One Single Click is enough – an Empirical Study on Human Threats in Family Firm Cyber Security

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

Vanessa Frank
Aalen University
vanessa.frank@hs-aalen.de

Ricardo Büttner
Aalen University
Ricardo.buettner@hs-aalen.de

Abstract

The present study focuses on the tension between human versus technical risks in German companies. It examines how employees counter cybercrime and how this affects the company. Aim is to analyze human threats in family businesses and to create opportunities to use the human factor as an opportunity in the context of technological change. For this, an empirical study among 184 German firms was conducted. In general, the results demonstrate an insufficient awareness of the topic in the companies. Although companies are aware of the need for trained employees, there is a backlog of demand for workshops and awareness raising. Employees are detected as the main security risk, especially in family businesses. Better employee training is therefore indispensable. However, even training courses cannot prevent employees from making mistakes in the area of cyber security. Therefore, it can be emphasized that additional organizational security measures are necessary.

1. Introduction

Everyday working life has seen a growing digital change in recent years. Within service and manufacturing companies people are increasingly using a wide variety of technologies to encourage networking and to simplify work [1]. Companies, irrespective of their size and characteristics, are faced with new opportunities but also risks in terms of the changing framework conditions [2]. Due to the advancing digitalization and networking, companies offer an ever-growing target for cybercrime [3]. Various potential dangers for companies can be derived from this. For instance, cyber-attacks can be launched with the intention of spying on, manipulating or destroying data, which can have significant economic consequences for companies and can eventually lead to sustainable reputational damage [4]. Companies are already making several technical and procedural attempts to secure information. However, these approaches appear to be flawed, as the economic damage to businesses caused by cyber-attacks remains immense [5]. According to an estimate by the German Association for Information Technology, Telecommunications and New Media [6], the overall economic damage to businesses in the years 2018 - 2019 was almost 205.7 billion euros [6]. Cyber security, as a decisive competition factor, is not only an essential issue for large corporations and companies. The advancing digitalization has changed a tremendous amount in the last years and small and medium-sized companies are using an increasing number of digital tools to create value due to the increasing offer of information technology. Although there are still differences between medium and large companies, small and medium-sized businesses in general offer a growing target for criminal activities by changing and developing their business models [7].

Many of these attacks exploit human vulnerability to extract information and thereby damage companies. A study conducted by the consulting firm KPMG [8] concluded, that phishing, malware and social engineering are frequently used instruments in the context of cybercrime [8]. Such attacks exploit human behavior and characteristics such as fear, vulnerability, trust or curiosity in order to influence them. By feigning a false identity and an unrecognizable intention of the perpetrator, victims are pressured to reveal confidential information, to circumvent security functions or to install malicious software on a device used for business purposes [9]. In such cases, employees are confronted with psychological distortions as they do not have sufficient information to make sustainable, targeted and rational decisions [10]. Employees are aware of the dangers and precautions involved, but often behave ignorantly and carelessly in dealing with cyber-risks, such as by recklessly handling their passwords and opening unknown emails and attachments [11]. Many companies try to counteract these problems by warning messages on employees' computers. Vance et al. [12]

URI: https://hdl.handle.net/10125/71168
978-0-9981331-4-0

addressed this issue in 2018 and investigated the effectiveness of security warnings using fMRI (functional magnetic resonance imaging), eye tracking and field experiments. The results of the study confirmed a habituation to safety measures and thus once again highlighted the human factor as a safety gap [12].

Accordingly, the human factor is considered the most significant weakness in relationship to cyber security [13]. Companies hence need to become aware of these risks and implement measures and processes that can control and minimize them. While in the past, companies have focused on technological development as a countermeasure to the increasing number of cyber-attacks, entrepreneurs today are aware that human components, i.e. soft skills and an adapted mindset, can be crucial for an improved handling of cyber-risks [14]. Although science and literature have addressed the issue of cyber-risks for large, small and medium-sized enterprises in various studies, there is little to no research on this matter in relation to family-run enterprises.

Therefore, we addressed this issue and conducted a study on cyber security, with a special focus on the issue of human versus technical risks in family companies. For this purpose, a survey was conducted among German businesses, which investigated how employees counter cybercrime and how this affects the company. The aim was to uncover human weaknesses in companies and to create opportunities to use the human factor in the context of technological change as an opportunity. The present article is thus intended to illustrate weak points and technical risks in connection with human activity and reveal possibilities for improvement for companies.

