlement houses, which provide trusted services to market participants (Allen & Santomero, 2001). These intermediaries are involved in interconnected processes such as bond issuance, promissory bill trading, and ensuring secure settlements, leading to notable delays in settlement times and added costs (Kleinbauer & Stone, 2021). Engaging with the bond market involves transaction costs (TAC), which become evident with increasing complexity. This complexity results in inefficiencies such as additional expenses for coordinating stakeholders and addressing incompatibilities. These inefficiencies can lead to higher bid-ask spreads, increased market impact costs, and challenges in conducting large trades effectively (Edwards et al., 2007; Williamson, 1981). Furthermore, high TAC can result in significant drawbacks, such as discouraging market participation, reducing liquidity, and potentially distorting price discovery processes, resulting in less efficient markets (Benston & Smith, 1976). High TAC may also dissuade smaller investors or firms from participating in the market, particularly due to the disproportionate impact of these costs on smaller transactions (Williamson, 1981). Consequently, such an environment may heighten systemic risks, as hidden costs and inefficiencies contribute to market vulnerabilities (Coase, 1937). To cope with this challenge, there are multiple methods to minimize TAC. One of the most established ones is to reduce the number of required transactions, or transfers across different entities, through vertical integration, whereby activities that were previously external, like credit rating activities, are now integrated within the company (Ciborra, 1983; Feulner et al., 2022; Williamson, 1981). Research on achieving transaction efficiency has increasingly highlighted using digital technologies (Ciborra, 1983; Gurbaxani & Whang, 1991; Williamson, 1981). Until now, scholars have demonstrated how digital technologies can help to reduce TAC across various contexts and use cases beyond bond markets (Aubert et al., 1996; Grover et al., 1996; Gurbaxani & Whang, 1991; Lacity & Willcocks, 1995; C.-Y. Li & Fang, 2022). Among the foremost digital technologies

discussed for reducing TAC is blockchain technology. Blockchain solutions are well-regarded for enabling trustless transactions (Beck et al., 2016; Feulner et al., 2022), thereby promising to replace trusted intermediaries. The distinctive features of blockchains offer up-to-date, tamper-resistant ledgers, which boost trust among market participants, a crucial factor in the financial sector, and reduce opportunities for opportunism, hence lowering TAC (Rossi et al., 2019). Additionally, blockchain can improve transaction efficiency compared to current methods, where all actors must maintain their data and update each other via additional channels (Andersen & Bogusz, 2019). Consequently, multinational financial institutions have initiated projects exploring the potential of blockchain-based bonds (HSBC, 2024). Recent regulatory changes in Germany have facilitated the regulatory-compliant issuance, management, and trading of bearer bonds using blockchain technology (Federal Financial Supervisory Authority, 2021), prompting several companies to launch token-based bond issuance solutions (Siemens AG, 2023). Thus, blockchains offer viable and feasible solutions for reducing TAC in financial markets (Axelsen et al., 2023; Guggenberger et al., 2023), contributing to a body of literature on designing efficient financial markets using blockchain technology (Grossmann, 2024; Guggenberger et al., 2023; Kranz et al., 2019). Notably, while there is substantial literature in this field, there remains a lack of targeted research on bond markets, despite their significant use in financial practice today. Existing literature on bond markets often either presents broad theoretical perspectives (Chen, W., and Wang, Q., 2020; Grossmann, 2024; Kleinbauer & Stone, 2021) or focuses on niche applications, such as carbon emission markets (Axelsen et al., 2023), leaving a gap in research on designing TAC-efficient corporate bond markets (Guggenberger et al., 2023; Kölbel et al., 2022). This is concerning since TAC theory offers a well-established understanding of market mechanisms, providing theoretical guidance for designing efficient blockchain-based markets. In sum, because (1) TAC are significant in bond markets, (2) blockchain solutions can mitigate these costs, and (3) the existing literature lacks guidance on designing such solutions, this study aims to address this gap by posing and answering the following research question:

How can a blockchain-based bond system be designed to reduce transaction costs in bond markets? (Essay 1)

Complementary to this examination of structural changes on the market architectural level, e.g., through the introduction of a blockchain-token-based solution, the world of

(digital) sports is constantly evolving, too. As the use of new technologies in sports, especially virtual reality (VR), gains momentum, two main formats have emerged: The 1) format involves hybrid-sports, which merge real world physical activity, commonly associated with traditional sports, with digital elements like VR. For example, competitive cycling using stationary cycling equipped with a head-mounted display (HMD) or VR supports athlete skill assessment and scenario-based training through (Romeas et al., 2022). Or 2) fully 3D virtual environments for digital sports (instead of existing 2D screen-based environments) (Chen et al., 2024). In summary VR is a particularly relevant technology for hybrid and digital sports, enabling a strong sense of presence and immersion for multiple purposes (Haffner et al., 2025).

Prior research on VR has predominantly examined user, customer, and employee behavior in contexts such as shopping, retail, and training. These studies have compared 3D virtual environments to 2D screen-based settings to assess how participants perceive and accomplish performance advantages across different settings (Huygelier et al., 2019; Kim & Ko, 2019; Meißner et al., 2020; Menck et al., 2023; Rowen et al., 2019). Within the hybrid-sports domain, VR has been widely explored for its potential to enhance training and performance. Reviews and empirical evidence indicate that immersive technologies such as VR can improve perceptual-cognitive skills and training precision (Cariati et al., 2025; Kittel et al., 2024; Y. Li et al., 2025; Neumann et al., 2018), suggesting that VR provides substantial benefits for hybrid-sports. However, it remains unclear whether these benefits of the use of VR also extend to digital sports. Emerging studies suggest that VR experiences can enhance motivation and engagement in digital sports (Chengjie Zhang & Yu, 2024), yet systematic comparisons between 3D virtual environments and 2D screen-based settings are still limited. Previous research has investigated variables such as well-being, attitudes toward the sport task, involvement, acceptability, flow experience, and physiological responses (Banerski et al., 2025; Barbour et al., 2024; Kim & Ko, 2019). But yet it misses to explain how VR, as an immersive technology, increases visualization from 2D to 3D, influences athletes' subjective and objective performance in digital sports.

To address this gap, the present study provides a comprehensive assessment of performance by comparing 2D screen-based settings, the conventional mode of experiencing digital sports, with 3D virtual environments with the use of a HMD, capturing both athletes' subjective perceptions and objective performance measures. Additionally, we

examine whether athletes' perceived performance aligns with their objectively measured performance in digital sports, as this can reveal how interactions within 3D virtual environments affect athletes' perception and actual performance. Accordingly, this research addresses two primary questions:

Does the use of VR for athletes, shifting from 2D to 3D, have a positive effect on digital sport performance, in terms of both subjective perceptions and objective performance? Do athletes' subjective perceptions of digital sport performance correspond to their objective performance? (Essay 2)

3.2 RG2: Determine the Requirements that Arise from these Changes to Effectively and Efficiently Adapt Cybersecurity in Modern Organizations

After RG1 explored the changes with potential impacts on cybersecurity as a result of digitalization and digital transformation, RG2 examines the implications by deriving the corresponding requirements.

As introduced in the previous sections, the ongoing development and application of digital technologies have significantly transformed the business environment, resulting in notable technological advancements and evolving business practices. However, this has also led to an increase in sophisticated security threats (Mishra & Gochhait, 2023). As organizations pursue the digitalization of their operations to improve areas such as efficiency and customer service, they encounter the dual challenge of utilizing new technologies while protecting themselves against emerging cyber risks (Berawi et al., 2020; Bresciani et al., 2021). In this regard, cloud computing has become a pivotal element of digitalization, offering scalable and cost-effective IT solutions that enable businesses to outsource infrastructure management (Mell & Grance, 2011; Parast et al., 2022). Its rapid adoption allows companies to benefit from decentralization, fostering remote work and global collaboration (Alashhab et al., 2021; Parast et al., 2022). Nowadays, most organizations utilizes some form of cloud computing (Sadavarte et al., 2022). However, the complexity of modern cloud architectures presents new security challenges, as these systems often consist of multiple microservices and complex interactions, which can result in unpredictable outcomes (Araújo De Oliveira, 2017; Söylemez et al., 2022). As reliance on cloud solutions increases, addressing cybersecurity has become even more critical, requiring approaches tailored to the specific

vulnerabilities present in these environments (Albanese et al., 2014; Furrer, 2022). Traditional cybersecurity measures, employed by cloud users, are becoming less effective in the face of rapidly evolving and increasingly intricate cloud architectures (Shinde & Ansurkar, 2023; Taha, 2023). Historically, these measures have concentrated on achieving maximum cybersecurity through a combination of preventive and reactive strategies (Knudtson, 2021). In light of the limitations of traditional methods, recent research is investigating more proactive and integrated security strategies, with a particular focus on resilience as a key aspect of cybersecurity. The existing literature covers various dimensions of this evolution, including meta-studies on organizational and environmental issues (e.g., Saeed et al. (2023) and B. von Solms (2000, 2006)), specific strategies and concepts (e.g., Annarelli et al. (2020), Soomro et al. (2016), and Werlinger et al. (2009)), and specific aspects within this context (e.g., M. Tang et al. (2016), Terpstra et al. (2017), and Ramluckan and van Niekerk (2020)). While these studies provide valuable insights and contribute to field advancement, they do not offer a comprehensive perspective that integrates the socio-technical and overall organizational considerations effectively. To the best of our knowledge, there is no existing framework that strategically combines and structures these central developments while providing recommendations to assist companies in achieving sustainable levels of cloud security. Thus, we propose the following research question in the context of our study:

Which socio-technical changes must digitalized organizations address at a strategic level to ensure sustainable cloud security? (Essay 3)

In addition to challenges that must be addressed at a strategic level, there are also many important changes on the more practical and operational level that need to be tackled. To investigate this issue, we examined the disruptive developments and fundamental changes in the energy sector as the focus of another study. This choice of industry for our research is particularly relevant as, in recent decades, critical energy infrastructures have evolved from primarily centralized and predictable setups with stable energy sources to more decentralized and dynamic configurations (Bedi et al., 2018). This shift has been largely driven by the sustainability transformation, shifting from high-emission fossil fuels to low-emission renewable energy sources (Rekeraho et al., 2024). This transformation is not only influencing the demand for and the utilization of digital technologies within the energy sector but also impacts cybersecurity concerns

regarding these infrastructures (Bedi et al., 2018). For instance, the merging of physical and digital components has expanded the attack surface of critical energy infrastructures, enabling attacks that can be executed remotely through digital means rather than solely physical attacks (Rekeraho et al., 2024). The proliferation and diversification of digital technologies, along with the various actors involved in their deployment, introduce additional vulnerabilities, further elevating risks to modern critical energy infrastructures (Hasan et al., 2023). As a crucial infrastructure, maintaining the functionality of critical energy infrastructures is essential for the proper functioning of modern societies, as they support other vital infrastructures like healthcare, food supply, and transportation, also (Blokus-Roszkowska & Dziula, 2016; Georgiadou et al., 2023). Both academia and practitioners proposed and tested various solutions to address the numerous and diverse challenges arising from the growing use of digital technologies in the critical energy infrastructure sector, such as zero-trust architectures (ZTA) and cyber-physical security measures for smart grids (Buck et al., 2023; Hasan et al., 2023). Although researchers have thoroughly documented the technological and organizational evolution of critical energy infrastructures, their practical cybersecurity implications have rarely been explored from a comprehensive, system-wide perspective, that accounts for the differences between small and medium-sized enterprises (SMEs) and larger corporations. This gap is significant since cybersecurity (including regulatory) requirements for the sector are intensifying, yet implementation progress remains heterogenous, primarily because SMEs usually do not possess the same kinds of resources to ensure adequate cybersecurity as larger companies (Georgiadou et al., 2023). In highly interconnected and dynamic environments, a vulnerability of any single actor can compromise the functioning of the entire network. Consequently, research should move beyond isolated case studies that do not address the specific characteristics and requirements of the respective actors to identify patterns across different actors that can guide improvements, encourage mutual assistance, and scale effective measures (Zhao et al., 2024). Scholars in the information systems field are increasingly applying complex adaptive systems (CAS) theory, viewing energy infrastructures as a complex system of interacting agents exhibiting emerging patterns (Nan, 2011). While several studies have already classified the sector as a CAS (Bale et al., 2015; Korhonen & Snäkin, 2015; Pearson & Bardsley, 2022; Wildberger, 1997), the cybersecurity implications of this perspective remain largely unexplored. Building on this consensus, we pose the question:

Which patterns related to cybersecurity have emerged through the evolution of critical energy infrastructures as complex adaptive systems for small and medium sized enterprises? (Essay 4)

3.3 RG3: Develop Digital Solutions that Support the Adaptation of Cybersecurity in Modern Organizations to Meet the Identified Requirements

RG3, the final of the three RGs, addresses specific solutions based on digital technologies to meet the requirements identified in RG2, which arise from the digitalization and digital transformation of organizations examined throughout RG1.

In this context, we first focus on the challenges highlighted in Essay 3, which result from the new requirements as a consequence of widespread cloud computing technology adoption. This is a particularly relevant field of research, since cloud computing has revolutionized IT environments, shifting them from static, centralized to highly dynamic and distributed architectures characterized by rapid development and deployment cycles (Bolannavar, 2020; Sermpezis et al., 2024). This paradigm shift necessitates that cybersecurity, which was traditionally an "afterthought" implemented sporadically, evolves into a continuous and integrated process. This shift ensures that vulnerabilities are identified as soon as possible and that cybersecurity measures are seamlessly incorporated into the workflows of developers and operators (Parast et al., 2022; Rinehart & Shortridge, 2020; Sermpezis et al., 2024). The traditional approach to cloud security audits, which are usually mostly manual and infrequently performed prior to major releases or certifications, proved to be costly and insufficient to keep up with the fast-paced modern environment (Lins et al., 2018; Majumdar et al., 2019). Therefore, organizations have to change to performing frequent and comprehensive audits, ideally with automated checks at least whenever significant changes are expected, to maintain compliance and to mitigate risks effectively (Lins et al., 2018; Rinehart & Shortridge, 2020). This need is particularly pressing in Infrastructure as a Service (IaaS) environments, where tenants bear responsibility for everything except the underlying hardware, necessitating the securing of every operating system (OS) configuration, patch, and service (Bennett & Robertson, 2019; Lane et al., 2017). Moreover, the OS layer presents a critical attack surface, where vulnerabilities could lead to complete virtual machine (VM) compromises or data breaches (Jasti et al., 2010; S. Zhang et al., 2014). Thus, effectively securing and auditing this layer requires deep

technical expertise and significant organizational effort (Bolannavar, 2020; Parast et al., 2022). While commercial tools can automate most of this work, their cost and need for customization are prohibitive for many smaller firms, despite these firms facing the same security responsibilities as larger entities under the shared responsibility model (Kandpal et al., 2023; Roy & Patil, 2023; Tenable, 2025). Given that nearly 80% of small and medium-sized enterprises (SMEs) using cloud services depend on IaaS (Eurostat, 2023), this poses a significant issue. Therefore, affordable, automated tools that can deliver accurate, on-demand OS-level assessments are crucial for securing and scaling modern cloud infrastructures, especially for companies unable to afford costly commercial solutions (Roy & Patil, 2023). Besides commercial solutions, associated open-source tools often fall short of supporting comprehensive cloud-native audits. They typically focus on a single OS (e.g., Linux or Windows) and do not incorporate automated compliance checks (like "CIS Benchmarks" or "NIST STIGs") across diverse OS environments. Until today, academic research has yielded valuable design knowledge in related areas, such as cloud vulnerability prioritization (Ullman et al., 2024), privacy-preserving IoT architectures (Chanson et al., 2019), optimization of identity and access management (Baumer et al., 2023; Yang et al., 2024), and secure information systems methodologies (Heikka et al., 2006), but lacks tangible audit tools or adaptations necessary for the dynamic, distributed nature of modern IaaS. Additionally, information systems research on auditing is limited in accounting contexts (Chanyuan Zhang et al., 2022), which differ fundamentally in data sources, workflows, and success metrics from those related to cloud security audits. This gap implies that especially SMEs lack cost-effective, reusable solutions to continually ensure OS-level security compliance, leading to periods of unmonitored vulnerability. To address this, we aim to develop and assess a cloud-native, multi-OS cloud security auditing artifact that integrates continuous compliance checks into development and operation processes to enhance the frequency, scope, and cost-efficiency of audits and derive generalizable design principles for OS-level security tools. Therefore, we raise the following research question:

How should an artifact for automated cloud security audits on the OS-level be designed to allow for more frequent, complete, and cost-effective audits? (Essay 5)

