5-11-2023

Chasing Cyber Security Unicorns: A Taxonomy-based Analysis of Cyber Security Start-ups’ Business Models

Florian Schütz
University of Goettingen, florian.schuetz@uni-goettingen.de

Bastian Spierau
University of Goettingen, bastian.spierau@stud.uni-goettingen.de

Florian Rampold
University of Goettingen, florian.rampold@uni-goettingen.de

Robert C. Nickerson
San Francisco State University, rnick@sfsu.edu

Simon Trang
Paderborn University, simon.trang@uni-paderborn.de

Recommended Citation

Schütz, Florian; Spierau, Bastian; Rampold, Florian; Nickerson, Robert C.; and Trang, Simon, "Chasing Cyber Security Unicorns: A Taxonomy-based Analysis of Cyber Security Start-ups’ Business Models" (2023). *ECIS 2023 Research Papers*. 262.
https://aisel.aisnet.org/ecis2023_rp/262

CHASING CYBER SECURITY UNICORNS: A TAXONOMY-BASED ANALYSIS OF CYBER SECURITY START-UPS' BUSINESS MODELS

Research Paper

Schütz, Florian, University of Goettingen, Goettingen, Germany, florian.schuetz@uni-goettingen.de

Spierau, Bastian, University of Goettingen, Goettingen, Germany, bastian.spierau@stud.uni-goettingen.de

Rampold, Florian, University of Goettingen, Goettingen, Germany, florian.rampold@uni-goettingen.de

Nickerson, Robert C., San Francisco State University, San Francisco, USA, rnick@sfsu.edu

Trang, Simon, Paderborn University, Paderborn, Germany, simon.trang@uni-paderborn.de

Abstract

As the number of security incidents increases, a market is emerging for established and new providers of security measures. However, we lack an idea of the business models of cyber security start-ups, which are seen as innovation and security drivers, to protect the economy from existence-threatening incidents. Due to the intangible nature of the cyber threats that security solutions aim to address, previous research on business models cannot be fully transferred. We address this research gap by developing a taxonomy following Nickerson et al. (2013) based on 90 cyber security start-ups and performing a cluster analysis to understand the business activities of cyber security start-ups concerning the protection of critical infrastructures. Our taxonomy will benefit interested decision-makers such as CISOs who want to identify custom-fit cyber security solutions for their organizations. Furthermore, investors and cyber security providers understand the market holistically and can identify innovative product approaches to adopt themselves.

Keywords: Cyber Security Start-up, Business Model, Cyber Security Innovation, Taxonomy.

1 Introduction

In 2021, 157 billion dollars were spent worldwide to protect individual and organizational security (Gartner, 2022). Many organizations, such as the government, financial institutions, or universities, collect, process, and store tremendous amounts of data, including confidential information transmitted via networks (Goutam, 2015). New technologies such as the Internet of Things and Big Data provide many opportunities (Legner et al., 2017) but also make it challenging to safeguard vulnerable assets and confidential information (Bujari et al., 2018). As a result, cyber security has become a challenge all organizations face (Kesswani and Kumar, 2015; Fielder et al., 2016). First, digitization is changing many organizational processes (e.g., cloud applications, process mining) (Legner et al., 2017), and second, the number of cyber security incidents is steadily increasing (Siponen et al., 2014; Romanosky, 2016). The demand for security solutions to secure these processes is also growing by implication (Fielder et al., 2016). Different studies arrive at varying estimates in market sizes, but the basic premise of a growing market for cyber security solutions remains (AustCyber, 2022; Gartner, 2022; DeWalt et al., 2022). With the continuous growth of cyber security budgets (CyberEdge, 2022; ISACA, 2022; Hiscox, 2022) and the rise of both financially and legally significant data breaches (Roumani, 2022; Sen and Borle, 2015), we observe an environment that becomes fruitful for novel business models that are being leveraged by evolving cyber security start-ups (Arora and Nandkumar, 2011). Cyber security start-ups are young enterprises whose business model is enabled by digital technologies and whose solutions are suitable for protecting assets in critical infrastructures. This is worth considering, since start-ups are regarded as innovation drivers and economic factors because they are responsible for economic innovations and are elementary in digital transformation (Richter et al., 2018; Wrobel, 2018). Thereby, the innovative products of start-ups have significantly contributed to the rapid technical progress in both the economy and society (Kollmann et al., 2022). The fact that start-ups also play a significant role in the cyber security sector is evident, for example, in countries like Australia (AustCyber, 2022) or Israel (Barnea, 2018; IVC Research Center, 2022). Also, the German government's start-up strategy has recognized the potential for raising the cyber security level and even envisages supporting interested founders with product ideas in the cyber security sector during their implementation in the start-up ecosystem (Federal Ministry for Economic Affairs and Climate Action, 2022).

However, most cyber security start-ups' solutions are niche products, thus not "one-size-fits-all" solutions, making the market unmanageable and fragmented (Ramsinghani, 2016). Organizations must consequently weigh what risks they face from cyber-attacks and how the damage they cause can be minimized (Fielder et al., 2016; Srinidhi et al., 2015). As cyber security is gaining importance, this area has become one of the most attractive business fields for investors (DeWalt et al., 2022) and founders (Arora and Nandkumar, 2011). Yet, we know little about how cyber security start-ups address these issues. To understand the fragmentation in the cyber security start-up sector, two questions arise:

***RQ1**: How can cyber security start-ups be classified in a taxonomy based on their business models?*

***RQ2**: What business model patterns characterize cyber security start-ups' archetypes?*

We pursue our research objectives by analyzing the characteristics of 90 cyber security start-ups based on their business models using a taxonomy according to Nickerson et al. (2013). The formation of clusters is based on this. To our knowledge, we are the first to define cyber security start-ups in IS research explicitly. Thus, we make two key contributions. Based on our research questions, we make a theoretical contribution to the cyber security and business model literature by identifying the specifics of cyber security start-ups. Also, the taxonomy is relevant to a wide range of stakeholders such as B2B and B2C customers, suppliers, investors, government cyber security agencies, incubators, academia, and cyber security start-ups, as discussed in the following. In the subsequent chapter, we evaluate the conceptual background of the characteristics of start-ups and the role of cyber security in protecting against the monetary and non-monetary consequences of cyber-attacks for society. Based on this, the taxonomy development process and the results of its application will be described. Then, we discuss the emerging findings of our study in terms of extensions of the body of knowledge on the characteristics of cyber security start-ups, the consequences for the protection solutions for concerned consumers and organizations to protect social welfare, and the further potentials of cyber security start-ups in IS research. In the final chapters, we discuss the boundaries of our study and summarize its contributions.

2 Conceptual Background

2.1 Start-ups and their Business Models from a Managerial Point of View

Before classifying underlying business models of cyber security start-ups in a taxonomy, the terms "business model", "start-up" and "cyber security" must first be precisely defined to identify and distinguish suitable objects for our purpose of classification. Regardless of inconsistent definitions, we understand a "business model" as a *"design of organizational structures to enact a commercial opportunity"* (George and Bock, 2011), thus creating value for customers (Osterwalder et al., 2005).

Comparable to the literature in the field of business model research, there is no common sense regarding a universal definition of "start-up" (Zaech and Baldegger, 2017). Following Kollmann et al. (2022), criteria for the designation as a start-up are required to distinguish start-ups from large companies and conventional company foundation processes in particular. Based on Luger and Koo (2005), three criteria should be met to obtain reliable study results when examining start-ups: (1) "newly" established in a specified period, but no mere changes in attributes such as name, address, or legal status, (2) "actively" engaged in trading goods or offering services, (3) "independent" and thus not subsidiaries of existing businesses (Luger and Koo, 2005). Luger and Koo's (2005) criterion of "new" may be specified by Kollmann et al. (2022) with their criterion of "recently founded" as start-ups that are not older than ten years. In particular, the start-up age is often used as the most decisive definitional criterion (Zaech and Baldegger, 2017). In contrast, Luger and Koo's (2005) criterion of "independent" is not part of Kollmann et al.'s (2022) more recent delineation criteria. Instead, Kollmann et al. (2022) emphasizes the need for start-ups to offer highly innovative products or services, with or without technology. However, only a very small proportion of start-up founders consider their business model innovative, i.e., start-ups with a far-reaching R&D component, whereas the vast majority attribute their start-up to the possibilities offered by the Internet or digital technologies (Metzger, 2021). DaSilva and Trkman (2014) understand innovative business models as a company constantly modernizing from its old model to differentiate itself from other market participants and thus create an advantage.

Analogous to the "active" criterion of Luger and Koo (2005), Kollmann et al. (2022) uses a more useful indicator, according to which start-ups must show a planned growth in revenue or employees. Congruently, start-ups are characterized by a native scaling potential to open up new markets and industries internationally and drive established competitors to a constant renewal through their dynamism (Federal Ministry for Economic Affairs and Climate Action, 2022). However, there are interactions, as the growth ambition of entrepreneurs are influenced by the perceived barriers of their market environment and the scalability of their inherent business models (Wallin et al., 2016). Hence, we need to examine the cyber security domain as a market context before we can make statements about the scalability of the business model of cyber security start-ups using the taxonomy development.