2. Humans as a cyber threat

The word ´Cyber´ is one of the most ubiquitous and powerful terms used in the context of security studies. However, there is no comprehensive and universal definition of this term in the literature and it is used unequally by different persons in different contexts [15]. As a broad definition, cyberspace can be defined as the space created by the global network, which is generally characterized by the elements processes, people and technology and is characterized by the interaction and decentralization of the actors. Here the physical elements enable connections, data transfers, processing and reproduction, but also exploitation and manipulation [16]. Based on the above, the term cybercrime describes a broad spectrum of activities and techniques that aim to use the virtual framework provided by internal and external networks and accordingly mainly by the World Wide Web to extract information from private individuals or companies, to generate a monetary advantage for the perpetrators themselves and to harm the victims in an economic or reputational manner [17]. The way in which criminals carry out cyber-attacks is increasing in both quantity and complexity, resulting in increased costs for companies. Since humans are still a weak link in the defense of cyber security, this gap in particular needs to be filled by improved cyber security.

Accordingly, the need of a decreasing number of human errors and the success of security programs causing from a better human awareness, 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 [18]. 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 [19].

Jakobsson et al. [20] elaborate that criminals are becoming increasingly sophisticated and brazen in their actions. Thus, it seems inevitable that phishing mails in the future will contain a larger element of context with them and thus it will be more difficult for the victim to decide to what extent the message is real or fake, making phishing as such more effective and a greater threat to society. For this reason, this issue should be taken seriously [20]. One of the greatest dangers in the context of phishing and business activities is the so-called spear phishing. Spear phishing describes a targeted form of phishing which, based on investigations of potential victims, contains personalized messages, usually in the form of e-mails, and thereby drives the victim to carry out a supposedly necessary action [21]. Dhamja et al. [22] illustrate various factors that favor the success of such phishing mails. They conclude that visual deception is a successful instrument within phishing mails. By using visual tricks to reinforce the appearance of authenticity of an email, victims find it difficult to distinguish between a real and a fraudulent email or website. The study demonstrates a success rate of the phishing attack from a good phishing website from 90%. For the analysis, 22 test persons were tested on 22 different websites [22].

In connection with phishing and the exploitation of human error sources, social engineering is also frequently mentioned in scientific literature. 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 [23]. The literature presents various definitional approaches to social engineering. The following definition proposed by Abraham and Chengalur-Smith [24] will be used for the presented work: They describe social engineering as "the use of social disguises, cultural ploys, and psychological tricks to get computer users to assist hackers in their illegal intrusion or use of computer system and networks" [24].

Social engineering can occur in various forms. Such methodologies of criminals can be carried out by means of messages on social networks, by telephone, face-to-face, but also especially by e-mail. Thereby the age and gender of the potential victim is of minor relevance and therefore such attacks represent a potential threat for all parties involved within a company [25] and the human error source should be considered for the entirety of the employees.

As stated by a study by the US company KnowBe4 [26], which specializes in conducting security training on cyber-risks, 96 percent of the companies surveyed consider phishing fraud to be the greatest risk to their company's security. In addition, 76 percent consider the inattention of end users to be the main threat to their business. Another 70 percent consider social engineering a serious threat to their business [26]. Accordingly, the present research focuses specifically on the human factor of cyber security, employee's security awareness and, in this context, phishing attacks and social engineering. This is intended to show companies and specifically family owned companies their current status of their cyber security and to demonstrate potential improvement measures.

3. Cyber security in family firms

As stated by Koeberle-Schmid [27], a family business can be defined as a business in which at least one family member is an active member of the top management or supervisory board and more than 50 percent of the voting rights are actually held by the family [27]. This definition is also assumed for the following work.

