Organizational aspects of cybersecurity in German family firms – Do opportunities or risks predominate?

Patrick Sven Ulrich
Aalen University of Applied Sciences, Aalen, Germany and University of Bamberg, Bamberg, Germany, and
Alice Timmermann and Vanessa Frank
Aalen University of Applied Sciences, Aalen, Germany

Received 24 March 2021
Revised 11 October 2021
18 October 2021
26 October 2021
Accepted 2 November 2021

Abstract

Purpose – The starting point for the considerations the authors make in this paper are the special features of family businesses in the area of management discussed in the literature. It has been established here that family businesses sometimes choose different organizational setups than nonfamily businesses. This has not yet been investigated for cybersecurity. In the context of cybersecurity, there has been little theoretical or empirical work addressing the question of whether the qualitative characteristics of family businesses have an impact on the understanding of cybersecurity and the organization of cyber risk defense in the companies. Based on theoretically founded hypotheses, a quantitative empirical study was conducted in German companies.

Design/methodology/approach – The article is based on a quantitative-empirical survey of 184 companies, the results of which were analyzed using statistical-empirical methods.

Findings – The article asked – based on the subjective perception of cybersecurity and cyber risks – to what extent family businesses are sensitized to the topic and what conclusions they draw from it. An interesting tension emerges: family businesses see their employees more as a security risk, but do less than nonfamily businesses in terms of both training and organizational establishment. Whether this is due to a lack of technical or managerial expertise, or whether family businesses simply think they can prevent cybersecurity with less formal methods such as trust, is open to conjecture, but cannot be demonstrated with the research approach taken here. Qualitative follow-up studies are needed here.

Originality/value – This paper represents the first quantitative survey on cybersecurity with a specific focus on family businesses. It shows tension between awareness, especially of risks emanating from employees, and organizational routines that have not been implemented or established.

Keywords Cybercrime, Cyber risks, Cybersecurity, Family firms, Empirical study, CISO, Germany, CIRP

Paper type Research paper

1. Introduction

Cybersecurity, as a decisive competitive factor, is not only an essential topic for large corporations and companies (Kabanda *et al.*, 2018). Progressive digitization has changed an enormous amount in recent years, and even small and medium-sized enterprises and family businesses are integrating more and more digital tools into almost all processes for value creation (Prügl and Spitzley, 2021). At the same time, however, the use of these tools is also

"The early version of the paper has been presented in the 2021 Hawaii International Conference on System Sciences."

Organizational Cybersecurity Journal: Practice, Process and People
Vol. 2 No. 1, 2022
pp. 21-40
Emerald Publishing Limited
e-ISSN: 2635-0289
p-ISSN: 2635-0270
DOI 10.1108/OCJ-03-2021-0010

making companies a bigger target for external and internal hackers and exposing them to cyberattacks.

Because family businesses have a reputation for particular innovation (Erdogan *et al.*, 2020) and are usually still involved in collaborations (Feranita, 2021), attackers may target their specialized knowledge as well as recognize that family businesses can be a useful conduit to larger organizations through the supply chain. Also, SMEs and family businesses are often said to have insufficient cybersecurity system maturity (Kabanda *et al.*, 2018). Therefore, family businesses are attractive targets for cyberattackers. According to the National Institute of Standards and Technology (NIST), cybersecurity is the "ability to protect or defend the organization from cyberattacks" (Sedgewick, 2014). Failure to protect against cyberattacks can result in business disruption or downtime, as well as significant costs to investigate incidents and recover IT systems.

Claims for damages against companies due to delays in delivery, damage due to loss of data, damage to reputation (Gennen, 2018) or disadvantages due to reduced competitiveness (Gabel *et al.*, 2019) should also not be underestimated. According to the results of a study by the German Association for Information Technology, Telecommunications and New Media e.V. (BITKOM), the overall economic damage caused to companies in Germany by cyberattacks in the last two years amounts to 205.7 billion euros (BITKOM, 2020).

There is a discussion in the literature about the "preparedness" of German companies in general for cyberattacks. Literature reviews (Bartsch and Frey, 2018), as well as empirical data (Kolek, 2018), show that a holistic approach such as COSO (Committee of Sponsoring Organizations of the Treadway Commission) (Rae *et al.*, 2017), ISACA (Schatz *et al.*, 2017) and NIST (National Institute of Standards and Technology) (Shen, 2014) that integrates cybersecurity into organization-wide operations and processes is particularly relevant here. Family businesses also need to take measures not only at the technological level but also at the organizational as well as process level to achieve an appropriate maturity of cybersecurity. The organization can be seen as a system composed of complementary roles. To make cybersecurity effective and avoid breaches, it is not only important to balance the knowledge within different departments of an organization, but furthermore to establish a culture that provides the entire organizational unit with a certain understanding of cybersecurity (Clark *et al.*, 2020). Furthermore, the effectiveness of cybersecurity depends critically on how explicitly tasks are assigned to individual roles and how motivated and capable the holders of those roles are to perform the tasks assigned to them. Therefore, employee performance is a function of both the organization and the individual (Welbourne *et al.*, 1998).

A recent study by the consulting firm KPMG shows that attackers often use human vulnerabilities as a gateway into organizations (KPMG, 2017). Phishing, malware and social engineering deceive employees in the company, put them under pressure, exploit human errors and thus obtain confidential data (Thomas, 2018). Companies need to be aware of these risks in the enterprise and use appropriate measures and processes to prevent certain incidents. As human components such as soft skills and an adapted mindset can be crucial for improved handling of cyber risks, this gap in particular needs to be closed by improved cybersecurity, which especially aims at raising awareness and strengthening user security. As organizational implementation measures to prevent risk and strengthen resilience in the event of a cyberattack, internal rules, such as protocols and policies, are essential to commit members of the organization to certain courses of action (Bayuk *et al.*, 2012).

Structuring in terms of responsibilities, communication and decision-making processes enables decision-makers to take appropriate action and make decisions even under time pressure (Gabel *et al.*, 2019). This is the only way to limit the resulting and ultimately unavoidable damage in the event of a cyberattack and to ensure the fastest possible undisturbed continuation of business operations. To date, there is limited evidence on the perception, prevalence and implementation of an organizational framework for cybersecurity

in family businesses (Ulrich *et al.*, 2021a). However, previous studies in other management areas show that family businesses tend to be less organized than nonfamily businesses, e.g. family businesses use management tools to a lesser extent and are less likely to establish standalone management accounting departments than nonfamily businesses (Becker *et al.*, 2011; Hiebl *et al.*, 2015). They are also less open to new technologies than nonfamily businesses (Arzubiaga *et al.*, 2021).

The focus of this paper is therefore on the following research question:

> Do German family businesses exhibit special features concerning organizational cybersecurity compared to nonfamily businesses?

This paper investigates this question based on an empirical survey of 184 German companies. The remainder of this paper is as follows: Sections 2 and 3 describe the relevant theoretical foundations. Hypotheses are derived on this basis. Section 4 then describes the survey design and the sample before presenting the respective empirical results in Section 5. Section 6 sums up the paper with a discussion and Section 7 contains a conclusion with some limitations.