In addition to enabling organizations with limited cybersecurity budgets to conduct cloud security audits, our research identified another significant challenge in ensuring

cybersecurity. Specifically, this involves the selection of information security measures (ISM), particularly for organizations with limited cybersecurity budgets, which must carefully trade off how to allocate their resources best. For this investigation, we chose the finance industry as a research environment due to the critical importance of information security as well as the industry's dynamic nature, characterized by new business models and emerging companies (Goldstein et al., 2019). In particular, we decided to focus on FinTechs, i.e., organizations that use digital technologies to innovate and improve financial services, offering efficient, accessible, and often more user-friendly alternatives to traditional financial institutions (Alt et al., 2018; Dorfleitner et al., 2017; Gimpel et al., 2018; Goldstein et al., 2019). However, the competitive nature of the business landscape (Chuen & Teo, 2015; Gimpel et al., 2018; Werth et al., 2023) necessitates that FinTechs rapidly develop their offerings (Murinde et al., 2022). As a result, the efficient use of technologies like cloud computing emerged as a critical technology for delivering FinTech services (Ali et al., 2020; Fong et al., 2021; Werth et al., 2023). The cloud's capabilities, particularly the provision of flexible on-demand IT resources that mainly involve utility-based operational expenditures rather than capital expenditures, have made it integral to the FinTech industry and central to its disruptive impact (Mell & Grance, 2011; Schneider & Sunyaev, 2015; Tchernykh et al., 2019). Because of limited resources and an opportunistic development approach, FinTechs are, unfortunately, prone to information security breaches and regulatory violations (Gai et al., 2017; Goldstein et al., 2019). Consequently, their strategy in utilizing cloud computing poses a significant risk to becoming reliable, trustworthy, and profitable (Mahalle et al., 2018). Building customer trust by ensuring information security are vital for the success of FinTechs, too (Mehrban et al., 2020). According to Werth et al. (2023), information security is one of the most critical concerns regarding cloud computing within FinTechs, impacting their overall success. Although computing resources are outsourced to the cloud, security responsibilities are not fully transferred but rather shared between providers and users (Armbrust et al., 2010; Mahalle et al., 2018). These concerns, along with the division of responsibility, make information security management even more crucial for FinTechs. However, to date, FinTechs often tend to deprioritize information security and adherence to certain regulations, or their prioritization methods lack sophistication (Gai et al., 2017; Haupert et al., 2017). The associated risks can lead to regulatory difficulties, like financial penalties, or significantly impact revenue due to eroding customer trust (Mahalle et al., 2018). Therefore, existing literature

suggests various clusters of ISM for FinTechs, focusing on data protection, regulatory compliance, cryptography, responsibility-based access control, and secure application logic (Gai et al., 2017; Kaur et al., 2021; Singh et al., 2021). Moreover, it underscores the impact of the cloud service model on information security (Mahalle et al., 2018). However, as previous research concentrated on establishing suitable ISM for FinTechs, studies on their prioritization are limited. Thus, FinTechs lack a comprehensive strategy to determine which ISM to implement first to ensure adequate information security and regulatory compliance levels in the face of limited resources. Therefore, we pose the following research question:

How should FinTechs prioritize information security measures for cloud services? (Essay 6)

Overall, this dissertation comprises six essays addressing the specific RGs outlined in Section 3. While Essays 1 and 2 address RG1, Essays 3 and 4 address RG2, and Essays 5 and 6 RG3. Table 1 summarizes the essays, including their respective publication outlets, according to the VHB publication media ranking (VHB PMR), and current publication status. Additional publications not included in this dissertation are listed in Appendix B.

Table 1: Essays on the Three Research Goals of this Dissertation

Title	Publication outlet	VHB PMR ranking	Publication status
RG1: Identify the environmental changes that necessitate an adaptation of cybersecurity for modern organizations			
Essay 1: Designing the Future of Bond Markets: Reducing Transaction Costs Through Tokenization	Electronic Markets	B	Published as Cisar et al. (2025)
Essay 2: From Flat Screens to Immersive Virtual Reality: How Virtual Reality Influences Subjective and Objective Performance in Digital Sports	Proceedings of the 34th European Conference on Information Systems	A	Published as Lauer et al. (2026)
RG2: Determine the requirements that arise from these changes to effectively and efficiently adapt cybersecurity in modern organizations			
Essay 3: Proactivity and Resilience: An Examination of Strategic Foundations for Cloud Security from an Organization Theory Perspective	Wirtschaftsinformatik Proceedings	B	Ready for Submission as Strobel et al. (2026)

Title	Publication outlet	VHB PMR ranking	Publication status
Building upon: From Observing to Understanding: Empirical Insights on the Organizational Foundations of Security Chaos Engineering	Proceedings of the 44th International Conference on Information Systems	(A)[1]	Published as Strobel et al. (2023)
Essay 4: The David-Goliath Gap throughout the Evolution of Critical Energy Infrastructure Cybersecurity: An Analysis from a Complex Adaptive Systems Theory Perspective	Proceedings of the 34th European Conference on Information Systems	A	Published as Weiss et al. (2026)
RG_3: Develop digital solutions that support the adaptation of cybersecurity in modern organizations to meet the identified requirements			
Essay 5: From Planned Security to Reality: Towards an Open-Source Artifact for Automated Cloud Security Auditing on the OS-Level	IEEE Access	B	Ready for Submission as Port et al. (2025)
Essay 6: Towards Secure Cloud-Computing in FinTechs – An Artefact for Prioritizing Information Security Measures	Proceedings of the 57th Hawaii International Conference on Information Systems	B	Published as Leuthe et al. (2024)

[1] Published as “Short Paper”.

4 Research Design

This section offers a summary of the research designs employed throughout the six essays to achieve the respective research objectives. Subsequently, I outline the research methodologies, data collection methods, and analysis techniques used to answer the research questions. Table 2 provides a concise overview of the chosen research designs.

Table 2: Research Designs of the Essays included in this Dissertation

Title	Research design
RG1: Identify the environmental changes that necessitate an adaptation of cybersecurity for modern organizations	
Essay 1: Designing the Future of Bond Markets: Reducing Transaction Costs Through Tokenization	**Design science research** • Design of a blockchain token-based bond market instantiation • Examination and evaluation regarding its potential to reduce transaction costs (Williamson, 1981) based on n=14 semi-structured expert interviews
Essay 2: From Flat Screens to Immersive Virtual Reality: How Virtual Reality Influences Subjective and Objective Performance in Digital Sports	**Experiment research** • Experiment comparing 2D monitor-based and virtual 3D environments with n=80 participants • Between subject-based approach in a laboratory environment • Data analysis based on Mann-Whitney-U-Test and Partial Least Squares Structural Equation Modeling complemented with Spearman correlation analysis
RG2: Determine the requirements that arise from these changes to effectively and efficiently adapt cybersecurity in modern organizations	
Essay 3: Proactivity and Resilience: An Examination of Strategic Foundations for Cloud Security from an Organization Theory Perspective	**Interview study** • Empirical qualitative research by conducting an interview study with n=18 interview partners • Open, axial, and selective coding following the approach by Gioia et al. (2013) • Triangulation of findings with related literature and adoption of an organizational theory framework for structuring results
Building upon: From Observing to Understanding: Empirical Insights on the Organizational Foundations of Security Chaos Engineering	**Interview study** • Inductive research study by conducting qualitative expert interviews with n=17 interviews • Derivation of first-order concepts, second-order themes, and aggregate dimensions according to Gioia et al. (2013)
Essay 4: The David-Goliath Gap throughout the Evolution of Critical Energy Infrastructure Cybersecurity: An Analysis from a Complex Adaptive Systems Theory Perspective	**Interview study** • Inductive study based on n=19 qualitative semi-structured expert interviews • Multi-phase data collection and analysis process according to Gioia et al. (2013) throughout coding steps and workshops

Title	Research design
RG_3: Develop digital solutions that support the adaptation of cybersecurity in modern organizations to meet the identified requirements	
Essay 5: From Planned Security to Reality: Towards an Open-Source Artifact for Automated Cloud Security Auditing on the OS-Level	**Design science research** • Design of an instantiation for automated OS-level cloud security audits following the approach of Peffers et al. (2007) and evaluation based on n=14 semi-structured interviews • Derivation of design knowledge through generalizable design principles according to Gregor and Hevner (2013)
Essay 6: Towards Secure Cloud-Computing in FinTechs – An Artefact for Prioritizing Information Security Measures	**Design science research** • Development of an information security measure prioritization prototype for FinTechs, based on the shared responsibility model by adopting the DSR paradigm (Hevner et al., 2004) • Evaluation based on Sonnenberg and vom Brocke (2012)

In Essay 1, we examined how a blockchain-based bond system can reduce transaction costs in the bond market by following the design science research (DSR) paradigm. Since transaction costs in traditional bond markets were found to be significant and blockchain technologies could potentially reduce these costs, we adopted the approach by Peffers et al. (2007) to analyze this complex, real-world problem, develop and evaluate an innovative IS artifact to resolve this issue and extent the existing body of design knowledge with through the generation of generalizable design principles (DP). Doing so, we iteratively executed six steps: problem identification, defining solution objectives, designing and developing the artifact, demonstration, evaluation, and communication. Overall, we implemented three design cycles. Starting with step one (Problem Identification), we pinpointed the core issues by reviewing pertinent literature and conducting expert interviews, which allowed us to formally articulate these issues as meta-requirements (MR). These MRs acted as the foundation for crafting design objectives (DOs) in step two (Objective Definition). Moving to step three (Design and Development), we developed, functionally tested, and continuously improved the artifact. This iterative enhancement was guided by feedback from industry experts, particularly during design cycles two and three (Peffers et al., 2007; Sonnenberg & vom Brocke, 2012). To maintain a comprehensive view of the prototype, we also incorporated insights from researchers specializing in blockchain technology across various institutions and industries. Given that the artifact represents an instantiation (Hevner et al., 2004), step four (Demonstration) was divided into showcasing the functional architecture to clarify procedural, legal, and regulatory requirements, followed by executing the technical implementation. Step five (Evaluation) concentrated on successfully implementing the DOs. Finally, step six (Communication) entailed conveying the

theoretical and practical insights gained. We formulated DPs by integrating descriptive knowledge, principally using transaction cost (TAC) theory as a foundational theory (Gregor & Hevner, 2013; Heger, 2020; Walls et al., 1992; Williamson, 1981). The communication phase aligned with the suggestions of Hevner et al. (2004) and Peffers et al. (2007), culminating in the dissemination of our findings through academic publication, which included the source code and documentation of the artifact. Moreover, our practical and theoretical insights were incorporated into a publicly funded research project, collaborating with an interdisciplinary team exploring the tokenization of financial products and markets. Finally, our evaluation found that the defined DOs were successfully implemented and that our blockchain token-based bond market design could reduce the overall TAC incurred.

In Essay 2, we examined the extent to which virtual 3D environments offer added value in digital sports and which effects on athlete performance can be measured. An experimental design was utilized to compare user experiences between a 2D and a 3D setting. The experiment was structured using a between-subjects approach in a laboratory setting, adhering to established norms from previous literature and studies (Elsey et al., 2019; Huygelier et al., 2019; Kim & Ko, 2019; Kinzinger et al., 2022; Meißner et al., 2020; Menck et al., 2023; Suh & Lee, 2005; Urbach & Ahlemann, 2010). Validated scales were employed for all constructs in this study. Most items were assessed using a seven-point Likert scale. Immersion was evaluated using four items (α=0.90) based on the scale from Daassi and Debbabi (2021). Presence measurement was adapted from Nah et al. (2011) using five items (α=0.92), as previously utilized in VR studies like Menck et al. (2023). Subjective Performance was measured with five items (α=0.89) from Rowen et al. (2019). Additionally, demographic data (gender, age, and highest degree) and context data (experience with the technologies used in the experiment) were collected, while Objective Performance was assessed based on the measured lap times. More specifically, participants performed standardized tasks using either traditional 2D monitors and controllers or 3D glasses and gesture-based controls. The sample consisted of 80 participants, equally divided between the two conditions (3D environment vs. 2D interface). Beyond descriptive analysis, a Spearman correlation analysis examined the relationship between task performance and participant responses to control questions. The data analysis was conducted using a Mann-Whitney-U-Test, because it does not rely on normally distributed data which was the case in our study, and Partial Least Squares Structural Equation Modeling for its ability to analyze complex

models with multiple latent constructs, tolerate non-normal data, and accommodate less stringent sample size requirements, aligning with established methodological guidelines and precedents in related empirical research (Benitez et al., 2020; Chin & Marcoulides, 1998; Gefen et al., 2000; Hair et al., 2022; Kinzinger et al., 2022; Menck et al., 2023; Nah et al., 2011; Rigdon et al., 2017; Urbach & Ahlemann, 2010). The model exhibited an acceptable fit, as evidenced by a relative Chi-square of 1.793, which is well within the widely accepted threshold of 2.0 (Bentler & Bonett, 1980; Kelloway, 1999; Tabachnick & Fidell, 2014). Ultimately, both the descriptive results and the visualization-format effects measured in isolation showed significant improvements in subjective and objective performance for the 3D virtual environment. However, these effects were no longer statistically significant in the structural equation model once the mediators presence and immersion were included. This suggests that the observed advantages arise primarily from VR-induced experiential factors rather than from the technology itself.

In Essay 3, we synthesized and complemented existing literature with an in-depth interview study (Schultze & Avital, 2011). For data analysis, we employed the method by Gioia et al. (2013), utilizing both existing literature and semi-structured interviews for data collection. More precisely, our data collection was structured in four iterative stages. Initially, we conducted a literature review to grasp the relevant aspects and challenges related to modern cloud security. Subsequently, drawing from the literature review's findings, we crafted an initial interview guide and started our interview study. Overall, we conducted interviews with 18 partners from German companies with differing professional backgrounds and a focus on cloud computing across multiple industries. Each interview lasted between 45 and 60 minutes, was conducted and recorded via Microsoft Teams, with two researchers present to ensure completeness and avoid biases. The focus varied between most interviews to optimally exploit the interviewees' individual expertise and experience. As the data collection progressed, both the guide and initially identified research questions were updated to align with emerging insights. The data analysis followed a four-step process. Initially, researchers created first-order concepts by coding interviews with informant-based terms, aiming to capture all relevant information, leading to numerous initial codes (Gioia et al., 2013). Next, the researchers examined the first-order concepts for similarities and differences, categorizing them into second-order themes, thereby streamlining the number of unstructured codes. During these steps, we used the open coding feature in

MAXQDA to transcribe and code the interview recordings. Coding workshops conducted with three authors ensured a shared understanding of the data and coding structure, resulting in 1,350 text excerpts, 288 first-order concepts, and 15 second-order themes. In the third step, we distilled the second-order themes into five aggregate dimensions, which formed the basis for a descriptive framework that illustrated the relationships among the emerging concepts, clarifying the link between data and developed theory (Gioia et al., 2013). Our analysis revealed that our interview data had parallels with organizational theory, particularly in the context of change, pertinent to companies. Consequently, we structured our findings based on the model by Scott (1981), which is a recognized framework in organization research and has been applied in various academic IS literature, e.g., Lavassani and Movahedi (2017) and Jonathan (2020). As a result, we provide a framework structuring fundamental changes for cloud security across five dimensions and contribute recommended actions in an exploratory manner regarding organizational considerations in both proactivity and resilience.

In Essay 4, we examined the evolution of cybersecurity within critical energy infrastructures, employing an empirical qualitative approach by conducting an interview study. A total of 19 experts were selected based on their technical expertise and professional experience in cyber- and network security, grid operations, and power generation, all of whom are active within the German critical energy infrastructure sector. Leveraging the diverse expertise of these experts, we conducted semi-structured interviews that allowed for flexibility in focusing on specific topics and adapting in-depth questions based on the course of the conversation. The interview guide was continuously refined throughout the research process to incorporate newly gained insights, such as additional queries regarding network protocols and their attributes. Theoretical saturation was considered to be achieved when the introduction of new codes from interviews had significantly declined (Saunders et al., 2018). The analysis of the data comprised a five-step process following the methodology of Gioia et al. (2013). Initially, interviews were transcribed and coded into 220 first-order concepts, capturing individual experiences with specific technologies and procedures, including their strengths and weaknesses, utilizing the coding function of MAXQDA. Subsequently, these first-order concepts were organized into 21 second-order themes, categorized based on commonalities among frequently used technology groups and procedures. To ensure methodological rigor and intercoder reliability, multiple authors participated in the coding process, engaging in regular collaborative sessions to discuss results and

address any ambiguities or inconsistencies. In the third phase, these second-order themes were further refined into seven aggregate dimensions through a series of coding workshops. In the final step, these insights were synthesized into a comprehensive graphical representation of the results. As a result, we identified central emerging patterns along the evolution of cybersecurity in the critical energy infrastructure sector, thus contributing a practical review to the current technology and strategy-dominated discourse, which allows us to create new solutions where necessary or adapt existing measures to new requirements.

