Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Wirtschaft

CARF Luzern 2020
Controlling.Accounting.Risiko.Finanzen.

Konferenzband

Konferenz Homepage: www.hslu.ch/carf

A holistic management of Cyber-Risks in German SMEs - An empirical Study

Extended Abstract

Prof. Dr. habil. Patrick Ulrich
Hochschule Aalen, 73430 Aalen, patrick.ulrich@hs-aalen.de

Alice Timmermann, LL.M., M.Sc.
Hochschule Aalen, 73430 Aalen, alice.timmermann@hs-aalen.de

Vanessa Frank, M.Sc.
Hochschule Aalen, 73430 Aalen, vanessa.frank@hs-aalen.de

Abstract
In the literature there is a discussion regarding the "Preparedness" of German SMEs for Cyber-Attacks. A holistic approach is particularly relevant here. For German SMEs it is assumed that they need to catch up in terms of an Organisational Framework and Governance Structure in order to reduce their vulnerability to Cyber-Attacks. This article examines this thesis based on an empirical survey of 372 German SMEs.

1 Introduction

Cyber-Security is no longer seen as just an IT-task but rather due to its influence on almost all areas of an institution it concerns the organization as a whole as a cross-divisional, group-wide challenge (Sowa, 2017, p. 21). It is necessary to enforce the Information Security process at all levels thus affecting the organizational structure (BSI, 200-2, p. 36). Various groups of experts must work together to establish effective as well as efficient structures for managing Cyber-Risks, controlling and monitoring Cyber-Security. The necessary cooperation of all stakeholders involved must be organized in a consistent role and responsibility structure, in particular, to avoid gaps and frictional losses (Klotz, 2016, p. 146). In order to make sure every single project process complies with the company's Cyber-Security policies issued right from the beginning, Cyber-Security needs to be an integral part of the enterprise-architecture (Deutscher S. et al., 2014) and therefore of the Corporate Strategy. This is due to the right mindset having to be first and foremost reflected at the board level while at the same time approving risk acceptance.

The article is based on the following research question:

Does the functionality of certain processes regarding Cyber-Attacks in companies where Cyber-Security is already an integral part of their Corporate Strategy differ from that in enterprises who haven't integrated Cyber-Security into their Company Strategy yet?

The further course of the contribution is as follows: Chapter 2 contains the methodology followed by chapter 3 presenting the results before in chapter 4 a brief conclusion and recommendations for action are given.

2 Methodology and structural features

The data collection was carried out by using a standardized online questionnaire containing open and closed questions. The survey was conducted in the period from 23.10.2019 to 31.12.2019. For this purpose, e-mail addresses of German companies were randomly selected in advance using the Nexis database.

A total of 12,883 companies received the link to the online survey. 372 companies answered the questions, with 188 companies having terminated the survey prematurely. The sample size thus amounts to 184 companies and the response rate to 1.43 percent. In this context, it should be noted that individual questions may nevertheless be mentioned differently, as the partial non-response (item non-response) is not taken into account in this report. This is due to the fact that the questionnaire was deliberately designed without specifying mandatory questions, since in some cases very topic-specific and sensitive data was requested. The data was evaluated using Microsoft Excel and SPSS.

More than half (55 percent) of the companies surveyed operate in the legal form of a GmbH and 24 percent as GmbH & Co. KG. 24 percent of the companies are active in the service sector, 16 percent in mechanical and plant engineering and 9 percent in the automotive industry. In terms of company size, the test persons generate an average annual turnover of 714 million euros and employ an average of 974 people. 54 percent of the companies surveyed are family businesses. 54 percent of the respondents are employed in IT, 28 percent are management members.

3 Results

The results of the study show that technical security measures such as virus scanners and firewalls are already part of the standard repertoire of SMEs. In order to find out to what extent Cyber-Security is already anchored in the organization and integrated into the processes of the survey participants, the respondents were asked in particular to indicate by means of a closed question whether Cyber-Security is part of their Corporate Strategy. The results of the study show that for less than half (39 percent) of those surveyed, Cyber-Security is an integral part of Corporate Strategy.

Figure 1 shows the evaluation of the functionality of certain processes with regarding Cyber-Attacks in contrast to whether Cyber-Security is part of the Corporate Strategy. The graph shows that the functionality of all processes mentioned below is consistently rated significantly higher by companies that have integrated Cyber-Security into their Corporate Strategy than by companies for which Cyber-Security is not part of the Corporate Strategy; on average by 0.6 points (between 0.4 and 0.8 points). The difference is most evident in the evaluation (Mean (POCS): 3.5; Mean (NPOCS): 2.6) and identification (Mean (POCS): 3.4; Mean (NPOCS): 2.8) of Cyber-Attacks as well as the response (Mean (POCS): 3.6; Mean (NPOCS): 2.9) to them.