2.2 Cyber Security from a Technological Point of View

Although, following Hirschfeld et al. (2020), cyber security can be seen as a fundament for current and future societal development, there seems to be no standard definition of cyber security, and researchers address different aspects of this issue (Humayun et al., 2020). However, especially when experts from various domains such as computer science, risk science, or management collaborate, a shared and inherent understanding of cyber security is needed in the face of increasing cyber threats (Cains et al., 2022). Schatz et al. (2017) conducted a semantic similarity analysis and found that one of the most representative terms to define the concept of cyber security is “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets” (International Telecommunication Union, 2008). Although the term cyber security often seems to go hand in hand with (cyber) threat and (cyber) risk (Craigen et al., 2014; Schatz et al., 2017; Strupczewski, 2021), a definitional disentanglement should be made here (Refsdal et al., 2015). Solms and van Niekerk (2013) emphasize that cyber security is about protecting vulnerable assets in the face of multiple cyber threats enabled by information and communication technology (ICT). Insofar as tangible cyber threats (e.g., negligent employees) or intangible cyber threats (e.g., malware) encounter vulnerable assets, this can result in the emergence of cyber risks (Refsdal et al., 2015).

Therefore, the National Institute of Standards and Technology (2018) has published a cyber security framework to create awareness of potential risk threats and second, define five application areas for security solutions (i.e., identify [ID], protect [PR], detect [DE], respond [RS], and recover [RC]) to protect critical infrastructure from threats. Since some Cyber Risk Assessment Tools are also guided by the five core functions of the NIST (2018) Framework, identifying vulnerabilities in enterprises (Benz and Chatterjee, 2020), the products and services offered in the cyber security market to reduce vulnerabilities should also be guided by these criteria to support the customer's decision-making process. This is crucial because protecting their assets' availability, integrity, and confidentiality is the critical reason organizations invest in cyber security solutions (Bojanc and Jerman-Blažič, 2008).

2.3 Cyber Security Start-ups as Innovation and Security Driver

The findings from both technological and managerial perspectives support our research process as follows: Although start-ups have been researched on many occasions in IS research, their exact delimitation has remained imprecise to date. Due to the specifics of the cyber security domain (among other things, protecting assets with cyber security products and services against partially intangible cyber threats), generic research results from entrepreneurship or IS research can only be transferred to a limited extent. That's why based on the definitions for "start-up" and "cyber security," "cyber security start-up" is introduced as the term for our research. By cyber security start-ups, we refer to young firms founded less than ten years ago with revenue and/or headcount growth orientation, whose business model is enabled by the Internet and digital technologies, and whose innovative products & services are suitable for protecting critical infrastructure and thus promoting the cyber security of the assets it contains.

Thus, concerning the subsequent development of a taxonomy, our delineation criteria of cyber security start-ups affect whether or not they are included in our analysis. Beyond Kollmann et al. (2022), we also follow Weber et al. (2022), who defined analogous criteria for a study of AI start-up business models. In Table 1, we summarize the criteria that a cyber security start-up must meet to (1) be considered as such according to our initial definition and (2) be included in our taxonomy development.

Topic	Criteria for Inclusion of Companies	Implications for our Study
Founding Year	Not older than ten years, based on Kollmann et al. (2022)	Seeking start-ups that are evolving quickly to meet rapidly changing cyber security needs
Business Model	Have to fit into at least one of the NIST (2018) core functions: ID, PR, DE, RS, or PR	Excluding all companies that do not consider the specifics of the cyber security domain
Growth Orientation	Positive revenue and/or headcount growth (forecast), based on Kollmann et al. (2022)	Ensuring that all companies are growth-oriented apart from innovative products & services
Provided Information	Information on revenue and/or headcount growth must be available in German or English via datasets, websites, or brochures	Ensuring that all companies offer sufficient information to verify their compulsory start-up criteria and to determine their characteristics

Table 1. Criteria for Including Companies [based on Weber et al. (2022) & Kollmann et al. (2022)].

3 Taxonomy Development as Methodology

We methodically use a taxonomy development based on Nickerson et al. (2013) to answer the research question of how cyber security start-ups can be classified based on their business models. Following Glass and Cessey (1995), taxonomies help to provide the necessary generalizability, structuring the existing body of knowledge. Consequently, taxonomies are essential in research and practice because they support users in comprehensibly analyzing complex structures in a particular area of interest (Nickerson et al., 2009), providing users with deeper insight into the specific domain (Nickerson et al., 2013). According to Bailey (1994), a taxonomy is a type of classification that categorizes objects according to their similarities and differences. In summary, taxonomy development as a method is particularly suitable in (1) little-studied research areas and (2) research areas that tend to be heterogeneous (Hengstler et al., 2022). Since cyber security start-ups have played a minor role in research, a taxonomy lends itself to a shared understanding of our research object. Thus, we enable research and practice to have common ground for discussing cyber security start-ups that are understandable and perceived to add value for customers interested in cyber security solutions.

Taxonomies are commonplace in IS research (Szopinski et al., 2019). Researchers often refer to the Nickerson et al. (2013) NVM method (Kundisch et al., 2021; Schöbel et al., 2020). The main reason for using the method, according to Nickerson et al. (2013), is that this approach combines knowledge from multiple sources. In doing so, the knowledge gained initially from the literature can be merged with the knowledge gained from analyzing objects (Nickerson et al., 2013). Based on our review, taxonomies have been used object-specifically to determine general object characteristics across domains and domain-specifically to better understand research objects within domains. Schulze et al. (2021) used the

NVM method to classify Digital Labor Platforms (DLPs) as an example of object-specific taxonomies. They provided an overview of the possible configurations of platform governance. Concerning domain-specific taxonomies, Gimpel et al. (2018) created a taxonomy for consumer-oriented FinTech Start-ups to classify their service offerings. Zeier Röschmann et al. (2022) investigated the characteristics of on-demand insurance offerings as a hybrid, object-specific, and domain-specific taxonomy. The NVM method is also suitable for our study based on the examples above. Thus, we draw on the seven-step taxonomy development process of Nickerson et al. (2013), adopting the best practice realizations of Schulze et al. (2021) and Torno et al. (2021). After the meta-characteristic and ending conditions have been defined, the iterative taxonomy development process starts (Nickerson et al., 2013). The iterative choice between the two possible approaches, *Conceptual-to-Empirical (C2E)* or *Empirical-to-Conceptual* (E2C), is repeated until all ending conditions are met (Torno et al., 2021).

3.1 Determination of Meta-Characteristics & Ending Conditions (Steps 1-2)

As a crucial starting point of taxonomy development, determining a meta-characteristic is essential for identifying adequate, research subject-specific dimensions and characteristics (Nickerson et al., 2013). Nickerson et al. (2013) suggest that meta-characteristics should consider both intended users and related objectives of taxonomies. As the primary purpose of our taxonomy is to obtain a common understanding of cyber security start-ups and provide a tool for cyber security purchasing and investment decisions, we determine the meta-characteristic congruently as *characteristics of cyber security start-ups based on their business models*.

Step 2 is to define the objective and subjective ending conditions that signal the termination of taxonomy development, given the iterative nature of this method (Hengstler et al., 2022). This is necessary to avoid endless development loops and to create a taxonomy characterized by usefulness in the eyes of the target group (Nickerson et al., 2013). Our paper follows the conditions Nickerson et al. (2013) presented, including eight objective ending conditions and another five subjective ending conditions (see Appendix). Furthermore, Nickerson et al. (2013) also specified two conditions for each taxonomy. The first criterion is "mutually exclusive," meaning that each object may be assigned to only one characteristic within a dimension at a time. The second criterion is "collectively exhaustive," meaning that each object can be assigned to at least one feature in a dimension (Nickerson et al., 2013).

3.2 Development Approaches (Steps 3-6)

After the meta-characteristics and ending conditions have been defined, the taxonomy development begins. Beyond Bailey (1994), Nickerson et al. (2013) allow a purposeful combination of the deductive "empirical-to-conceptual" (E2C) and inductive "conceptual-to-empirical" (C2E) approach in the further steps. The decision for one of these paths has to be made anew in each iteration (Step 3) and depends, besides the researcher's knowledge of the domain, mainly on the data availability (Nickerson et al., 2013). If the user has little data but an extensive knowledge base, then the C2E approach is chosen, whereas if the level of knowledge is low, the E2C approach is preferred (Nickerson et al., 2013).

Conceptual-to-Empirical Iterations (Steps 4c-6c). Concerning our research question, the characteristics of start-ups regarding their business models are known to be the subject of research in several research domains, such as IS, entrepreneurship, and finance. However, these interdisciplinary characteristics of cyber security start-ups cannot be determined directly from the previous knowledge base or a single source. Following Nickerson et al. (2013), we used a C2E approach for our first iteration. For this purpose, we conduct a systematic sequential literature review following Webster and Watson (2002), Vom Brocke et al. (2015), and Vom Brocke et al. (2009). So, our first step is to define the search scope (Vom Brocke et al., 2015) and thus address an identified research gap (Webster and Watson, 2002). Considering our C2E iterations, the literature review is used to get an overview of research contributions in taxonomies related to business models, start-ups, or cyber security.

By selecting appropriate sources of search following Vom Brocke et al. (2015), IS research as well as economics databases (i.e., AIS Library, JSTOR, and ScienceDirect) were selected to cover both technological and managerial perspectives. Based on vom Brocke et al. (2015), we then determined our search parameters by using the logical operators "*AND*" and "*OR,*", which resulted in the following search string: *("Taxonomy" AND ("Business model" OR "Startup" OR "Cyber Security")).* Moreover, the parameter "*Taxonomy*" was included and searched for to rule out whether a taxonomy already existed in our field (Vom Brocke et al., 2015; Webster and Watson, 2002). For quality assurance purposes, we included publications of databases of the IS domain, as well as economics databases (i.e., AIS Library, JSTOR, and ScienceDirect) that have achieved at least a "C" ranking at VHB ranking (Heinzl et al., 2018; VHB, 2022). We visualize our results using the PRISMA method according to Moher et al. (2009).

