Secondary Publication

Ulrich, Patrick; Timmermann, Alice

Organizational Aspects of Cyber Security in Family Firms : an Empirical Study of German Companies

Date of secondary publication: 02.07.2026

Version of Record (Published Version), Conferenceobject

Persistent identifier: urn:nbn:de:bvb:473-irb-115908x

Primary publication

Ulrich, Patrick; Timmermann, Alice (2021): Organizational Aspects of Cyber Security in Family Firms: an Empirical Study of German Companies, in: Proceedings of the 54th Hawaii International Conference on System Sciences, 2021, Honolulu, HI: University of Hawai'i at Manoa, Hamilton Library, pp. 6216–6225, doi: 10.24251/hicss.2021.750

Legal Notice

This work is protected by copyright and/or the indication of a licence. You are free to use this work in any way permitted by the copyright and/or the licence that applies to your usage. For other uses, you must obtain permission from the rights-holders.

This document is made available under a Creative Commons license.

The license information is available online:
https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode

Organizational Aspects of Cyber Security in Family Firms – an Empirical Study of German Companies

Patrick Ulrich
Aalen University/University of Bamberg
patrick.ulrich@hs-aalen.de

Alice Timmermann
Aalen University
alice.timmermann@hs-aalen.de

Abstract

In the context of increasing digitalization and networking, the importance of cyber security for family businesses is also growing and is moving onto the management agenda as a cross-divisional, group-wide challenge. A study of 184 German companies shows that although family businesses identify cyber security as a relevant field of action, they do not take sufficient account of the organizational framework and process implementation. This paper is dedicated to the investigation of this phenomenon. Possible causes of this phenomenon are discussed. Based on this, recommendations for action are given.

1. Introduction

In the course of increasing digitalization, family businesses are also becoming an ever greater target for hackers and are thus exposed to cyber attacks [1]. Since family businesses are known for their particular ability to innovate and usually still cooperate, attackers can target their specialized knowledge as well as understand that family businesses can be a useful channel for larger organizations through the supply chain. In addition, family businesses are often perceived to be insufficiently mature in the area of cyber security [1]. As such, family businesses are attractive targets for cyber attackers.

According to the National Institute of Standards and Technology (NIST), cybersecurity is the "ability to protect or defend the organization from cyber attacks"[2]. A lack of protection against cyber attacks can lead to business interruption or downtime, as well as significant incident investigation and IT system recovery costs. Claims for damages against companies due to delayed deliveries, damage due to data loss, damage to reputation [3] or disadvantages due to reduced competitiveness should also not be underestimated [4]. According to the results of a study by the German Federal Association for Information Technology, Telecommunications and New Media (BITKOM), the overall economic damage caused to companies in Germany by cyber attacks in the last two years amounts to 205.7 billion euros [5].

There is a discussion in the literature about the "readiness" of German companies for cyber attacks. Literature research [6, 7, 8, 9, 10, 11] as well as empirical data [12, 13] show that a holistic approach [14, 15], which integrates cyber security into organization-wide procedures and processes, is particularly relevant here. This means that even family businesses must take measures not only at the technological level but also at the organizational and process level to achieve an appropriate level of cyber security. In order to secure an organization, all employees must act in a risk-reducing manner. The organization can be seen as a system consisting of complementary roles. The effectiveness of cybersecurity depends crucially on how explicitly the tasks are assigned to the various roles and how motivated and capable the holders of these roles are to perform the tasks assigned to them. Therefore, the performance of employees is a function of both the organization and the individual [16].

As organizational implementation measures to avoid risks and to strengthen resistance in the event of a cyber attack, internal rules, such as protocols and guidelines, are essential in order to commit the members of the organization to certain procedures [17]. In addition to organization charts, these internal guidelines define who is responsible for which intermediate step and which areas are involved in decisions, and for which forms of action it is ensured that the individual measures are determined as planned. Structuring in terms of responsibilities, communication and decision-making processes enables decision-makers to take appropriate measures and make decisions even

URI: https://hdl.handle.net/10125/71370
978-0-9981331-4-0
(CC BY-NC-ND 4.0)

under time pressure [4]. This is the only way to limit the damage caused by a cyber attack, which is ultimately unavoidable, and to ensure the fastest possible uninterrupted continuation of business activities.