In Essay 5, we developed an artifact aimed at enabling automated OS-level cloud security audits for IaaS systems, specifically addressing the needs of SMEs with constrained resources for such audits. To achieve this, we adopted the DSR paradigm and followed the approach by Peffers et al. (2007). Initially, we identified the challenges auditors face in executing cloud security audits through a comprehensive literature review and expert interviews. In addition, our structured literature review, grounded in the methodology of Webster and Watson (2002), highlighted a gap in design knowledge for creating such automated audit artifacts. Our interview partners were carefully selected based on their expertise in cloud security audits, cloud, and OS management, along with their professional experience. The insights from expert interviews and literature review informed the development of four meta-requirements (MRs), which, subsequently, were further developed into six design objectives (DOs). We then iteratively designed, implemented, demonstrated, and evaluated the artifact over three distinct design cycles. During the first cycle, the concept and architecture were established; the second cycle centered on the development of a minimum viable product (MVP); and the third cycle involved enhancing the artifact based on feedback and addressing identified limitations. Given that the artifact is an instantiation (Hevner et al., 2004), the demonstration included a technical presentation to security experts and its application within a public research project for practical testing. A total of 14 semi-structured interviews were conducted with 12 experts from various fields, aimed at identifying core challenges (cycle 1), evaluating the MVP's quality and limitations (cycle 2), and assessing the final artifact (cycle 3). Each cycle was concluded upon reaching theoretical saturation, as indicated by a significantly decreasing number of new codes (Saunders et al., 2018). Interviews were conducted by two researchers, recorded, and transcribed, with data coded in MAXQDA by marking key statements for extraction. The qualitative data analysis employed coding strategies by Corbin and Strauss (1990), chosen for

their structured yet adaptable approach conducive to iterative, in-depth analysis. The study's final step involved disseminating our theoretical and practical findings (Hevner et al., 2004; Peffers et al., 2007). As a result, our evaluation concluded that the developed DOs were successfully implemented and, in addition, we extended the existing body of design knowledge with five generalizable design principles following (Gregor et al., 2020; Hevner et al., 2004).

In Essay 6, we addressed the challenge of a missing practical framework to aid FinTechs with prioritizing information security measures (ISMs) to ensure adequate information security. Therefore, we developed an artifact to facilitate this prioritization process by adhering to the DSR paradigm (Gregor & Hevner, 2013). Our research was structured using the DSR methodology proposed by Peffers et al. (2007) to guide the overall process and the one by Sonnenberg and vom Brocke (2012) for our evaluation phase. Initially, in the Problem Identification & Motivation phase (Step 1), we identified the critical difficulties FinTechs face in prioritizing ISMs. In Step 2, Definition of Design Objectives (DOs), the critical factors influencing ISM prioritization were identified. Drawing on a comprehensive literature review, our experience in the FinTech domain, and semi-structured interviews, we formulated eight DOs emphasizing information security for cloud services utilized and offered by FinTechs. Step 3 (Design Development) included the creation of the artifact, guided by the formulated DOs and domain expertise, employing the shared responsibility model to incorporate foundational cloud service models (Lane et al., 2017; Mell & Grance, 2011). In Step 4 (Demonstration), we instantiated the artifact with exemplary measures by conducting a structured literature review on Ebsco Host, ProQuest, and IEEE Xplore, yielding 116 papers. We scrutinized abstracts for contributions to information security in cloud environments, excluding those limited to a single ISM or threat. This process resulted in 16 relevant papers, leading to a final selection of 12 after a thorough full-text review and a forward and backward search. From these, we extracted 82 pertinent topics organized into 18 clusters, categorized into three information protection goals, six threats, and nine measures (Sumner, 2009). The comprehensive catalog of ISMs addressing both IS threats and regulatory requirements consisted of 17 measures, used to instantiate our artifact. Step 5 (Evaluation) involved testing the artifact's real-world applicability through prototypical implementation, using additional semi-structured interviews with the same information providers involved in the problem definition and DO evaluation phases. These interviews spanned 90 to 120 minutes to guarantee a

complete and in-depth evaluation. Upon achieving all DOs, we presented our findings to industry experts from a leading international management consultancy as part of the final Step 6 (Communication). This consultancy has adopted the artifact's methodology to elucidate its ISM identification processes to clients in the FinTech industry. As a result, we closed the gap in research regarding the design of ISM prioritization artifact for FinTechs by developing such a tool and transferred our knowledge gained into practice by disseminating our work at the end of our research process.

5 Summary of Results

As previously introduced, this dissertation is structured around three research goals corresponding to Darwin's evolution theory. Corresponding to these three research goals, the dissertation comprises three parts, each containing two essays. In this section, these essays are presented by describing the respective motivation, methodology, and results.

5.1 Essay 1: Designing the Future of Bond Markets: Reducing Transaction Costs Through Tokenization

In Essay 1, we designed, implemented, and evaluated a prototype for a blockchain token-based bond market architecture. In this regard, our research confirms that the prototype's issuance mechanism considerably reduces transaction costs. Nonetheless, it is crucial to recognize these costs as intrinsic barriers that, given the expenses associated with the current Ethereum-based prototype design, remain resistant to complete elimination. These costs, while substantial, should be considered within the larger context of the prototype's overall effectiveness and contribution to the information systems field, acknowledging that technological advances and regulatory changes may eventually mitigate these inherent constraints. Additionally, we discover that although our prototype democratizes financial access, its implementation still relies on intermediaries and their essential services, particularly those provided by security token offering platforms. This reliance arises not only because crucial technical expertise and time resources might be lacking outside the core business area but also due to the need to adhere to regulatory requirements for issuing tokenized bonds. Despite being a significant bottleneck, this dependency allows for potential efficiency gains by consolidating multiple issuances into a single contract, which reduces the fixed unit costs per issuance. As a result, security token offering platforms managing multiple issuances provide the opportunity to mitigate the aforementioned limitations.

5.2 Essay 2: From Flat Screens to Immersive Virtual Reality: How Virtual Reality Influences Subjective and Objective Performance in Digital Sports

In Essay 2, we explored the potential benefits of virtual 3D environments in digital sports by conducting an experiment with n=80 participants that assessed the impact

on Subjective and Objective Performance of athletes compared to traditional settings with 2D monitors. To achieve this goal, our research questions were structured sequentially. First, we aimed to determine whether the performance (subjective and objective) in digital sports generally differs depending on whether they are performed in virtual 3D sports environments or 2D screen-based settings. Our first analysis reveals that using 3D virtual environments instead of a 2D screen-based setting has a statistically significant positive direct effect on both subjective and objective performance. In the second step, we explored to what extent effects repeatedly documented in the literature for 3D virtual environments could explain the observed improvements in subjective and objective performance. To this end, our research model was expanded to include presence and immersion as mediating constructs. The results showed that presence has a statistically significant positive effect on both subjective and objective performance, whereas immersion only significantly improves subjective performance. Interestingly, the direct path coefficients between visualization format (3D vs. 2D) reversed to negative values, but these were not statistically significant. Our research contributes to the body of literature on VR by examining if previously found positive effects of isolated cognitive tasks or physical training exercises can be measured in competitive digital sport settings, too. Our results align with studies in other fields such as healthcare, manufacturing, and product design and demonstrate that the adoption of 3D virtual environments could positively impact athletes' performance. More importantly, our study shows that if the trend moves toward greater adoption of 3D virtual environments instead of 2D screen-based settings, the effects partially mediated by enhanced presence and immersion will play a crucial role in maximizing both subjective and objective athlete performance as would be required by the Olympic motto “Faster, Higher, Stronger – Together”.

5.3 Essay 3: Proactivity and Resilience: An Examination of Strategic Foundations for Cloud Security from an Organization Theory Perspective

In Essay 3, our research was driven by the evolving technology landscape as a result of progressing digitalization and the growing use of cloud computing, which has created both unprecedented opportunities and notable challenges for organizations. Consequently, traditional security controls were found to be inadequate for addressing the complexities of today’s cloud environments. Unfortunately, necessary strategic

adjustments have been previously explored only in isolation or not from the required socio-technical perspective. This study addresses this gap by reviewing existing literature and complementing it with the insights from 18 practitioners and industry experts. Our development of the individual dimensions and perspectives into an organizational-theoretical framework illustrates which dimensions are essential for strategic adjustments and how these have evolved throughout digitalization and the increased adoption of cloud computing. By answering our research question, we provide a synthesis of existing cloud security research, establishing a common foundation for future academic work on cloud security throughout digitalization and digital transformation. Practically, we derived nine recommended actions to enhance cloud security practices, to promote collaboration among stakeholders, and to integrate cloud security within organizational structures.

5.4 Essay 4: The David-Goliath Gap throughout the Evolution of Critical Energy Infrastructure Cybersecurity: An Analysis from a Complex Adaptive Systems Theory Perspective

In Essay 4, we explored how the sustainability transformation and digitalization impact the cybersecurity of critical energy infrastructures. Utilizing complex adaptive systems theory as a theoretical framework, we conducted an interview study with 19 participants to uncover associated emerging patterns. This analysis enabled us to identify seven emerging patterns related to ensuring cybersecurity in critical energy infrastructures, highlighting the differences between SMEs and larger enterprises. Our findings reveal that smaller energy producers and network operators are particularly challenged by the new demands from the convergence of IT and OT, as well as by the various digital technologies (including AI) employed and the multitude of stakeholders involved. Ultimately, we found and described specific challenges and opportunities for enhancement in the areas of network connectivity, data transfer, and control signal transmission in these distributed systems, which employ a notably diverse array of hardware, communication channels, and network protocols.

5.5 Essay 5: From Planned Security to Reality: Towards an Open-Source Artifact for Automated Cloud Security Auditing on the OS-Level

In Essay 5, we developed an artifact for automated cloud security audits at the OS-level for IaaS systems, targeting the needs of SMEs with limited resources for performing

such audits. The modular design of our solution was found to significantly reduce the setup and execution efforts for conducting comprehensive cloud security audits on a regular basis, thereby addressing the typical challenges faced by SMEs. By employing the audit host- and target system configuration and integrating Steampipe and osquery, which are established solutions and frameworks in the field, a large number of systems can be audited while keeping setup, usage, and maintenance efforts minimal, thereby enabling regular cost-efficient audits across all relevant systems. Utilizing established benchmarks, such as those from the CIS, removes the need for users to create their own metrics and assures that guidelines are both complete and up-to-date. Consequently, SMEs are no longer required to “assume” their systems' security but can now audit them regularly. As a theoretical contribution, this research offers design knowledge through five generalizable design principles. This is complemented by our practical contributions, consisting of the artifact's ability to address the hurdles SMEs encounter in executing regular, comprehensive cloud security audits. Also, the artifact's open-source, lightweight nature allows for smooth integrations into existing processes and structures. A promising area for future research includes investigating the integration of cloud security auditing tools with configuration management solutions to automatically trigger corrective actions based on audit results.

5.6 Essay 6: Towards Secure Cloud-Computing in FinTechs – An Artefact for Prioritizing Information Security Measures

In Essay 6, we tackle the critical issue of information security in FinTechs. Due to the current lack of a practical method for aiding FinTechs in prioritizing information security measures to attain adequate information security levels, we developed a tool to facilitate this process. Our tool calculates the priority of information security measures by considering relevant factors such as regulations, threats, protection goals, and the FinTech’s business model. To ensure the tool's practicality and applicability in real-world scenarios, we consulted industry experts, who informed the formulation of design objectives and the artefact's evaluation. We encourage information security researchers to challenge and expand the artefact further to additional application areas and integrate more relevant factors for prioritizing information security measures.

6 Discussion and Conclusion

In this section, I conclude the introduction of my dissertation by providing a brief summary across all essays, outlining the overarching contributions to theory and practice, and presenting important limitations as well as relevant approaches for future research.

6.1 Summary

The overarching goal of this dissertation is to examine the evolution of cybersecurity in the context of digitalization and digital transformation of organizations, as well as to develop solutions and approaches for successfully mastering the resulting "survival of the fittest".

To achieve this, the dissertation has been structured in a cumulative manner and comprises six essays, evenly divided into two essays per RG. To achieve RG1, Essay 1 provides insights into IT architectural changes using the example of modern financial markets, while Essay 2 demonstrates how virtual 3D environments could impact the future of (competitive) digital sports. For the completion of RG2, Essay 3 explores the requirements arising for organizations in the context of increasing cloud technology usage from an organizational theory perspective. These findings are complemented by Essay 4, which focuses on the energy sector and shows how cybersecurity requirements have evolved along the entire value chain from originally highly centralized to increasingly decentralized structures and which patterns SMEs as well as larger enterprises have adopted to tackle them. To accomplish RG3, Essay 5 builds on the insights gained from the previous RGs by presenting an artifact for conducting automated cloud security audits as a blueprint for transforming traditionally reactive cybersecurity tools into proactive and resilience-enhancing solutions. Essay 6 concludes the dissertation by contributing a second technical artifact for prioritizing cybersecurity controls, focusing on organizations with particularly limited cybersecurity resources, balancing criticality and resource requirements using the example of organizations in the financial sector.

6.2 Contributions to Theory and Implications for Practice

In addition to the core findings illustrated above, my research provides several theoretical and practical contributions. Starting with the theoretical contributions,

specifically those achieved in reaching RG1, Essay 1 extends the existing literature on blockchain-based bonds by providing novel design knowledge in the form of generalizable design principles following Gregor and Hevner (2013) that complement existing work on tokenization, including equity tokens and green bond markets. Our research introduces new approaches that utilize claim functions and reinforce the significant role of security token offering platforms, contributing to the discussion on blockchain's impact on market intermediation (e.g., Bauer et al. (2019)). Additionally, our work applies TAC theory as a theoretical lens on blockchain technology, stressing its benefits in reducing transaction costs and automating corporate bond processing. This highlights the necessity of aligning blockchain applications with compelling business cases, augmented by our prototype's demonstration of blockchain's feasibility for corporate bonds and contribution to TAC-driven research. In addition, Essay 2 contributes to the academic discourse regarding the use of VR in the digital sports by examining the benefits of virtual 3D environments compared to traditional 2D monitor settings, which constitutes a topic that has been insufficiently addressed in the literature especially for competitive digital sports settings. Our investigation fills existing gaps in research by demonstrating how VR technology can enhance the Subjective and Objective Performance of athletes, valuable insights into exploiting the potential of digitalization. While existing literature confirmed positive effects of VR technology for physical training exercises, isolated cognitive tasks or customer experiences, we assessed its impact in competitive digital sports settings, as well as the mediating effects of Presence and Immersion.

To achieve RG2, Essay 3 contributes to cloud security literature by synthesizing insights from literature and semi-structured expert interviews that were processed into an evolutionary framework based on organization theory. Through adopting the model by Scott (1981), we highlight essential dimensions required for proactive cybersecurity as well as resilience and encourage the comprehensive exploration of dynamic cybersecurity landscapes. More precisely, understanding the identified dimensions enables researchers to construct more sophisticated models capable of analyzing and forecasting organizational behavior in reaction to emerging threats. Furthermore, Essay 4 enriches IS literature by employing the complex adaptive systems (CAS) theory to understand the evolution of critical energy infrastructure cybersecurity. It addresses practical and operational strengths and weaknesses, contributing to a differentiated understanding of cybersecurity challenges. Additionally, our work demonstrates the CAS

theory's applicability in IS literature, focusing on the energy sector and bridging the gap between technological and strategic considerations in cybersecurity discourse.

In the course of fulfilling RG3, Essay 5 extends existing (design) knowledge by introducing five design principles for cloud security auditing, enabling OS-level audits to integrate seamlessly into standard processes, reducing barriers and costs. Also, our work reviews and structures existing literature, and points out the strengths of complementary auditing and configuration management tools to maintain planned system states. Ultimately, Essay 6 adds to IS research by presenting a structured method to prioritize ISMs for FinTechs quantitatively. Unlike existing broad concepts, the approach integrates current knowledge on threats and regulations.

In addition to the theoretical contributions presented above, my research provides numerous practical contributions, too. By achieving RG1, Essay 1 offers an open-source prototype, complemented with detailed documentation for practitioners to modify for their needs. Practically, the prototype offers a basic architecture for a blockchain-based bond market that minimizes TAC incurred, i.e., through the elimination of intermediaries. Our work encourages discussions on blockchain viability, helps managers evaluate business cases through the TAC perspective, and outlines multi-token standard opportunities, informing future endeavors, including regulatory adaptations based on the German model. Furthermore, Essay 2 illustrates how VR technologies can improve athlete performance in virtual 3D digital sports environments, which helps the responsible stakeholders of digital sports competitions to create optimal conditions for the best possible athlete performance.

