J Manag Control (2016) 27:7–32
DOI 10.1007/s00187-015-0210-5

ORIGINAL PAPER

Levers of enterprise security control: a study on the use, measurement and value contribution

Jürgen Harrer[1] · Andreas Wald[2]

Published online: 30 June 2015

Abstract The assets of enterprises are increasingly exposed to internal and external threats like fraud, theft, embezzlement, sabotage, terrorism and industrial espionage. As a result, enterprise security (ES) as a support function is becoming more important and expenses for ES are significant. An important characteristic of ES setting it apart from other support functions is that in addition to the protection of material and immaterial assets, it is concerned with the physical integrity and survival of employees as a the most valuable asset. The management and control of ES is a challenging task as it requires the cooperation and coordination of security experts, individual managers receiving protection and several functional areas of the enterprise. Notwithstanding this development, there is virtually no research on management control of ES. Therefore, the aim of the paper is to present first empirical evidence on the use, measurement, and value contribution of ES and to introduce fundamental concepts and processes of ES management. We present a study based on qualitative interviews with security experts of German DAX-30 companies which we supplement with a standardized survey. Applying Simons' levers of control-framework we find that all four levers of control are used although there are significant differences regarding their elaboration and measurement practice as well as their integration in a consistent management control system. Our study lays conceptual and empirical foundations for future research on ES control. We contribute to research on management control by unlocking a new and increasingly important field of study.

✉ Andreas Wald
andreas.wald@uia.no

[1] EBS Business School, EBS Universität für Wirtschaft und Recht, Rheingaustraße 1,
65375 Oestrich-Winkel, Germany

[2] School of Business and Law, University of Agder, Postboks 422, 4604 Kristiansand, Norway

Keywords Enterprise security · Security management · Management control · Management control system · Levers of control · Performance measurement

Mathematics Subject Classification L210 · L230 · M490

1 Introduction

For many business activities enterprises have to expose their assets to internal and external threats like fraud, theft, embezzlement, sabotage, terrorism and industrial espionage. In particular, intensive competition and saturated markets in developed countries drive international corporations to emerging markets with high risk profiles (Kotabe 2005; Talbot and Jakeman 2009; Ramos and Ashby 2013). In these markets, corporate assets are subjected to significant local threats. In 2015, there were 115 countries with a medium, high, or extreme security risk level. In both Latin America and in Asia, 48 countries are assigned to these risk categories. In the Middle East and Africa together there were 56 countries and in Europe 6 countries with such risk profiles (Control Risks 2015). Official statistics show that in these regions organized crime and terrorism are on the rise and have already reached record levels (UNODC 2015). Additionally, political or social unrest and war have become immediate threats to many multinational enterprises that conduct business operations, e.g. in Ukraine, Russia, Middle East, Hong Kong and Thailand (Allianz 2015).

However, many of these countries represent attractive markets with high growth rates or they provide access to important raw materials (Bader and Berg 2013). To counter risks and ensure security, enterprises have developed central and regional security functions (Ast 2010). Depending on local conditions, enterprise security (ES) often causes significant costs (Spich and Grosse 2005; Czinkota et al. 2010). Our research revealed that in some emerging markets security costs can amount to more than ten percent of the local revenue. For 2010 the total worldwide spending on risk management and security services was estimated to exceed $300 billion (Blyth 2008). For 2011 the turnover of the security industry in Germany was estimated to be around €35 billion (Gummer et al. 2013).

When investments in certain areas of activities are significant and their impact on business is crucial, companies usually establish management control systems (MCS) which can lead to significant efficiency gains (Otley 2003; Berry et al. (2009); Watts and McNair-Connolly 2012; De Waal and Kourtit 2013). “Management control systems are the formal, information-based routines and procedures managers use to maintain or alter patterns in organizational activities” (Simons 1995: 5). Research on MCS includes functional areas and support functions such as R&D and innovation management (Akroyd et al. 2009; McCarthy and Gordon 2011), manufacturing (Fullerton et al. 2013), project management (Bernroider and Ivanov 2011), human resource management (Liao 2006) and environmental management (Pondeville et al. 2013).