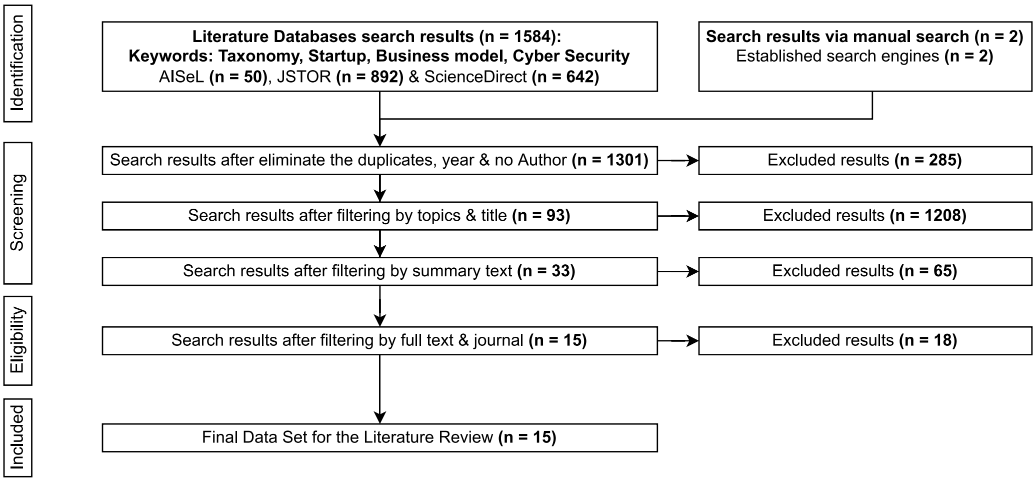

Identification
Literature Databases search results (n = 1584):
Keywords: Taxonomy, Startup, Business model, Cyber Security
AISeL (n = 50), JSTOR (n = 892) & ScienceDirect (n = 642)
Search results via manual search (n = 2)
Established search engines (n = 2)
Screening
Search results after eliminate the duplicates, year & no Author (n = 1301)
Excluded results (n = 285)
Search results after filtering by topics & title (n = 93)
Excluded results (n = 1208)
Search results after filtering by summary text (n = 33)
Excluded results (n = 65)
Eligibility
Search results after filtering by full text & journal (n = 15)
Excluded results (n = 18)
Included
Final Data Set for the Literature Review (n = 15)

Figure 1. Literature Review for the Conceptual-to-Empirical Iteration [based on Moher et al. (2009)].

Among the 1586 research papers identified via the literature review (Figure 1), no taxonomy that addressed the impact of cyber security specifications on the business models of cyber security start-ups could be identified. Furthermore, it could be demonstrated that there is no previous research paper in the databases that (1) meets all the search criteria or at least (2) contains the two critical keywords "start-up" and "cyber security." Finally, 15 research papers were identified that met all criteria and consequently were included in our analysis of potential characteristics of cyber security start-ups.

Empirical-to-Conceptual Iterations (Steps 4e - 6e). Based on the literature review in the previous iteration loop, characteristics of cyber security start-ups have already been identified. The next step is to test these empirically in the form of an E2C approach. In E2C approaches, objects within our research scope must be identified (e.g., using a convenience or systematic sample) and categorized into dimensions and characteristics following the meta-characteristic (Nickerson et al., 2013). As far as this approach is iteratively repeated, new objects can be examined for already identified characteristics. If necessary, new ones can be added, or existing ones can be modified (Nickerson et al., 2013).

Regarding our data collection, we follow Nickerson et al.'s (2013) advice and rely on convenience sampling, which is also evident in much other taxonomy research IS papers such as Rouse (2010), Susha et al. (2018), and Lis and Otto (2021). According to Döring and Bortz (2016), convenience sampling is characterized by the arbitrary selection of objects of study because they may be easier to reach, which covers Nickerson's (2013) reasoning. In our case, we have to identify suitable cyber security start-ups. For example, Weber (2022) uses Crunchbase in a study within the start-up context, as it is one of the most exhaustive databases on this topic. Following Dalle et al. (2017), Crunchbase is a trusted and widely used source of information on the activity and funding of start-ups worldwide. Beyond papers that apply Crunchbase as a tangible data source, such as Liang and Yuan (2016), a meta-study by Besten (2020) already exists that examines the role of Crunchbase in digital entrepreneurship research.

All datasets we used were identified based on the search parameters "Cyber Security," "Start Up," "Seed funding," and "early stage venture funding." As indicated in the figure below, we used nine data sets (Q1-Q9) to identify cyber security start-ups. The four datasets (Q1-Q4) from Crunchbase were exported on 05/29/2022 (Crunchbase, 2022a, 2022b, 2022c, 2022d). Besides Crunchbase, we adopted five external sources (Q5-Q9) to avoid sampling bias (Howarth, 2022; Failory, 2022; Seedtable, 2022; Analytics Insight, 2021; Cyberdefense Magazine, 2022), exported on 07/25/2022. After data cleaning and removing duplicates, 1559 eligible cyber security start-ups remained worldwide (Figure 2), which were prepared for analysis via MAXQDA. Similar to Beinke et al. (2018), in addition to the data from the cyber security start-up datasets (e.g., turnover, headquarter), we also obtained information from the Dealroom (2022) datasets (e.g., headcount) as well as data from the websites and brochures of the respective start-ups. This was needed to derive findings about the start-ups' business models hereafter.

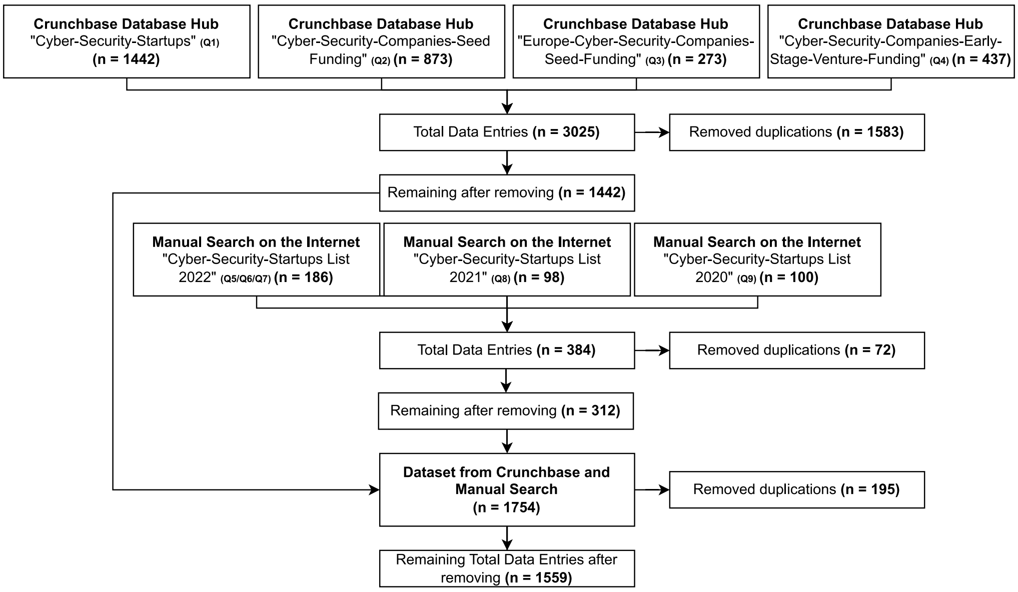

Crunchbase Database Hub "Cyber-Security-Startups" (Q1) (n = 1442)
Crunchbase Database Hub "Cyber-Security-Companies-Seed Funding" (Q2) (n = 873)
Crunchbase Database Hub "Europe-Cyber-Security-Companies-Seed-Funding" (Q3) (n = 273)
Crunchbase Database Hub "Cyber-Security-Companies-Early-Stage-Venture-Funding" (Q4) (n = 437)
Total Data Entries (n = 3025)
Removed duplications (n = 1583)
Remaining after removing (n = 1442)
Manual Search on the Internet "Cyber-Security-Startups List 2022" (Q5/Q6/Q7) (n = 186)
Manual Search on the Internet "Cyber-Security-Startups List 2021" (Q8) (n = 98)
Manual Search on the Internet "Cyber-Security-Startups List 2020" (Q9) (n = 100)
Total Data Entries (n = 384)
Removed duplications (n = 72)
Remaining after removing (n = 312)
Dataset from Crunchbase and Manual Search (n = 1754)
Removed duplications (n = 195)
Remaining Total Data Entries after removing (n = 1559)

Figure 2. Data Collection for Empirical-to-Conceptual Iteration [based on Moher et al. (2009)].