So far, there is little knowledge about the perception, dissemination and implementation of an organizational framework for cyber security in family businesses. However, earlier studies show that family businesses are generally less organized than non-family businesses, e.g. family businesses use management and management accounting tools to a lesser extent and are less inclined to set up independent management accounting departments than non-family businesses [18, 19, 20, 21, 22, 23]. Therefore, the focus of this paper is on the following research question:

Do German family firms show peculiarities in regards to organizational cyber security in comparison to non-family firms?

This paper examines this question on the basis of an empirical survey of 184 German companies.

The further course of this paper is as follows: Chapters 2 and 3 describe the relevant theoretical foundations. Hypotheses are derived on this basis. Subsequently, in chapter 4 the survey design and the sample are described before the respective empirical results are presented. In chapter 6, a short conclusion is drawn and recommendations for action are given.

2. Theory

2.1 Family businesses

The term "family business" is not uniformly defined in the economic literature [24, 25], which makes it difficult to quantify. Family businesses can be large as well as small and medium-sized enterprises controlled by a family [26]. The main distinguishing feature of the criterion for defining family enterprises is the level of ownership of the family [27, 28].

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. This is due to the fact that many entrepreneurial families focus on passing on the business to the next generation [29, 30]. As a rule, this means that long-term success is given much more weight than short-term profit [30]. This could have an impact on cyber security in that the family business is willing to make a high short-term investment in cyber security 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. 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 own interests in the company. This power of the entrepreneurial family can also have a concrete impact on cyber security. 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 CISO or another manager responsible for cyber security, the need for formal regular reporting is less. As a third characteristic, family businesses place more emphasis on non-financial aspects than non-family 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 non-family businesses. The goal of preserving the company for the next generation and passing it on to the next generation, or other goals refer to values within the company and to positive effects of the company on the family, 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. The way in which cyber security is managed is influenced by the specifics of family businesses and may be less formalized than in non-family businesses, for example.

2.2 Organizational aspects of cyber security

It is necessary to enforce the cyber security process at all levels and thus influence the organizational structure [31]. Different groups of experts need to work together to create both effective and efficient structures for cyber-risk management, cyber-security 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 [32]. In order to ensure that each individual project process complies with the company's cyber-security 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 [33]. Depending on the organization's own cyber security requirements, we strongly recommend the use of frameworks such as COBIT and COSO [14, 15] as a reference for building an individual framework.

2.2.1 Process

In order to operate a 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 cyber security event or to determine the key cyber risks, risk appetite, and assessment of controls and vulnerabilities [2, 10]. Therefore, it is primarily necessary to define and understand the business model, business objectives and assets of the organization in order to determine the relevance of IT to the business and ultimately agree on a level of cyber security [34, 35]. 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 [10], e.g. using a risk matrix [34, 35, 36]. From there, organizational measures can be developed and implemented to address risks that exceed the risk appetite of the organization. In addition, 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 [10]. In addition, the adequacy of risk management measures must be regularly reviewed (risk control) [34, 35, 36]. In addition, it is essential to develop and implement appropriate activities to take action in response to a detected cyber security event [2]. 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 [37].

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 [4]. In addition, the internal threat posed by human behavior should not be neglected. Raising the cyber security awareness of all employees, e.g. in the form of training and instructions [38], 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 cyber security culture can make a decisive contribution to increasing cyber-resilience and steering employee behavior in the right direction [39].

2.2.2 CISO

To ensure effective and efficient prevention cyber resilience, it must be clearly regulated and communicated who is responsible for cyber security 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 [31]. In this context, knowledge recording, knowledge sharing and succession planning to avoid critical dependencies on key persons naturally also plays a major role [31]. Due to the increasing demands on cyber security management and its degree of complexity, more and more companies are not only adapting existing management positions, such as those of the CIO, but are also creating new positions, such as the position of the CISO. The CISO is usually responsible for implementing the cyber security strategy. Thus the CISO does not only have to take on responsibility as a technical manager but rather as business visionary, innovator and strategist, driving both change and strategic initiatives [40]. 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 [41]. For this reason the CISO should not only be an excellent communicator [40]. 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 [42].