Given the increasing importance and scope of ES and the fact that there is virtually no research on management control systems in this area, the aim of our research is to lay the conceptual and empirical foundations for future research on management control of ES. We deliver a first exploratory study on the use and measurement of management control and on the value contribution of ES. As research on ES is scarce, our paper also aims to present the fundamental concepts and processes of enterprise security management. Thus, our paper contributes to both, research on management control by examining a previously not researched field of application, and research on ES by setting out conceptual foundations for future research in this field and not limiting our research to IT-related issues. We therefore take a comprehensive view and refer to enterprise security as the generic concept that comprises all security-generating activities and their effects inside an enterprise. The management and control of ES is a challenging task as it requires the cooperation and coordination of security experts, business managers, the individuals receiving protection and several functional areas of the firm. Research on ES control is not only motivated by its important role due to the increasing threats and related high spending, but ES also differs from most other support functions in one important characteristic: In addition to the protection of tangible and intangible assets, ES is concerned with the physical integrity, health and survival of employees. Any physical or financial asset cannot counterbalance human life as the most valuable asset. It is difficult to estimate the cost of an employee's death. The British Health and Safety Executive proposes calculating on the basis of GBP 1,558,000 per fatal injury (HSE 2014). Protecting human assets from any kind of impairment during their global activities is extremely costly and therefore, from a purely economic point of view, not desirable (Entorf 2013). But cost efficiency is not the only important variable for multinational enterprises. There are also issues of trustworthiness, corporate responsibility and sustainability. And from these non-financial perspectives many enterprises implicitly or explicitly follow a current paradigm they call “Zero Harm Culture” (Siemens 2015), “Zero Accident Program” (Beiersdorf 2015) or “Responsible Care” (BASF 2015). This means that enterprises try to provide the best possible protection for employees who expose themselves to severe health hazards during their business operations.

Research on MCS has underlined the multi-dimensionality and internal consistency of control systems (Widener 2007; Strauß and Zecher 2013). Accordingly, different conceptualizations of MCS suggest a variety of frameworks for a holistic description and categorization of MCS (Malmi and Brown 2008; Ferreira and Otley 2009; Broadbent and Laughlin 2009). The different elements of MCS may function independently (MCS as a package), but to unfold their full effectiveness, MCS must be designed and implemented as a coherent system of complementary elements (Chenhall 2003; Malmi and Brown 2008; Grabner and Moers 2013). Therefore, our exploratory study not only seeks to identify how MCS are used, which measurements are applied and how ES contributes to value creation, but also if and to what extent the different elements of the MCS form a coherent system. We apply the model of Simons (1995) as a comprehensive conceptualization of MCS. Simons' distinction of four levers of control takes into account that management control can be used in a diagnostic way for supporting strategy implementation but also in an interactive way for enabling emergent strategies.

The paper is organized as follows. In the next section we introduce Simons' levers of control framework that we use as a conceptual foundation for studying MCS in ES. This is followed by an introduction to ES and a review of the existing literature of management control in this field. In the fourth section, we describe the research method before we present the results by applying Simons' levers of control framework. The empirical results are discussed and evaluated in the final sections of the paper.

2 Management control systems: Simons' levers of control framework

The literature has proposed several analytical conceptualizations of MCS (Strauß and Zecher 2013). Among the most prominent ones are the frameworks of Anthony and Govindarajan (2007), Ferreira and Otley (2009), Malmi and Brown (2008), and Simons (Simons 1995, 2000). These frameworks partly differ in the way they conceptualize MCS and some frameworks have a narrower conceptualization focusing on diagnostic control whereas others take on a more holistic understanding of MCS (Strauß and Zecher 2013). In particular, Simons' levers of control (LOC) framework includes interactive control systems and takes emergent strategies into account. Accordingly, MCS may not only serve as a means of strategy implementation but may influence strategy formulation and lead to emergent strategies.

The LOC framework (Simons 1995; 2000) considers both elements which foster stability and those which aim for flexibility. It consists of four distinct levers of control: beliefs systems, boundary systems, diagnostic control systems and interactive control systems. These levers complement each other and generate a dynamic tension by the interplay of inspirational and constraining forces (Simons 2000; Widener 2007). Therefore, these forces are supposed to simultaneously allow for a predictable goal achievement and for innovation (Henri 2006).