3.3 Cluster Analysis

We carried out a cluster analysis based on our taxonomy to characterize archetypes of cyber security start-ups based on their business models to answer RQ2. Following Jansen and Laatz (2013) and Kaufman and Rousseeuw (2005), a cluster analysis is used to identify sets of classified objects (as in our case, cyber security start-ups) that minimize within-group differences and maximize between-group differences. Methodologically, to determine the clusters, we use an agglomerative hierarchical method according to Ward's method (Blashfield and Aldenderfer, 1978). Although a variety of methods for cluster analysis have been established (Blashfield and Aldenderfer, 1978; Janssen and Laatz, 2013), Ward's method is one of the most common (Tönnissen et al., 2020) and has been used in several IS research taxonomy papers, e.g., Beinke et al. (2018), Remane et al. (2016), or Weber et al. (2022). Based on the mean values of the individual clusters, (1) a calculation of the squared Euclidean distance is performed, and (2) those two clusters with the smallest increase are thereby combined into a new cluster (Wentura and Pospeschill, 2015; Janssen and Laatz, 2013). For this purpose, based on our taxonomy, a similarity matrix as a calculation basis was exported from MAXQDA (version 2020) and transferred to SPSS (version 28) for cluster analysis. Like Beinke et al. (2018), we used a dendrogram and the distance measure to determine the number of clusters. Our approach is supported by Gimpel et al. (2018), finding that the different measures to decide on a cluster solution do not necessarily result in a robust decision. Following Backhaus et al. (2021) and Milligan and Cooper (1985), the number of clusters is intended to compromise the manageability of clusters and object homogeneity within clusters.

3.4 Taxonomy of Cyber Security Start-ups

Our development included five iterations (Figure 3), two with the C2E approach and three with the E2C approach, until the ending conditions were met. All iterations to answer RQ1 are specified below.

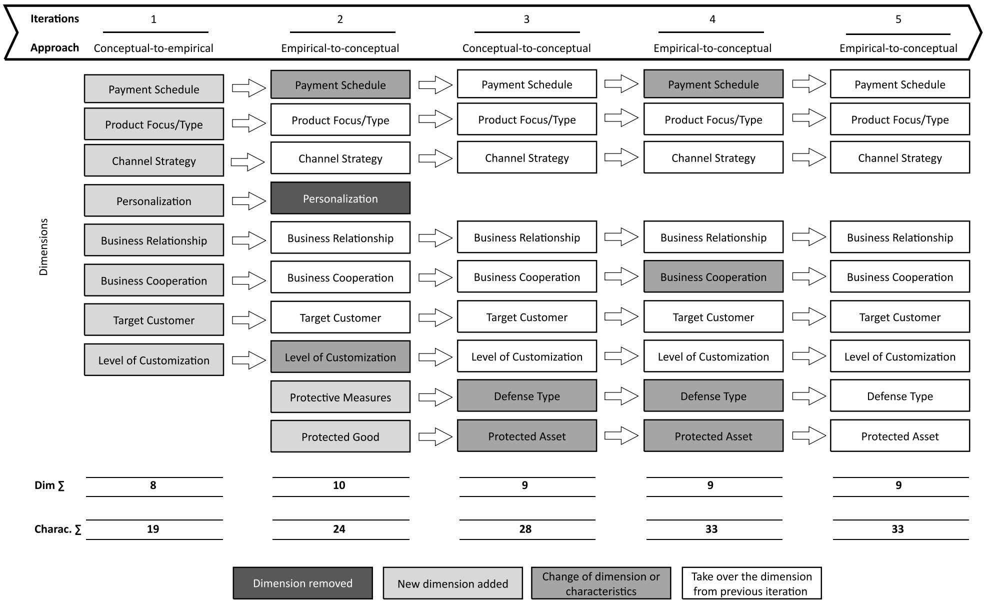


Figure 3. Dimensions of the Iterative Taxonomy Development Process [based on Torno et al. (2021)].

Iteration 1 (C2E). The C2E approach was chosen for the first iteration, as previous research has already dealt with start-ups, business models, and cyber security (cf. chapter 3.2). For instance, Gimpel et al. (2018) have created a taxonomy of FinTech start-ups and their consumer-oriented service offerings by identifying "personalization" as a dimension. Including this dimension coincides with the results from Jonas et al. (2022). Hence, the characteristics "personalized" and "not personalized" are derived. Two dimensions adapted from Jonas et al. (2022) are "business relationship" with "short-term" and "long-term" as well as "Business cooperation" with "stand-alone" and "third-party-integrable." Since both Weber et al. (2022) and Hartmann et al. (2016) outline the payment process, the dimension "payment schedule" with the characteristics "transactional," "subscription," and "one-time payment" is adopted from Gimpel et al. (2018). Analogous to Gimpel et al. (2018), Weber et al. (2022) deal with distribution channel strategy exactly, which we adopt with the two characteristics of "digital exclusive" and "digital non-exclusive." It was also deduced that the business model is characterized by its "product type," that is either "software" or "hardware." Since business models, by definition, aim to address customers, our "target customer" dimension was classified as "B2B" and "B2C" (Hartmann et al., 2016). Finally, the dimension "degree of individualization" with the characteristics "standardized product/service," "tailoring/individualization," and "complete individualization" adapted from Weber et al. (2022) were included if products are subsequently customized.

Iteration 2 (E2C). In the second iteration, a subsample of 30 cyber security start-ups was filtered from the database Q1 and sorted in descending order of "funding amount" to identify companies with the largest sum. As a result, the dimension "personalization" was removed from the taxonomy since, for a large part of the 30 companies, no freely available information could be found, and concrete product inquiries would have had to be directed to customer service. Furthermore, the dimension "payment schedule" was supplemented by the characteristics "commission," "per user," and "free & subscription." Also, the dimension "degree of customization" was extended by the characteristic "none." Additionally, it was found that start-ups offer different types of protection measures against different goods, so the dimensions "protection measure" and "protected good" were included in our taxonomy for the first time.

Iteration 3 (C2E). Given the two dimensions of "protective measure" and "protected good" included in the previous E2C iteration, the C2E approach was again chosen in the third iteration to identify possible characteristics based on the cyber security literature. Kolini and Janczewski (2015) describe "protected good" as an asset. Accordingly, the dimension "protected asset" is designed with the characteristics "hardware," "software," "information," and "people." In contrast, the literature describes the "protected measure" dimension differently. We, therefore, make use of the subdivision "passive defense," "active defense," and "collaborative defense," according to Kolini and Janczewski (2015), and subsume these new characteristics under the new dimension "defense type."

Iteration 4 (E2C). The fourth iteration was carried out as an E2C approach using a subsample from Q2 to check previous modifications from the C2E approach. Although we also sorted by descending "funding amount," this was lower on average in the fourth iteration (approx. eight to fifteen million) than in the second iteration (approx. 200 million to 1.4 billion). In this iteration, we studied 55 start-ups, of which 20 met all the criteria of our cyber security start-up definition. Changes occurred in four dimensions. In the "protected asset" dimension, "digital asset" and "cloud security" were added as new characteristics. An existing characteristic, "information," was redefined and renamed to "information/data." The "payment schedule" dimension has been adjusted by including the characteristic "customized plans." Furthermore, the combined characteristic "hardware & software" was added to the dimension "product focus/type" to meet the mutually exclusive criterion still. The same procedure has been applied in the "business cooperation" dimension, where the new combined characteristic "third-party integrable & stand-alone" has been added.

Iteration 5 (E2C). For the fifth iteration in the form of an E2C approach, start-ups from Q4 were selected because the funding amounts of these cyber security start-ups (approx. 20 to 90 million) are in the mid-range of the funding amounts of Q1 and Q2. This allows us better to cover the range and maturity of cyber security start-ups. In doing so, 40 start-ups were included in the study, and no changes were made to the dimensions and characteristics due to their coding, thus confirming the consistency of our taxonomy. Our development ended after fulfilling the ending conditions (see Appendix).

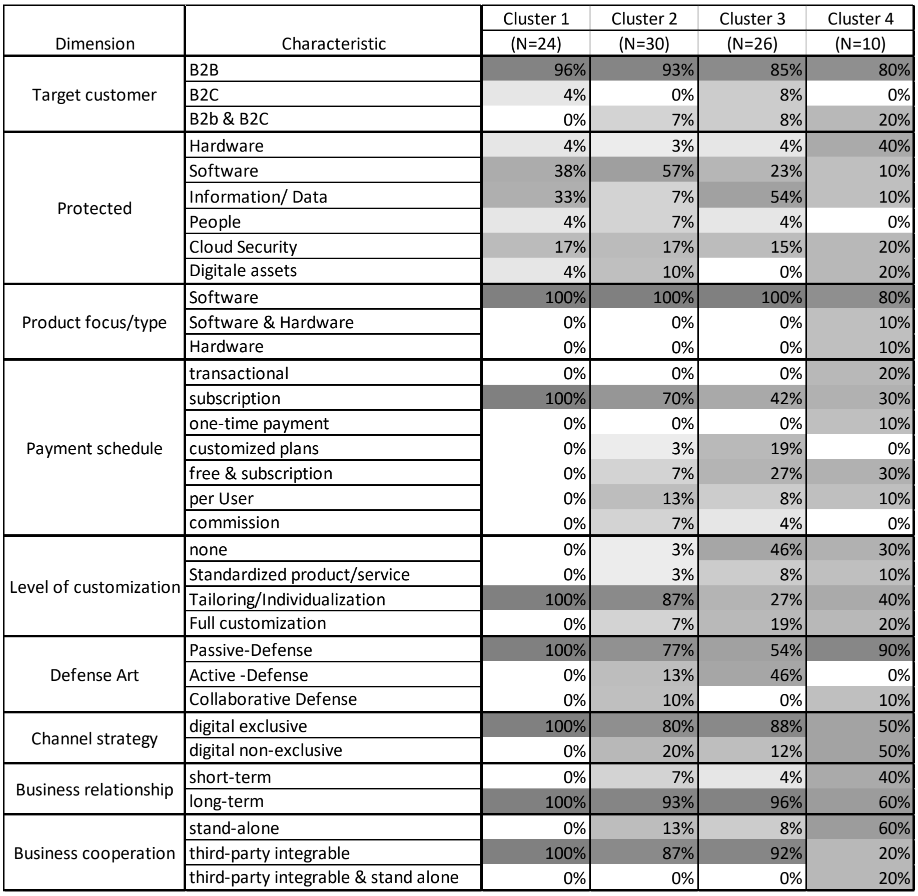
Final Taxonomy. Our taxonomy of cyber security start-ups with all dimensions and the corresponding characteristics is depicted in Table 2, which is intended to answer RQ1. Based on 90 cyber security start-ups in our convenience sample, nine different dimensions and 33 different characteristics can be identified. These represent the differences & characteristics of cyber security start-ups' business models.