2. Theoretical insights

> A deeper understanding of family businesses and cybersecurity is necessary to better categorize the various constructs within the scope of this study. These terms have not yet been linked in the literature, or have been linked only insufficiently. Moreover, there are definitely different operationalizations here, so we start with the discussion of family business

2.1 Family businesses

The term "family business" is not uniformly defined in the economic literature (Astrachan *et al.*, 2002), which makes it difficult to quantify. Family businesses can be large as well as small and medium-sized enterprises controlled by a family (Ayyagari *et al.*, 2007). The main distinguishing feature of the criterion for defining family enterprises is the level of ownership of the family (Berrone *et al.*, 2012). According to Koeberle-Schmid *et al.* (2012), a family company can be classified as a family business if at least one family member is an active member of the top management or supervisory board and at least 50% of the company's voting rights are held by the family.

Due to the influence of the respective families, family businesses have some qualitative peculiarities. First, family businesses are known for their long-term orientation compared to other companies (Ward, 1997). This is because many entrepreneurial families focus on passing on the business to the next generation (Vallejo Martos, 2007). Typically, this means that long-term success is given much more weight than short-term profit (Danes *et al.*, 2009). This could have an impact on cybersecurity in that the family business is willing to make a high short-term investment in cybersecurity to protect intangible assets in the long term.

Second, family businesses differ from publicly traded companies in the power or influence of the entrepreneurial family (Villalonga and Amit, 2010). Compared to the power of small shareholders in publicly traded companies, it is significantly greater. The family is thus comparatively well placed to assert its interests in the company. This power of the entrepreneurial family can also have a concrete impact on cybersecurity. In many cases, it enables family members to access company information on an ad hoc basis. For example, if a family member can spontaneously seek a conversation with the Chief Information Security Officer (CISO) (Hooper and McKissack, 2016) or another manager responsible for cybersecurity, the need for formal regular reporting is less.

As a third characteristic, family businesses place more emphasis on non-financial aspects than nonfamily businesses. For example, many family businesses combine the reputation of the company with the reputation of the family. As a result, the non-financial goal of maintaining reputation is given significantly more weight than in nonfamily businesses.

The goal of preserving the company for the next generation and passing it on to the next generation or other goals refers to values within the company and to positive effects of the company on the family (Astrachan *et al.*, 2020), such as strengthening family cohesion. In some cases, it may also be a family goal – without regard to the economic impact – that cooperation within the company is based more on trust and less on control. How cybersecurity is managed is influenced by the specifics of family businesses and may be less formalized than in nonfamily businesses, for example.

With the focus on the subject of cybersecurity, it can be said that despite the increasing importance of the topic, especially in small and medium-sized companies, the establishment of processes and measures for the development of a holistic cybersecurity architecture is handled too carelessly (Benz and Chatterjee, 2020). Family businesses are especially strongly connected with traditions and their history. Therefore, it seems to be more difficult to break old patterns and to proceed innovatively in terms of personnel and organization. Appropriate security systems or security systems, in general, are therefore implemented only hesitantly or not at all in certain companies (Feninger *et al.*, 2019).

2.2 Organizational aspects of cybersecurity

It is necessary to enforce the cybersecurity process at all levels and thus influence the organizational structure (BITKOM, 2020). Different groups of experts need to work together to create both effective and efficient structures for cyber risk management, cybersecurity control and monitoring. The necessary cooperation of all actors involved must be organized in a consistent role and responsibility structure, especially to avoid gaps and frictional losses (Institute of Internal Auditors, 2013).

To ensure that each project process complies with the company's cybersecurity guidelines, which have been issued from the outset, it is first and foremost crucial to establish an organizational framework that is aligned with the company's strategy; the translation of an abstract management task into an operational and structurally manageable material. Depending on the organization's cybersecurity requirements, it is strongly recommended to use frameworks such as COBIT (Control Objectives for Information and Related Technology) (Haes *et al.*, 2013) and COSO as a reference for building an individual framework.

2.2.1 Process. To operate proactive cyber risk management, the introduced process should include the following functions. First of all, it is crucial to perform appropriate activities to identify the occurrence of a cybersecurity event or to determine the key cyber risks, risk appetite, and assessment of controls and vulnerabilities. Therefore, it is primarily necessary to define and understand the business model, business objectives, and assets of the organization to determine the relevance of IT to the business and ultimately agree on a level of cybersecurity (Kosub, 2015). After the identified cyber risks and their relevance to the organization have been analyzed, they must each be quantified, assessed and evaluated in terms of probability of occurrence and potential impact (McKinsey, 2019), e.g. using a risk matrix (Kosub, 2015).

From there, organizational measures can be developed and implemented to address risks that exceed the risk appetite of the organization. It is imperative to continuously monitor and proactively control cyber risks in terms of their relevance to the organization, including scheduled board-level status updates on top cyber risks, treatment strategy and remediation actions (McKinsey, 2019). Additionally, the adequacy of risk management measures must be regularly reviewed (risk control) (Kosub, 2015).

It is essential to develop and implement appropriate activities to take action in response to a detected cybersecurity event.

This includes contingency planning, which, in addition to an emergency team as a core element, includes the response plan for cyber incidents. This plan defines immediate reactions and contains specifications taking into account technical, organizational, communication and legal challenges (Leitner *et al.*, 2018). This creates the prerequisite for the company not being forced to act exclusively in a reactive manner, but rather being able to control and act (Gabel *et al.*, 2019). Also, the internal threat posed by human behavior should not be neglected. Raising the cybersecurity awareness of all employees, e.g. in the form of training and instructions (Wilson and Hash, 2003), should be an essential part of a cross-company security concept. Finally, a set of policies, procedures, guidelines and standards is of little use if they are not used and implemented by employees. In this respect, the establishment of a cybersecurity culture can make a decisive contribution to increasing cyber resilience and steering employee behavior in the right direction (Huang and Pearlson, 2019).

2.2.2 Chief information security officer. To ensure effective and efficient prevention of cyber resilience, it must be regulated and communicated who is responsible for cybersecurity at an operational management level. It should be mandatory to establish a single point of contact for security issues, coordination, management and communication of the information security process (Teufel *et al.*, 2020). In this context, knowledge recording, knowledge sharing and succession planning to avoid critical dependencies on key persons naturally also play a major role (Teufel *et al.*, 2020).

Due to the increasing demands on cybersecurity management and its degree of complexity, more and more companies are not only adapting existing management positions, such as those of the chief information officer (CIO) but are also creating new positions, such as the position of the chief information security officer (CISO) (Fitzgerald, 2007; Bradford *et al.*, 2021). The CISO is usually responsible for implementing the cybersecurity strategy. Thus, the CISO does not only have to take on responsibility as a technical manager but rather as a business visionary, innovator and strategist, driving both change and strategic initiatives (Hooper and McKissack, 2016). A lot of leadership energy must be put into breaking down the cultural barriers between IT and the core organization. CISOs therefore must educate the employees of the business potentials of technology to achieve a change in mindset (Ashenden and Sasse, 2013). For this reason, the CISO should not only be an excellent communicator (Hooper and McKissack, 2016). In this respect expertise, credibility including stature and prestige in the organization, political access to senior management, and control of rewards and sanctions are key success factors (Hardy, 1996).

2.2.3 Cybersecurity awareness. Companies try to address the risks of cyberattacks through various technological and procedural adaptations. However, an approach that attempts to prevent risks arising from such attacks based solely on technological factors does not necessarily create a secure and comprehensive information security environment. Rather, the actual user, i.e. the human factor, also contributes significantly to this. Human factors influence how individuals deal with information security and to what extent they integrate measures and guidelines into their practical actions (Parsons *et al.*, 2010).

Psychological and extrinsic motivational factors make human actions unpredictable and accordingly the human factor is considered the weakest link within the security chain (Happ *et al.*, 2016). Problems of information security can be characterized above all by omissions and errors of employees (Swain and Guttmann, 1983).