The psychological aspect of the employees is particularly critical within small and medium-sized family businesses, and the human factor in the light of cybercriminal activities must therefore be considered explicitly [28]. Despite a gain in relevance in the context of an increasing economic and social discussion regarding cyber security, many companies, especially within the small and medium-sized sector, are to careless to establish processes and measures to establish a holistic cyber security architecture [29]. A survey conducted in 2019 by the social research and statistics company Forsa [30] shows that 65% of small and medium-sized companies have not checked whether their data is already in circulation and data leaks exist in the company. Furthermore, the companies state that 70% of the cyber-attacks that have taken place are connected to phishing mails attacks, which underlines the central importance of human factors and of methods such as phishing and social engineering in the context of small and medium-sized companies [30]. Aspects such as traditions and the history of the company occupy an essential role in relation to family businesses. This framework, the strong links with the respective stakeholders and the emphasis on routines often result in an implementation of adequate data security systems and security systems in general being implemented only very hesitantly or not at all. Such behavior inevitably increases the risk of cyber-attacks per se and consequently family businesses are particularly exposed to this danger [31].

4. Cyber security awareness

Companies try to address the risks of cyber-attacks 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 [32]. Psychological and extrinsic motivational factors make human actions unpredictable and accordingly the human factor is considered the weakest link within the security chain [33]. Problems of information security can be characterized above all by omissions and errors of employees [34]. Increasingly, studies show the need for qualified specialists, who can also be brought into the company externally if required [35]. The actions of the employees are decisive for the success of cyber security 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 [36], examine the level of knowledge of the test persons and the quality of safety

training [37] 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 [38]. Clark, Espinosa and DeLone [39] conclude that knowledge within organizations in the context of different dimensions of cyber security is unevenly distributed between different organizational, technical or non-technical roles. However, in order to make cyber security effective and avoid breaches, it is essential to balance knowledge within several departments of an organization and establish a culture that provides a certain understanding of cyber security for the entire organizational unit. The study also indicates that various industries and companies have a different understanding of the threats posed by cyber-attacks [39]. These differences can also occur in small and medium-sized companies and must be reduced to a consensus in order to deal effectively with cyber-risks. Furthermore, Pienta, Tams and Thatcher [40] point out that the factors of trust and attention play an essential role within the framework of cyber security 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 [40].

5. Derivation of hypotheses

Based on the following hypotheses, the problem of the human element as a source of error in family businesses is addressed. Family businesses are typically small or medium-sized enterprises; therefore, they are often classified among such businesses. As can be seen in the literature, analyses of small and medium-sized enterprises, and thus especially family businesses, often highlight the human factor as an area for improvement in order to provide effective cyber security [41]. Mainly small and medium-sized companies tend to be negligent in establishing processes and measures [42], which offers attackers great potential to exploit humans as a security hole. Additionally, the mentioned differences between sectors and companies regarding their perceiption of the threats associated with cyber-attacks [43] leads to the fact, that the human factor is involved in security measures to varying degrees. Based on the literature listed, however, it can be assumed that particularly family businesses have recognized the employee and thus the human factor as a security vulnerability. Accordingly, the following hypothesis H1 can be made, which following must be checked:

H1: Family Firms see employees more often as security risks than non-family firms.

As already mentioned, especially problems related to information security are attributed to human failure [44]. However, information security in particular is a sensitive topic in the public perception. Therefore, trust and long-term thinking within the company is often emphasized as the business fundamentals of family businesses, which is why customers and suppliers assume appropriate data protection [45]. Hence, the training of employees on issues related to cyber security is essential. Often family businesses also bear the family name of their owners; damages to their business reputation therefore also affects family members as private individuals [46]. For these reasons, it can be concluded that family businesses in particular should show a special interest in providing training in relation to the prevention of cyber-attacks. Based on the hypothesis H2, it should thus be examined whether family businesses have recognised the need for cyber security measures or whether there is still a requirement for clarification in this area.

H2: Family Firms perceive educating their employees more often as a requirement for the future than non-family firms.

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 analysed. While non-family 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 channelled into other areas of the company due to an underlying emotional bias [47]. In addition, family businesses, as described above, usually have smaller company sizes and, consequently, limited financial resources for further training of employees. In this paper we address this statement with reference to hypothesis H3. This hypothesis assumes that family enterprises offer fewer training and educational opportunities than non-family enterprises and thus do not sufficiently cover the demand for further training measures.

H3: Employees in family firms show lower levels in cyber training and education than those in non-family firms.