Dimension	Characteristics						
Payment Schedule	Transactional (2)	Subscription (59)	One-time Payment (1)	Commission (3)	Per User (7)	Free & Subscription (12)	Customized Plans (6)
Product Focus/Type	Software (88)	Hardware (1)	Hardware & Software (1)				
Channel Strategy	Digital Exclusive (76)	Digital Non-Exclusive (14)					
Business Relationship	Short-Term (7)	Long-Term (83)					
Business Cooperation	Stand Alone (12)	Third-Party Integrable (76)	Third-Party Integrable & Stand-Alone (2)				
Target Customer	B2B (81)	B2C (3)	B2B & B2C (6)				
Level of Customization	Standardized Product/ Service (4)	Tailoring/ Individualization (61)	Full Customization (9)	None (16)			
Defense Type	Passive Defense (70)	Active Defense (16)	Collaborative Defense (4)				
Protected Asset	Hardware (7)	Software (32)	Information/ Data (25)	People (4)	Digital Asset (6)	Cloud Security (16)	

Table 2. Final Taxonomy of Cyber Security Start-ups [based on Torno et al. (2021)].

3.5 Archetypes of Cyber Security Start-ups

Based on the taxonomy, we conducted a cluster analysis that yielded four clusters to address RQ2. This chapter outlines these four clusters (each with between 10 and 30 start-ups) based on their archetypal characteristics (Figure 4), including real-world examples from cyber security start-ups. The naming and characterization of the clusters were done after the clusters were compared to each other. Thereby, the shades of gray visualize the dominance of the particular characteristic within a cluster.



Dimension	Characteristic	Cluster 1 (N=24)	Cluster 2 (N=30)	Cluster 3 (N=26)	Cluster 4 (N=10)
Target customer	B2B	96%	93%	85%	80%
	B2C	4%	0%	8%	0%
	B2b & B2C	0%	7%	8%	20%
Protected	Hardware	4%	3%	4%	40%
	Software	38%	57%	23%	10%
	Information/ Data	33%	7%	54%	10%
	People	4%	7%	4%	0%
	Cloud Security	17%	17%	15%	20%
	Digitale assets	4%	10%	0%	20%
Product focus/type	Software	100%	100%	100%	80%
	Software & Hardware	0%	0%	0%	10%
	Hardware	0%	0%	0%	10%
Payment schedule	transactional	0%	0%	0%	20%
	subscription	100%	70%	42%	30%
	one-time payment	0%	0%	0%	10%
	customized plans	0%	3%	19%	0%
	free & subscription	0%	7%	27%	30%
	per User	0%	13%	8%	10%
	commission	0%	7%	4%	0%
Level of customization	none	0%	3%	46%	30%
	Standardized product/service	0%	3%	8%	10%
	Tailoring/Individualization	100%	87%	27%	40%
	Full customization	0%	7%	19%	20%
Defense Art	Passive-Defense	100%	77%	54%	90%
	Active -Defense	0%	13%	46%	0%
	Collaborative Defense	0%	10%	0%	10%
Channel strategy	digital exclusive	100%	80%	88%	50%
	digital non-exclusive	0%	20%	12%	50%
Business relationship	short-term	0%	7%	4%	40%
	long-term	100%	93%	96%	60%
Business cooperation	stand-alone	0%	13%	8%	60%
	third-party integrable	100%	87%	92%	20%
	third-party integrable & stand alone	0%	0%	0%	20%

Figure 4. Results of the Cluster Analysis [based on Torno et al. (2021)].

Archetype 1 – "Digital Exclusive". This cluster is considered the most dominant and has 100% similarity in eight of the nine dimensions, i.e., their characteristics are the same except for their "target customer" and "protected asset". This cluster was named "Digital Exclusive" because all cyber security start-ups offer their products and/or services on a digitally exclusive basis. Here, the products focus 100% on cyber security software solutions. One example is "SkyFlow," which offers data privacy vault APIs for a safer interaction between digital personal data (SkyFlow, 2022).

Archetype 2 – "Software Security". Although a strong digital strategy can be observed similar to the first cluster, the software distributed by these cyber security start-ups is not so much used to protect information (i.e., modification or deletion of data), but in particular to protect unauthorized access to third-party software. This also means that, for example, more granular payment schedules in the form of "per user" licenses can be applied. Here, almost 60% of the cyber security start-ups offer a solution such as "Cylus", which monitors very specific software for train control and protects it from attackers (Cylus, 2022), or "Guardio", which is specialized in browser security (Guardio, 2022).

Archetype 3 – "Information and Data Security". Analogous to the previous archetype, this cluster includes cyber security start-ups designed to protect a specific asset (here: information/data). One example would be "Persona", which specializes in securing personal customer data (Persona, 2022). Another example is the cyber security start-up "Suridata", which structures and protects sensitive data in unstructured repositories (Suridata, 2022; Israel Colorado Innovation Fund, 2021).

Archetype 4 – "Hardware Security with Standalone Solutions". The fourth and smallest archetype has two distinctive characteristics. On the one hand, 40% of the cyber security start-ups in this archetype offer cyber security solutions for protecting hardware, which is above average compared to other archetypes. For example, the cyber security start-up "Socure" offers products that automatically install Socure's protection software when a device is set up (Socure, 2022). On the other hand, 80% of the cyber security start-ups within this cluster offer a product that is considered as "stand alone" solution in the "business cooperation" dimension. In other words, the product does not require any further integration into another system or environment. A good example is "Ledger", which offers a hardware crypto wallet on which cryptocurrencies of all kinds can be stored and managed (Ledger, 2022a). The wallet is only equipped with software from "Ledger" and therefore does not need any other software from third parties to fulfill its function (Ledger, 2022b).

4 Discussion and Implications

The cluster analysis classified the 90 cyber security start-ups studied into four clusters. Partly, the underlying dimensions of the clusters show a similarity of more than 80% concerning the five dimensions target customer, product type, channel strategy, business relationship, and business cooperation (Figure 4). This can be explained by the attempt of cyber security start-ups to satisfy market demand in the most customer-oriented way possible. At the same time, across archetypes 2-4, it is evident that start-ups are trying to position themselves clearly in terms of protected customer assets, i.e., protect software (2), data (3), or hardware (4). The fact that most cyber security start-ups (90%) target, in particular, B2B customers could be explained by a greater willingness to pay for cyber security solutions on the part of business customers compared with private customers.

As the portfolio of many cyber security start-ups includes software products primarily (98%), their distribution via exclusively digital channels (84%) is inferred. Moreover, the dominant digital distribution strategy could be explained primarily by newly formed cyber security start-ups that choose this path given digital product scaling effects and replicability analogous to the remarks of the Federal Ministry for Economic Affairs and Climate Action (2022). This lowered barrier to entry (esp., archetype 1) makes the market for cyber security solutions lucrative even for resource-constrained start-ups, e.g., in terms of equity or headcount. We noticed that 84% of cyber security start-ups offer their products as "third-party integrable" for interaction with third-party products or objects. This confirms the assumption that organizational cyber security must be understood holistically (King et al., 2018).

Implications for Practice. Our taxonomy provides the relevant dimensions and characteristics useful for understanding cyber security start-ups' business models. Thus, the taxonomy applies to a wide range of stakeholders such as B2B and B2C customers, suppliers, investors, government cyber security agencies, incubators, academia, and cyber security start-ups themselves, as discussed in the following. Considering the tremendous efforts of governments in the domain of cyber security (especially for the protection of critical infrastructures) as well as the implications for society as a whole in the event of cyber-attacks, the characteristics of cyber security start-ups in any form of contractual relationships such as purchase, sale or cooperation must be known to the involved stakeholders. Using our taxonomy, B2B and B2C customers can identify cyber security start-ups with innovative, custom-fit, and budget-compatible cyber security solutions. The fact that the dominant dimension in three of the four clusters is the protected asset can be explained by the peculiarities of the cyber security domain, as an investment in cyber security solutions is particularly justified depending on the asset under threat (Solms and van Niekerk, 2013; McGill et al., 2007). For example, if an elderly private customer is looking for standard antivirus software for his computer, or a global organization is looking for protection for its networked cloud infrastructure, taxonomy users can get decision support in making consumption decisions in the market of cyber security solutions. The core role of assets in achieving security is consistent with current research approaches in competency-based SETA programs (Schütz et al., 2023). In addition to customers, however, suppliers also benefit from our taxonomy, as they can specifically draw on the product focus of the cyber security start-ups in archetype four, focusing on security-related hardware and therefore place increased requirements on the process security of the supply chain as well as and start collaborations with third-parties. However, cyber security start-ups can also use the above taxonomy to benchmark their business model to the market, modify it, or innovate by combining existing characteristics of cyber security start-ups.