3. Hypotheses

A possible cause for the existing phenomenon that family businesses are well aware of the importance of cyber security, but the degree of implementation of measures and the establishment of systematic cyber security management is insufficient, could be due to the "socio-emotional wealth" (SEW) in family businesses.

The inventors of this approach postulate that in family businesses the founding family sometimes does things that are negative for the company. In contrast to previous approaches, 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. 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-Meija et al. [28], in which non-financial questions were explained as the key to the performance of family businesses, which 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 [28].

Berrone et al. [43] 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 [28] and organizational structure [44].

It is assumed that family businesses have the necessary knowledge in dealing with cyber security 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 in order to protect their socio-emotional assets, even if this entails financial costs [45]. Instead of leveraging managerial levers in a way that builds a cyber security culture driving cyber security behavior to prevent, detect and respond to cyber attacks effectively, family businesses are often prepared to take considerable business risks by diversifying less, only to preserve SEW as a consequence [43]. One reason for this is that owners of a family business often associate their identity with the organization, they are proud to be part of a family business [30]. Usually the company even bears the name of the family [43]. 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 [46].

Based on the SEW theory, the following hypotheses are formulated:

Previous studies show that family businesses devote fewer resources to training and attach less importance to education and have smaller proportion of managers with a university degree. Furthermore they give less importance to the improvement of detailed and rigorous management planning and are prone to underemploy management accounting techniques [47]. 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. This lack of formalization is argumentatively transferred to the field of cyber security.

Even though family businesses may be well aware of the importance of cyber security, we therefore assume that they are not as well prepared in terms of having implemented a cyber incident response compared to non-family businesses due to their fear of losing control. The typical reaction to a cyber attack is a so-called cyber incident response plan (CIRP).

We therefore formulate as follows:

H1: Family businesses show lesser rates of implementation of a CIRP than non-family businesses.

Previous studies show that family businesses are generally less sensitized to risks and their economic evaluation in the area of risk management. 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. They use fewer methods and instruments such as scenario techniques, sensitivity analyses and simulations. Fluctuation margins are less often taken into account in planning [48]. For the present study, it is therefore assumed that family businesses are less aware of the significance of cyber risks in the area of cyber security 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 non-family businesses.

Family businesses have implemented less formalized systems and are as well often lacking documentation and reporting compared to non-family businesses [45]. Therefore, family businesses might be less sensitized to detecting security vulnerabilities.

We therefore formulate as follows:

H3: Family businesses are slower to detect security vulnerabilities than non-family businesses.

Previous studies show that family-owned businesses are less likely to establish independent controlling departments than non-family businesses [8]. The same applies to positions such as Chief Compliance Officer (CCO) [49]. 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. We therefore formulate as follows:

H4: Family businesses are less likely to hire a CISO than non-family businesses.

4. Methodology

4.1 Methodology and design

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 non-family businesses. The study does not claim to be representative; it aims to collect a broad opinion on cyber security. The company sizes were limited to 50 employees and 10,000 workers.

A total of 14,495 companies were contacted by e-mail, 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 percent. 372 companies answered the questions asked, with 188 companies having ended the survey early (usage rate: 89.64 percent). This brings the sample size to 184 companies and the response rate to 1.43 percent. For the study, we conducted a test for non-response bias according to Armstrong/Overton (1977) [50] 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 partial non-response (item non-response) was not considered in this report. This is due to the fact that the questionnaire was deliberately designed without the specification of mandatory questions, since in some cases very topic-specific and sensitive data was queried. The data was evaluated using Microsoft Excel and SPSS.

4.2 Characterization of the sample

55 percent of the surveyed companies operate in the legal form of a limited liability company (GmbH), 24 percent as a limited partnership with a limited liability company as general partner (GmbH & Co. KG), 6 percent of the companies to be examined wear the legal form of a stock corporation (AG), 2 percent are formed as a limited partnership (KG) and 1 percent as an economic company constituted under civil law (GbR). 11 percent state that they have a different legal form.