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 [48]. A lack of training and education indicates a lower cyber security 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 [49]. Consequently, hypothesis H4 will be used to test whether employees in family businesses are less sensitive to security-related issues than employees in non-family businesses.

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

6. Methodology

6.1 Sample description

The data collection was carried out by means of a standardized online questionnaire containing open and closed questions. In order to check the questionnaire, a pre-test was first carried out with several test persons. Subsequently, the actual survey was conducted in the period from October to December 2019. For this purpose, e-mail addresses of German companies were randomly selected in advance using the Nexis database.

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 terminated the survey prematurely (utilization rate: 89.64 percent). The sample size thus amounts to 184 companies and the response rate to 1.43 percent.

It should also be mentioned that the number of answers may vary. This is related to the fact that the questionnaire was deliberately designed without specifying mandatory questions, as in some cases very topic-specific and sensitive data was requested. The data was evaluated using Microsoft Excel and SPSS.

6.2 Independent variables

The independent variable in the study is family influence. There are several operationalizations for this variable in the literature. 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.

6.3 Dependent variables

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

For H1, the dependent variable is SEC_RISK. This variable describes whether companies assess employees as a security risk. The variable was queried as a single-item variable on a five-level Likert scale with the response alternatives 1=very low to 5=very high.

For H2 the dependent variable is EMPL_EDUC. The question here is whether companies see deficits in the training and further education of their employees in the area of cyber security. This is also a five-level Likert scale with the answer alternatives 1=very low backlog demand to 5=very high backlog demand.

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 cyber security.

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.

6.4 Control variables

As a control variable, as in other, organisation-related studies, 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.

7. 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.

7.1 Correlations

Table 1: Correlations

	FAMILY	99	100-999	1000-9999	10000	EMPL_EDUC	TRAIN_LEV	SEC_RISK	SENS_ISSUES
FAMILY	1	-0.016	0.040	-0.030	-0.023	0.068	0.056	**0.217****	-0.026
99		1	**-0,751****	**-0,171***	-0.080	-0.107	-0.123	**-0,213****	**-0,160***
100-999			1	**-0.448****	**-0.209****	0.015	0.123	0.097	-0.024
1000-9999				1	-0.048	0.092	0.000	0.133	**0.186***
10000					1	0.074	-0.046	0.030	**0.165***
EMPL_EDUC						1	**0.337****	**0.605****	-0.017
TRAIN_LEV							1	**0.507****	-0.076
SEC_RISK								1	0.021
SENS_ISSUES									1

Table 1 shows the correlation of this study. Interestingly, as can be observed, there is no correlation between family influence and the number of employees. Even at first glance, FAMILY correlates with the variable SEC_RISK. It seems interesting that in the group of companies with up to 99 employees a different perception seems to exist here. There are some correlations between the various dependent variables, which are marked in the table here.

7.2 Test of hypothesis 1

To test hypothesis 1, a linear regression was applied (model 2). The results of the regression are shown in Table 2. The hypothesis test shows a correlation between FAMILY and SEC_RISK. Family businesses perceive their employees as a security risk significantly more often. Also significant are size effects in the two groups of employee numbers up to 9,999 employees. Hypothesis 1 can therefore be retained.

Table 2: Test of hypothesis 1

	Model 1			
Dependent Variable	SEC_RISK			
Independent Variable	ß-Coeff.	p-Value	Tolerance	VIF
FAMILY	0.218	0.002	0.998	1.002
SIZE100_999	0.215	0.009	0.746	1.340
SIZE1000_9999	0.240	0.003	0.779	1.284
SIZE10000	0.091	0.214	0.931	1.074
Model fit				
R^2	0.103			
Adjusted R^2	0.083			
F (Model, global)	5.135 ***			

7.3 Test of hypothesis 2

To test hypothesis 2, a linear regression was applied. The results of the regression are shown in Table 3.

In contrast to hypothesis 1, this model does not show good model quality. In addition, no effect of FAMILY can be seen. A significant explanatory contribution is only found in the group of companies between 1,000 and 9,999 employees. These companies see stronger deficits in the training and further training of their employees. Hypothesis 2 is therefore rejected.