Increasingly, studies show the need for qualified specialists, who can also be brought into the company externally if required (Baiden, 2011). The actions of the employees are decisive for the success of cybersecurity measures. Consequently, it is essential to minimize human vulnerabilities, which goes hand in hand with a certain degree of information security awareness. Accordingly, employees should be aware of cyber risks and be familiar with

security measures and actions to be taken in case of damage. Various studies, therefore, investigating the influence of human awareness on the success of security programs (Zwilling *et al.*, 2020) examine the level of knowledge of the test persons and the quality of safety training (Hyla and Fabisiak, 2020) and aim to highlight and combine methods that strengthen the security awareness of employees. In this context, the research shows positive effects especially in the combination of different measures (Abawajy, 2014).

In general, various programs are being researched for training and education of employees, which aim to strengthen user safety. Recommended programs tend to refer specifically to the handling of phishing attacks, whereby the tendency of the test persons' reaction is analyzed and evaluated (Augustine and Dodge, 2006). Phishing is a criminal methodology whereby perpetrators send falsified emails to individuals that contain links to infected websites and have an official character. By clicking on the embedded link, the victim unconsciously allows the perpetrator access to personal information or even access to the entire network of the company in which the recipient is operating (Kratchman *et al.*, 2008).

In connection with phishing and the exploitation of human error sources, social engineering is frequently mentioned in the scientific literature (Wang *et al.*, 2020). While phishing attacks are the gateways for criminals to access sensitive data, social engineering tactics are used as the underlying methodology and act as an enabler. Social engineering challenges the weakest point of the security chain, the human weakness, and tries to gain secret information through contact on a personal level. For this reason, social engineering is an important part of current research (Thomas, 2018).

Clark, Espinosa and DeLone (Clark *et al.*, 2020) conclude that knowledge within organizations in the context of different dimensions of cybersecurity is unevenly distributed between different organizational, technical or non-technical roles. However, to make cybersecurity effective and avoid breaches, it is essential to balance knowledge within several departments of an organization and provide a common understanding of the threats posed by cyberattacks (Clark *et al.*, 2020).

These differences can also occur in small and medium-sized companies and must be reduced to a consensus to deal effectively with cyber risks. Furthermore, Pienta, Tams and Thatcher (Pienta *et al.*, 2020) point out that the factors of trust and attention play an essential role within the framework of cybersecurity awareness and that these factors must be taken into account within the alignment of the internal security infrastructure. The study illustrates the necessity of trust on the one hand and the problem of thoughtless compliance on the other (Pienta *et al.*, 2020).

3. Theoretical basis

Various approaches exist in the literature to explain the behavior of family firms, but so far they have not been considered in an integrated way and most of them have not been applied to the technology context. For this reason, we first present a theoretical framework in the following, which we subsequently supplement with hypotheses to be developed.

3.1 Framework

A possible cause for the existing phenomenon that family businesses are well aware of the importance of cybersecurity, but the degree of implementation of measures and the establishment of systematic cybersecurity management is insufficient, could be due to the so-called "socio-emotional wealth" (SEW) in family businesses (Gómez-Mejía *et al.*, 2007). The inventors of this approach postulate that in family businesses the founding family sometimes

does things that are negative for the company although they know that they should do otherwise (Martínez-Romero and Rojo-Ramírez, 2016). In contrast to previous, more rational approaches such as the theory of planned behavior (Harrison *et al.*, 1997), the SEW goes further in that it does not generally assume that family businesses have a more unprofessional approach. Rather, the point is that family businesses are well aware in the area of methods and instruments that their use can be positive for the company.

It is assumed, however, that the family does not use these instruments in some cases because the formalization that goes along with them makes knowledge available to other decision-makers and therefore the position of the family in the company becomes less important. This has already been researched and documented for aspects such as family business growth (Moreno-Menéndez and Casillas, 2021), the use of management accounting tools (Bisogno and Vaia, 2017) as well as the implementation of new technologies such as artificial intelligence, big data and analytics (Arzubiaga *et al.*, 2021).

The SEW suspects that the family is weighing up the pros and cons and deciding against the continued existence of its own company out of self-interest and thus by deliberately not implementing certain methods and instruments. The origins of the SEW approach are related to the emergence of research contributions from Gómez-Mejia *et al.* (2007), in which nonfinancial questions were explained as the key to the performance of family businesses, that were taken into account by emotional requirements such as reputation issues, the family friendliness itself and their influence on external factors and follow-up discussions (Gómez-Mejía *et al.*, 2007).

Cennamo *et al.* (2012) prove that SEW is the most important characteristic parameter for explaining the behavior of family businesses. Developments in thematically subdivided silos include among others risk management (Gómez-Mejía *et al.*, 2007) and organizational structure (Barros *et al.*, 2017). It is assumed that family businesses have the necessary knowledge in dealing with cybersecurity and see the necessity of establishing a holistic approach but refrain from implementing it for fear of losing control. This should explain why family members occasionally behave opportunistically; they do so to protect their socio-emotional assets, even if this entails financial costs (Hiebl, 2013).

Instead of leveraging managerial levers in a way that builds a cybersecurity culture driving cybersecurity behavior to prevent, detect and respond to cyberattacks effectively, family businesses are often prepared to take considerable business risks by diversifying less, only to preserve SEW as a consequence (Berrone *et al.*, 2012). One reason for this is that owners of a family business often associate their identity with the organization, and they are proud to be part of a family business. Usually, the company even bears the name of the family (Berrone *et al.*, 2012). The possible sources of SEW are manifold, taking into account authority and power, status and prestige, succession and duty as well as capital formation and altruism (Gomez-Mejia *et al.*, 2011).

3.2 Derivation of hypotheses

3.2.1 Fear of losing control. Previous studies show that family businesses devote fewer resources to training (Neckebrouck *et al.*, 2018) and attach less importance to education and have a smaller proportion of managers with a university degree (Cromie *et al.*, 1995). Furthermore, they give less importance to the improvement of detailed and rigorous management planning and are prone to underemployed management accounting techniques (de Lema and Duréndez, 2007). Management accounting techniques are methodically structured tools that solve problems of management accounting and are usually supported by IT in companies. Examples are investment calculations, budgeting, transfer prices and the balanced scorecard. They are also very skeptical when it comes to the adaption of new technologies, which has been shown e.g. for big data (Arzubiaga *et al.*, 2021) and artificial intelligence (Ulrich *et al.*, 2021b).

This lack of formalization is argumentatively transferred to the field of cybersecurity. Even though family businesses may be well aware of the importance of cybersecurity, we, therefore, assume that they are not as well prepared in terms of having implemented a cyber incident response compared to nonfamily businesses due to their fear of losing control. The typical reaction to a cyberattack is a so-called cyber incident response plan (CIRP) (Brooks, 2017). We, therefore, formulate as follows:

H1. Family businesses show lesser rates of implementation of a CIRP than nonfamily businesses.

3.2.2 Lack of awareness of cyber risks. Previous studies show that family businesses are generally less sensitized to risks (Hiebl *et al.*, 2019; Falkner and Hiebl, 2015) and their economic evaluation in the area of risk management (Kraus *et al.*, 2018). This is shown, among other things, by the fact that family businesses, although they are generally more long-term oriented, do not implement this long-term orientation methodically (Camfield and Franco, 2019b). They use fewer methods and instruments such as scenario techniques, sensitivity analyses and simulations. Fluctuation margins are less often taken into account in planning (Ulrich, 2018). For the present study, it is therefore assumed that family businesses are less aware of the significance of cyber risks in the area of cybersecurity and therefore consider them to be strategically less relevant for their company. Quantifiable risks are captured insufficiently, at the most qualitatively clustered. We, therefore, formulate as follows:

H2. Family businesses quantitatively assess cyber risks with less formal methods than nonfamily businesses.