24 percent of the companies are active in the service sector, 17 percent in mechanical and plant engineering and 9 percent in the automotive industry. 6 percent of the subject group are logistics companies, 3 percent medical technicians. The remaining 42 percent 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 percent of the companies surveyed are family businesses. Therefore, 46 percent are non-family firms.

The test persons were also asked to state their position in the company. Of the respondents, 54 percent are employed in IT. 28 percent state that they belong to company management. In addition, 4 percent work in management accounting, 2 percent in human resources, another 2 percent in production and 9 percent in other corporate areas.

4.3 Independent variables

The independent variable in the study is family influence. There are several operationalizations for this variable in the literature [51] [52] [53] [54]. 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 non-family enterprises.

4.4 Dependent variables

A different dependent variable was defined for each of the four hypotheses.

For H1 the dependent variable is the existence of a reaction plan (REAC_PLAN). The variable was measured at binary level 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 SPEED. This variable was measured in four steps: 1=less than 1 day; 2=1-7 days; 3=1-4 weeks; 4=more than one month.

For H4 the dependent variable CISO. This variable was again measured in binary at the 0/1 level.

Table 1: correlations

	FAMILY	99	100-999	1000-9999	10000	REAC_PLAN	ASSESS_METH	SPEED	CISO
FAMILY	1	-0.016	0.040	-0.030	-0.023	**-0.169***	**-0.218****	0.035	**-0.202****
99		1	**-0.751****	**-0.171***	-0.080	-0.060	-0.045	-0.022	-0.124
100-999			1	**-0.448****	**-0.209****	0.051	-0.114	-0.010	-0.102
1000-9999				1	-0.048	-0.011	**0.178***	-0.010	**0.171***
10000					1	0.027	0.144	0.116	**0.345****
REAC_PLAN						1	0.142	-0.061	**0.182***
ASSESS_METH							1	0.096	**0.440****
SPEED								1	0.098
CISO									1

Unfortunately, the target group of family businesses has a tendency 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 [55], 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:

- SIZE_99: enterprises with up to 99 employees (n=34);
- SIZE_100_999: enterprises with between 100 and 999 employees (n=122);
- SIZE_1000_9999: companies with between 1,000 and 9,999 employees (n=17);
- SIZE_10000: enterprises with 10,000 or more employees (n=4).

The class 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. For each logistic regression model, the ß-coefficient describes the regression coefficient of logistic regression, and Sig. shows the probability of the Wald statistics. As for the significances: * Significance at the 10% level (Wald test); ** Significance at the 5% level (Wald test); *** Significance at the 1% level (Wald test).

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 less frequently. 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.

Table 2: Test of hypothesis 1

	MODEL 1		
Dependent Variable	REAC_PLAN		
Independent Variable	ß-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		

The model quality and the explanatory contribution in this model are not particularly good at just 3.4

percent. Nevertheless, it is shown that family businesses have a significantly lower probability of having an emergency response plan. H1 is confirmed.

5.3 Test of hypothesis 2

A binary logistic regression was created for H2.

Table 3: Test of hypothesis 2

	Model 2		
Dependent Variable	ASSESS_METH		
Independent Variable	ß-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		

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 percent.

5.4 Test of hypothesis 3

A linear regression was performed for H3.

Table 4: Test of hypothesis 3

	Model 3			
Dependent Variable	SPEED			
Independent Variable	ß-Coeff.	p-Value	Tolerance	VIF
FAMILY	0.069	0.617	0.998	1.002
SIZE100_999	0.029	0.862	0.746	1.340
SIZE1000_9999	0.011	0.968	0.779	1.284
SIZE10000	0.748	0.120	0.931	1.074
Model fit				
R^2	0.015			
Adjusted R^2	-0.007			
F (Model, global)	0.682			

The model does not provide sufficient model quality and there are no significant results. H3 is rejected. In addition, the adjusted r^2 shows that the model is not really well suited to analyze this question.

5.5 Test of hypothesis 4

A binary logistic regression was used for hypothesis 4.

Table 5: Test of hypothesis 4

	Model 4		
Dependent Variable	CISO		
Independent Variable	ß-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		

Model 4 delivers the expected results. Family businesses have significantly less CISO. In contrast, companies with more than 1,000 employees have a CISO more often. H4 is confirmed. In addition, the goodness-of-fit – measured with Nagelkerkes r^2 - is relatively good at 25.8 percent.