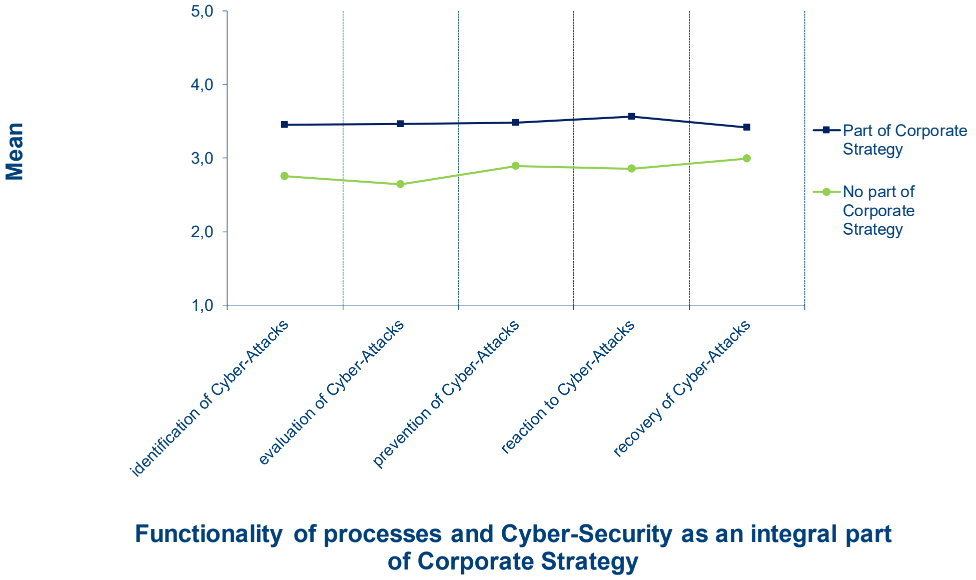

Figure 1: Functionality of processes and Cyber-Security as an integral part of Corporate Strategy

Figure 1 thus illustrates that certain processes with regard to Cyber-Attacks in companies where Cyber-Security is an integral part of their Corporate Strategy (which is only the case for 39 percent of the sample) function better than in enterprises who haven't integrated Cyber-Security into their Company Strategy yet.

4 Conclusion and recommendations for action

The results confirm the assumption that there is certainly a need to catch up for German SMEs in terms of integrating Cyber-Security into their Corporate Strategy otherwise leading to worse functioning of processes. Cyber-Security Governance is both preventive and corrective. It covers the preparations and precautions taken against Cyber-Risks and -Attacks. Especially the early detection of relevant attacks requires a holistic approach that integrates Cyber-Security into the organization-wide procedures and processes (cf. in this context COSO as well as COBIT). Indispensable in dealing with Cyber-Attacks is the establishment of a company-wide policy for Cyber-Security (BSI, 200-2, p. 36). From this, guidelines with concrete security objectives can be derived. To ensure security is borne out in practice by how the employees work it is necessary to communicate the defined rules and to anchor the ideas in the organization. All affected areas should be involved in the creation of policies, guidelines and work instructions especially to increase acceptance and willingness to implement them. (Grünendahl et al, 2017, p. 259). Roles must be defined which need to perform the various tasks in order to achieve the safety objectives (vgl. BSI, 2017, p. 40). In addition, it should be mandatory to define a contact person for security issues and to announce responsibilities as well as reporting and escalation paths for security incidents (BSI, 200-2, pp. 44, 59). In this context, an Information Security Management System (ISMS) based on the international standard ISO/IEC 27001 and the standards of the Federal Office for Information Security (BSI-Standard 200-1, 200-2) can be an effective tool putting the company in a position to control, monitor and maintain Information Security in the long term (Deloitte, p. 28; cf. in this context Hanschke, 2019, pp. 29 ff.).

- Bereich (Controlling, Accounting & Audit, Risk & Compliance, Finanzen oder Lehre)

References

BSI Federal Office for Information Security (2017): Standard 200-2 - IT-Grundschutz-Methodik.

BSI Federal Office for Information Security (2017): Standard 200-1-Managementsysteme für Informationssicherheit (ISMS).

COSO Committee of Sponsoring Organizations of the Treadway Commission (2017): Enterprise Risk Management - Integrated Framework.

Deloitte, Cyber-Security Report 2019, Teil 2: Die Gefährdung steigt – hält die Sicherheit Schritt? Accessible online: https://www.deloitte-mail.de/custloads/141631293/md_1683118.pdf?sc_src=email_4023913&sc_lid=166504800&sc_uid=eqeXgXf0ho&sc_llid=265 [latest view 04.05.20].

Hanschke, I. (2019): Informationssicherheit und Datenschutz systematisch und nachhaltig gestalten, Springer Verlag.

ISACA Information Systems Audit and Control Association (2019): Control Objectives for Information and related Technology (COBIT) - IT-Governance Framework.

Deutscher S., Bohmayr M., Yin W., Russo M (2014): Cyber-Security meets IT-Risk Management, accessible online: https://www.bcg.com/de-de/publications/2014/technology-strategy-organization-cybersecurity-meets-it-risk-management.aspx (last access on: 13.04.2020).

Grünendahl Ralf-T. et al. (2017): Das IT-Gesetz: Compliance in der IT-Sicherheit, Wiesbaden: Vieweg + Teubner Verlag, 3. Auflage.

Klotz, M. (2016): IT-Governance nach dem Modell der "Three Lines of Defense" in CIO Handbuch-Strategien für die digitale Transformation, pp. 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, p.1.

Sowa, A. (2017): Management der Informationssicherheit - Kontrolle und Optimierung, (Hrsg.): Hower, W., Wiesbaden: Springer Vieweg.