3.2.3 Limited financial resources. In addition to the interest in further training measures for employees in the company, the actual coverage of the need for this must also be analyzed. While nonfamily businesses use their financial resources in an economically target-oriented manner to improve employee education and training, the financial resources of family businesses could be channeled into other areas of the company due to an underlying emotional bias (Gómez-Mejía *et al.*, 2007). Also, family businesses, as described earlier, usually have smaller company sizes and, consequently, limited financial resources for further training of employees (Camfield and Franco, 2019a). The next hypothesis assumes that family enterprises offer less training and educational opportunities than nonfamily enterprises and thus do not sufficiently cover the demand for further training measures. We, therefore, formulate as follows:

H3. Employees in family firms show lower levels in cyber training and education than those in nonfamily firms.

3.2.4 Sensitiveness to address human weakness. However, the appropriate actions of employees are crucial for the success of security measures already implemented. A sufficient sensitization of the employees is essential to minimize human weaknesses and ensures that they are prepared in case of damage (Eminağaoğlu *et al.*, 2009). A lack of training and education indicates a lower cybersecurity awareness among employees. Furthermore, it can be assumed that routines and very hesitantly implemented security measures in family businesses contribute to a reduced level of awareness among employees (Feninger *et al.*, 2019). Consequently, hypothesis H4 will be used to test whether employees in family businesses are less sensitive to security-related issues than employees in nonfamily businesses. We, therefore, formulate as follows:

H4. Employees in family businesses are less sensitized to security-related issues than employees in nonfamily firms.

3.2.5 Hypothesis 5. Previous studies show that family-owned businesses are less likely to establish independent management accounting departments than nonfamily businesses

(Hiebl and Mayrleitner, 2019). The same applies to positions such as Chief Compliance Officer (CCO) (Behringer *et al.*, 2019). The question of whether and to what extent one establishes one's position for a topic has to do with awareness of the topic and also with the priority one gives to the topic. In addition, the fact that there is competition for free financial resources within the company could also play a role. It could be, for example, that in addition to the CISO, the establishment of a Chief Digital Officer (CDO) (Singh *et al.*, 2020) is also being discussed, and possibly only one of the positions is established at the same time.

For the present study, it is therefore assumed that family businesses overall are less differentiated in their organization and therefore do not recruit a CISO either (Ulrich *et al.*, 2021a). We, therefore, formulate as follows:

H5. Family businesses are less likely to hire a CISO than nonfamily businesses.

Within the framework of hypothesis derivation, it has become apparent that family businesses – as we postulate – not only assess the topic area of cybersecurity and the risks arising here differently than nonfamily businesses, but also have different organizational responses to the perceived threat.

4. Research method

The hypotheses derived are subsequently subjected to quantitative empirical testing. For this purpose, a large-scale empirical questionnaire was conducted.

4.1 Data collection

The data collection was carried out using a standardized online questionnaire with open and closed questions. To check the questionnaire, a pre-test with several test persons was first conducted. Two were owners of family businesses, one was the CISO of a family business and one was an IT consultant. Subsequently, the actual survey was conducted between October and December 2019. For this purpose, the e-mail addresses of German companies were randomly selected in advance using the Nexis database, which includes both German family and nonfamily businesses. The study does not claim to be representative; it aims to collect a broad opinion on cybersecurity.

The company sizes were limited to 50 employees and 10,000 workers. A total of 14,495 companies were contacted by email, of which 1,612 e-mails could not be delivered. Thus 12,883 companies received the link to the online survey. The online questionnaire was accessed 415 times during the survey period, which corresponds to a participation rate of 3.22%. 372 companies answered the questions asked, with 188 companies having ended the survey early (usage rate: 89.64%). This brings the sample size to 184 companies and the response rate to 1.43%.

For the study, we conducted a test for non-response bias according to Armstrong/Overton (Armstrong and Overton, 1977) by examining the first and last third of responses for differences in structure and content. There was no evidence of bias. In this context, it should be noted that individual questions may nevertheless be mentioned differently, as the partial non-response (item non-response) was not taken into account in this paper. This is since the questionnaire was deliberately designed without specifying mandatory questions since in some cases very topic-specific and sensitive data were requested. The data were evaluated using Microsoft Excel and SPSS.

4.2 Characterization of the sample

The main structural details of the sample are presented below. 55% of the surveyed companies operate in the legal form of a limited liability company (GmbH), 24% as a limited partnership with a limited liability company as general partner (GmbH & Co. KG), 6% of the

companies to be examined wear the legal form of a stock corporation (AG), 2% are formed as a limited partnership (KG) and 1% as an economic company constituted under civil law (GbR). 11% state that they have a different legal form. 24% of the companies are active in the service sector, 17% in mechanical and plant engineering, and 9% in the automotive industry. 6% of the subject group are logistics companies, 3% medical technicians. The remaining 42% are assigned to another industry. In terms of company size, the surveyed companies have an arithmetic mean of 714 million euros in terms of turnover and an arithmetic mean of 974 employees in terms of staff numbers. 54% of the companies surveyed are family businesses. Therefore, 46% are nonfamily firms. The test persons were also asked to state their position in the company. Of the respondents, 54% are employed in IT. 28% state that they belong to company management. In addition, 4% work in management accounting, 2% in human resources, another 2% in production, and 9% in other corporate areas.

4.3 Independent variables

The methodological principles of the independent variables are discussed below. The independent variable in the study is family influence. There are several operationalizations for this variable in the literature (Westhead and Cowling, 1998; Astrachan *et al.*, 2002). Since the companies in the survey are primarily small and medium-sized enterprises and family businesses, which tend to answer less when questions are too complex, a single-item approach was chosen for the present study. To measure family influence, a 0/1 coded question "Is your company a family business" was used, which yields the variable FAMILY. Of the 184 companies in the study, 106 are family enterprises and 78 are nonfamily enterprises. Measurement with the binary measure is likely to result in lower validity and reliability of measurement. However, empirical studies show that SMEs and family businesses are very rarely willing to answer questions that contain too many and too complex questions and scales (Handler, 1989; Wortman, 1994).

4.4 Dependent variables

The model of the study is based on several independent variables. A different dependent variable was defined for each of the five hypotheses. A simple formative measure at the 0/1 or 1–5 level was mostly used to measure the constructs. On the one hand, this can be justified by the problem already described above that family businesses are not very open to complex scales. On the other hand, there are no established measurement instruments in the literature so far for the topics we investigated. In this respect, the possible loss of validity and reliability was accepted.

For H1 the dependent variable is the existence of a reaction plan (REAC_PLAN). The variable was measured at binary levels 0 = no and 1 = yes. For H2 the dependent variable is whether there are methods for cyber risk assessment (ASSESS_METH). The issue was whether companies were using a cyber risk measurement methodology with categories such as high/medium/low or maturity models. This was also measured in binary on the 0/1 scale. For H3 the dependent variable is TRAIN_LEV. Here, a binary 0/1 level was used to measure whether the companies have a lot of catching up to do in terms of the training and further training of their employees in the area of cybersecurity. For H4 the dependent variable is SENS_ISSUES. Here, the questionnaire used five-level Likert scales from 1 = very low to 5 = very high to ask employees about their awareness of ten aspects, including data protection, Internet security, password security, phishing and social engineering.