In order to fulfill RG2, Essay 3 provides actionable guidance for organizations aiming to improve cloud security, combining proactive security strategies with resilience. Our framework bridges technical and strategic elements, supporting practitioners through transformative processes. The holistic integration of dimensions allows organizations, from technical staff to executives, to use the framework for strategic decision-making and collaboration, promoting a unified approach to cybersecurity enhancement. In Essay 4, we highlight the necessity for action regarding cybersecurity among smaller energy grid operators and energy producers, emphasizing the standardization of control and data transmissions and the internal development of digitalization, as well as cybersecurity competencies. This proactive approach towards adopting and securing digital technologies ensures stakeholder readiness in a future, even more digital

technology-based business environment.

For completing RG3, Essay 5 introduces an artifact that simplifies integrating OS-level cloud security audits into regular processes, making them accessible for broader application. Specifically, the developed tool lowers the adoption barriers for SMEs, making respective security measures feasible and efficient, aiding them in addressing their security needs comprehensively. Finally, Essay 6 presents a structured approach for information security measure prioritization for FinTechs utilizing cloud services based on various individual inputs. Consequently, the artifact developed assists with efficient resource allocation for cloud security efforts, allowing FinTechs to balance risk management with resource limitations. Additionally, our approach aligns with established standards like NIST, aiding FinTechs in navigating complex security landscapes.

6.3 Limitations and Future Research

Of course, the essays included in this dissertation are subject to several limitations that present promising avenues for future research. For instance, by completing RG1, Essay 1 is limited by the fact that the developed artifact was only tested at the proof-of-concept level using the virtual test network within the Remix development IDE, which only simulates the real Ethereum main network. As a result, our findings related to transaction efficiency and actual costs may differ from real-world applications. Future work should close this gap by deploying our or similar artifacts in the actual Ethereum main network to investigate the effects and differences compared to test networks. Also, our evaluation does not explicitly address whether private or public networks should be used, as transaction costs and scalability remain major concerns, posing another starting point for further investigations. Although technological advancements such as sharding may help to eliminate these limitations in the future, they currently present challenges for practical deployment.

Additionally, the limitations of Essay 2 include the sample composition of experiment participants, which primarily consists of younger individuals from a university-related environment, potentially biasing the findings, given the anticipated wider adoption of virtual 3D digital sports environments. Moreover, while the controlled laboratory experiment setting improves reliability, further research should also explore non-laboratory environments to assess constructs like concentration and reaction speed more realistically. Finally, the experimental task involved digital racing sport to ensure

validity and reproducibility. Although suitable for assessing the constructs of interest, it only partially represents the broader range of digital sport disciplines, highlighting the need for future studies.

Regarding the achievement of RG2, we acknowledge that Essay 3 significantly builds upon qualitative data collected throughout German-based interviews, which may lead to limited transferability to other industry or regional contexts. Consequently, the selected interview partners may introduce biases not reflective of broader organizational perspectives. Hence, future research should challenge and complement our work by obtaining more diverse and international data. Additional studies could also benefit by integrating quantitative methods to test our findings and further develop the proposed framework. Similarly, Essay 4 is limited by its national scope, focusing primarily on German experts to derive emerging patterns concerning critical energy infrastructure cybersecurity. To extend the validity of our findings, future studies should examine these patterns in broader, e.g., international contexts, especially considering the interconnectedness of global energy systems. Moreover, due to our research's focus on critical energy infrastructures from generation to grid operation, emerging downstream technologies, such as smart metering and the emergence of prosumage, were rendered out of scope. However, as these developments have introduced significant changes to the energy sector, future work should explore these developments, too. Finally, our work highlighted the insufficient digitalization and cybersecurity capabilities of small and medium-sized energy producers and grid operators. Therefore, future research should explore how these stakeholders can acquire the necessary expertise, as well as how corresponding standardized (technical) solutions can be developed, implemented, and scaled.

In the course of addressing RG3, the limitations of Essay 5 include the conduct of 14 semi-structured interviews conducted with 12 experts. Although these interviews provided a rich and diverse exchange of ideas, the limited number of participants may not encompass all possible perspectives on the subject and may still be prone to bias. Additionally, the artifact's practical evaluation occurred within a single setting, potentially posing unforeseen implementation challenges elsewhere. Because of constituting a Proof-of-Concept, the artifact covers representative control examples but not all relevant controls of established benchmarks, necessitating further expansion for robust practical testing and productive application. Consequently, future research should

address these limitations to further explore the potential of cloud security audit artifacts. At this point, another avenue worth exploring could be how traditional established methods can be adapted to ensure proactive cybersecurity and resilience (e.g., complementing the work of Hu et al. (2020) for the case of penetration testing). Additionally, research could focus on how these methods can be seamlessly integrated into standard processes and organizational structures. Concerning Essay 6, we acknowledge three main limitations. Firstly, our artifact streamlines a complex set of influencing factors and their interactions, which aids in decision-making. Nevertheless, it is important to note that this simplification cannot provide a universal solution. For instance, the final score calculated does not take into account a FinTech's strategic goals, size, the type of data processed, or the dependencies between multiple ISMs. Hence, practitioners should apply the artifact thoughtfully and enhance it with detailed expert insights when necessary. However, this limitation also opens up opportunities for research to refine our artifact based on current gaps in its framework. Secondly, the artifact captures a specific snapshot that requires continuous updating (e.g., its application is constrained by temporal and contextual factors, including regional and industry-specific regulations). Consequently, it currently encompasses only 17 exemplary ISMs from an extensive literature review, which is why its correctness and completeness depend on the corresponding state of IS literature. Furthermore, the artifact primarily incorporates German regulations, and implementing it can be resource-intensive, especially for smaller FinTechs with limited means. Thus, future research should explore methods to automate the calculation of final scores and improve the generalizability of the results. Thirdly, we assessed the problem definition, design objectives, and our final score using semi-structured expert interviews, whereas the same four experts were involved in all three phases. Hence, the evaluation remains limited to specific FinTech examples, and we recommend conducting real-world applications for broader validation.

After presenting the specific limitations and avenues for future work of each Essay, I would like to highlight some overarching insights along the process of writing this dissertation. Firstly, across several Essays, we repeatedly identified the necessity for a fundamental shift from predominantly maximum security to additional complementary cybersecurity objectives. In this context, proactive cybersecurity and resilience offer particularly relevant and promising approaches for further research. As shown in Essay 5, this change of overarching cybersecurity objectives does not mean that

traditional approaches are no longer applicable. It rather means that these established solutions must be adapted to meet new requirements. In particular, automation, agile process integration, and artificial intelligence can help traditional cybersecurity controls to meet the demands of modern decentralized, diverse, and fast-paced business environments. Research in this area, i.e., not only demonstrating technical feasibilities or developing theoretical concepts but continuously evolving suitable solutions and testing as well as evaluating them in practice, is still in its early stages in many areas. In this regard, my research adopted the design science research paradigm in multiple Essays but has not covered the full lifecycle of the developed artifacts until productive implementation. Future research should precisely build on this and either further develop the solutions created within this dissertation or evolve its own artifacts to this stage. Furthermore, the recently published design echelon-based approach by Tuunanen et al. (2024) can help to make design science research projects more modular and more accessible for further studies, which can increase the chance for artifacts to achieve the stage of real-world testing and productive implementation. Consequently, I encourage scholars to adopt this approach and to pursue joint work.

Ultimately, I would like to highlight the benefits of evolution theory as a theoretical lens as it was used in this dissertation, but has scarcely been applied in both cybersecurity and IS research. While cybersecurity research has been very successful in developing well-evaluated solutions for various problems and publishing many comprehensive works like literature reviews or meta-studies, the step into practice often lacks an overarching orientation and alignment to fully realize the potential added value. Not as an implementation of many individual solutions, but as a composite and strategically aligned comprehensive entity, can research transfer its results into real-world applications most effectively. Future research can and should utilize the possibilities offered by evolution theory to recognize fundamental evolutionary developments, derive the resulting requirements for survival, and build upon them to develop respective optimum solutions that present value not only in the short but also in the long term. This dissertation aimed to provide an example of how such an approach can be implemented in future investigations inside and outside of the cybersecurity domain. It will hopefully inspire and guide researchers throughout their future journeys.

References

Abdullayeva, F. (2023). Cyber Resilience and Cyber Security Issues of Intelligent Cloud Computing Systems. *Results Control Optim.*, *12*, 100268. https://doi.org/10.1016/j.rico.2023.100268

Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O. (2024). A Review of Cybersecurity Strategies in Modern Organizations: Examinig the Evolution and Effectiveness of CyberSecurity Measures for Data Protection. *Comp. Sci. IT Res. J.*, *5*(1), 1–25. https://doi.org/10.51594/csitrj.v5i.699

Adamovic, M., Gahan, P., Olsen, J., Gulyas, A., Shallcross, D., & Mendoza, A. (2022). Exploring the adoption of virtual work: the role of virtual work self-efficacy and virtual work climate. *The International Journal of Human Resource Management*, *33*(17), 3492–3525. https://doi.org/10.1080/09585192.2021.1913623

Akkirman, A. D., & Harris, D. L. (2005). Organizational communication satisfaction in the virtual workplace. *Journal of Management Development*, *24*(5), 397–409. https://doi.org/10.1108/02621710510598427

Akpan, I. J., & Brooks, R. J. (2014). Experimental evaluation of user performance on two-dimensional and three-dimensional perspective displays in discrete-event simulation. *Decision Support Systems*, *64*, 14–30. https://doi.org/10.1016/j.dss.2014.04.002

Akpan, I. J., & Shanker, M. (2017). The confirmed realities and myths about the benefits and costs of 3D visualization and virtual reality in discrete event modeling and simulation: A descriptive meta-analysis of evidence from research and practice. *Computers & Industrial Engineering*, *112*, 197–211. https://doi.org/10.1016/j.cie.2017.08.020

Alashhab, Z. R., Anbar, M., Singh, M. M., Leau, Y.-B., Al-Sai, Z. A., & Abu Alhayja'a, S. (2021). Impact of Coronavirus Pandemic Crisis on Technologies and Cloud Computing Applications. *J. Electron. Sci. Technol.*, *19*(1), 100059. https://doi.org/10.1016/j.jnlest.2020.100059

Albanese, M., Jajodia, S., Jhawar, R., & Piuri, V. (2014). Securing Mission-Centric Operations in the Cloud. In S. Jajodia, K. Kant, P. Samarati, A. Singhal, V. Swarup, & C. Wang (Eds.), *Secure Cloud Computing* (pp. 239–259). Springer New York. https://doi.org/10.1007/978-1-4614-9278-8_11

Ali, O., Ally, M., & Dwivedi, Y. (2020). The state of play of blockchain technology in the financial services sector: A systematic literature review. *International Journal of Information Management*, *54*, 102199.

Allen, F., & Santomero, A. M. (2001). What do financial intermediaries do? *Journal of Banking & Finance*, *25*(2), 271–294. https://doi.org/10.1016/S0378-4266(99)00129-6

Alt, R., Beck, R., & Smits, M. T. (2018). FinTech and the transformation of the financial industry. *Electronic Markets*, *28*(3), 235–243. https://doi.org/10.1007/s12525-018-0310-9

Andersen, J. V., & Bogusz, C. I. (2019). Self-Organizing in Blockchain Infrastructures: Generativity Through Shifting Objectives and Forking. *Journal of the Association for Information Systems*, *20*(9), 1242–1273. https://doi.org/10.17705/1jais.00566

Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the Management of Cyber Resilient Systems. *Comput. Ind. Eng.*, *149*, 106829. https://doi.org/10.1016/j.cie.2020.106829

Araújo De Oliveira, P. (2017). Predictive Analysis of Cloud Systems. In *2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C)* (pp. 483–484). IEEE. https://doi.org/10.1109/ICSE-C.2017.39

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., Patterson, D. A., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A View of Cloud Computing. *Communications of the ACM*, *53*(4), 50–58. https://doi.org/10.1145/1721654.1721672

Aubert, B. A., Rivard, S., & Patry, M. (1996). A transaction cost approach to outsourcing behavior: Some empirical evidence. *Information & Management*, *30*(2), 51–64. https://doi.org/10.1016/0378-7206(95)00045-3

Axelsen, H., Rasmussen, U., Jensen, J., Ross, O., & Henglein, F. (2023). Trading Green Bonds Using Distributed Ledger Technology. In *Proceedings of the Thirty-first European Conference on Information Systems*. https://aisel.aisnet.org/ecis2023_rp/340

Ba, S., Whinston, A. B., & Zhang, H. (2000). The Dynamics of the Electronic Market: An Evolutionary Game Approach. *Information Systems Frontiers*, *2*(1), 31–40. https://doi.org/10.1023/A:1010041819361

Bacis, E., Di Capitani Vimercati, S. de, Foresti, S., Paraboschi, S., Rosa, M., & Samarati, P. (2020). Securing Resources in Decentralized Cloud Storage. *IEEE Trans. Inf. Forensics Secur.*, *15*, 286–298. https://doi.org/10.1109/TIFS.2019.2916673

Bacon, C. J. (1992). The Use of Decision Criteria in Selecting Information Systems/Technology Investments. *MIS Quarterly*, *16*(3), 335. https://doi.org/10.2307/249532

Bale, C. S., Varga, L., & Foxon, T. J. (2015). Energy and complexity: New ways forward. *Applied Energy*, *138*, 150–159. https://doi.org/10.1016/j.apenergy.2014.10.057

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered Information Security: Managing a Strategic Balance Between Prevention and Response. *Inf. Manag.*, *51*(1), 138–151. https://doi.org/10.1016/j.im.2013.11.004

Bauer, I., Zavolokina, L., Leisibach, F., & Schwabe, G. (2019). Exploring Blockchain Value Creation: The Case of the Car Ecosystem. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*.

Baumer, T., Müller, M., & Pernul, G. (2023). System for Cross-Domain Identity Management (SCIM): Survey and Enhancement With RBAC. *IEEE Access*, *11*, 86872–86894. https://doi.org/10.1109/ACCESS.2023.3304270

Bayuk, J. L. (2013). Security as a theoretical attribute construct. *Computers & Security*, *37*, 155–175. https://doi.org/10.1016/j.cose.2013.03.006

Beach, P. M., Mailloux, L. O., Langhals, B. T., & Mills, R. F. (2019). Analysis of Systems Security Engineering Design Principles for the Development of Secure and Resilient Systems. *IEEE Access*, *7*, 101741–101757. https://doi.org/10.1109/ACCESS.2019.2930718

Beck, R., Czepluch, J. S., Lollike, N., & Malone, S. (2016). Blockchain – The Gateway to Trust-Free Cryptographic Transactions. In *Twenty-Fourth European Conference on Information Systems (ECIS),* İstanbul,Turkey.