Table 3: Test of hypothesis 2

	Model 2			
Dependent Variable	EMPL_EDUC			
Independent Variable	ß-Coeff.	p-Value	Tolerance	VIF
FAMILY	0.071	0.336	0.998	1.002
SIZE100_999	0.097	0.255	0.746	1.340
SIZE1000_9999	0.142	0.090	0.779	1.284
SIZE10000	0.103	0.179	0.931	1.074
Model fit				
R^2	0.027			
Adjusted R^2	0.005			
F (Model, global)	1.245			

7.4 Test of hypothesis 3

To test hypothesis 3, a binary logistic regression was applied. The results of the regression are shown in Table 4. 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.

Table 4: Test of hypothesis 3

	Model 3	
Dependent Variable	TRAIN_LEV	
Independent Variable	ß-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	

7.5 Test of hypothesis 4

To test hypothesis 4, a linear regression was applied. The results of the regression are shown in Table 5. 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 cyber security and cyber risk issues among their employees. Hypothesis 4 is also rejected, however.

Table 5: Test of hypothesis 4

	Model 4			
Dependent Variable	SENS_ISSUES			
Independent Variable	ß-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 ***			

8. Discussion and Conclusion

In connection with the topic of the impact of human threats on the cyber security of family businesses, the responses of a total of 184 German companies were analyzed. 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. Accordingly, companies should be made more aware of the need for cyber security measures.

On the basis of the analyses, it was found that employee companies are classified as a risk to the company in terms of their respective cyber security, with family companies more often recognizing their employees as a security problem than non-family companies. These results show that although the need for trained employees in the company has been identified, the measures are not sufficiently implemented. In summary, there is still a backlog demand for workshops and training courses to increase the cyber security awareness of employees, close security gaps and be prepared for incidents. With regard to the postulated connection with family influence, however, the expected effects only became apparent with regard to the assessment of employees as security risks. In the other areas, no difference was found between family businesses and non-family businesses.

Rather, there is the impression that cyber security is rather a topic of organisational complexity, as some economies of scale are evident. Whether and to what extent family businesses in the field of cyber security address potential deficits through organizational measures or informal variables such as trust could not be investigated by our research design.

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 cyber security.

However, it should be noted at this point that even training cannot prevent all the mistakes made by employees in the area of cyber security. For this reason, organisational security measures such as the integration of information security management systems and the establishment of ISO 27001 are necessary for effective cyber security in the company, and the introduction of a Chief Information Security Officer (CISO) is also advisable.

The present study is subject to some restrictions: In our opinion, this is the first survey-based survey on cyber security in family businesses. However, the study focuses purely on German companies. In addition, the rather low response rate and a possible single informant bias should also be mentioned. Follow-up studies should be conducted here.

In general, the present study opens up the relevance of further research on the topic of cyber security in family businesses, as this is so far a barely researched topic, but will become considerably more important in the future due to the advancing digitalization. Analyses using fMRI and eye tracking could prove to be

particularly exciting and insightful for a better understanding in the given context.

9. References

[1] C. Gerdenitsch, and C. Korunka, Digitale Transformation der Arbeitswelt – Psychologische Erkenntnisse zur Gestaltung von aktuellen und zukünftigen Arbeitswelten, Springer, Berlin, 2019.

[2] J. Abawjy "User preference of cyber security awareness delivery methods", Behaviour & Information Technology, Taylor and Francis, Milton Park, 2014, pp. 236-247.

[3] PwC, Managing risks and enabling growth in the age of innovation – 2018 Risk in Review Study, 2018.

[4] Marsh and Microsoft, By the Numbers: Clobal Cyber Risk Perception Survey, 2018.

[5] J.M. Blythe, "Cyber security in the workplace: Understanding and promoting behaviour change", Conference: Proceedings of CHItaly 2013 Doctoral Consortium, 2013.

[6] Bitkom e.V., Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt – Studienbericht 2020, 2020.

[7] Verizon, Data Brach Investigation Report 2020, 2020.

[8] KPMG, Neues Denken, Neues Handeln – Insurance Thinking Ahead – Versicherungen im Zeitalter von Digitalisierung und Cyber Studienteil B: Cyber, 2017.

[9] Bundesamt für Sicherheit in der Informationstechnik, Social Engineering, https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/IT_Sicherheit_am_Arbeitsplatz/SoEng/Social_Engineering_node.html, 2020.