An explorative factor analysis was then carried out, as all ten start variables correlate with each other. According to eigenvalue criteria, only one factor was extracted. This factor forms the basis for the variable SENS_ISSUES. For H5 the dependent variable CISO. This variable was again measured in binary at the 0/1 level. Unfortunately, the target group of family

businesses tends to quickly abandon empirical surveys in the case of many multi-item scales or ordinal variables. Measuring several variables using binary constructs is, therefore, a painful but necessary compromise in questionnaire design and evaluation.

4.5 Control variables

As a control variable, as in other organization-related studies (Speckbacher and Wentges, 2012; Schachner *et al.*, 2006; Posch and Speckbacher, 2012), the company size was also chosen as a complexity-generating factor. The size of the enterprise – variable SIZE – was operationalized by the number of employees. The number of employees was surveyed in four classes:

(1) SIZE_99: enterprises with up to 99 employees ($n = 34$);

(2) SIZE_100_999: enterprises with between 100 and 999 employees ($n = 122$);

(3) SIZE_1000_9999: companies with between 1,000 and 9,999 employees ($n = 17$);

(4) SIZE_10000: enterprises with 10,000 or more employees ($n = 4$).

The class of companies with up to 99 employees was chosen as the reference class.

5. Empirical results

Various regression models were used to test the hypotheses depending on the scale level of the dependent variables. The following section first shows the correlations of the variables processed in the study.

5.1 Correlations

Table 1 shows the correlations in the sample. At first glance, family businesses seem to have a response plan less frequently, a method for assessing cyber risks less frequently, and CISO. Companies with more than 1,000 employees are more likely to have formal assessment methods. Companies with more than 1,000 employees also have more frequent CISOs. The emergency response plan, the assessment, and the CISO variable correlate significantly.

5.2 Test of hypothesis 1

A binary logistic regression was created for H1.

The model quality and the explanatory contribution in this model are not particularly good at just 3.4%. Nevertheless, it is shown that family businesses have a significantly lower probability of having an emergency response plan. H1 is confirmed.

Dependent Variable	REAC_PLAN	
Independent Variable	β-Coeff.	Sig.
FAMILY	–0.762	0.021**
SIZE100_999	0.341	0.371
SIZE1000_9999	0.141	0.817
SIZE10000	0.625	0.607
Constant	0.890	0.020
Model fit		
–2LL	228.813	
Cox and Snell R^2	0.034	
Nagelkerkes R^2	0.047	

Table 1.
Correlations in the study

	FAMILY	99	100–999	1000–9999	10000	REAC	ASSESS	TRAIN	SENS	CISO
FAMILY	1	−0.016	0.040	−0.030	−0.023	*−0.169*	0.0218**	0.056	−0.026	−0.0202**
99		1	−0.0751**	−0.0171*	−0.080	−0.060	0.016	−0.123	−0.0160*	−0.124
100–999			1	−0.0448**	−0.0209**	0.051	0.0145*	0.123	−0.024	−0.102
1000–9999				1	−0.048	−0.011	−0.0189*	0.000	0.0186*	0.0171*
10000					1	0.027	−0.141	−0.046	0.0165*	0.0345**
REAC_PLAN						1	−0.0430**	−0.046	0.0148*	0.0182*
ASSESS_METH							1	0.062	−0.0210**	−0.0350**
TRAIN_LEV								1	−0.076	−0.0148*
SENS_ISSUES									1	0.0286**
CISO										1

5.3 Test of hypothesis 2

A binary logistic regression was created for H2.

Family businesses are less likely to have assessment metrics for cyber risk. Larger companies with more than 1,000 employees do. H2 is thus confirmed. Goodness-of-fit for this model, measured with.

Nagelkerkes r^2 is relatively good at 14.9%.

Dependent Variable	ASSESS_METH	
Independent Variable	*β*-Coeff.	Sig.
FAMILY	−1.264	0.005***
SIZE100_999	0.048	0.933
SIZE1000_9999	1.419	0.049**
SIZE10000	2.046	0.078*
Constant	−1.414	0.005
Model fit		
−2LL	140.489	
Cox and Snell R^2	0.086	
Nagelkerkes R^2	0.149	

5.4 Test of hypothesis 3

To test hypothesis 3, a binary logistic regression was applied. Hypothesis 3 does not provide satisfactory results either. The model quality is not sufficient and FAMILY shows no effects. Only the companies in the size category 100–999 employees see a large backlog demand in the training and further training of employees. H3 is therefore also rejected.

Dependent Variable	TRAIN_LEV	
Independent Variable	*β*-Coeff.	Sig.
FAMILY	0.224	0.476
SIZE100_999	0.642	0.083*
SIZE1000_9999	0.468	0.433
SIZE10000	−0.133	0.899
Constant	0.021	0.953
Model fit		
−2LL	235.078	
Cox and Snell R^2	0.021	
Nagelkerkes R^2	0.029	

5.5 Test of hypothesis 4

To test hypothesis 4, a linear regression was applied. The model quality is good. However, the explanatory contribution refers exclusively to the size effects to be found in the model. From 1,000 employees upwards, companies are noticing a greater awareness of cybersecurity and cyber risk issues among their employees. Hypothesis 4 is also rejected, however.

Dependent Variable	SENS_ISSUES			
Independent Variable	*β*-Coeff.	*p*-Value	Tolerance	VIF
FAMILY	−0.019	0.792	0.998	1.002
SIZE100_999	0.134	0.108	0.746	1.340
SIZE1000_9999	0.255	0.002	0.779	1.284
SIZE10000	0.205	0.006	0.931	1.074
Model fit				
R^2	0.079			
Adjusted R^2	0.058			
F (Model, global)	3.820***			

5.6 Test of hypothesis 5

A binary logistic regression was used for hypothesis 5. Model 5 delivers the expected results. Family businesses have significantly less CISO. In contrast, companies with more than 1,000 employees have a CISO more often. H5 is confirmed. Also, the goodness-of-fit – measured with Nagelkerkes r^2 – is relatively good at 25.8%.

Dependent Variable	CISO	
Independent Variable	*β*-Coeff.	Sig.
FAMILY	−1.273	0.007 ***
SIZE100_999	0.709	0.288
SIZE1000_9999	2.003	0.013 **
SIZE10000	23.973	0.999
Constant	−1.995	0.001
Model fit		
−2LL	130.469	
Cox and Snell R^2	0.150	
Nagelkerkes R^2	0.258	

The hypothesis tests show a mixed picture. Family businesses are less likely to have a response plan against cyber risks and also less likely to have formalized assessment methods for these risks. However, the training level of employees is not reported to be lower. Employee awareness of cyber risks is also rated similarly. A difference again arises with the CISO, who exists less frequently in family businesses than in nonfamily businesses.

6. Discussion

This study represents what we believe to be the first international study on the perception and management of cyber risks in family businesses. The main contribution to the literature is the application of the SEW as a theoretical framework to the field of cybersecurity. Contrary to what has been theorized at least so far, family businesses see their employees as even greater security risks than nonfamily businesses. However, the companies do not counter this skeptical assessment with an expected higher investment in employee education and training in this area.