Although the NIST (2018) Framework was only considered as an underlying criterion when including cyber security start-ups in the taxonomy – and not as a dimension in the taxonomy itself or when conducting the cluster analysis – a strong trend emerged, however, that could also be relevant to the field of cyber security in general. With a value of 51.1%, cyber security start-ups offer products or services that serve to "protect" a good. Almost tied, the portfolio of cyber security start-ups covers the NIST functions of "detect" at 22.2% and "identify" at 17.8%. Few cyber security start-ups, on the other hand, offer products in the NIST functions "respond" (6.7%) or "recover" (2.2%). This creates the potential for universities and institutes to establish cyber security start-ups in the supply gap through targeted spin-offs and incubators specializing in these hitherto non-dominant cyber solution areas.

Implications for Research. Based on a literature review, it became apparent that cyber security start-ups have been of minor relevance in IS research, despite the threat of cyber-attacks outlined in practice, which can affect organizations and private individuals. First, we contribute to the cyber security literature by defining cyber security start-ups and their business model characteristics as innovation drivers, thus creating a common understanding among researchers. Similar to Hengstler et al. (2022), our taxonomy can serve as a theoretical foundation for more specific research investigating the phenomenon of cyber security start-ups, such as the success factors of cyber security start-ups or the customers' adoption factors of cyber security solutions based on Gimpel el al. (2018). Second, cyber security researchers can identify innovative research potentials through previously disregarded configurations of the taxonomy's characteristics at an early stage. Third, we found that business model research with taxonomies on start-ups in other disciplines inadequately accounts for cyber-related specifics (i.e., vulnerable assets). Although start-ups are not only rising in the cyber security sector, our findings can only partly be applied to other innovative sectors. For instance, the number of start-ups and SMEs that result in disruptive changes is also increasing in the FinTech domain (Li et al., 2017). Thus, even as their business models are also being affected by digitization, our findings on specific dimensions (e.g., protected assets, level of customization) cannot be fully applied to start-ups in these sectors.

5 Limitations and Future Research

Our study's limitations must be considered from both the technological and managerial perspectives when interpreting the findings. After fulfilling all the ending conditions in the fifth iteration, our taxonomy contains 90 cyber security start-ups. Due to the international search scope, the cyber security start-ups examined within our study are not limited to a single geographical area. Although the focus of the taxonomy was on the business models (and thus valid worldwide) of the cyber security start-ups, a specification of our taxonomy for individual countries could be helpful from the perspective of interested customers and investors. One reason is that specific organizations cannot rely on all cyber security start-ups as suppliers due to internal corporate and political regulations (e.g., regarding the protection of critical infrastructure). Another reason for a country-specific taxonomy of cyber security start-ups could be the different economic contributions to GDP. Here, for example, one could geographically refer to the Middle East. Although Israel is a very small country, it received 40% of the global cyber security investment in 2021 and has 33% of global unicorns in cyber security start-ups (Israel National Cyber Directorate, 2022). Hence, Israel's cyber security innovation capability could lead to combinations of characteristics not found in another country-specific sample.

From a managerial perspective, a further limitation is the broad investment spectrum underlying the start-ups examined. Here, so-called "unicorns" (i.e., following Acs et al. (2017), start-ups whose listed value exceeds one billion dollars) were compared with companies with a valuation of just eight million dollars at that time. To exclude large start-ups, the definitional time window of 10 years could be shortened in studies that build on this. Since business models are constantly changing, especially in this day and age due to digital transformation (Klös et al., 2021), a taxonomy with start-ups that are exclusively five years old or younger would be an extension worthy of research concerning emerging archetypes. Likewise, it would be insightful to examine cyber security firms beyond the start-up criteria in terms of their business model and thus elaborate differences. Also, a potential limitation arises from a technology perspective since we have used the NIST (2018) framework to identify start-ups to be included in our taxonomy. Accordingly, our research approach is based on the premise that NIST's established standard reflects the current cyber security landscape. Thus, no relevant start-ups from other threat functions were missed, or start-ups from cyber threat domains no longer relevant were included. Although there is evidence that the taxonomy has been completed, it has not yet been validated by a third party outside the research team. Therefore, we suggest using complementary research methods such as interviews (Szopinski et al., 2019) to identify potential boundary conditions of the taxonomy application and cyber security start-up archetypes. Since the taxonomy was created according to the specifications of Nickerson et al. (2013), it will be possible to add new dimensions and characteristics based on this taxonomy and adapt or delete existing ones (Torno et al., 2021). While our taxonomy represents the current range of cyber security start-ups with security solutions, given a continuously changing cyber threat situation and the resulting adjustments to the providers' product portfolios, continuous adjustments to the taxonomy are feasible.

6 Conclusion

Cyber security start-ups offer a range of products and services as part of their portfolios, which they sell through various distribution channels to B2B and B2C customers. However, the product promise of cyber security start-ups always seems to be to protect their customers from cyber-attacks and their consequences. By analyzing and synthesizing the characteristics of 90 cyber security start-ups based on their business models using a taxonomy according to Nickerson et al. (RQ1), we shed light on exactly this important industry that could save the economy from social welfare losses. We identified nine dimensions with a total of 33 characteristics by conducting conceptual-to-empirical iterations (i.e., systematic literature review with 15 preliminary theoretical works) and empirical-to-conceptual iterations (i.e., content analysis based on public information like websites or information brochures).

Based on the taxonomy, we performed a cluster analysis to answer RQ2, examining archetypes of cyber security start-ups. We identified four different archetypes of business models behind cyber security start-ups: (1) Digital Exclusive, (2) Software Security, (3) Information and Data Security, and (4) Hardware with Standalone Solutions. Overall, it can be said that the characteristics and archetypes provide an initial understanding of the business models of cyber security start-ups. Our taxonomy will benefit interested decision makers such as CISOs who want to identify custom-fit cyber security solutions for their organizations. Furthermore, cyber security solution providers understand the market holistically and can quickly identify innovative product approaches to adopt themselves (and thus become unicorns).

Appendix

Ending Conditions	Iteration	1	2	3	4	5
Def.	Mutually exclusive: In one dimension, an object can have two different characteristics			X	X	X
	Collectively exhaustive: One object must have one characteristic in every dimension		X			X
Objective	All objects (or a representative sample) were evaluated				X	X
	No objects were merged or split		X	X	X	X
	At least one object is assigned to each characteristic in each dimension		X		X	X
	No new dimensions or characteristics were added in the last iteration					X
	In the last iteration, no dimensions or characteristics were merged or split				X	X
	Every dimension is unique and not repeated			X	X	X
	Every combination of characteristics is unique			X	X	X
Subjective	Concise: The quantity of dimensions is limited	X	X		X	X
	Robust: Differentiation among the dimensions and characteristics of the objects			X	X	X
	Comprehensive: Classification and identification for all or a sample of the objects				X	X
	Extendible: Is it adding a new dimension/characteristic in the next iteration possible?	X		X	X	X
	Explanatory: Dimension and characteristic amply explain the object				X	X

Appendix. Ending conditions of the Taxonomy Development Process [based on Torno et al. (2021)].

References

Acs, Z. J., E. Stam, D. B. Audretsch and A. O'Connor (2017). "The lineages of the entrepreneurial ecosystem approach" *Small Business Economics* 49 (1), 1–10.

Analytics Insight (2021). *Q8 - Top 100 Cybersecurity Startups to look out for in 2021*. URL: https://www.analyticsinsight.net/top-100-cybersecurity-startups-to-look-out-for-in-2021 (visited on 09/14/2022).

Arora, A. and A. Nandkumar (2011). "Cash-Out or Flameout! Opportunity Cost and Entrepreneurial Strategy: Theory, and Evidence from the Information Security Industry" *Management Science* 57 (10), 1844–1860.

AustCyber (2022). *Australia's Cyber Security Sector Competitiveness Plan 2022. SCP - Chapter 1 - The Australian cyber security sector today*. URL: https://www.austcyber.com/resources/sector-competitiveness-plan/chapter1 (visited on 11/16/2022).

Backhaus, K., B. Erichson, S. Gensler, R. Weiber and T. Weiber (2021). *Multivariate Analysemethoden. Eine anwendungsorientierte Einführung.* 16th Edition. Wiesbaden: Springer Gabler.

Bailey, K. D. (1994). *Typologies and taxonomies. An introduction to classification techniques.* Thousand Oaks, Calif.: Sage Publ.

Barnea, A. (2018). "Israeli start-ups – especially in cyber security: Can a new model enhance their survival rate?" *Journal of Intelligence Studies in Business* 8 (1), 37–45.

Beinke, J. H., D. N. Ngoc and F. Teuteberg (2018). "Towards a Business Model Taxonomy of Startups in the Finance Sector using Blockchain" *ICIS 2018 Proceedings* (9), 1–9.

Benz, M. and D. Chatterjee (2020). "Calculated risk? A cybersecurity evaluation tool for SMEs" *Business Horizons* 63 (4), 531–540.

Besten, M. L. den (2020). "Crunchbase Research: Monitoring Entrepreneurship Research in the Age of Big Data" *SSRN Electronic Journal*, 1–28.

Blashfield, R. K. and M. S. Aldenderfer (1978). "The Literature On Cluster Analysis" *Multivariate Behavioral Research* 13 (3), 271–295.

Bojanc, R. and B. Jerman-Blažič (2008). "An economic modelling approach to information security risk management" *International Journal of Information Management* 28 (5), 413–422.