6. Discussion and conclusion

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 above all organizational requirements.

The present study examined the status quo of organizational cyber security at 184 German companies.

The manuscript thus moves in an interesting field of tension between family businesses, SMEs, organizational routines and cyber security. Even though it has already been established that there is still some catching up to do in the area of cyber security 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.

It is confirmed that family businesses do indeed have organizational catch-up needs to reduce their vulnerability to cyber attacks. The hypotheses regarding the influence of family influence have been largely confirmed. Family businesses and non-family 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 own level of cybersecurity maturity means that one has to measure something - that one has some defined metrics. This raises awareness. A process that needs to be repeated regularly in order 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 [37], 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 in order to achieve a change in mentality that overcomes the cultural barriers between IT and the core organization.

The results show that non-family businesses clearly make a greater contribution to the holistic management of cyber risks and ensure that the process of cyber security 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 cyber security 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 in order to maintain their own position in the family network can also be transferred to the area of cyber security. 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 cyber security. 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.

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

[1] P. Engermann, D. Fischer, B. Gosdzik, T. Koller, N. Moore, Im Visier der Cyber-Gangster, So gefährdet ist die Informationssicherheit im deutschen Mittelstand, PWC PricewaterhouseCoopers, Studienbericht, 2017.

[2] NIST National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, 2018.

[3] J. Byok, „Informationssicherheit von Kritischen Infrastrukturen im Wettbewerbs- und Vergaberecht", Betriebs-Berater, 2017, pp. 451-454.

[4] D. Gabel, T. A. Heinrich, A. Kiefner, Rechtshandbuch Cyber-Security, Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft, 2019.

[5] M. Barth, N. Hellemann, T. Kob, C. Krösmann, U. Morgenstern, T. Tscherich, T. Ritter, H. Shulman, D. Trapp, R. Wintergerst, „Spionage, Sabotage und Diebstahl. Wirtschaftsschutz in der vernetzten Welt, BITKOM e. V. Studienbericht, 2020.

[6] M. Bartsch, S. Frey, Cybersecurity – Best Practices, Springer, 2018.

[7] I. Corradini, E. Nardelli, "Building Organizational Risk Culture in Cyber Security: The Role of Human Factors", International Conference on Applied Human Factors and Ergonomics, in Advances in Human Factors in Cybersecurity, Springer, 2018, pp. 193-202.

[8] K. Hausken, "Cyber resilience in firms, organizations and societies", Internet of Things, Vol. 11, 2020 (forthcoming).

[9] S. Kraemer, P. Carayon, J. Clem, "Human and organizational factors in computer and information security: Pathways to vulnerabilities", Computers & Security 28. 2009, pp. 509 – 520.

[10] McKinsey & Company, Perspectives on transforming cybersecurity, 2019.

[11] P. E. Roege, Z. A. Collier, V. Chevardin, P. Chouinard, M. V. Florin, J. H. Lambert, K. Nielsen, M. Nogal, B. Todorovic, Bridging the Gap from Cyber Security to Resilience, in Resilience and Risk, Methods and Application in Environment, Cyber and Social Domains, Nato Science for Peace and Security Series – C: Environmental Security, Springer, 2017.

[12] COSO Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management – Integrated Framework, 2017.

[13] ISACA Information Systems Audit and Control Association, Control Objectives for Information related Technology (COBIT) – IT-Governance Framework, 2019.

[14] E. Kolek, "IT-Sicherheit der Digitalisierung in Kleinen und Mittleren Unternehmen: Eine literaturbasierte und empirische Studie von Effekten und Barrieren", Multikonferenz Wirtschaftsinformatik, 2018, pp. 1706-1717.

[15] D. Wrede, T. Freers, J. M. Graf von der Schulenburg, „Herausforderungen und Implikationen für das Cyber-Risikomanagement sowie die Versicherung von Cyberrisiken – Eine empirische Analyse.", Zeitschrift für die gesamte Versicherungswirtschaft, 107, pp. 405-434.