During the creative search for new strategic courses employees need orientation. Management must determine reference points in the form of beliefs systems (Lever #1) which communicate core values. Beliefs systems often have the form of vision and mission statements and help to focus the positive search and development energy of the employees (Simons 1995). To reduce the risk of misguided developments and the waste of resources, enterprises implement boundary systems (Lever #2). They represent guardrails for individual creativity and comprise, for example, codes of business conduct (Simons 1995). For daily business and the implementation of intended strategies, diagnostic control systems are required (Lever #3). They serve to control critical performance variables and comprise formal information systems like strategic planning systems and budgets that monitor organizational outcomes. Diagnostic control systems align employees' behaviors with organizational objectives and measure the results of their actions. While diagnostic control systems facilitate the implementation of intended strategies, interactive control systems support processes of learning and development, enable a flexible response to unexpected changes and drive the generation of emergent strategies (Gladen 2011). They represent "information systems managers use to involve themselves regularly and personally in the decision activities of subordinates" (Simons 1995: 95). Although Simons' framework has been criticized for not explicitly considering informal controls (Ferreira and Otley 2009), all four levers can also be used as informal controls.

The individual elements of MCS, such as budgets, performance measures or incentives, can be designed and used independently, i.e. without taking into account potential interdependencies of the elements. This approach to management control considers

MCS more as a package (Malmi and Brown 2008; Grabner and Moers 2013) than a system. More recent research has criticized this view of management control as being too reductionist. Ignoring potential interdependencies between the elements of MCS can reduce their effectiveness and efficiency (Chenhall 2003; Ferreira and Otley 2009). Proponents of the system approach to management control stress that the different elements of MCS may be complements or substitutes and as such may reinforce each other. The design and use of MCS should therefore consider the interdependency of the elements and try to achieve internal consistency of MCS (Ferreira and Otley 2009; Grabner and Moers 2013). The need to integrate and mutually adjust the different elements of MCS has also been emphasized by Simons with regard to his LOC framework (Simons 1995, 2000). He underlines that the levers may complement each other when used together (Simons 2000: 301). Henri (2006) and Mundy (2010) have empirically shown that a balanced use of control systems can enhance performance. Our application of Simons' LOC framework for studying management control of ES therefore analyses to which extent the different controls are designed and used as a system of interdependent elements.

3 The security function and management control

One of the tasks of enterprise risk management is to provide transparency over the risks and the risk mitigation strategies of an enterprise in order to ensure the achievement of business targets (COSO 2004). In the literature there are different approaches to risk classification. For example, Cokins (2009) proposes six categories: price risk, market risk, credit risk, operational risk, strategic risk and legal risk. Security risks belong to the category of "operational risks" and security experts support risk managers during security risk identification and security risk mitigation (Talbot and Jakeman 2009).

The security function, often equated with corporate security, represents support processes whose purpose is the protection of the assets of an enterprise against security threats (Dalton 2003). A threat is defined as the product of intent and capability. Security threats are assessed through the analysis of the malicious intents of people and their capability to cause harm (Smith and Brooks 2013).

Aligned with enterprise risk management and corporate functions like corporate information technology, corporate security develops and deploys risk mitigation strategies and supports the fulfillment of legal requirements (Fumy and Sauerbrey 2006). ES comprises several areas of activity. In the literature there is no homogenous description of these areas (Fay 2007; Sennewald 2011). Kovacich and Halibozek for instance, identify 18 areas which they assign to three different categories (Table 1).

According to this categorization "administrative security" comprises central activities of analysis, planning, informing, training and monitoring. "Physical security" incorporates local protection measures for sites and people that are normally well recognized by employees. "Security operations" contains special operations and functions that do not fit into the other categories (Kovacich and Halibozek 2006).

One important element of ES is information which appears in the categories "Administrative Security" as well as "Security Operations". *Information security* refers to data or information as valuable assets. Examples are the personal data of clients

Table 1 Areas of activity (source: Kovacich and Halibozek 2006: 281–282)

Administrative security	Physical security	Security operations
Information security	Guard force	Investigations and noncompliance Inquiries
Personnel security	Technical security systems	Government security
Security education and awareness training	Locks and keys	Information systems security
Security compliance audits	Fire protection	Mergers/acquisitions/ divestitures security
Surveys and risk management	Event security	Outsourcing of security services
Contingency planning	Executive protection	
Corporate assets protection program		

or intellectual property like designs. Important measures for their protection are corporate policies and directives for the handling of critical information. In contrast, *information systems security* (or IT security) protects stored content and hardware and software components of the IT and telecommunication infrastructure by administrative and technology-based measures like passwords, firewalls and applications for intrusion detection and countering malware (Kovacich and Halibozek 2006; Talbot and Jakeman 2009). Among the different areas of corporate security shown in Table 1, information systems security, M&A security and divestitures security are some more recent areas, whereas guard force, executive protection and investigations represent the more established areas (Kovacich and Halibozek 2006; Talbot and Jakeman 2009).