[10] H. Acquisti, "Privacy in electronic commerce and economics of immediate gratification", ACM Press, 2004, pp. 21-29; B.K. Wiederhold, "The role of Psychology in Enhancing Cybersecurity", Cyberpsychology, Behavior and Social Networking, Mary Ann Liebert Inc. Publishers, New Rochelle, 2014, pp. 1-2.

[11] J. Abawjy, "User preference of cyber security awareness delivery methods", Behaviour & Information Technology, Taylor and Francis, Milton Park, 2014, 236-247.

[12] A. Vance, J.L. Jenkins, B.B. Anderson, D.K. Bjornn and C.B. Kirwan, "Tuning out security warnings: A longitudinal examination of habituation through fMRI, eye tracking, and field experiments", MIS Quarterly, Management Information Systems Research Center, Minneapolis, 2018, pp. 355-380.

[13] B.K Wiederhold, "The role of Psychology in Enhancing Cybersecurity", Cyberpsychology, Behavior and Social Networking, Mary Ann Liebert Inc. Publishers, New Rochelle, 2014, pp. 1-2.

[14] Marsh and Microsoft, By the Numbers: Clobal Cyber Risk Perception Survey, 2018, PwC, Managing risks and enabling growth in the age of innovation. 2018 Risk in Review Study, 2018.

[15] A. Futter, "´Cyber´ semantics: why we should retire the latest buzzword in security studies", Journal of Cyber Policy, Taylor and Francis, Milton Park, 2018, pp. 201-216.

[16] U.M. Mbanaso and E.S. Dandaura, "The Cyberspace: Redefining a New World", IOSR Journal of Computer Engineering, IOSR Journals, 2015, pp. 17-24.

[17] S. Kratchman, J.L. Smith, and M. Smith, "The Perpetration and Prevention of Cybercrimes. Understanding types of cybercrime and basic prevention techniques will benefit internal auditors, who can help evaluate whether a company has adequate anti-cybercrime defenses", Internal Auditing, 2008, pp. 3-12.

[18] R.C. Dodge, C.A. Carver, and A.J. Ferguson, "Phishing for user security awareness", computers & security, Elsevier, 2007, pp. 73-80.

[19] S. Kratchman, J.L. Smith, and M. Smith, "The Perpetration and Prevention of Cybercrimes. Understanding types of cybercrime and basic prevention techniques will benefit internal auditors, who can help evaluate whether a company has adequate anti-cybercrime defenses", Internal Auditing, publisher unknown, 2008, pp. 3-12.

[20] T.M. Jagatic, N.A. Johnson, M. Jakobsson, and F. Menczer, "Social Phishing", Communications of the ACM, ACM, 2007, pp. 39-44.

[21] J. Thomas, "Individual Cyber Security: Empowering Employees to Resist Spear Phishin to Prevent Identity Theft and Ransomware Attacks", International Journal of Business and Management, Canadian Center of Science and Education, Richmond Hill, 2018, pp. 1-24.

[22] R. Dhamija, J.D. Tygar, and M. Hearst, "Why phishing works.", Proceedings of the ACM CHI 2006 Conference on Human Factors in Computing Systems, ACM, 2006, pp. 581-590.

[23] J. Thomas, "Individual Cyber Security: Empowering Employees to Resist Spear Phishin to Prevent Identity Theft and Ransomware Attacks", International Journal of Business and Management, Canadian Center of Science and Education, Richmond Hill, 2018, pp. 1-24.

[24] S. Abraham, and I.S. Chengalur-Smith, "An overview of social engineering malware. Trends, tactics, and implications", Technology in Society, Elsevier, 2010, pp. 183-196.

[25] J-W H. Bullée, and M. Junger, Social Engineering, Springer Nature, Berlin, 2020, pp. 1-28.

[26] KnowBe4, Security Threats and Trend Report, 2019.

[27] A. Koeberle-Schmid, „Das System der Family Business Governance", ZCG Zeitschrift für Corporate Governance, Erich Schmidt Verlag, Berlin, 2008, pp 149-150.

[28] W. Becker, and P. Ulrich, Begriffsabgrenzung und Volkswirtschaftliche Bedeutung, Kohlhammer, Stuttgart, 2015, pp. 19-38.