Bujari, A., M. Furini, F. Mandreoli, R. Martoglia, M. Montangero and D. Ronzani (2018). "Standards, Security and Business Models: Key Challenges for the IoT Scenario" *Mobile Networks and Applications* 23 (1), 147–154.

Cains, M. G., L. Flora, D. Taber, Z. King and D. S. Henshel (2022). "Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation" *Risk Analysis* 42 (8), 1643–1669.

Craigen, D., N. Diakun-Thibault and R. Purse (2014). "Defining Cybersecurity" *Technology Innovation Management Review* 4 (10), 13–21.

Crunchbase (2022a). *Q1- Cyber Security Startups*. URL: https://www.crunchbase.com/hub/cyber-security-startups (visited on 05/29/2022).

Crunchbase (2022b). *Q2- Cyber Security Companies with Seed Funding*. URL: https://www.crunchbase.com/hub/cyber-security-companies-seed-funding (visited on 05/29/2022).

Crunchbase (2022c). *Q3 - Cyber Security Companies with Early-Stage Venture Funding*. URL: https://www.crunchbase.com/hub/cyber-security-companies-early-stage-venture-funding (visited on 05/29/2022).

Crunchbase (2022d). *Q4 - Europe Cyber Security Companies Seed Funding*. URL: https://www.crunchbase.com/hub/europe-cyber-security-companies-seed-funding (visited on 05/29/2022).

Cyberdefense Magazine (2022). *Q9 - Top 100 Cybersecurity Startups*. URL: https://www.cyberdefensemagazine.com/top-100-cybersecurity-startups/ (visited on 09/14/2022).

CyberEdge (2022). *2022 Cyberthreat Defense Report*. URL: https://www.isc2.org/-/media/ISC2/Research/Cyberthreat-Defense-Report/2021/CyberEdge-2021-CDR-Report-v10--ISC2-Edition.ashx (visited on 11/17/2022).

Cylus (2022). *The Leader in Railway Cybersecurity*. URL: https://www.cylus.com/product (visited on 11/17/2022).

Dalle, J.-M., M. den Besten and C. Menon (2017). "Using Crunchbase for economic and managerial research" *OECD Science, Technology and Industry Working Papers* 2017/08 (8), 1–29.

DaSilva, C. M. and P. Trkman (2014). "Business Model: What It Is and What It Is Not" *Long Range Planning* 47 (6), 379–389.

Dealroom (2022). *Dealroom.co Dashboard. Discover the world's most promising companies and tech ecosystems*. URL: https://app.dealroom.co/dashboard (visited on 11/17/2022).

DeWalt, D., E. McAlpine, M. Tedesco, K. Skirbe, D. Boukouris, A. Krongold, C. McDowell, A. Sztejnberg, V. Yegikyan, R. Joseph and J. Gould (2022). *Cybersecurity Almanac 2022.* Momentum Cyber. URL: https://momentumcyber.com/docs/Yearly/2022_Cybersecurity_Almanac_Public_Edition.pdf (visited on 11/16/2022).

Döring, N. and J. Bortz (2016). *Forschungsmethoden und Evaluation in den Sozial- und Humanwissenschaften.* 5th Edition. Berlin, Heidelberg: Springer.

Failory (2022). *Q6 - 135 Startups in the Cyber Security Industry*. URL: https://www.failory.com/startups/cyber-security (visited on 09/13/2022).

Federal Ministry for Economic Affairs and Climate Action (BMWK) (2022). *Die Start-up-Strategie der Bundesregierung*. URL: https://www.bmwk.de/Redaktion/DE/Publikationen/Existenzgruendung/start-up-strategie-der-bundesregierung.pdf?__blob=publicationFile&v=10 (visited on 11/16/2022).

Fielder, A., E. Panaousis, P. Malacaria, C. Hankin and F. Smeraldi (2016). "Decision support approaches for cyber security investment" *Decision Support Systems* 86, 13–23.

Gartner (2022). *Gartner Identifies Three Factors Influencing Growth in Security Spending*. URL: https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i (visited on 11/16/2022).

George, G. and A. J. Bock (2011). "The Business Model in Practice and its Implications for Entrepreneurship Research" *Entrepreneurship Theory and Practice* 35 (1), 83–111.

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

Glass, R. L. and I. Vessey (1995). "Contemporary application-domain taxonomies" *IEEE Software* 12 (4), 63–76.

Goutam, R. K. (2015). "Importance of Cyber Security" *International Journal of Computer Applications* 111 (7), 14–17.

Guardio (2022). *Safe web, Great technology*. URL: https://guard.io/tech/ (visited on 11/17/2022).

Hartmann, P. M., M. Zaki, N. Feldmann and A. Neely (2016). “Capturing value from big data – a taxonomy of data-driven business models used by start-up firms” *International Journal of Operations & Production Management* 36 (10), 1382–1406.

Heinzl, A., W. van der Aalst and M. Bichler (2018). “Why the Community Should Care About Technology-Centric Journal Rankings” *Business & Information Systems Engineering* 60 (2), 91–93.

Hengstler, S., R. C. Nickerson and S. Trang (2022). “Towards a Taxonomy of Information Security Policy Non-Compliance Behavior” *HICSS 2022 Proceedings*, 4826–4835.

Hirschfeld, A., J. Gilde and V. Walk (2020). *Cyber security an der RUHR. Startups als Treiber digitaler Sicherheit.* Bundesverband Deutsche Startups e.V. URL: https://startupverband.de/fileadmin/startupverband/mediaarchiv/research/innovation_ruhr/ruhr_cybersecurity_2020.pdf (visited on 03/23/2023).

Hiscox (2022). *Hiscox Cyber Readiness Report 2022.* Hiscox. URL: https://www.hiscoxgroup.com/sites/group/files/documents/2022-05/22054%20-%20Hiscox%20Cyber%20Readiness%20Report%202022-EN_0.pdf (visited on 11/16/2022).

Howarth, J. (2022). *Q5 - Top 20 Cybersecurity Startups to Watch in 2022*. URL: https://explodingtopics.com/blog/cybersecurity-startups (visited on 09/15/2022).

Humayun, M., M. Niazi, N. Z. Jhanjhi, M. Alshayeb and S. Mahmood (2020). “Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study” *Arabian Journal for Science and Engineering* 45 (4), 3171–3189.

International Telecommunication Union (ITU) (2008). *ITU-T Recommendation X.1205 (04/2008).* Series X: Data Networks, Open System Communications and Security. URL: https://www.ccdcoe.org/uploads/2018/10/ITU-080418-RecomOverviewOfCS.pdf (visited on 03/26/2023).

ISACA (2022). *State of Cybersecurity 2022. Global Update on Workforce Efforts, Resources and Cyberoperations*. URL: https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/white-papers/state-of-cybersecurity-2022_whpsc22_res_eng_0322.pdf (visited on 11/17/2022).

Israel Colorado Innovation Fund (ICI Fund) (2021). *Suridata.ai Closes Seed Round led by the Israel – Colorado Innovation Fund*. URL: https://www.globenewswire.com/en/news-release/2021/01/26/2164658/0/en/Suridata-ai-Closes-Seed-Round-led-by-the-Israel-Colorado-Innovation-Fund.html (visited on 03/26/2023).

Israel National Cyber Directorate (INCD) (2022). *Israeli Cyber Security Industry Continued to Grow in 2021: Record of $8.8 Billion Raised*. URL: https://www.gov.il/en/departments/news/2021cyber_industry (visited on 11/14/2022).

IVC Research Center (2022). *Israeli Tech Review: Q3 2022*. URL: https://www.ivc-online.com/LinkClick.aspx?fileticket=d5lfCuaQqpo%3D&portalid=0&timestamp=1666505893828 (visited on 11/16/2022).

Janssen, J. and W. Laatz (2013). “Clusteranalyse”. In J. Janssen and W. Laatz (eds.) *Statistische Datenanalyse mit SPSS. Eine anwendungsorientierte Einführung in das Basissystem und das Modul Exakte Tests*. 8th Edition, pp. 489–519. Berlin, Heidelberg: Springer Gabler.

Jonas, C. M., A. M. Oberländer, K. Schmitt and S. Wethmar (2022). “Demystifying Industrial Internet of Things start-ups – A multi-layer taxonomy” *Wirtschaftsinformatik 2022 Proceedings* (11).

Kaufman, L. and P. J. Rousseeuw (2005). *Finding Groups in Data*. *An Introduction to Cluster Analysis.* Hoboken, NJ, USA: John Wiley & Sons, Inc.

Kesswani, N. and S. Kumar (2015). “Maintaining Cyber Security: Implications, Cost and Returns”. In: *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*. Ed. by D. Burley, I. R. Guzman, D. P. Manson, L. E. Potter. New York: ACM, pp. 161–164.

King, Z. M., D. S. Henshel, L. Flora, M. G. Cains, B. Hoffman and C. Sample (2018). “Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment” *Frontiers in Psychology* 9, 1–19.

Klös, H.-P., R. Neuburger, T. Sattelberger and D. Werner (2021). “Geschäftsmodelle und berufliche Bildung im digitalen Wandel” *IW-Policy Paper* (9), 1–32.

Kolini, F. and L. Janczewski (2015). “Cyber Defense Capability Model: A Foundation Taxonomy” *CONF-IRM 2015 Proceedings* (32).

Kollmann, T., C. Strauß, A. Pröpper, C. Faasen, A. Hirschfeld, J. Gilde and V. Walk (2022). *Deutscher Startup Monitor 2022. Innovation – gerade jetzt!* Berlin: Bundesverband Deutsche Startups e. V.