[16] T. M. Welbourne, D.E. Johnson and A. Erez, "The Role-Based Measure", Academy of Management Journal, vol. 41, no. 5, 1998, pp. 540-555.
[17] Bensinger/Kozok, "Kampf gegen Cyber Crime und Hacker Angriffe", Compliance Berater, 2015, pp. 376 - 380.
[18] W. Becker, P. Ulrich, M. Staffel, "Management accounting and controlling in German SMEs: do company size and family influence matter?", International Journal of Entrepreneurial Venturing, Vol. 3 No. 3, 2011, pp. 28-300.
[19] M. R. W. Hiebl, „Einfluss von Controlling-Systemen auf die Unternehmensführung mittelgroßer Familienunternehmen", Controlling & Management Review, Vol. 57, No. 1, 2013, pp. 78-84.
[20] M. R. W. Hiebl, B. Feldbauer-Durstmüller, C. Duller, „Die Organisation des Controllings in österreichischen und bayerischen Familienunternehmen", Zeitschrift für KMU und Entrepreneurship, Vol. 61, No. 1-2, 2013, pp. 83-114.
[21] E. K. Laitinen, "Value drivers in Finnish family-owned firms: profitability, growth and risk", International Journal of Accounting and Finance, Vol. 1 No. 1, 2008, pp. 1–41.
[22] B. Feldbauer-Durstmüller, C. Duller, D. Greiling "Strategic Management Accounting in Austrian Family Firms", International Journal of Business Research, Vol. 12, No. 1, 2012, pp. 26-42.
[23] B. Feldbauer-Durstmüller, T. Haas, S. Mühlböck, „Controlling-Praxis oberösterreichischer Familien-unternehmen", Controller Magazin, Vol 34, No. 2, 2009, pp. 36-40.
[24] J. H. Astrachan, S. B. Klein, K. X. Smyrnios, "The F-PEC scale of family influence: A proposal for solving the family business definition problem", Family Business Review, 15(1), 2002, pp. 45-58.
[25] J. H. Astrachan, M. C. Shanker, "Family businesses' contribution to the U.S. economy: A closer look" Family Business Review, 16(3), 2003, pp. 211-219.
[26] M. Ayyagari, T. Beck, A. Demirguc-Kunt, "Small and medium enterprises across the globe. Small Business Economics", 29(4), 2007, pp. 415-434.
[27] P. Berrone., C. Cruz, C., L. R. Gómez Mejia, M. Larraza Kintana, "Socioemotional wealth and corporate responses to institutional pressures: Do family-controlled firms pollute less?", Administrative Science Quarterly, 55(1), 2010, pp. 82-113.
[28] L. R. Gómez-Mejia, K. T. Haynes, M. Nu-ez-Nickel, K. J. L. Jacobson, J. Moyano-Fuentes, "Socioemotional wealth and business risks in family-controlled firms: Evidence from Spanish olive oil mills", Administrative Science Quarterly, 52 (1), 2007, pp. 106-137.
[29] M. C. Vallejo Martos, "What is a family business? A discussion of an integrative and operational definition" International Journal of Entrepreneurship and Small Business, 4(4),2007, pp. 473-488.
[30] Friedrichshafener Institut für Familienunternehmen, Deutschlands nächste Unternehmergeneration, Eine empirische Untersuchung der Einstellungen, Werte und Zukunftspläne, 4. Auflage, Stiftung Familienunter-nehmen, 2017.
[31] BSI, Federal Office for Information Security, Standard 200-2 - IT-Grundschutz-Methodik, 2017.
[32] IIA (The Institute of Internal Auditors): The Three Lines of Defense in Effective Risk Management and Control, position paper, 2013, p.1.
[33] OECD Organization for Economic Cooperation and Development, Digital Risk Management for Economic and Social Prosperity, 2015.
[34] T. Kosub, „Components and challenges of integrated cyber risk management", Zeitschrift für die gesamte Versicherungswissenschaft, Vol. 104, No. 5, pp. 615-634.
[35] P. Taveras, "Cyber Risk Management, Procedures and Considerations to Address the Threats of a Cyber Attack", Proceedings of the ForenSeccure: Cybersecurity and Forensics Conference, Chicago, 2019, pp. 1-10.
[36] R. Giebichenstein, C. A. Schirp, Step-by-step: Vorgehensweise und praktische Umsetzung der ISO 27001, für Unternehmen, Compliance Berater, Vol. 4, 2015, pp. 108-113.
[37] Neufeld/Schemmel, „Notfallmanagement bei Cyber-Angriffen durch Cyber-Incident Response Plan", Datenschutz-Berater 2017, pp. 209 - 211.
[38] M. Wilson, J. Hash, "Building an Information Technology Security Awareness and Training Program, NIST National Institute of Standards and Technology Special Publication 800-50, 2003.
[39] K. Huang, K. Pearlson, "For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture, Proceedings of the 52nd Hawaii International Conference on System Sciences, 2019, pp. 6398-6407.
[40] V. Hooper, J. McKissack, „The emerging role of the CISO", Business Horizons, Vol. 59, No. 6, 2016, pp. 585-591.
[41] D. Ashenden, A. Sasse, "CISOs and organizational culture: Their own worst enemy?", Computers & Security, 39, 2013, pp. 396-405.
[42] C. Hardy, "Understanding power: `bringing about strategic change`", Br J Manage (Special Issue), 1996, pp. 3-16.
[43] P. Berrone, C. Cruz, and L.R. Gomez-Mejia, "Socioemotional Wealth in Family Firms: Theoretical Dimensions, Assessment Approaches, and Agenda for Future Research", Family Business Review 25 (3), 2012, pp. 258-279
[44] I. Barros, J. Hernangómez, N. Martin-Cruz, "Familiness and socioemotional wealth in Spanish family firms: An empirical examination", European Journal of Family Business, 7 (1-2), pp. 14-24.
[45] M. R. W. Hiebl, "Risk Aversion in Family Firms: What do we really know?", The Journal of Risk Finance, 14 (1), 2013, pp. 49-70.
[46] L. R. Gomez-Mejia, C. Cruz, P. Berrone, and J. De Castro "The bind that ties. Socioemotional Wealth preservation in internet family firms", The Academy of Management Annals, 5:1, 2011, pp. 653-707.
[47] D. García-Pérez-de-Lema, A. Duréndez,, "Managerial behaviour of small and medium-sized family businesses: an empirical study", International Journal of Entrepreneurial Behaviour & Research, Vol. 13 No. 3, 2007, pp. 151-172.