For companies of all sizes, information has become a decisive competitive factor, which they protect intensively. Literature research and empirical data show that this protection must not only meet technical but particularly also organizational requirements. The present study examined the status quo of organizational cybersecurity at 184 German companies. The manuscript thus moves in an interesting field of tension between family businesses, SMEs, organizational routines and cybersecurity. Even though it has already been established that there is still some catching up to do in the area of cybersecurity in the Anglo-American and SME sector, we do not believe that German companies or the subgroup of family businesses have been influenced in this way in the literature to date.

Family businesses should adapt their cybersecurity organization where appropriate. The results show that German companies – at least those companies in the sample that mainly represent small and medium-sized family businesses – are generally not very sensitive to this topic. The hypotheses put forward regarding the family influence have been largely confirmed. Family businesses and nonfamily businesses differ considerably in their assessment of cyber risks.

The same applies to the implementation of a plan to respond to cyber incidents. Furthermore, family businesses are less likely to hire a CISO. This could be the result of a fear of losing control. Family members occasionally behave opportunistically to preserve their socio-emotional assets, even if this involves financial costs. Nevertheless, dealing with one's

level of cybersecurity maturity means that one has to measure something–that one has some defined metrics. This raises awareness.

This is a process that needs to be repeated regularly to reap the full benefits. That's why risk assessment is crucial to prevent the company from being compromised. This includes contingency planning, which includes an emergency team as well as the response plan for cyber incidents as a core element. This plan defines immediate responses and contains specifications taking into account technical, organizational, communication, and legal challenges, which enable decision-makers to take appropriate measures and make decisions even under time pressure.

In addition, there must be someone in addition to top management who assumes responsibility primarily as a change agent. A so-called CISO, which primarily educates employees about the business potential of technology to achieve a change in mentality that overcomes the cultural barriers between IT and the core organization.

As the literature shows, there is a particular need to train employees in areas such as phishing and social engineering. While the literature also frequently assumes psychological backgrounds among employees as sources of error, the present study clearly emphasizes the need for better employee awareness as a solution approach. By sensitizing employees and providing better training within the company, it is possible to reduce human error and to see people less as a source of problems and more as an opportunity for improved cybersecurity.

The results show that nonfamily businesses make a greater contribution to the holistic management of cyber risks and ensure that the process of cybersecurity is enforced at all levels. We, therefore, recommend that further research be conducted in this area to derive measures and, based on this, to develop tools that can help to further develop organizational cybersecurity in family businesses. From a theoretical point of view, it can be seen that the view postulated in the SEW that family businesses sometimes omit organizational aspects and routines to maintain their position in the family network can also be transferred to the area of cybersecurity.

However, if the lack of formal routines in areas such as management accounting or planning can be compensated by informal mechanisms such as trust, there is a suspicion that this will not be as successful for cybersecurity. However, we did not discuss this in the manuscript and unfortunately did not check it in questions and variables in the underlying survey. This should be an exciting question for qualitative and quantitative follow-up studies.

7. Conclusion

This study added an empirical study among German companies to the international discussion on cybersecurity in family businesses. An analysis of the data collected among 184 companies shows that family businesses and nonfamily businesses deal with cyber risks differently *per se* and also find different organizational responses to the corresponding actions. Our study is subject to some limitations. These include the purely empirical approach with a rather low response rate and the focus on German companies. A national qualitative follow-up study, as well as an international quantitative study, will follow.

References

Abawajy, J. (2014), "User preference of cyber security awareness delivery methods", *Behaviour and Information Technology*, Vol. 33 No. 3, pp. 237-248.

Armstrong, J.S. and Overton, T.S. (1977), "Estimating nonresponse bias in mail surveys", *Journal of Marketing Research*, Vol. 14 No. 3, pp. 396-402.

Arzubiaga, U., Diaz-Moriana, V., Bauweraerts, J. and Escobar, O. (2021), "Big data in family firms: a socioemotional wealth perspective", *European Management Journal*, Vol. 39 No. 3, pp. 344-352.

Ashenden, D. and Sasse, A. (2013), "CISOs and organisational culture: their own worst enemy?", *Computers & Security*, Vol. 39, pp. 396-405.

Astrachan, J.H., Klein, S.B. and Smyrnios, K.X. (2002), "The F-PEC scale of family influence: a proposal for solving the family business definition problem1", *Family Business Review*, Vol. 15 No. 1, pp. 45-58.

Astrachan, J.H., Astrachan, C.B., Campopiano, G. and Baù, M. (2020), "Values, spirituality and religion: family business and the roots of sustainable ethical behavior", *Journal of Business Ethics*, Vol. 163 No. 4, pp. 637-645.

Augustine, T. and Dodge, R.C. (2006), "Cyber defense exercise: meeting learning objectives thru competition", *Proceedings of the 10th Colloquium for Information Systems Security Education*, June 5-8, 2006, University of Maryland.

Ayyagari, M., Beck, T. and Demirguc-Kunt, A. (2007), "Small and medium enterprises across the globe", *Small Business Economics*, Vol. 29 No. 4, pp. 415-434.

Baiden, J.E. (2011), "Cyber crimes", available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1873271&__cf_chl_captcha_tk__=pmd_DhnQaC7nFcLhvurw.uOjlv4ZoNnNd6vwYwo3TAXcHv8-1635234788-0-gqNtZGzNAzujcnBszQol.

Barros, I., Hernangómez, J. and Martin-Cruz, N. (2017), "Familiness and socioemotional wealth in Spanish family firms: an empirical examination", *European Journal of Family Business*, Vol. 7 Nos 1-2, pp. 14-24.

Bartsch, M. and Frey, S. (2018), *Cybersecurity Best Practices*, Springer, Wiesbaden.

Bayuk, J.L., Healey, J., Rohmeyer, P., Sachs, M.H., Schmidt, J. and Weiss, J. (2012), *Cyber Security Policy Guidebook*, Wiley, London.

Becker, W., Ulrich, P. and Staffel, M. (2011), "Management accounting and controlling in German SMEs–do company size and family influence matter?", *International Journal of Entrepreneurial Venturing*, Vol. 3 No. 3, pp. 281-300.

Behringer, S., Ulrich, P. and Unruh, A. (2019), "Compliance management in family firms: a systematic literature analysis", *Corporate Ownership and Control*, Vol. 17 No. 1, pp. 140-157.

Benz, M. and Chatterjee, D. (2020), "Calculated risk? A cybersecurity evaluation tool for SMEs", *Business Horizons*, Vol. 63 No. 4, pp. 531-540.

Berrone, P., Cruz, C. and Gomez-Mejia, L.R. (2012), "Socioemotional wealth in family firms: theoretical dimensions, assessment approaches, and agenda for future research", *Family Business Review*, Vol. 25 No. 3, pp. 258-279.

Bisogno, M. and Vaia, G. (2017), "The role of management accounting in family business succession", *African Journal of Business Management*, Vol. 11 No. 21, pp. 619-629.

BITKOM (2020), *Spionage, Sabotage und Wirtschaftsschutz in der vernetzten Welt*, BITKOM, Berlin.

Bradford, M., Taylor, E.Z. and Seymore, M. (2021), "A view from the CISO: insights from the data classification process", *Journal of Information Systems*. doi: 10.2308/ISYS-2020-054.

Brooks, F. (2017), "Why cyber incident response planning is a critical enterprise capability", *Governance Directions*, Vol. 69 No. 6, pp. 343-345.

Camfield, C. and Franco, M. (2019a), "The influence of personal values on family firm succession: a structural model", *International Journal of Entrepreneurial Venturing*, Vol. 11 No. 4, pp. 335-372.