Bécue, A., Praça, I., & Gama, J. (2021). Artificial Intelligence, Cyber-threats and Industry 4.0: Challenges and Opportunities. *Artif. Intell. Rev.*, *54*(5), 3849–3886. https://doi.org/10.1007/s10462-020-09942-2

Bedi, G., Venayagamoorthy, G. K., Singh, R., Brooks, R. R., & Wang, K.-C. (2018). Review of Internet of Things (IoT) in Electric Power and Energy Systems. *IEEE Internet of Things Journal*, *5*(2), 847–870. https://doi.org/10.1109/JIOT.2018.2802704

Benitez, J., Henseler, J., Castillo, A., & Schuberth, F. (2020). How to perform and report an impactful analysis using partial least squares: Guidelines for confirmatory and explanatory IS research. *Information & Management*, *57*(2), 103168. https://doi.org/10.1016/j.im.2019.05.003

Bennett, K. W., & Robertson, J. (2019). Security in the Cloud: Understanding Your Responsibility. In I. V. Ternovskiy & P. Chin (Eds.), *Proceedings of SPIE: Vol. 11011, Cyber Sensing 2019* (Article 1101106). SPIE. https://doi.org/10.1117/12.2521821

Benston, G. J., & Smith, C. W. (1976). A Transactions Cost Approach to the Theory of Financial Intermediation. *The Journal of Finance*, *31*(2), 215. https://doi.org/10.2307/2326596

Bentler, P. M., & Bonett, D. G. (1980). Significance tests and goodness of fit in the analysis of covariance structures. *Psychological Bulletin*, *88*(3), 588–606. https://doi.org/10.1037/0033-2909.88.3.588

Berawi, M. A., Suwartha, N., Asvial, M., Harwahyu, R., Suryanegara, M., Setiawan, E. A., Surjandari, I., Zagloel, T. Y. M., & Maknun, I. J. (2020). Digital Innovation: Creating Competitive Advantages. *Int. J. Technol.*, *11*(6), 1076–1080. https://doi.org/10.14716/ijtech.v11i6.4581

Berg, L. P., & Vance, J. M. (2017). Industry use of virtual reality in product design and manufacturing: a survey. *Virtual Reality*, *21*(1), 1–17. https://doi.org/10.1007/s10055-016-0293-9

Bishop, M. (2007). About Penetration Testing. *IEEE Secur. Privacy*, *5*(6), 84–87. https://doi.org/10.1109/MSP.2007.159

Bitzer, M., Häckel, B., Leuthe, D., Ott, J., Stahl, B., & Strobel, J. (2023). Managing the Inevitable – A Maturity Model to Establish Incident Response Management Capabilities. *Comput. Secur.*, *125*, 103050. https://doi.org/10.1016/j.cose.2022.103050

Blokus-Roszkowska, A., & Dziula, P. (2016). An approach to identification of critical infrastructure systems. In *AIP Conference Proceedings* (p. 440005). Author(s). https://doi.org/10.1063/1.4952223

Boakye, D., Sarpong, D., Meissner, D., & Ofosu, G. (2024). How TalkTalk did the walk-walk: strategic reputational repair in a cyber-attack. *Information Technology & People*, *37*(4), 1642–1673. https://doi.org/10.1108/ITP-08-2022-0589

Bolannavar, J. (2020). CSPM- Cloud Security Posture Management (Comprehensive Security for Cloud Environment). *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *6*(2), 251–257. https://doi.org/10.32628/cseit206268

Bresciani, S., Huarng, K.-H., Malhotra, A., & Ferraris, A. (2021). Digital Transformation as a Springboard for Product, Process and Business Model Innovation. *J. Bus. Res.*, *128*, 204–210. https://doi.org/10.1016/j.jbusres.2021.02.003

Buck, C., Eymann, T., Jelito, D., Schlatt, V., Schweizer, A., Strobel, J., & Weiß, F. (2023). Cyber-Sicherheit für kritische Energieinfrastrukturen – Handlungsempfehlungen zur Umsetzung einer Zero-Trust-Architektur. *HMD Praxis Der Wirtschaftsinformatik*. Advance online publication. https://doi.org/10.1365/s40702-023-00944-6

Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never Trust, Always Verify: A Multivocal Literature Review on Current Knowledge and Research Gaps of Zero-Trust. *Computers & Security*, *110*, Article 102436. https://doi.org/10.1016/j.cose.2021.102436

Cascio, W. F. (2000). Managing a virtual workplace. *Academy of Management Perspectives*, *14*(3), 81–90. https://doi.org/10.5465/ame.2000.4468068

Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E., & Wortmann, F. (2019). Blockchain for the IoT: Privacy-Preserving Protection of Sensor Data. *Journal of the Association for Information Systems*, *20*(9), 1274–1309. https://doi.org/10.17705/1jais.00567

Chen, W., and Wang, Q. (2020). *The Role of Blockchain for the European Bond Market: FSBC Working Paper*.

Chin, W. W., & Marcoulides, G. A. (1998). The Partial Least Squares Approach to Structural Equation Modeling. *Advances in Hospitality and Leisure*, *8*(2).

Christine, D. I., & Thinyane, M. (2022). Socio-technical Cyber Resilience: A Systematic Review of Cyber Resilience Management Frameworks. In J. Marx Gómez & M. R. Lorini (Eds.), *Progress in IS. Digital Transformation for Sustainability* (pp. 573–597). Springer International Publishing. https://doi.org/10.1007/978-3-031-15420-1_28

Chuen, D. L. K., & Teo, E. G. S. (2015). Emergence of fintech and the LASIC principles. *The Journal of Financial Perspectives: Fintech*, 24–37.

Ciborra, C. U. (1983). Markets, bureaucracies and groups in the information society. *Information Economics and Policy*, *1*(2), 145–160. https://doi.org/10.1016/0167-6245(83)90024-0

Cisar, D., Schellinger, B., Stoetzer, J.-C., Urbach, N., Weiß, F. L., Gramlich, V., & Guggenberger, T. (2025). Designing the future of bond markets: Reducing transaction costs through tokenization. *Electronic Markets*, *35*(1). https://doi.org/10.1007/s12525-025-00753-3

Coase, R. H. (1937). The Nature of the Firm. *Economica*, *4*(16), 386–405. https://doi.org/10.1111/j.1468-0335.1937.tb00002.x

Corbin, J., & Strauss, A. (1990). Grounded Theory Research: Procedures, Canons, and Evaluative Criteria. *Qualitative Sociology*, *13*(1), 3–21. https://doi.org/10.1515/zfsoz-1990-0602

Cuervo-Cazurra, A., Doz, Y., & Gaur, A. (2020). Skepticism of Globalization and Global Strategy: Increasing Regulations and Countervailing Strategies. *Glob. Strategy J.*, *10*(1), 3–31. https://doi.org/10.1002/gsj.1374

Daassi, M., & Debbabi, S. (2021). Intention to reuse AR-based apps: The combined role of the sense of immersion, product presence and perceived realism. *Information & Management*, *58*(4), 103453. https://doi.org/10.1016/j.im.2021.103453

Darwin, C. (1859). *On the Origin of Species: By Means of Natural Selection*. John Murray.

Diesch, R., Pfaff, M., & Krcmar, H [Helmut] (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security*, *92*, 101747. https://doi.org/10.1016/j.cose.2020.101747

Dorfleitner, G., Hornuf, L., Schmitt, M., & Weber, M. (2017). The fintech market in Germany. In *FinTech in Germany* (pp. 13–46). Springer.

Edwards, A. K., Harris, L. E., & Piwowar, M. S. (2007). Corporate Bond Market Transaction Costs and Transparency. *The Journal of Finance*, *62*(3), 1421–1451. http://www.jstor.org/stable/4622305

Elsey, J. W., van Andel, K., Kater, R. B., Reints, I. M., & Spiering, M. (2019). The impact of virtual reality versus 2D pornography on sexual arousal and presence. *Computers in Human Behavior*, *97*, 35–43. https://doi.org/10.1016/j.chb.2019.02.031

Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the EU, 2022.

Eurostat (Ed.). (2023). *Cloud Computing - Statistics on the Use by Enterprises*. https://ec.europa.eu/eurostat/statistics-explained/

Executive Office of the President (Ed.). (2024). *Strategy for Cyber-Physical Resilience: Fortifying Our Critical Infrastructure for a Digital World*.

Federal Financial Supervisory Authority. (2021). *Now also in electronic form: securities*. https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2021/fa_bj_2107_eWpG_en.html

Feroz, A. K., Zo, H., & Chiravuri, A. (2021). Digital Transformation and Environmental Sustainability: A Review and Research Agenda. *Sustainability*, *13*(3), 1530. https://doi.org/10.3390/su13031530

Feulner, S., Guggenberger, T., Stoetzer, J.-C., & Urbach, N. (2022). *Shedding Light on the Blockchain Disintermediation Mystery: A Review and Future Research Agenda*.

Fong, D., Han, F., Liu, L., Qu, J., & Shek, A. (2021). *Seven technologies shaping the future of fintech*. https://www.mckinsey.com/cn/our-insights/seven-technologies-shaping-the-future-of-fintech

Fox, J., Arena, D., & Bailenson, J. N. (2009). Virtual Reality. *Journal of Media Psychology*, *21*(3), 95–113. https://doi.org/10.1027/1864-1105.21.3.95

Furrer, F. J. (2022). Principles for Security. In F. J. Furrer (Ed.), *Springer eBook Collection. Safety and Security of Cyber-Physical Systems: Engineering Dependable Software Using Principle-based Development* (pp. 449–505). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-37182-1_11

Gai, K., Qiu, M., Sun, X., & Zhao, H. (2017). Security and Privacy Issues: A Survey on FinTech. In M. Qiu (Ed.), *Lecture Notes in Computer Science: Vol. 10135. Smart computing and communication: First international conference, SmartCom 2016* (Vol. 10135, pp. 236–247). https://doi.org/10.1007/978-3-319-52015-5_24

Gefen, D., Straub, D., & Boudreau, M.-C. (2000). Structural Equation Modeling and Regression: Guidelines for Research Practice. *Communications of the Association for Information Systems*, *4*(7). https://doi.org/10.17705/1CAIS.00407

Georgiadou, A., Michalitsi-Psarrou, A., & Askounis, D. (2023). A security awareness and competency evaluation in the energy sector. *Computers & Security*, *129*, 103199. https://doi.org/10.1016/j.cose.2023.103199

Gimpel, H., Rau, D., & Röglinger, M. (2018). Understanding FinTech start-ups–a taxonomy of consumer-oriented service offerings. *Electronic Markets*, *28*(3), 245–264.

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking Qualitative Rigor in Inductive Research. *Organizational Research Methods*, *16*(1), 15–31. https://doi.org/10.1177/1094428112452151

Goldstein, I., Jiang, W., & Karolyi, G. A. (2019). To FinTech and Beyond. *The Review of Financial Studies*, *32*(5), 1647–1661. https://doi.org/10.1093/rfs/hhz025

Gregor, S., & Hevner, A. R. (2013). Positioning and Presenting Design Science Research for Maximum Impact. *MIS Quarterly*, *37*(2), 337–355. https://doi.org/10.25300/MISQ/2013/37.2.01

Gregor, S., Kruse, L., & Seidel, S. (2020). Research Perspectives: The Anatomy of a Design Principle. *Journal of the Association for Information Systems*, *21*, 1622–1652. https://doi.org/10.17705/1jais.00649

Grossmann, M. M. (2024). *Blockchain-Based Bonds*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-45311-4

Grover, V., Cheon, M. J., & Teng, J. T. (1996). The Effect of Service Quality and Partnership on the Outsourcing of Information Systems Functions. *Journal of Management Information Systems*, *12*(4), 89–116. https://doi.org/10.1080/07421222.1996.11518102

Grubert, J., Ofek, E., Pahud, M., & Kristensson, P. O. (2018). The Office of the Future: Virtual, Portable, and Global. *IEEE Computer Graphics and Applications*, *38*(6), 125–133. https://doi.org/10.1109/MCG.2018.2875609

Guggenberger, T., Schellinger, B., Wachter, V. von, & Urbach, N. (2023). Kickstarting blockchain: designing blockchain-based tokens for equity crowdfunding. *Electronic Commerce Research*. Advance online publication. https://doi.org/10.1007/s10660-022-09634-9

Gurbaxani, V., & Whang, S. (1991). The impact of information systems on organizations and markets. *Communications of the ACM*, *34*(1), 59–73. https://doi.org/10.1145/99977.99990

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). *5443-9640*.

Hasan, M. K., Habib, A. A., Shukur, Z., Ibrahim, F., Islam, S., & Razzaque, M. A. (2023). Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. *Journal of Network and Computer Applications*, *209*, 103540. https://doi.org/10.1016/j.jnca.2022.103540

Haupert, V., Maier, D., & Müller, T. (2017). Paying the Price for Disruption. In *Proceedings of the 1st Reversing and Offensive-oriented Trends Symposium*. ACM. https://doi.org/10.1145/3150376.3150383

He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A Survey on Zero Trust Architecture: Challenges and Future Trends. *Wireless Communications and Mobile Computing*, *2022*, 1–13. https://doi.org/10.1155/2022/6476274

Heger, S. (2020). *Information Systems Design Knowledge for Sustainable Development Along a Social-Technical Continuum* [Doctoral Thesis]. RIS.

Heikka, J., Baskerville, R., & Siponen, M. (2006). A Design Theory for Secure Information Systems Design Methods. *Journal of the Association for Information Systems*, *7*(11), 725–770. https://doi.org/10.17705/1jais.00107

Hevner, March, Park, & Ram (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75. https://doi.org/10.2307/25148625

Hofma, C. C., Avital, M., & Jensen, T. B. (2017). Liquid Workplaces: The Potential Implications of Virtual Reality on the Workplace, *9*(8) (Selected Papers of the IRIS).

HSBC. (2024). *HSBC Delivers World's First Multi-Currency Digital Bond Offering*. https://www.gbm.hsbc.com/en-gb/insights/financing/first-multi-currency-digital-bond-offering

Hu, Z., Beuran, R., & Tan, Y. (2020). Automated Penetration Testing Using Deep Reinforcement Learning. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 2–10). IEEE. https://doi.org/10.1109/EuroSPW51379.2020.00010

Huygelier, H., Schraepen, B., van Ee, R., Vanden Abeele, V., & Gillebert, C. R. (2019). Acceptance of immersive head-mounted virtual reality in older adults. *Scientific Reports*, *9*(1), 4519. https://doi.org/10.1038/s41598-019-41200-6

International Capital Market Association. (2020). *Bond Market Size*. https://www.icmagroup.org/market-practice-and-regulatory-policy/secondary-markets/bond-market-size/

Jahn, K., Oschinsky, F. M., Kordyaka, B., Machulska, A., Eiler, T. J., Gruenewald, A., Klucken, T., Brueck, R., Gethmann, C. F., & Niehaves, B. (2022). Design elements in immersive virtual reality: The impact of object presence on health-related outcomes. *Internet Research*, *32*(7), 376–401. https://doi.org/10.1108/INTR-12-2020-0712

Jasti, A., Shah, P., Nagaraj, R., & Pendse, R. (2010). Security in Multi-Tenancy Cloud. In *44th Annual 2010 IEEE International Carnahan Conference on Security Technology* (pp. 35–41). IEEE. https://doi.org/10.1109/CCST.2010.5678682

Jiang, Z., & Benbasat, I. (2004). Virtual Product Experience: Effects of Visual and Functional Control of Products on Perceived Diagnosticity and Flow in Electronic Shopping. *Journal of Management Information Systems*, *21*(3), 111–147. https://doi.org/10.1080/07421222.2004.11045817

Johnson, R. D., Lukaszewski, K. M., & Stone, D. L. (2016). The Evolution of the Field of Human Resource Information Systems: Co-Evolution of Technology and HR Processes. *Communications of the Association for Information Systems*, *38*, 533–553. https://doi.org/10.17705/1CAIS.03828

Jonathan, G. M. (2020). *Information Technology Alignment : The Role of Organisational Structure* (DSV Report Series 20-006). Stockholm University, Faculty of Social Sciences, Department of Computer and Systems Sciences. https://www.diva-portal.org/smash/get/diva2:1423531/FULLTEXT01

Kandpal, S., Bhatt, S., Mohan, L., Patwal, A., & Kumar, P. (2023). Cyber Security Implementation Issues in Small to Medium-sized Enterprises (SMEs) and their Potential Solutions: A Comprehensive Analysis. In *2023 14th International Conference on Computing Communication and Networking Technologies* (Article 56998). IEEE. https://doi.org/10.1109/ICCCNT56998.2023.10307363

Kaur, G., Habibi Lashkari, Z., & Habibi Lashkari, A. (2021). Information Security Governance in FinTech. In G. Kaur, Z. Habibi Lashkari, & A. Habibi Lashkari (Eds.), *Understanding Cybersecurity Management in FinTech* (pp. 35–64). Springer International Publishing. https://doi.org/10.1007/978-3-030-79915-1_3

Kaur, J., Tonejc, J., Wendzel, S., & Meier, M. (2015). Securing BACnet's Pitfalls. In H. Federrath & D. Gollmann (Eds.), *IFIP Advances in Information and Communication Technology*. *ICT Systems Security and Privacy Protection* (Vol. 455, pp. 616–629). Springer International Publishing. https://doi.org/10.1007/978-3-319-18467-8_41

Kelloway, E. K. (1999). *Using LISREL for structural equation modeling: A researcher's guide* [Nachdr.]. SAGE Publ.