[48] P. Ulrich, “ Integration von Risikoaspekten in operative Planung und Budgetierung: Was unterscheidet mittelständische Familienunternehmen von anderen Unternehmen?," Zeitschrift für KMU und Entrepreneurship, Vol. 66, No. 1, pp 13-33.
[49] S. Behringer, P. Ulrich, A. Unruh, “Compliance Management in Family Firms – a Systematic Literature Analysis“, Corporate Ownership & Control, Vol. 17, No. 1, pp. 140-157.
[50] J. S. Armstrong, T. S. Overton, “Estimating nonresponse bias in mail surveys”, Journal of marketing research, Vol 14., No. 3, pp. 396-402.
[51] P. Westhead, P. Cowling, “Family firm research: the need for a methodological rethink”, Entrepreneurship Theory and Practice, Vol. 23, No. 1, pp. 31-56.
[52] J.H. Astrachan, S.B. Klein, K.X. Smyrnios, “The F-PEC Scale of Family Influence: A Proposal for Solving the Family Business Definition Problem”, Family Business Review, Vol. 4, No. 1, pp. 45-58.
[53] W.G. Dyer, “The family: the missing variable in organizational research”, Entrepreneurship Theory and Practice, Vol. 27, No. 4, pp. 401-416.
[54] M.R.W. Hiebl, C. Duller, B. Feldbauer-Durstmüller, P. Ulrich, “Family Influence and Management Accounting Usage–Findings from Germany and Austria”, Schmalenbach Business Review, Vol. 67, No. 3, pp. 368-404.
[55] G. Speckbacher, P. Wentges, “The impact of family control on the use of performance measures in strategic target setting and incentive compensation: A research note”, Management Accounting Review, Vol. 23. No. 1, pp. 34–46.