Camfield, C. and Franco, M. (2019b), "Theoretical framework for family firm management: relationship between personal values and professionalization and succession", *Journal of Family Business Management*, Vol. 9 No. 2, pp. 201-227.

Cennamo, C., Berrone, P., Cruz, C. and Gomez–Mejia, L.R. (2012), "Socioemotional wealth and proactive stakeholder engagement: why family–controlled firms care more about their stakeholders", *Entrepreneurship Theory and Practice*, Vol. 36 No. 6, pp. 1153-1173.

Clark, M., Espinosa, J. and Delone, W. (2020), "Defending organizational assets: a preliminary framework for cybersecurity success and knowledge alignment", in Bui, T. (Ed.), *Proceedings of*

the 53rd Hawaii International Conference on System Sciences, Hawaii International Conference on System Sciences.

Cromie, S., Stephenson, B. and Monteith, D. (1995), "The management of family firms: an empirical investigation", *International Small Business Journal*, Vol. 13 No. 4, pp. 11-34.

Danes, S.M., Stafford, K., Haynes, G. and Amarapurkar, S.S. (2009), "Family capital of family firms: bridging human, social, and financial capital", *Family Business Review*, Vol. 22 No. 3, pp. 199-215.

de Lema, D.G.P. and Duréndez, A. (2007), "Managerial behaviour of small and medium-sized family businesses: an empirical study", *International Journal of Entrepreneurial Behavior and Research*, Vol. 13 No. 3, pp. 151-172.

Eminağaoğlu, M., Uçar, E. and Eren, Ş. (2009), "The positive outcomes of information security awareness training in companies–A case study", *Information Security Technical Report*, Vol. 14 No. 4, pp. 223-229.

Erdogan, I., Rondi, E. and Massis, A.de (2020), "Managing the tradition and innovation paradox in family firms: a family imprinting perspective", *Entrepreneurship Theory and Practice*, Vol. 44 No. 1, pp. 20-54.

Falkner, E.M. and Hiebl, M.R.W. (2015), "Risk management in SMEs: a systematic review of available evidence", *The Journal of Risk Finance*, Vol. 16 No. 2, pp. 122-144.

Feninger, M., Kammerlander, N. and de Massis, A. (2019), "Family business innovation: a circular process model", *Family Firms and Institutional Contexts*, Edward Elgar Publishing.

Feranita, F. (2021), "The transaction cost approach to collaborative innovation in family firms: a process of internal collaboration through integration of human assets", *Journal for International Business and Entrepreneurship Development*, Vol. 13 No. 1, pp. 91-113.

Fitzgerald, T. (2007), "Clarifying the roles of information security: 13 questions the CEO, CIO, and CISO must ask each other", *Information Systems Security*, Vol. 16 No. 5, pp. 257-263.

Gabel, D., Heinrich, T. and Kiefner, A. (2019), *Rechtshandbuch Cyber-Security: IT-Sicherheit, Datenschutz, Gesellschaftsrecht, Compliance, M&A, Versicherungen, Aufsichtsrecht, Arbeitsrecht, Litigation*, Fachmedien Recht und Wirtschaft, Deutscher Fachverlag, Frankfurt.

Gennen, K. (2018), "Ausgewählte rechtliche implikationen", *Sicherheitskritische Mensch-Computer-Interaktion*, Springer, pp. 139-162.

Gómez-Mejía, L.R., Haynes, K.T., Núñez-Nickel, M., Jacobson, K.J.L. and Moyano-Fuentes, J. (2007), "Socioemotional wealth and business risks in family-controlled firms: evidence from Spanish olive oil mills", *Administrative Science Quarterly*, Vol. 52 No. 1, pp. 106-137.

Gomez-Mejia, L.R., Cruz, C., Berrone, P. and Castro, J.de (2011), "The bind that ties: socioemotional wealth preservation in family firms", *Academy of Management Annals*, Vol. 5 No. 1, pp. 653-707.

Haes, S.de, van Grembergen, W. and Debreceny, R.S. (2013), "COBIT 5 and enterprise governance of information technology: building blocks and research opportunities", *Journal of Information Systems*, Vol. 27 No. 1, pp. 307-324.

Handler, W.C. (1989), "Methodological issues and considerations in studying family businesses", *Family Business Review*, Vol. 2 No. 3, pp. 257-276.

Happ, C., Melzer, A. and Steffgen, G. (2016), "Trick with treat–Reciprocity increases the willingness to communicate personal data", *Computers in Human Behavior*, Vol. 61, pp. 372-377.

Hardy, C. (1996), "Understanding power: bringing about strategic change", *British Journal of Management*, Vol. 7, pp. S3-S16.

Harrison, D.A., Mykytyn, P.P. Jr and Riemenschneider, C.K. (1997), "Executive decisions about adoption of information technology in small business: theory and empirical tests", *Information Systems Research*, Vol. 8 No. 2, pp. 171-195.

Hiebl, M.R.W. (2013), "Risk aversion in family firms: what do we really know?", *The Journal of Risk Finance*, Vol. 14 No. 1, pp. 49-70.

Hiebl, M.R.W. and Mayrleitner, B. (2019), "Professionalization of management accounting in family firms: the impact of family members", *Review of Managerial Science*, Vol. 13 No. 5, pp. 1037-1068.

Hiebl, M.R.W., Duller, C., Feldbauer-Durstmüller, B. and Ulrich, P. (2015), "Family influence and management accounting usage—findings from Germany and Austria", *Schmalenbach Business Review*, Vol. 67 No. 3, pp. 368-404.

Hiebl, M.R.W., Duller, C. and Neubauer, H. (2019), "Enterprise risk management in family firms: evidence from Austria and Germany", *The Journal of Risk Finance*, Vol. 20 No. 1, pp. 39-58.

Hooper, V. and McKissack, J. (2016), "The emerging role of the CISO", *Business Horizons*, Vol. 59 No. 6, pp. 585-591.

Huang, K. and Pearlson, K. (2019), "For what technology can't fix: building a model of organizational cybersecurity culture", *Proceedings of the 52nd Hawaii International Conference on System Sciences*.

Hyla, T. and Fabisiak, L. (2020), "Measuring cyber security awareness within groups of medical professionals in Poland", in Bui, T. (Ed.), *Proceedings of the 53rd Hawaii International Conference on System Sciences*.

Institute of Internal Auditors (2013), *The Three Lines of Defense in Effective Risk Management and Control*, IIA, Lake Mary, Florida.

Kabanda, S., Tanner, M. and Kent, C. (2018), "Exploring SME cybersecurity practices in developing countries", *Journal of Organizational Computing and Electronic Commerce*, Vol. 28 No. 3, pp. 269-282.

Koeberle-Schmid, A., Witt, P. and Fahrion, H.-J. (2012), "Family business governance als erfolgsfaktor von Familienunternehmen", *Family Business Governance. Erfolgreiche Führung in Familienunternehmen*, 2nd ed., ESV, Berlin, pp. 26-44.

Kolek, E. (2018), "IT-Sicherheit der Digitalisierung in kleinen und mittleren Unternehmen: eine literaturbasierte und empirische Studie von Effekten und Barrieren", *Multikonferenz Wirtschaftsinformatik (MKWI)*, pp. 1706-1717.

Kosub, T. (2015), "Components and challenges of integrated cyber risk management", *Zeitschrift für die gesamte Versicherungswissenschaft*, Vol. 104 No. 5, pp. 615-634.

