Hochschule Aalen

AAUF
Aalener Institut für Unternehmensführung
Wertorientierung – Governance

Cybercrime as a Topic for Risk Governance in German medium-sized Businesses

8th Annual Conference Risk Governance

Risk Governance in Change. October 29 - October 30, 2020

Prof. Dr. habil. Patrick Ulrich
Alice Timmermann
Vanessa Frank

Agenda

TOP 1	Motivation
TOP 2	Current State of Research and Hypotheses
TOP 3	Methodology and Sample
TOP 4	Empirical Results
TOP 5	Conclusion and Recommendation for Action
TOP 6	Open Discussion

TOP 1 Motivation (I)

Problem

- Increasing **networking** of various business processes via the Internet

- **Family business** as an attractive target for cyber attackers (PWC 2017)
  - Innovative ability ➡ Special knowledge
  - Cooperations ➡ Gateway for larger companies
  - Perception: Insufficient cyber security

➡ **Consequences:** Operational disruptions or breakdowns as well as considerable costs for the investigation of the incidents and the restoration of the IT systems (BSI 2019)

- **Overall economic damage:** 205.7 billion euros within the last two years (BITKOM 2020)

TOP 1 Motivation (II)

Problem

- The National Institute of Standards and Technology (NIST) defines **cyber security** as „the ability to protect or defend the organization from cyber attacks“(NIST 2018)
- **Cross-divisional, group-wide challenge:** Not just a task for IT. Due to its influence on almost all areas of an institution, it affects the organization as a whole (Sowa 2017)
- Need for a **holistic approach** (COSO, COBIT): Integration into company-wide procedures and processes
- Measures on technological, procedural and organizational level

Necessary cooperation between the stakeholders involved must be organized in a **consistent role and responsibility structure**, in particular to avoid gaps and frictional losses (Klotz 2016)

TOP 2 Current State of Research (I)

- So far, there is only limited knowledge about how well family businesses are organized in the area of cyber security

- Studies on family businesses show that they are less organized than non-family businesses in various other areas:

  → Family businesses, for example, use controlling instruments to a lesser extent and have a separate controlling department less often than non-family businesses (Becker et al. 2011, Hiebl et al. 2013)

- Possible cause: phenomenon of the „**socio-emotional-wealth**“ (SEW) (Berrone et al. 2017):
  - Assumption: Family businesses have the necessary **knowledge** in dealing with cyber security and also see the need to establish a **holistic approach**, but are **afraid of losing control** and therefore refrain from implementing

TOP 2 Current State of Research (II)

Research Question

Is there an effect of family influence in the cyber security management of German SMEs?

TOP 2 Hypotheses (I)

Hypotheses 1+2

H1: Family businesses have implemented a CIRP less frequently than non-family businesses.

H2: Family businesses quantitatively assess cyber risks with less formal methods than non-family businesses.

TOP 2 Hypotheses (II)

Hypotheses 3+4

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

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

TOP 3 Methodology and Sample

Methodology

- Online questionnaire with open and closed questions
- Survey was conducted between October and December 2019
- Sample size amounts to 184 companies
- Nevertheless, deviations in the mentions due to partial non-response occur in some cases

Legal form	79 % GmbH/GmbH & Co. KG
Turnover	79 % below 100 Million € Total Turnover
Employees	73 % between 100 and 1,000 Employees
Functional area	54 % IT, 28 % Management
Family business	54 % Yes, 46 % No

TOP 4 Empirical Results (I)

Correlations

	FAMILY	99	100-999	1000-9999	10000	REAC_PLAN	ASESS_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 ***
ASESS_METH							1	0,096	**0.440 ****
SPEED								1	0,098
CISO									1

- Family businesses are less likely to have an emergency response plan, less likely to have a method for assessing cyber-risks and less likely to have a CISO.
- Companies with more than 1,000 employees are more likely to have formal assessment methods and also more often have CISOs.
- The emergency response plan, the assessment and the CISO variable correlate significantly.

TOP 4 Empirical Results (II)

Test of Hypotheses 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	

ß-coefficient describes the regression coefficient of logistic regression, and Sig. shows the probability of the Wald statistics..
* Significance at the 10% level (Wald test).
** Significance at the 5% level (Wald test).
*** Significance at the 1% level (Wald test).