Kim, D., & Ko, Y. J. (2019). The impact of virtual reality (VR) technology on sport spectators' flow experience and satisfaction. *Computers in Human Behavior*, *93*, 346–356. https://doi.org/10.1016/j.chb.2018.12.040

Kinzinger, A., Steiner, W., Tatzgern, M., & Vallaster, C. (2022). Comparing low sensory enabling (LSE) and high sensory enabling (HSE) virtual product presentation modes in e-commerce. *Information Systems Journal*, *32*(5), 1034–1063. https://doi.org/10.1111/isj.12382

Kleinbauer, D., & Stone, G. (2021). *Acceleration of electronic trading trends hits new issue corporate bonds*. https://www.bloomberg.com/professional/blog/acceleration-of-electronic-trading-trends-hits-new-issue-corporate-bond/

Knudtson, T. (2021). *Security Chaos Engineering: How to Security Differently* [verica.io]. Verica. https://www.verica.io/blog/security-chaos-engineering-how-to-security-differently/

Kock, N. (2009). Information Systems Theorizing Based on Evolutionary Psychology: An Interdisciplinary Review and Theory Integration Framework. *MIS Quarterly*, *33*(2), 395. https://doi.org/10.2307/20650297

Kölbel, T., Lamberty, R., Sterk, F., & Weinhardt, C. (2022). Spotlight on DeFi Centerpieces: Towards an Economic Perspective on Asset Tokenization Services. In *Proceedings of the Pacific Asia Conference on Information Systems*. https://aisel.aisnet.org/pacis2022/94

Kopanaki, E. (2022). Conceptualizing Supply Chain Resilience: The Role of Complex IT Infrastructures. *Systems*, *10*(2), 35. https://doi.org/10.3390/systems10020035

Korhonen, J., & Snäkin, J.-P. (2015). Quantifying the relationship of resilience and eco-efficiency in complex adaptive energy systems. *Ecological Economics*, *120*, 83–92. https://doi.org/10.1016/j.ecolecon.2015.09.006

Kranz, J., Nagel, E., & Yoo, Y. (2019). Blockchain Token Sale. *Business & Information Systems Engineering*, *61*(6), 745–753. https://doi.org/10.1007/s12599-019-00598-z

Krüger, K., Weking, J., Fielt, E., Böttcher, T., Kowalkiewicz, M., & Krcmar, H [H.] (2025). Value Drivers for Metaverse Business Models: A Complementor Perspective. *Journal of Management Information Systems*, *42*(1), 143–173. https://doi.org/10.1080/07421222.2025.2452679

Lacity, M. C., & Willcocks, L. P. (1995). Interpreting information technology sourcing decisions from a transaction cost perspective: Findings and critique. *Accounting, Management and Information Technologies*, *5*(3-4), 203–244. https://doi.org/10.1016/0959-8022(96)00005-7

Laland, K., Uller, T., Feldman, M., Sterelny, K., Müller, G. B., Moczek, A., Jablonka, E., Odling-Smee, J., Wray, G. A., Hoekstra, H. E., Futuyma, D. J., Lenski, R. E., Mackay, T. F. C., Schluter, D., & Strassmann, J. E. (2014). Does evolutionary theory need a rethink? *Nature*, *514*(7521), 161–164. https://doi.org/10.1038/514161a

Lane, M., Shrestha, A., & Ali, O. (2017). Managing the Risks of Data Security and Privacy in the Cloud: A Shared Responsibility between the Cloud Service Provider and the Client Organisation. In *Bright Internet Global Summit 2017* (pp. 1–8). Association for Information Systems.

Lavassani, K. M., & Movahedi, B. (2017). Applications Driven Information Systems: Beyond Networks toward Business Ecosystems. *Int. J. Innov. Digit. Econ.*, *8*(1), 61–75. https://doi.org/10.4018/IJIDE.2017010104

Leuthe, D., Weiss, F., Dersch, J., & Bitzer, M. (2024). Towards Secure Cloud-Computing in FinTechs – An Artefact for Prioritizing Information Security Measures. *Proceedings of the 57th Hawaii International Conference on System Sciences*.

Lewis, J., & Wang, C [C.]. (2019). *Chaos Engineering: New Approaches to Security*. Rain Capital.

Li, C.-Y., & Fang, Y.-H. (2022). The more we get together, the more we can save? A transaction cost perspective. *International Journal of Information Management*, *62*, 102434. https://doi.org/10.1016/j.ijinfomgt.2021.102434

Lins, S., Schneider, S., & Sunyaev, A. (2018). Trust is Good, Control is Better: Creating Secure Clouds by Continuous Auditing. *IEEE Transactions on Cloud Computing*, *6*(3), 890–903. https://doi.org/10.1109/TCC.2016.2522411

Mahalle, A., Yong, J., Tao, X., & Shen, J. (2018). Data Privacy and System Security for Banking and Financial Services Industry based on Cloud Computing Infrastructure. In W. Shen, J. Luo, J.-P. Barthès, F. Dong, J. Zhang, & H. Zhu (Chairs), *2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design (CSCWD)*.

Majumdar, S., Madi, T., Jarraya, Y., Pourzandi, M., Wang, L., & Debbabi, M. (2019). Cloud Security Auditing: Major Approaches and Existing Challenges, *11358*, 61–77. https://doi.org/10.1007/978-3-030-18419-3_5

Mehrban, S., Nadeem, M. W., Hussain, M., Ahmed, M. M., Hakeem, O., Saqib, S., Kiah, M. M., Abbas, F., Hassan, M., & Khan, M. A. (2020). Towards secure FinTech: A survey, taxonomy, and open research challenges. *IEEE Access*, *8*, 23391–23406.

Meier, C. (2017). Managing Digitalization: Challenges and Opportunities for Business. *Manage. Sci.*, *12*(2), 111–113. https://doi.org/10.26493/1854-4231.12.111-113

Meißner, M., Pfeiffer, J., Peukert, C., Dietrich, H., & Pfeiffer, T. (2020). How virtual reality affects consumer choice. *Journal of Business Research*, *117*, 219–231. https://doi.org/10.1016/j.jbusres.2020.06.004

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology* (SP 800-145). NIST. https://doi.org/10.6028/NIST.SP.800-145

Menck, J., Lechte, H., Riedel, M., Jaja, J., & Tümler, J. (2023). Realism and Experiments: Investigating Virtual Reality Experiments. *ICIS 2023 Proceedings*. https://aisel.aisnet.org/icis2023/adv_theory/adv_theory/1

Messenger, J. C., & Gschwind, L. (2016). Three generations of Telework: New ICT s and the (R)evolution from Home Office to Virtual Office. *New Technology, Work and Employment*, *31*(3), 195–208. https://doi.org/10.1111/ntwe.12073

Mishra, S., & Gochhait, S. (2023). Emerging Cybersecurity Attacks in the Era of Digital Transformation. In *2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 1442–1447). IEEE. https://doi.org/10.1109/ICICCS56967.2023.10142357

Moosavi, S. A., Asgari, M., & Kamel, S. R. (2024). Developing a comprehensive BACnet attack dataset: A step towards improved cybersecurity in building automation systems. *Data in Brief*, *57*, 111192. https://doi.org/10.1016/j.dib.2024.111192

Moskaliuk, J., Burmeister, C. P., Landkammer, F., Renner, B., & Cress, U. (2017). Environmental effects on cognition and decision making of knowledge workers. *Journal of Environmental Psychology*, *49*, 43–54. https://doi.org/10.1016/j.jenvp.2016.12.001

Mouratidis, H., Zdravkovic, J., & Stirna, J. (2020). Cyber Security Resilience in Business Informatics: An Exploratory Paper. In R. A. Buchmann, A. Polini, B. Johansson, & D. Karagiannis (Eds.), *Lecture Notes in Business Information Processing*. *Perspectives in Business Informatics Research* (Vol. 398, pp. 53–66). Springer International Publishing. https://doi.org/10.1007/978-3-030-61140-8_4

Muñoz, F. R., Armas Vega, E. A., & Villalba, L. J. G. (2018). Analyzing the Traffic of Penetration Testing Tools with an IDS. *J. Supercomput.*, *74*(12), 6454–6469. https://doi.org/10.1007/s11227-016-1920-7

Murinde, V., Rizopoulos, E., & Zachariadis, M. (2022). The impact of the FinTech revolution on the future of banking: Opportunities and risks. *International Review of Financial Analysis*, 102103. https://doi.org/10.1016/j.irfa.2022.102103

Nagel, B., Gerth, C., Yigitbas, E., Christ, F., & Engels, G. (2012). Model-Driven Specification of Adaptive Cloud-Based Systems. In *Proceedings of the 1st International Workshop on Model-Driven Engineering for High Performance and Cloud computing* (pp. 1–6). ACM. https://doi.org/10.1145/2446224.2446228

Nah, Eschenbrenner, & DeWester (2011). Enhancing Brand Equity Through Flow and Telepresence: A Comparison of 2D and 3D Virtual Worlds. *MIS Quarterly*, *35*(3), 731. https://doi.org/10.2307/23042806

Nan, N. (2011). Capturing Bottom-Up Information Technology Use Processes: A Complex Adaptive Systems Model. *MIS Quarterly*, *35*(2), 505. https://doi.org/10.2307/23044054

Nelson, R. R. (1995). Recent Evolutionary Theorizing About Economic Change. *Journal of Economic Literature*, *33*(1), 48–90. http://www.jstor.org/stable/2728910

Nelson, R. R., & Winter, S. G. (1982). *An evolutionary theory of economic change*. Harvard University Press.

Nguyen, V. T., Nguyen, C. T. H., Yooc, S.-C., & Jung, K. (2023). Unveiling Augmented Reality Applications: Exploring Influential Factors Through Comprehensive Review. *SN Computer Science*, *4*(5). https://doi.org/10.1007/s42979-023-02175-4

Nguyen Duc, A., & Chirumamilla, A. (2019). Identifying Security Risks of Digital Transformation - An Engineering Perspective. In I. O. Pappas, P. Mikalef, Y. K. Dwivedi, L. Jaccheri, J. Krogstie, & M. Mäntymäki (Eds.), *Lecture Notes in Computer Science: Vol. 11701, Digital Transformation for a Sustainable Society in the 21st Century: 18th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2019 Trondheim, Norway, September 18-20, 2019 Proceedings* (pp. 677–688). Springer International Publishing. https://doi.org/10.1007/978-3-030-29374-1_55

NIST. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). NIST. https://doi.org/10.6028/NIST.CSWP.29

Nurse, J. R. C., Williams, N., Collins, E., Panteli, N., Blythe, J., & Koppelman, B. (2021). Remote Working Pre- and Post-COVID-19: An Analysis of New Threats and Risks to Security and Privacy. In C. Stephanidis, M. Antona, & S. Ntoa (Eds.), *Communications in Computer and Information Science: Vol. 1421, HCI International 2021 - Posters: 23rd HCI International Conference, HCII 2021 Virtual Event, July 24-29, 2021 Proceedings, Part III* (pp. 583–590). Springer International Publishing. https://doi.org/10.1007/978-3-030-78645-8_74

Parast, F. K., Sindhav, C., Nikam, S., Izadi, H. Y., Kent, K. B., & Hakak, S. (2022). Cloud Computing Security: A Survey of Service-Based Models. *Comput. Secur.*, *114*, 102580. https://doi.org/10.1016/j.cose.2021.102580

Pearson, R., & Bardsley, D. K. (2022). Applying complex adaptive systems and risk society theory to understand energy transitions. *Environmental Innovation and Societal Transitions*, *42*, 74–87. https://doi.org/10.1016/j.eist.2021.11.006

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Peukert, C., Pfeiffer, J., Meißner, M., Pfeiffer, T., & Weinhardt, C. (2019). Shopping in Virtual Reality Stores: The Influence of Immersion on System Adoption. *Journal of Management Information Systems*, *36*(3), 755–788. https://doi.org/10.1080/07421222.2019.1628889

Ramluckan, T., & van Niekerk, B. (2020). A Change Management Perspective to Implementing a Cyber Security Culture. In T. Eze, L. Speakman, & C. Onwubiko (Eds.), *19th European Conference on Cyber Warfare and Security (ECCWS 2020)* (pp. 442–448). ACPI.

Rekeraho, A., Cotfas, D. T., Cotfas, P. A., Bălan, T. C., Tuyishime, E., & Acheampong, R. (2024). Cybersecurity challenges in IoT-based smart renewable energy. *International Journal of Information Security*, *23*(1), 101–117. https://doi.org/10.1007/s10207-023-00732-9

Rigdon, E. E., Sarstedt, M., & Ringle, C. M. (2017). On Comparing Results from CB-SEM and PLS-SEM: Five Perspectives and Five Recommendations. *Marketing ZFP*, *39*(3), 4–16. https://doi.org/10.15358/0344-1369-2017-3-4

Rinehart, A., & Shortridge, K. (2020). *Security Chaos Engineering: Gaining Confidence in Resilience and Safety at Speed and Scale*. O'Reilly Media, Inc.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). *Developing Cyber-Resilient Systems* (SP 800-160). https://doi.org/10.6028/NIST.SP.800-160v2r1

Rossi, M., Mueller-Bloch, C., Thatcher, J. B., & Beck, R. (2019). "Blockchain Research in Information Systems: Current Trends and an Inclusive Future Research Agenda". *Journal of the Association for Information Systems*, 1388–1403. https://doi.org/10.17705/1jais.00571

Rowen, A., Grabowski, M., & Rancy, J.-P. (2019). Through the Looking Glass(es): Impacts of Wearable Augmented Reality Displays on Operators in a Safety-Critical System. *IEEE Transactions on Human-Machine Systems*, *49*(6), 652–660. https://doi.org/10.1109/THMS.2019.2944384

Roy, A., & Patil, K. (2023). Framework for Cloud Security Initiatives in Small and Medium-Sized Enterprises. In *2023 International Conference on Advancement in Computation & Computer Technologies* (pp. 444–449). IEEE. https://doi.org/10.1109/InCACCT57535.2023.10141743

Ruse, M. (1975). Charles Darwin's Theory of Evolution: An Analysis. *Journal of the History of Biology*, *8*(2), 219–241. http://www.jstor.org/stable/4330635

Sadavarte, R. K., Kurundkar, G. D., & Bhopi, S. A. (2022). Cloud Computing - An Insight to Latest Trends and Developments. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, *8*(3), Article CSEIT228227, 242–247. https://doi.org/10.32628/cseit228227

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors*, *23*(15), 6666. https://doi.org/10.3390/s23156666+

Safitra, M. F., Lubis, M., & Kurniawan, M. T. (2023). Cyber Resilience: Research Opportunities. In *Proceedings of the 2023 6th International Conference on Electronics, Communications and Control Engineering* (pp. 99–104). ACM. https://doi.org/10.1145/3592307.3592323

Salnitri, M., Paja, E., & Giorgini, P. (2014). Preserving Compliance with Security Requirements in Socio-Technical Systems. In F. Cleary & M. Felici (Eds.), *Communications in Computer and Information Science. Cyber Security and Privacy* (Vol. 470, pp. 49–61). Springer International Publishing. https://doi.org/10.1007/978-3-319-12574-9_5

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2018). Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality & Quantity*, *52*(4), 1893–1907. https://doi.org/10.1007/s11135-017-0574-8

Schneider, S., & Sunyaev, A. (2015). CloudLive: a life cycle framework for cloud services. *Electronic Markets*, *25*(4), 299–311.

Schneier, B., & Vance, A. (2025). “Complexity is the Worst Enemy of Security”: Studying Cybersecurity through the Lens of Organizational Complexity. *MIS Quarterly*, *49*(1), 205–210.

Schultze, U., & Avital, M. (2011). Designing Interviews to Generate Rich Data for Information Systems Research. *Inf. Org.*, *21*(1), 1–16. https://doi.org/10.1016/j.infoandorg.2010.11.001

Schumpeter, J. (1949). *The Theory of Economic Development: An Inquiry into Profits, Credit, Interest, and the Business Cycle*. Harvard University Press.

Scott, W. R. (1981). *Organizations: Rational, Natural, and Open Systems* (2nd ed.). Prentice-Hall.

Sermpezis, E., Karapiperis, D., & Tjortjis, C. (2024). Integration of Security in the DevOps Methodology. In *2024 15th International Conference on Information, Intelligence, Systems & Applications* (pp. 1–6). IEEE. https://doi.org/10.1109/IISA62523.2024.10786669

Shinde, S. S., & Ansurkar, G. (2023). Upcoming Threats in Cyber-Security. *Int. J. Sci. Res. Sci. Technol.*, *10*(2), Article IJSRST523102121, 806–816. https://doi.org/10.32628/IJSRST523102121

Siemens AG. (2023). *Press release: Siemens issues first digital bond on blockchain*. https://assets.new.siemens.com/siemens/assets/api/uuid:313284ea-53db-4fea-8eb6-f1ceb33a518d/HQCOPR20230213665OEN.pdf

Singh, G., Gupta, R., & Vatsa, V. (2021, October 11 – December 11). A Framework for Enhancing Cyber Security in Fintech Applications in India. In *2021 International Conference on Technological Advancements and Innovations* (pp. 274–279). IEEE. https://doi.org/10.1109/ICTAI53825.2021.9673277

Solms, B. von (2000). Information Security - The Third Wave? *Comput. Secur.*, *19*(7), 615–620. https://doi.org/10.1016/S0167-4048(00)07021-8

Solms, B. von (2006). Information Security – The Fourth Wave. *Comput. Secur.*, *25*(3), 165–168. https://doi.org/10.1016/j.cose.2006.03.004

Solms, R. von, & van Niekerk, J. (2013). From Information Security to Cyber Security. *Comput. Secur.*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Sonnenberg, C., & vom Brocke, J. (2012). Evaluation Patterns for Design Science Research Artefacts. In M. Helfert & B. Donnellan (Eds.), *Communications in Computer and Information Science. Practical Aspects of Design Science* (Vol. 286, pp. 71–83). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-33681-2_7

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Söylemez, M., Tekinerdogan, B., & Kolukısa Tarhan, A. (2022). Challenges and Solution Directions of Microservice Architectures: A Systematic Literature Review. *Appl. Sci.*, *12*(11), 5507. https://doi.org/10.3390/app12115507

Strobel, J., Weiß, F., & Bitzer, M. (2023). From Observing to Understanding: Empirical Insights on the Organizational Foundations of Security Chaos Engineering. In *International Conference on Information Systems (ICIS)*. Symposium conducted at the meeting of AIS, Hyderabad, India. https://aisel.aisnet.org/icis2023/cyber_security/cyber_security/10

Suh, & Lee (2005). The Effects of Virtual Reality on Consumer Learning: An Empirical Investigation. *MIS Quarterly*, *29*(4), 673. https://doi.org/10.2307/25148705

Sumner, M. (2009). Information Security Threats: A Comparative Analysis of Impact, Probability, and Preparedness. *Information Systems Management*, *26*(1), 2–12. https://doi.org/10.1080/10580530802384639

Tabachnick, B. G., & Fidell, L. S. (2014). *Using multivariate statistics* (Sixth edition, Pearson new international edition). *Always learning*. Pearson Education Limited.