KPMG (2017), *Neues Denken, Neues Handeln – Insurance Thinking Ahead – Versicherungen im Zeitalter von Digitalisierung und Cyber Studienteil B: Cyber*, KPMG, München.

Kratchman, S., Smith, J.L. and Smith, M. (2008), "The perpetration and prevention of cybercrimes", *Internal Auditing*, Vol. 23 No. 2, pp. 3-12, March/April, available at: SSRN 1123743.

Kraus, S., Kallmuenzer, A., Stieger, D., Peters, M. and Calabrò, A. (2018), "Entrepreneurial paths to family firm performance", *Journal of Business Research*, Vol. 88, pp. 382-387.

Leitner, M., Pahi, T. and Skopik, F. (2018), "Das Konzept von Situationsbewusstsein und Cyber-Lagebildern", *Cyber Situational Awareness in Public-Private-Partnerships*, Springer, pp. 1-41.

Martínez-Romero, M.J. and Rojo-Ramírez, A.A. (2016), "SEW: looking for a definition and controversial issues", *European Journal of Family Business*, Vol. 6 No. 1, pp. 1-9.

McKinsey (2019), "Perspectives on transforming cybersecurity", available at: https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/perspectives-on-transforming-cybersecurity.

Moreno-Menéndez, A.M. and Casillas, J.C. (2021), "How do family businesses grow? Differences in growth patterns between family and non-family firms", *Journal of Family Business Strategy*, Vol. 12 No. 3, 100420.

Neckebrouck, J., Schulze, W. and Zellweger, T. (2018), "Are family firms good employers?", *Academy of Management Journal*, Vol. 61 No. 2, pp. 553-585.

Parsons, K., McCormac, A., Butavicius, M. and Ferguson, L. (2010), *Human Factors and Information Security: Individual, Culture and Security Environment*, Defence Science and Technology Organization, Edinburgh, South Australia.

Pienta, D., Tams, S. and Thatcher, J. (2020), "Can trust be trusted in cybersecurity?", in Bui, T. (Ed.), *Proceedings of the 53rd Hawaii International Conference on System Sciences*.

Posch, A. and Speckbacher, G. (2012), "Führung in Familienunternehmen: besonderheiten der Entscheidungsfindung und Verhaltenssteuerung und deren Auswirkung auf den Unternehmenserfolg", *Zeitschrift für Betriebswirtschaft*, Vol. 82 No. 3, pp. 5-23.

Prügl, R. and Spitzley, D.I. (2021), "Responding to digital transformation by external corporate venturing: an enterprising family identity and communication patterns perspective", *Journal of Management Studies*, Vol. 58 No. 1, pp. 135-164.

Rae, K., Sands, J. and Subramaniam, N. (2017), "Associations among the five components within COSO internal control-integrated framework as the underpinning of quality corporate governance", *Australasian Accounting, Business and Finance Journal*, Vol. 11 No. 1, pp. 28-54.

Schachner, M., Speckbacher, G. and Wentges, P. (2006), "Steuerung mittelständischer Unternehmen: größeneffekte und Einfluss der Eigentums-und Führungsstruktur", *Zeitschrift für Betriebswirtschaft*, Vol. 76 No. 6, pp. 589-614.

Schatz, D., Bashroush, R. and Wall, J. (2017), "Towards a more representative definition of cyber security", *Journal of Digital Forensics, Security and Law*, Vol. 12 No. 2, pp. 53-74.

Sedgewick, A. (2014), "Framework for improving critical infrastructure cybersecurity, version 1.0". doi: 10.6028/NIST.CSWP.02122014.

Shen, L. (2014), "The NIST cybersecurity framework: overview and potential impacts", *Scitech Lawyer*, Vol. 10 No. 4, p. 16.

Singh, A., Klarner, P. and Hess, T. (2020), "How do chief digital officers pursue digital transformation activities? The role of organization design parameters", *Long Range Planning*, Vol. 53 No. 3, p. 101890.

Speckbacher, G. and Wentges, P. (2012), "The impact of family control on the use of performance measures in strategic target setting and incentive compensation: a research note", *Management Accounting Research*, Vol. 23 No. 1, pp. 34-46.

Swain, A.D. and Guttmann, H.E. (1983), *Handbook of Human-Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, Final Report, Albuquerque.

Teufel, S., Teufel, B., Aldabbas, M. and Nguyen, M. (2020), "Cyber security canvas for SMEs", in Venter, H., Loock, M., Coetzee, M., Eloff, M., Eloff, J.H.P. and Botha, R.A. (Eds), *Information and Cyber Security: 19th International Conference*, Cham, Switzerland, Vol. 1339, Springer, pp. 20-33, ISSA 2020 Pretoria, South Africa, August 25-26, 2020, revised selected papers, Communications in Computer and Information Science.

Thomas, J. (2018), "Individual cyber security: empowering employees to resist spear phishing to prevent identity theft and ransomware attacks", Thomas, JE (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks, *International Journal of Business Management*, Vol. 12 No. 3, pp. 1-23.

Ulrich, P. (2018), "Integration von Risikoaspekten in operative Planung und Budgetierung: was unterscheidet mittelständische Familienunternehmen von anderen Unternehmen?", *ZfKE–Zeitschrift für KMU und Entrepreneurship*, Vol. 66 No. 1, pp. 13-33.

Ulrich, P., Frank, V. and Buettner, R. (2021a), in Bui, T. (Ed.), "One single click is enough – an empirical study on human threats in family firm cyber security", *Proceedings of the 54th Hawaii International Conference on System Sciences*.

Ulrich, P., Frank, V. and Kratt, M. (2021b), "Adoption of artificial intelligence techbologies in German SMES - results from an empirical study", *A Search for Emerging Trends in the Pandemic Times*, p. 76.

Vallejo Martos, M.C. (2007), "What is a family business? A discussion of an integrative and operational definition", *International Journal of Entrepreneurship and Small Business*, Vol. 4 No. 4, pp. 473-488.

Villalonga, B. and Amit, R. (2010), "Family control of firms and industries", *Financial Management*, Vol. 39 No. 3, pp. 863-904.

Wang, Z., Sun, L. and Zhu, H. (2020), "Defining social engineering in cybersecurity", *IEEE Access*, Vol. 8, pp. 85094-85115.

Ward, J.L. (1997), "Growing the family business: special challenges and best practices", *Family Business Review*, Vol. 10 No. 4, pp. 323-337.

Welbourne, T.M., Johnson, D.E. and Erez, A. (1998), "The role-based performance scale: validity analysis of a theory-based measure", *Academy of Management Journal*, Vol. 41 No. 5, pp. 540-555.

Westhead, P. and Cowling, M. (1998), "Family firm research: the need for a methodological rethink", *Entrepreneurship Theory and Practice*, Vol. 23 No. 1, pp. 31-56.

Wilson, M. and Hash, J. (2003), "Building an information technology security awareness and training program", *NIST Special Publication*, Vol. 800 No. 50, pp. 1-39.

Wortman, M.S. (1994), "Theoretical foundations for family-owned business: a conceptual and research-based paradigm", *Family Business Review*, Vol. 7 No. 1, pp. 3-27.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F. and Basim, H.N. (2020), "Cyber security awareness, knowledge and behavior: a comparative study", *Journal of Computer Information Systems*, pp. 1-16, doi: 10.1080/08874417.2020.1712269.

Corresponding author
Patrick Sven Ulrich can be contacted at: patrick.ulrich@hs-aalen.de