The model quality and the explanatory contribution in this model are not particularly good at just under 5%. Nevertheless, it is shown that family businesses have a significantly lower probability of having an emergency response plan. **H1 is confirmed.**

TOP 4 Empirical Results (III)

Test of Hypotheses 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	

ß-coefficient describes the regression coefficient of logistic regression, and Sig. shows the probability of the Wald statistics..
* Significance at the 10% level (Wald test).
** Significance at the 5% level (Wald test).
*** Significance at the 1% level (Wald test).

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.**

TOP 4 Empirical Results (IV)

Test of Hypotheses 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	0,826	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.**

TOP 4 Empirical Results (V)

Test of Hypotheses 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	

ß-coefficient describes the regression coefficient of logistic regression, and Sig. shows the probability of the Wald statistics..
* Significance at the 10% level (Wald test).
** Significance at the 5% level (Wald test).
*** Significance at the 1% level (Wald test).

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.**

TOP 5 Conclusion and Recommendation for Action

- Although some companies have recognized the relevance of cyber risks and cyber security, there is often a lack of strategic organizational implementation to successfully meet the challenges that companies face
- **Recommendation for action:** Carry out further investigations in this area in order to find out whether the cause is actually due to SEW protection
- Based on this, measures and tools are developed to overcome this obstacle in order to better position family businesses in the area of cyber security

TOP 6 Open Discussion

References

- Becker, W. et al. (2011): Management accounting and controlling in German SMEs: do company size and family influence matter?, International Journal of Entrepreneurial Venturing, Vol. 3 No. 3, S. 28-300.
- Berrone, P. et al. (2012): “Socio-emotional Wealth in Family Firms: Theoretical Dimensions, Assessment Approaches, and Agenda for Future Research”, Family Business Review 25 (3), S. 258-279.
- BITKOM e.V. (2020): Spionage, Sabotage und Diebstahl. Wirtschaftsschutz in der vernetzten Welt, Studienbericht.
- BSI Bundesamt für Sicherheit in der Informationstechnik (2017): Standard 200-2 – IT-Grundschutz-Methodik.
- BSI Bundesamt für Sicherheit in der Informationstechnik (2017): Standard 200-1 – Managementsysteme für Informationssicherheit (ISMS).
- COSO Committee of Sponsoring Organizations of the Treadway Commission (2017): Enterprise Risk Management - Integrated Framework.
- Hiebl, M. R. W. et al. (2013): Die Organisation des Controllings in österreichischen und bayerischen Familienunternehmen“, Zeitschrift für KMU und Entrepreneurship, Vol. 61, No. 1-2, 2013, S. 83-114.
- Klotz, M. (2016): IT-Governance nach dem Modell der "Three Lines of Defense" in CIO Handbuch-Strategien für die digitale Transformation, S. 145-160 with reference to IIA (The Institute of Internal Auditors): The Three Lines of Defense in Effective Risk Management and Control, position paper, 2013, S.1.

References

- NIST National Institute of Standards and Technology (2018): “Framework for Improving Critical Infrastructure Cybersecurity.
- PWC PricewaterhouseCoopers (2017): Im Visier der Cyber-Gangster, So gefährdet ist die Informationssicherheit im deutschen Mittelstand, Studienbericht.
- Sowa, A. (2017): Management der Informationssicherheit - Kontrolle und Optimierung, (Hrsg.): Hower, W., Wiesbaden: Springer Vieweg.

Prof. Dr. habil. Patrick Ulrich
Aalen University of Applied Sciences, Aalen Management Institute (AAUF),
Beethovenstraße 1, 73430 Aalen, Germany, patrick.ulrich@hs-aalen.de

Alice Timmermann, LL.M., M.Sc.
Aalen University of Applied Sciences, Aalen Management Institute (AAUF),
Beethovenstraße 1, 73430 Aalen,Germany, alice.timmermann@hs-aalen.de

Vanessa Frank, M.Sc.
Hochschule Aalen, Aalener Institut für Unternehmensführung (AAUF),
Beethovenstraße 1, 73430 Aalen, vanessa.frank@hs-aalen.de