Taha, K. (2023). Proactive Measures for Cyber-Physical Systems Cybersecurity. In *2023 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 353–358). IEEE. https://doi.org/10.1109/CSR57506.2023.10224929

Tang, L., Bhandari, C., Zhang, Y [Yongle], Karanika, A., Ji, S., Gupta, I., & Xu, T. (2023). Fail through the Cracks: Cross-System Interaction Failures in Modern Cloud Systems. In A. Fedorova, D. Narayanan, G. A. Di Luna, & L. Querzoni (Eds.), *Proceedings of the Eighteenth European Conference on Computer Systems* (pp. 433–451). ACM. https://doi.org/10.1145/3552326.3587448

Tang, M., Li, M., & Zhang, T. (2016). The Impacts of Organizational Culture on Information Security Culture: A Case Study. *Inf. Technol. Manage.*, *17*(2), 179–186. https://doi.org/10.1007/s10799-015-0252-2

Tchernykh, A., Schwiegelsohn, U., Talbi, E., & Babenko, M. (2019). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science*, *36*, 100581. https://doi.org/10.1016/j.jocs.2016.11.011

Tenable (Ed.). (2025). *Tenable and Nessus Pricing & Purchase Options*. https://www.tenable.com/buy

Terpstra, E., Daneva, M., & Wang, C [Chong] (2017). Agile Practitioners' Understanding of Security Requirements: Insights from a Grounded Theory Analysis. In *2017 IEEE 25th International Requirements Engineering Conference Workshops (REW)* (pp. 439–442). IEEE. https://doi.org/10.1109/REW.2017.54

Torkura, K. A., Sukmana, M. I., Cheng, F., & Meinel, C. (2019). Security Chaos Engineering for Cloud Services: Work In Progress. In A. Gkoulalas-Divanis & D. R. Avresky (Eds.), *18th International Symposium on Network Computing and Applications* (pp. 1–3). IEEE. https://doi.org/10.1109/NCA.2019.8935046

Tran, D. U., & Jøsang, A. (2023). Business Language for Information Security. In S. Furnell & N. Clarke (Eds.), *IFIP Advances in Information and Communication Technology*. *Human Aspects of Information Security and Assurance* (Vol. 674, pp. 169–180). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-38530-8_14

Tzavara, V., & Vassiliadis, S. (2024). Tracing the Evolution of Cyber Resilience: A Historical and Conceptual Review. *Int. J. Inf. Secur.*, *23*, 1695–1719. https://doi.org/10.1007/s10207-023-00811-x

Ullman, S., Samtani, S., Zhu, H [Hongyi], Lazarine, B., Chen, H., & Nunamaker, J. F. (2024). Enhancing Vulnerability Prioritization in Cloud Computing Using Multi-View Representation Learning. *Journal of Management Information Systems*, *41*(3), 708–743. https://doi.org/10.1080/07421222.2024.2376384

Urbach, N., & Ahlemann, F. (2010). Structural Equation Modeling in Information Systems Research Using Partial Least Squares. *Journal of Information Technology Theory and Application (JITTA)*, *11*(2). https://aisel.aisnet.org/jitta/vol11/iss2/2

van den Bergh, J. C., & Gowdy, J. M. (2000). Evolutionary Theories in Environmental and Resource Economics: Approaches and Applications. *Environmental and Resource Economics*, *17*(1), 37–57. https://doi.org/10.1023/A:1008317920901

Walls, J. G., Widmeyer, G. R., & El Sawy, O. A. (1992). Building an Information System Design Theory for Vigilant EIS. *Information Systems Research*, *3*(1), 36–59. https://doi.org/10.1287/isre.3.1.36

Wang, W [Weiyu], & Siau, K. (2019). Artificial Intelligence, Machine Learning, Automation, Robotics, Future of Work and Future of Humanity. *J. Database Manage.*, *30*(1), 61–79. https://doi.org/10.4018/JDM.2019010104

Wang, W [Wenye], & Lu, Z. (2013). Cyber security in the Smart Grid: Survey and challenges. *Computer Networks*, *57*(5), 1344–1371. https://doi.org/10.1016/j.comnet.2012.12.017

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Futur: Writing a Literature Review. *MIS Quarterly*, *26*(2), xiii–xxiii. https://www.jstor.org/stable/4132319

Welsh, T., & Benkhelifa, E. (2020). On Resilience in Cloud Computing: A Survey of Techniques across the Cloud Domain. *ACM Comput. Surv.*, *53*(3), 59. https://doi.org/10.1145/3388922

Weppler, M. (2017). 100-Percent Security – A Desirable Goal? In F. Abolhassan (Ed.), *Management for Professionals. The Drivers of Digital Transformation: Why There's No Way Around the Cloud* (pp. 115–120). Springer International Publishing. https://doi.org/10.1007/978-3-319-31824-0_11

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An Integrated View of Human, Organizational, and Technological Challenges of IT Security Management. *Inf. Manage. Comput. Secur.*, *17*(1), 4–19. https://doi.org/10.1108/09685220910944722

Werth, O., Cardona, D. R., Torno, A., Breitner, M. H., & Muntermann, J. (2023). What determines FinTech success?-A taxonomy-based analysis of FinTech success factors. *Electronic Markets*, *33*(1), 21. https://doi.org/10.1007/s12525-023-00626-7

Whitten, D., & Kayworth, T. (2010). Effective Information Security Requires a Balance of Social and Technology Factors. *MIS Quart. Executive*, *9*(3), Article 5.

Wildberger, A. M. (1997). Complex adaptive systems: concepts and power industry applications. *IEEE Control Systems*, *17*(6), 77–88. https://doi.org/10.1109/37.642976

Williamson, O. E. (1981). The Economics of Organization: The Transaction Cost Approach. *American Journal of Sociology*, *87*(3), 548–577. http://www.jstor.org/stable/2778934

Yang, H., Guo, Y [Yajun], & Guo, Y [Yimin] (2024). Fault-Tolerant Security-Efficiency Combined Authentication Scheme for Manned-Unmanned Teaming. *Computers & Security*, *146*, Article 104052. https://doi.org/10.1016/j.cose.2024.104052

Zhang, C., Thomas, C., & Vasarhelyi, M. A. (2022). Attended Process Automation in Audit: A Framework and a Demonstration. *Journal of Information Systems*, *36*(2), 101–124. https://doi.org/10.2308/ISYS-2020-073

Zhang, S., Zhang, X., & Ou, X. (2014). After We Knew It: Empirical Study and Modeling of Cost-Effectiveness of Exploiting Prevalent Known Vulnerabilities across IaaS Cloud. In *ASIA CCS '14: Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security* (pp. 317–328). ACM.

Zhang, Y [Yuanliang], He, H., Legunsen, O., Li, S [Shanshan], Dong, W., & Xu, T. (2021). An Evolutionary Study of Configuration Design and Implementation in Cloud Systems. In *2021 IEEE/ACM 43rd International Conference on Software Engineering* (pp. 188–200). IEEE. https://doi.org/10.1109/ICSE43902.2021.00029

Zhao, A. P., Li, S [Shuangqi], Gu, C., Yan, X., Hu, P. J.-H., Wang, Z [Zhaoyu], Da Xie, Cao, Z., Chen, X., Wu, C., Luo, T., Wang, Z [Zikang], & Hernando-Gil, I. (2024). Cyber Vulnerabilities of Energy Systems. *IEEE Journal of Emerging and Selected Topics in Industrial Electronics*, *5*(4), 1455–1469. https://doi.org/10.1109/JESTIE.2024.3434350

Appendices

Appendix A: Declarations of Co-Authorship and Individual Contributions

In the following, I present the co-authors' contributions to the essays.

Essay 1: Designing the Future of Bond Markets: Reducing Transaction Costs Through Tokenization

This research paper was co-authored by David Cisar, Benjamin Schellinger, Jens-Christian Stoetzer, Nils Urbach, Florian Lennart Weiß, Vincent Gramlich, and Tobias Guggenberger. The co-authors contributed as follows:

David Cisar (co-author)

David Cisar initiated and co-developed the research project and key artifact. He contributed by developing the paper's methodological approach. Jointly with the other authors, he developed and evaluated the artifact. He was responsible for writing parts of the original draft and was involved in reviewing and editing the entire paper. Thus, David Cisar's co-authorship is reflected in the entire research project.

Benjamin Schellinger (co-author)

Benjamin Schellinger initiated and co-developed the research project. He contributed by developing the paper's theoretical foundation and curating the methodological approach. Jointly with the other authors, he developed and evaluated the artifact. He was involved in reviewing and editing the entire paper. Thus, Benjamin Schellinger's co-authorship is reflected in the entire research project.

Jens-Christian Stoetzer (co-author)

Jens-Christian Stoetzer co-developed the research project. He contributed by developing the paper's theoretical foundation and curating the findings of the paper. Further, he was responsible for data collection. Jointly with the other authors, he developed and evaluated the artifact. He was responsible for writing parts of the original draft and was involved in reviewing and editing the entire paper. Thus, Jens-Christian Stoetzer's co-authorship is reflected in the entire research project.

Nils Urbach (co-author)

Nils Urbach provided mentorship and feedback on the paper's content and structure. Jointly with the other authors, he developed and evaluated the artifact. He also engaged in the textual elaboration with respect to reviewing and editing of the entire manuscript over the course of multiple rounds of revisions. Thus, Nils Urbach's co-authorship is reflected in the entire research project.

Florian Lennart Weiß (co-author)

Florian Weiß co-developed the research project. He contributed to the paper's theoretical foundation and contributed to the data collection. He participated in developing and evaluating the artifact. He was responsible for writing parts of the original draft and was involved in reviewing and editing the entire paper. Thus, Florian Weiß co-authorship is reflected in the entire research project.

Vincent Gramlich (subordinate author)

Vincent Gramlich provided mentorship and feedback on the paper's content and structure. He also engaged in the textual elaboration with respect to reviewing and editing of the entire manuscript over the course of the initial submission. He contributed as subordinate author of the research paper. Thus, Vincent Gramlich's co-authorship is reflected in the entire research project.

Tobias Guggenberger (subordinate author)

Tobias Guggenberger provided mentorship and feedback on the paper's content and structure. He also engaged in the textual elaboration with respect to reviewing and editing of the entire manuscript over the course of the initial submission. He contributed as subordinate author of the research paper. Thus, Tobias Guggenberger's co-authorship is reflected in the entire research project.

Essay 2: From Flat Screens to Immersive Virtual Reality: How Virtual Reality Influences Subjective and Objective Performance in Digital Sports

This research paper was co-authored by Dennis Lauer, Jens-Christian Stoetzer, Nina Weber, Florian Lennart Weiß, Christoph Buck, and Tobias Guggenberger. The co-authors contributed as follows:

Dennis Lauer (co-author)

Dennis Lauer initiated and co-developed the research project. He contributed by conceptualizing, conducting, and evaluating the experiment and participated in the manuscript development throughout the sections theoretical background and evaluation. Also, Dennis participated in research discussions, provided feedback on the paper's content and structure. Thus, Dennis Lauer's co-authorship is reflected in the entire research project.

Jens-Christian Stoetzer (co-author)

Jens-Christian Stoetzer co-developed the research project and provided mentorship. Furthermore, he participated in research discussions, provided feedback on the paper's content, fundamental contributions, and structure. Thus, his co-authorship is reflected in the entire research project.

Nina Weber (co-author)

Nina Weber initiated and co-developed the research project. She conceptualized the experiment and guided the evaluation process and developed the paper's research framework. In addition, she participated in research discussions, provided feedback on the paper's content and structure, and engaged in textual elaboration in the introduction, method, results, and evaluation sections. Hence, Nina Weber's co-authorship is reflected in the entire research project.

Florian Lennart Weiß (co-author)

Florian Weiß co-developed the research project, participated in research discussions, provided feedback on the paper's content and structure. Further, he was responsible for the textual elaboration throughout the introduction, theoretical background, discussion, and conclusion sections. Thus, Florian Weiß's co-authorship is reflected in the entire research project.

Christoph Buck (subordinate co-author)

Christoph Buck supervised the research project and provided mentorship. Furthermore, Christoph Buck participated in research discussions, provided feedback on the paper's content and structure. Thus, his co-authorship is reflected in the entire research project.

Tobias Guggenberger (subordinate co-author)

Tobias Guggenberger supervised the research project and provided mentorship. Further, he participated in research discussions, provided feedback on the paper's content and structure, and helped to strengthen the paper's contributions. Thus, Tobias Guggenberger's co-authorship is reflected in the entire research project.

Essay 3: Proactivity and Resilience: An Examination of Strategic Foundations for Cloud Security from an Organization Theory Perspective

This research paper was co-authored by Jacqueline Strobel, Florian Lennart Weiß, Michael Bitzer, Björn Häckel, and Nils Urbach. The co-authors contributed as follows:

Jacqueline Strobel (co-author)

Jacqueline Strobel initiated and co-developed the research project. She mainly contributed by conducting expert interviews and leading the analysis as well as evaluation. Moreover, she participated in textual elaboration across all sections of the manuscript. Additionally, she participated in research discussions and provided feedback on the paper's content and structure. Thus, Jacqueline Strobel's co-authorship is reflected in the entire research project.

Florian Lennart Weiß (co-author)

Florian Weiß initiated and co-developed the research project. He contributed by developing the paper's research design, recruiting experts as well as conducting and analyzing interviews, and engaging in textual elaboration across all sections. In addition, he participated in research discussions and provided feedback on the paper's content and structure. Consequently, Florian Weiß's co-authorship is reflected in the entire research project.

Michael Bitzer (subordinate co-author)

Michael Bitzer supervised the research project and provided mentorship. He contributed by co-developing the initial research project that this paper builds upon and helped to strengthen the essay's contributions. Furthermore, Michael Bitzer participated in research discussions, provided feedback on the paper's content and structure. Thus, his co-authorship is reflected in the entire research project.

Björn Häckel (subordinate co-author)

Björn Häckel supervised the research project and provided mentorship. He helped to setup the research project and provided methodological assistance. Also, Björn Häckel participated in research discussions, provided feedback on the paper's content and structure. Thus, his co-authorship is reflected in the entire research project.

Nils Urbach (subordinate co-author)

Nils Urbach supervised the research project and provided mentorship. In addition, he participated in research discussions, provided feedback on the paper's content and structure, including the developed research framework, and engaged in textual elaboration. Thus, Nils Urbach's co-authorship is reflected in the entire research project.

Essay 4: The David-Goliath Gap Throughout The Evolution Of Critical Energy Infrastructure Cybersecurity: An Analysis from a Complex Adaptive Systems Theory Perspective

This research paper was co-authored by Florian Lennart Weiß, Tobias Guggenberger, Alexander Rex, Moritz Schüll, and Nils Urbach. The co-authors contributed as follows:

Florian Lennart Weiß (co-author)

Florian Weiß was in lead role in initiating and developing the research paper. He recruited experts and conducted, analyzed, and evaluated all interviews. Florian was involved in the textual elaboration of all manuscript sections, developed the resulting framework and participated in research discussions. Thus, Florian Weiß's co-authorship is reflected in the entire paper.

Tobias Guggenberger (subordinate co-author)

Tobias Guggenberger supervised the research project and provided mentorship. Particularly, he participated in research discussions about the method and research motivation, provided feedback on the paper's content and structure, and engaged in textual elaboration. Hence, Tobias Guggenberger's co-authorship is reflected in the entire research project.

Alexander Rex (subordinate co-author)

Alexander Rex co-authored the research project and provided support throughout the evaluation and final textual elaboration phases. Further, he participated in research discussions, provided feedback on the paper's content and structure, and engaged in textual elaboration. Thus, Alexander Rex's co-authorship is reflected in the entire research project.

Moritz Schüll (subordinate co-author)

Moritz Schüll co-authored the research project and provided research support throughout the conduction and analysis of expert interviews. He contributed by participating in conceptual as well as coding sessions and was involved in the manuscript's textual elaboration. Furthermore, he participated in research discussions, provided feedback on the paper's content and structure. Therefore, Moritz Schüll's co-authorship is reflected in the entire research project.