Kundisch, D., J. Muntermann, A. M. Oberländer, D. Rau, M. Röglinger, T. Schoormann and D. Szopinski (2021). “An Update for Taxonomy Designers” *Business & Information Systems Engineering* 64, 421–439.

Ledger (2022a). *Der intelligentest Weg, ihre Kryptowährung abzusichern*. URL: https://www.ledger.com/de (visited on 11/17/2022).

Ledger (2022b). *Download and Install Ledger Live*. URL: https://support.ledger.com/hc/en-us/articles/4404389606417-Download-and-install-Ledger-Live?docs=true (visited on 11/17/2022).

Legner, C., T. Eymann, T. Hess, C. Matt, T. Böhmann, P. Drews, A. Mädche, N. Urbach and F. Ahlemann (2017). “Digitalization: Opportunity and Challenge for the Business and Information Systems Engineering Community” *Business & Information Systems Engineering* 59 (4), 301–308.

Li, Y., R. Spigt and L. Swinkels (2017). “The impact of FinTech start-ups on incumbent retail banks’ share prices” *Financial Innovation* 3 (1), 1–16.

Liang, Y. E. and S.-T. D. Yuan (2016). “Predicting investor funding behavior using crunchbase social network features” *Internet Research* 26 (1), 74–100.

Lis, D. and B. Otto (2021). “Towards a Taxonomy of Ecosystem Data Governance” *HICSS 2021 Proceedings*, 6067–6076.

Luger, M. I. and J. Koo (2005). “Defining and Tracking Business Start-Ups” *Small Business Economics* 24 (1), 17–28.

McGill, W. L., B. M. Ayyub and M. Kaminskiy (2007). “Risk analysis for critical asset protection” *Risk Analysis* 27 (5), 1265–1281.

Metzger, G. (2021). “KfW-Gründungsmonitor 2021. Gründungstätigkeit 2020 mit Licht und Schatten: Corona-Krise bringt Tiefpunkt im Vollerwerb, birgt für viele aber auch Chancen” *KfW Research*, 1–15.

Milligan, G. W. and M. C. Cooper (1985). “An examination of procedures for determining the number of clusters in a data set” *Psychometrika* 50 (2), 159–179.

Moher, D., A. Liberati, J. Tetzlaff and D. G. Altman (2009). “Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement” *The BMJ* 339 (b2535), 1-8.

National Institute of Standards and Technology (NIST) (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.* National Institute of Standards and Technology (NIST).

Nickerson, R. C., U. Varshney and J. Muntermann (2013). “A method for taxonomy development and its application in information systems” *European Journal of Information Systems* 22 (3), 336–359.

Osterwalder, A., Y. Pigneur and C. L. Tucci (2005). "Clarifying Business Models: Origins, Present, and Future of the Concept" *Communications of the Association for Information Systems* 16 (1), 1–25.

Persona (2022). *Security and privacy are not a feature. They're our identity.* URL: https://withpersona.com/security (visited on 11/17/2022).

Ramsinghani, M. (2016). *Cockroaches Versus Unicorns: The Golden Age Of Cybersecurity Startups*. URL: https://techcrunch.com/2016/01/06/cockroaches-vs-unicorns-the-golden-age-of-cybersecurity-startups/?guccounter=1 (visited on 11/17/2022).

Refsdal, A., B. Solhaug and K. Stølen (2015). *Cyber-Risk Management.* Cham, Heidelberg, New York, Dordrecht, London: Springer International Publishing.

Remane, G., R. Nickerson, A. Hanelt, J. F. Tesch and L. M. Kolbe (2016). "A Taxonomy of Carsharing Business Models" *ICIS 2016 Proceedings* (18), 1–19.

Richter, N., P. Jackson and T. Schildhauer (2018). "Entrepreneurial Behaviour and Startups: The Case of Germany and the USA". In N. Richter, P. Jackson and T. Schildhauer (eds.) *Entrepreneurial Innovation and Leadership*, pp. 1–14. Cham: Springer International Publishing.

Romanosky, S. (2016). "Examining the costs and causes of cyber incidents" *Journal of Cybersecurity* 2 (2), 121-135.

Roumani, Y. (2022). "Detection time of data breaches" *Computers & Security* 112 (102508), 1–14.

Rouse, A. C. (2010). "A Preliminary Taxonomy of Crowdsourcing" *ACIS 2010 Proceedings* (76), 1–10.

Schatz, D., R. Bashroush and J. Wall (2017). "Towards a More Representative Definition of Cyber Security" *The Journal of Digital Forensics, Security and Law* 12 (2), 53–74.

Schöbel, S. M., A. Janson and M. Söllner (2020). "Capturing the complexity of gamification elements: a holistic approach for analysing existing and deriving novel gamification designs" *European Journal of Information Systems* 29 (6), 1–28.

Schulze, L., M. Trenz and R. C. Nickerson (2021). "Fingers in the Pie: Characterizing Decision Rights Partitioning on Digital Labor Platforms" *ICIS 2021 Proceedings* (1), 1–17.

Schütz, F., F. Rampold, K. Masuch, P. Köpfer, D. Mann, J. Warwas and S. Trang (2023). "Bridging the Gap between Security Competencies and Security Threats: Toward a Cyber Security Domain Model" *HICSS 2023 Proceedings*, 6118–6127.

Seedtable (2022). *Q7 - 31 Cybersecurity Startups to Watch in 2022*. URL: https://www.seedtable.com/startups-cybersecurity (visited on 09/14/2022).

Sen, R. and S. Borle (2015). "Estimating the Contextual Risk of Data Breach: An Empirical Approach" *Journal of Management Information Systems* 32 (2), 314–341.

Siponen, M., M. Adam Mahmood and S. Pahnila (2014). "Employees' adherence to information security policies: An exploratory field study" *Information & Management* 51 (2), 217–224.

SkyFlow (2022). *What if privacy had an API?* URL: https://www.skyflow.com (visited on 11/17/2022).

Socure (2022). *Identity Starts Here*. URL: https://www.socure.com/ (visited on 11/17/2022).

Solms, R. von and J. van Niekerk (2013). "From information security to cyber security" *Computers & Security* 38, 97–102.

Srinidhi, B., J. Yan and G. K. Tayi (2015). "Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors" *Decision Support Systems* 75, 49–62.

Strupczewski, G. (2021). “Defining cyber risk” *Safety Science* 135 (105143).

Suridata (2022). *No-code SaaS Security, Visibility and Control*. URL: https://www.suridata.ai (visited on 11/17/2022).

Susha, I., M. Janssen and S. Verhulst (2018). “Data Collaboratives as a New Frontier of Cross-Sector Partnerships in the Age of Open Data: Taxonomy Development” *HICSS 2017 Proceedings*, 2691–2700.

Szopinski, D., T. Schoormann and D. Kundisch (2019). “Because your taxonomy is worth it: Towards a framework for taxonomy evaluation” *ECIS 2019 Research Papers* (104), 1–20.

Tönnissen, S., J. H. Beinke and F. Teuteberg (2020). “Understanding token-based ecosystems – a taxonomy of blockchain-based business models of start-ups” *Electronic Markets* 30 (2), 307–323.

Torno, A., O. Werth, R. C. Nickerson, M. H. Breitner and J. Muntermann (2021). “More than Mobile Banking - A Taxonomy-based Analysis of Mobile Personal Finance Applications” *PACIS 2021 Proceedings* (179), 1–14.

VHB (2022). *VHB-JOURQUAL3 (2015) - Gesamtliste*. URL: https://vhbonline.org/vhb4you/vhb-jourqual/vhb-jourqual-3/gesamtliste (visited on 03/25/2023).

Vom Brocke, J., A. Simons, B. Niehaves, K. Reimer, R. Plattfaut and A. Cleven (2009). “Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process” *ECIS 2009 Proceedings* (161), 1–12.

Vom Brocke, J., A. Simons, K. Riemer, B. Niehaves, R. Plattfaut and A. Cleven (2015). “Standing on the Shoulders of Giants. Challenges and Recommendations of Literature Search in Information Systems Research” *Communications of the Association for Information Systems* 37 (9), 206–220.

Wallin, A., K. Still and K. Henttonen (2016). “Entrepreneurial Growth Ambitions: The Case of Finnish Technology Startups” *Technology Innovation Management Review* 6 (10), 5–16.

Weber, M., M. Beutter, J. Weking, M. Böhm and H. Krcmar (2022). “AI Startup Business Models” *Business & Information Systems Engineering* 64 (1), 91–109.

Webster, J. and R. T. Watson (2002). “Analyzing the Past to Prepare for the Future. Writing a Literature Review” *MIS Quarterly* 26 (2), xiii–xxiii.

Wentura, D. and M. Pospeschill (2015). *Multivariate Datenanalyse. Eine kompakte Einführung.* Wiesbaden: Springer Fachmedien.

Wrobel, M. (2018). “Do You Have What It Takes to Become an Internet Entrepreneur? The Key Competencies of Successful Founders”. In N. Richter, P. Jackson and T. Schildhauer (eds.) *Entrepreneurial Innovation and Leadership*, pp. 51–63. Cham: Springer International Publishing.

Zaech, S. and U. Baldegger (2017). “Leadership in start-ups” *International Small Business Journal: Researching Entrepreneurship* 35 (2), 157–177.

Zeier Röschmann, A., M. Erny and J. Wagner (2022). “On the (future) role of on-demand insurance: market landscape, business model and customer perception” *The Geneva Papers on Risk and Insurance - Issues and Practice* 47, 603–642.