[29] L. Rühmann, O. Werth, N. Guhr, and M.H. Breitner, „Cyber-Risiko – Aktuelle Bedrohungslage und mögliche Lösungsansätze", IWI Diskussionsbeiträge, Universität Hannover 2018.

[30] Gesamtverband der Deutschen Versicherungswirtschaft e.V., Cyberrisiken im Mittelstand. Ergebnisse einer Forsa-Befragung Frühjahr 2019, 2019.

[31] M. Feninger, A. De Massis, and N. Kammerlander, Family business innovation: A circular process model,

Edward Elgar Publishing, Cheltenham, 2019, pp. 187-210.
[32] K. Parson, A. McCormac, M. Butavicius, and L. Ferguson, "Human Factors and Information Security: Individual, Culture and Security Environment", Australian Government Department of Defense, 2010.
[33] C. Happ, A. Melzer, and G. Steffgen, "Trick with treat - Reciprocity increases the willingness to communicate personal data", Computers in Human Behaviour, Elsevier, 2016, pp. 372-377.
[34] A.D. Swain, and H.E. Guttmann, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. Final Report, 1983.
[35] J. Baiden, Cybercrimes, Central University College, 2011.
[36] M. Eminağaoğlu, E. Uçar, and S. Eren, "The positive outcomes of information security awareness training in companies – A case study", Information Security Tech. Report, Elsevier, 2009, pp. 223-229.
[37] L. Fabisiak, and T. Hyla, "Measuring cyber security awareness within groups of medical professionals in Poland", Proceedings of the 53rd Hawaii International Conference on System Sciences, 2020, pp. 3871-3880.
[38] J. Abawjy "User preference of cyber security awareness delivery methods", Behaviour & Information Technology, Taylor and Francis, Milton Park, 2014, pp. 236-247.
[39] M.A. Clark, J.A. Espinosa, and W.H. DeLone, "Defending Organizational Assets: A Preliminary Framework for Cybersecurity Success and Knowledge Alignment", Proceedings of the 53rd Hawaii International Conference on System Sciences, 2020, pp. 4283-4292.
[40] D. Pienta, S. Tams, and J.B. Thatcher, "Can Trust be Trusted in Cybersecurity?", Proceedings of the 53rd Hawaii International Conference on System Sciences, 2020, pp 4264-4273.
[41] W. Becker, and P. Ulrich, Begriffsabgrenzung und Volkswirtschaftliche Bedeutung, Kohlhammer, Stuttgart, 2015, pp. 19-38.
[42] L. Rühmann, O. Werth, N. Guhr, and M.H. Breitner, „Cyber-Risiko – Aktuelle Bedrohungslage und mögliche Lösungsansätze", IWI Diskussionsbeiträge, Universität Hannover 2018.
[43] M.A. Clark, J.A. Espinosa, and W.H. DeLone, "Defending Organizational Assets: A Preliminary Framework for Cybersecurity Success and Knowledge Alignment", Proceedings of the 53rd Hawaii International Conference on System Sciences, 2020, pp. 4283-4292.
[44] A.D. Swain, and H.E. Guttmann, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. Final Report, 1983.
[45] Ernst & Young, Digitalisierung und Familienunternehmen, Haben Familienunternehmen die Chancen und Risiken durch die Digitalisierung erkannt?, 2018.
[46] S. Behringer, P. Ulrich, and A. Unruh, "Corporate Governance in Familienunternehmen.", ZCG Zeitschrift für Corporate Governance, Erich Schmidt Verlag, Berlin, 2020, pp. 12-16.
[47] L.R. Gomez-Mejia, K. Haynes, M. Nuñez-Nickel, K.J. Jacobson, and J. Moyano-Fuentes, "Socioemotional wealth and business risks in family-controlled firms: Evidence from Spanish olive oil mills.", Administrative Science Quarterly, SAGE Publications, Newbury Park, 2007, pp. 106-137.
[48] M. Eminağaoğlu, E. Uçar, and S. Eren, "The positive outcomes of information security awareness training in companies – A case study", Information Security Tech. Report, Elsevier, 2009, pp. 223-229.
[49] M. Feninger, A. De Massis, and N. Kammerlander, Family business innovation: A circular process model, Edward Elgar Publishing, Cheltenham, 2019, pp. 187-210.