Nils Urbach (subordinate co-author)

Nils Urbach supervised the research project and provided mentorship. From the beginning, Nils actively contributed to the research projects design and participated in research discussions, provided feedback on the paper's content and structure, and engaged in textual elaboration. Consequently, Nils Urbach's co-authorship is reflected in the entire research project.

Essay 5: From Planned Security to Reality: Towards an Open-Source Artifact for Automated Cloud Security Auditing on the OS-Level

This research paper was co-authored by Florian Port, Jacqueline Strobel, Florian Lennart Weiß, and Tobias Guggenberger. The co-authors contributed as follows:

Florian Port (co-author)

Florian Port initiated and co-developed the research project. His main contributions encompassed extensive market research and the development of the resulting artifact. Additionally, he conducted and analyzed expert interviews, engaged in textual elaboration, participated in research discussions and provided feedback on the paper's content and structure. Thus, Florian Port's co-authorship is reflected in the entire research project.

Jacqueline Strobel (co-author)

Jacqueline Strobel co-developed the research project. She was involved in conducting, analyzing, and evaluating expert interviews and conducted a literature review regarding existing (design) knowledge. Besides contributing through the textual elaboration of the introduction, theoretical background, and methodology sections, she participated in coding workshops, research discussions and provided feedback on the paper's content and structure. Consequently, Jacqueline Strobel's co-authorship is reflected in the entire research project.

Florian Lennart Weiß (co-author)

Florian Weiß initiated and co-developed the research project. He contributed by developing the research design, conceptualizing the resulting artifact, and conducting, analyzing, as well as evaluating expert interviews. Throughout the manuscript writing process, he engaged in textual elaboration across the whole manuscript. In addition, he participated in coding workshops, research discussions and provided feedback on the paper's content and structure. Therefore, Florian Weiß's co-authorship is reflected in the entire research project.

Tobias Guggenberger (subordinate co-author)

Tobias Guggenberger supervised the research project and provided mentorship. Further, he participated in research discussions, provided feedback on the paper's content and structure, and engaged in textual elaboration. Hence, Tobias Guggenberger's co-authorship is reflected in the entire research project.

Essay 6: Towards Secure Cloud-Computing in FinTechs – An Artefact for Prioritizing Information Security Measures

This research paper was co-authored by Daniel Leuthe, Florian Lennart Weiß, Julian Dersch, and Michael Bitzer. The co-authors contributed as follows:

Daniel Leuthe (co-author)

Daniel Leuthe played a leading role in initiating and co-developing the research project. His contributions included conducting and analyzing expert interviews, as well as textual elaboration of the introduction, theoretical background, methodology, discussion, and conclusion sections. He also participated in research discussions and provided valuable feedback on both the content and structure of the paper. His co-authorship is therefore reflected throughout the entire research project.

Florian Lennart Weiß (co-author)

Florian Weiß co-developed the research project. His main contributions included textual elaboration of the introduction, theoretical background, methodology, results, discussion, and conclusion sections. He also actively engaged in research discussions and provided feedback on the paper's content and structural composition. Accordingly, his co-authorship is reflected throughout the entire project.

Julian Dersch (subordinate co-author)

Julian Dersch initiated and co-developed the research project. He particularly contributed by leading the conceptualization and implementation of the developed artifact. Further, he engaged in textual elaboration, particularly in the introduction, theoretical background, and results sections. He also participated in research discussions and provided feedback on the paper's content and structure. Thus, Julian Dersch's co-authorship is reflected in the entire research project.

Michael Bitzer (subordinate co-author)

Michael Bitzer supervised the research project and provided mentorship. In addition, he actively contributed to research discussions, provided detailed feedback on both the content and structure, and participated in the refinement of the manuscript. Accordingly, Michael Bitzer's co-authorship is reflected in the entire research project.

Appendix B: Other Publications

Table 3: Overview of Other Publications

Reference	VHB PMR ranking	Publication status
Buck, C., Eymann, T., Jelito, D. et al. Cyber-Sicherheit für kritische Energieinfrastrukturen – Handlungsempfehlungen zur Umsetzung einer Zero-Trust-Architektur. HMD 60, 494–509 (2023). https://doi.org/10.1365/s40702-023-00944-6	C	Published
Gerlach, L., Götz, V., Guggenberger, T., Häckel, B., Helmus, B., Kreuzer, T., Principato, M., Urbach, N., Weber, N., Weiß, F. und Zipperling, D. (2025). SplitNFed: Datenschutzkonforme und effiziente künstliche Intelligenz mit Split & Federated Learning. Fraunhofer FIT Institutsteil Wirtschaftsinformatik, Augsburg / Bayreuth.	n/a	Published
Arnold, L., Götz, V. und Weiß, F. (2024). Potenziale digitaler Plattformen für die deutsche Milchwirtschaft. Fraunhofer-Institut für Angewandte Informationstechnik FIT - Institutsteil Wirtschaftsinformatik, Augsburg / Bayreuth.	n/a	Published

Designing the Future of Bond Markets: Reducing Transaction Costs Through Tokenization[2]

Authors

David Cisar, Benjamin Schellinger, Jens-Christian Stoetzer, Nils Urbach, Florian Lennart Weiß, Vincent Gramlich, and Tobias Guggenberger.

Abstract

This essay investigates how blockchain-based solutions can be designed to reduce transaction costs (TAC) in corporate bond markets, which are characterized by complex processes, multiple intermediaries, and substantial coordination and settlement frictions. While blockchain-based solutions are increasingly applied in practice, academic research offers mainly high-level conceptual discussions or narrow use-case analyses and lacks generic design knowledge for TAC-efficient blockchain-based bond market solutions. This essay closes this gap by answering the research question: How can a blockchain-based bond system be designed to reduce transaction costs in bond markets? Following the Design Science Research (DSR) paradigm and based on a literature review and expert interviews, the authors derive meta-requirements and design objectives that describe how TAC in bond markets should be reduced. They then design and implement an blockchain-based bond market artifact, covering e.g., CSR initialization, token minting, and issuance. The artifact is evaluated along the dimensions of efficacy, utility, and quality, based on 14 semi-structured expert interviews. The results highlight the capability of blockchain-based bond markets to reduce TAC in the three dimensions of asset specificity, uncertainty, and transaction frequency. Further, the essay provides design principles to contribute to both practice and the academic discourse on developing blockchain-based bond markets with reduced TAC.

Keywords: Bonds, Design science research, Transaction cost theory, Blockchain.

[2] This essay has been published in: Cisar, D., Schellinger, B., Stoetzer, J.-C., Urbach, N., Weiß, F.-L., Gramlich, V., Guggenberger, T. (2025). Designing the future of bond markets: Reducing transaction costs through tokenization. Electron Markets 35(9). https://doi.org/10.1007/s12525-025-00753-3

From Flat Screens to Immersive Virtual Reality: How Virtual Reality Influences Subjective and Objective Performance in Digital Sports[3]

Authors

Dennis Lauer, Jens-Christian Stoetzer, Nina Weber, Florian Lennart Weiß, Christoph Buck, and Tobias Guggenberger.

Abstract

This essay examines how a shift from non-immersive, screen-based setups to immersive virtual reality (VR) affects both the subjective and objective performance of players in digital sports. Digital sports are increasingly prominent in global competitions and VR is widely adopted to enhance presence and immersion in hybrid as well as fully digital sports formats. Despite this momentum, prior research has largely focused on either subjective experience or isolated performance metrics and has not covered investigations in actual competitive settings. The study addresses this gap by analyzing the mediating roles of presence and immersion in the relationship between display modality and subjective as well as objective performance.

The authors conduct a between-subject experiment with 80 players who perform the same digital sports tasks either in a 3D immersive VR condition or a 2D screen-based condition. The analysis combines a Mann-Whitney U test for direct condition comparisons with PLS-SEM to estimate the structural model and to test mediation effects. Presence and immersion are modelled as mediators between display modality and both subjective and objective performance.

Direct comparisons show that the immersive VR condition improves subjective and objective performance. When presence and immersion are included as mediators, presence enhances both performance measures, whereas immersion influences only subjective performance. The direct effect of the display modality becomes non-

[3] This essay has been published in: Lauer, D., Stoetzer, J.-C., Weber, N., Weiß, F., Buck, C., and Guggenberger, T. (2026). From Flat Screens To Immersive Virtual Reality: How Virtual Reality Influences Subjective and Objective Performance In Digital Sports. ECIS 2026 Proceedings. 6. https://aisel.aisnet.org/ecis2026/esports/esports/6

significant, indicating that performance improvements stem from players' experience of digital sports rather than from VR technology itself. Extending prior work that mainly examined subjective or isolated performance dimensions, this study considers both subjective and objective performance from a holistic perspective. The findings suggest that such a display modality shift could enhance players' performance.

Keywords**:** Virtual Reality, Immersive Platforms, Digital Sports, Performance, Experiment.

Proactivity and Resilience: An Examination of Strategic Foundations for Cloud Security from an Organization Theory Perspective [4]

Authors

Jacqueline Strobel, Florian Lennart Weiß, Michael Bitzer, Björn Häckel, and Nils Urbach.

Abstract

This essay analyzes how organizations must strategically reconfigure their cloud security approaches in response to increasingly heterogeneous, distributed IT architectures and evolving cyber threats. While cloud computing has become a foundational enabler of digitalization, its complexity introduces novel security challenges that cannot be adequately addressed by traditional, primarily preventive and reactive security measures. Existing literature on cloud security and resilience was found to be rather fragmented and techno-centric, rarely integrating organizational theory to capture the socio-technical foundations of proactive and resilient (cloud) security approaches. The study aims to close this gap by developing a framework that structures fundamental changes for cloud security across five organizational dimensions.

The authors adopt a qualitative research approach and the method by Gioia et al. (2013) combining a structured literature review with 18 semi-structured expert interviews. Data collection is based on semi-structured interviews, and data analysis follows iterative coding and clustering procedures, transforming interview material into first-order concepts, second-order themes, and aggregate dimensions. The framework by Scott (1981) provides the theoretical lens including five dimensions: Environment, Goals, Social Structure, Actors, and Technology and Processes.

The findings reveal that future-proof cloud security requires coordinated changes across all dimensions. More precisely, goal structures need to shift from pursuing maximum security towards combining proactive approaches with resilience, explicitly

[4] At the time of publication of this thesis, this essay is in preparation for submission in a scientific journal. Thus, I provide an extended abstract that covers the essay's content.

acknowledging that incidents are inevitable. Social structures and actor roles must be redesigned to integrate security into cross-functional collaboration and everyday decision-making, overcoming isolated, late-stage security practices. Finally, technology and processes must evolve from isolated, point-solution controls to integrated socio-technical arrangements.

As a theoretical contribution, the essay provides an organizational framework that connects proactivity and resilience extending the framework by Scott (1981) to contemporary cloud environment contexts. It synthesizes resilience and cloud security literature into a coherent structure and derives recommended actions to achieve resilient and proactive cloud security. As a practical contribution, the resulting framework offers a structured approach for organizations to assess their current cloud security posture and to plan holistic transformations, showing where strategic, structural, and technological adaptations are required to ensure resilient and proactive cloud security.

Keywords**:** Cloud Computing, Proactive Cloud Security, Resilience, Qualitative Research.

References

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. *Organ. Res. Methods*, *16*(1), 15–31. https://doi.org/10.1177/1094428112452151

Scott, W. R. (1981). *Organizations: Rational, Natural, and Open Systems* (2nd ed.). Prentice-Hall.

The David-Goliath Gap Throughout The Evolution Of Critical Energy Infrastructure Cybersecurity: An Analysis from a Complex Adaptive Systems Theory Perspective[5]

Authors

Florian Lennart Weiß, Tobias Guggenberger, Alexander Rex, Moritz Schüll, and Nils Urbach.

Abstract

This essay explores how the combined effects of sustainability transformation and digitalization impact the cybersecurity of critical energy infrastructures, with a specific focus on small and medium-sized enterprises (SMEs). Critical energy infrastructures have evolved from centralized, predictable systems based on fossil fuels to decentralized, dynamic architectures relying on renewable energy sources, increasing both the number of digital technologies employed and the diversity of actors involved. Although numerous corresponding technical and overarching strategic solutions were examined in academic literature, it has not sufficiently been investigated on how these developments affect SMEs compared to larger firms.

Using the complex adaptive systems theory as a theoretical lens and based on 19 expert interviews, the authors close this gap by providing eight emerging patterns, illustrating in how far SMEs successfully achieve cybersecurity. This essay contributes a practical review to the technology and strategy dominated discourse, allowing to create new solutions or adapt existing measures to actual requirements. The theoretical and practical contributions include the emerging patterns identified, the structuring of relevant trends, as well as the derivation of relevant implications for practitioners.

Keywords: Cybersecurity, Complex Adaptive Systems Theory, Empirical Research, Energy Infrastructure.

---

[5] This essay has been published in: Weiß, F., Guggenberger, T., Rex, A., and Schuell, M. (2026). The David-Goliath Gap Throughout The Evolution Of Critical Energy Infrastructure Cybersecurity: An Analysis From A Complex Adaptive Systems Theory Perspective. ECIS 2026 Proceedings. 21. https://aisel.aisnet.org/ecis2026/security/security/21

From Planned Security to Reality: Towards an Open-Source Artifact for Automated Cloud Security Auditing on the OS-Level[6]

Authors

Florian Port, Jacqueline Strobel, Florian Lennart Weiß, and Tobias Guggenberger.

Abstract

Cloud architectures have become increasingly complex, making sufficient security hardening crucial with cloud security audits playing an important role in ensuring its continuous effectiveness. However, commercial tools automating these audits are prohibitively expensive, particularly for small and medium-sized enterprises that lack the required resources for adopting such solutions. Further, adequate open-source solutions for critical OS-level audits remain unavailable. To address this gap, the authors follow the Design Science Research paradigm to develop an open-source artifact that automates OS-level cloud security audits building upon Steampipe and osquery. A structured literature review identifies limitations of current cloud security auditing practices and tools, and 14 semi-structured expert interviews allow the formulation of meta-requirements and design objectives. The resulting artifact consists of an audit host and a query service that collaboratively collect and evaluate OS configuration data across Linux and Windows systems in IaaS setups. Ultimately, the evaluation finds that the developed artifact reduces the effort and costs incurred through cloud security audits, enabling organizations to conduct regular, comprehensive assessments that were previously unfeasible. Additionally, the authors review existing literature on transforming traditionally isolated and selective cloud security measures like cloud security audits into proactive, regularly employable ones, and provide five generalizable design principles to support such transformations.

Keywords**:** Cloud Computing, Cloud Security, Security Hardening, Cloud Security Auditing, Design Science Research.

---

[6] At the time of publication of this thesis, this essay is in preparation for submission in a scientific journal. Thus, I provide an extended abstract that covers the essay's content.

Towards Secure Cloud-Computing in FinTechs – An Artefact for Prioritizing Information Security Measures[7]

Authors

Daniel Leuthe, Florian Lennart Weiß, Julian Dersch, and Michael Bitzer.

Abstract

This essay focuses on how FinTechs, which operate under tight budgets and intense competitive pressure, can systematically prioritize information security measures (ISMs) in cloud-based environments. FinTechs leverage cloud computing to rapidly develop and scale innovative financial services, benefiting from flexible, utility-based IT resources while remaining subject to stringent regulatory and security requirements. Due to limited resources and opportunity-driven developments, FinTechs face heightened risks of security incidents and regulatory violations, yet existing research and frameworks do not provide an integrated, FinTech-specific approach to prioritizing ISMs under the shared responsibility model. This study addresses this gap by developing an artifact that generates individual prioritized lists of ISMs for FinTechs. More precisely, the artifact enables FinTechs to provide key characteristics, such as FinTech type, regulatory context, and cloud usage model, and receive a structured, prioritized list of ISMs aligned with their specific threat and responsibility landscape. The evaluation found that the artifact enhances transparency, supports regulatory compliance, and helps focus scarce resources on the most critical measures, instead of ad hoc or checklist-driven security investments. The systematic derivation and iterative refinement of design objectives ensure that the artifact remains both theoretically grounded and practically relevant. As a result, this essay contributes to the conceptualization of integrated ISM prioritization for FinTechs and provides practitioners with a structured prioritization approach based on a standardized logic.

Keywords: FinTech, Cloud Computing, Information Security, Shared Responsibility Model, Regulation.

---

[7] This essay has been published in: Leuthe, D., Weiß, F., Dersch, J., and Bitzer, M. (2024). Towards Secure Cloud-Computing in FinTechs – An Artefact for Prioritizing Information Security Measures. Hawaii International Conference on System Sciences 2024 (HICSS-57). 3. https://aisel.aisnet.org/hicss-57/in/fintech/3