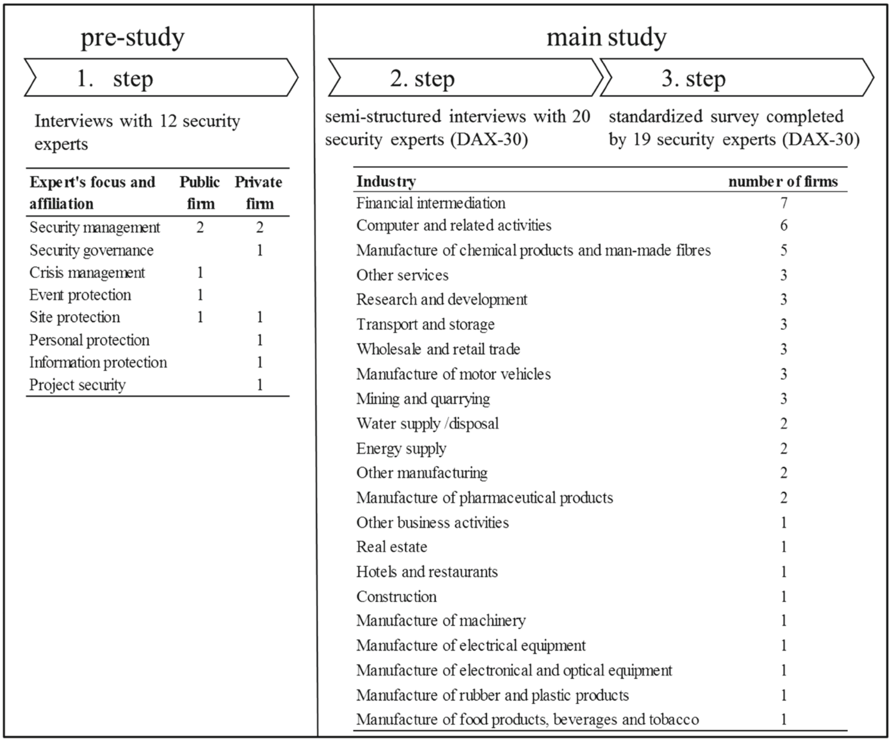
In most organizations, the Chief Information Officer (CIO) bears responsibility for information systems security, whereas the Chief Security Officer (CSO) accounts for all the other areas of activity. Internal and external threats, however, do not adhere to this distinction. Therefore practitioners from both spheres of responsibility started to develop joint approaches for their protection activities (Contos et al. 2007).

The literature on corporate security is predominantly practice-focused and based on professional experience. Authors point to three main challenges of corporate security; these are the increase in the quality of delivered services (Dalton 1995), the control of costs (Kovacich and Halibozek 2006) and the proof of security's value contribution (Burrill and Green 2011). Research on the management of ES in general and on management control systems in this area in particular is scarce. Our literature review focused on measurement concepts, specific metrics and experience gained in measuring security performance and value contribution. We found a few contributions regarding the areas of information security and IT Security, but no research that focuses on other areas presented in Table 1. In particular, we found only three empirical papers that focus on singular aspects of information (system) security but no empirical research on comprehensive security performance and its value contribution. Table 2 summarizes the results of the literature review.

Given the scarcity of research on enterprise security control we supplemented the literature review with insights on current practices and conducted a pre-study for

Table 2 Literature overview on ES

References	Country	Nature of article	Thematic area	Major issues adressed
Bojanc and Jerman-Blazie (2008)	Slovenia	Conceptual	Measurement concepts	Quantification of necessary ITC-security investments, based on combinations of economic indexes
Goel and Chen (2008)	USA	Empirical (case-study)	Measurement concepts	Integration of information security aspects into decision-making during business process reeingineering
Hagen et al. (2008)	Norway	Empirical (survey)	Measurement experience	Effectiveness of organizational information security measures
Herath et al. (2010)	Canada	Conceptual	Measurement concepts	Adoption of the balanced scorecard for the the implementation of IT security
Huang et al. (2006)	Taiwan	Empirical (survey)	Measurement concepts	Adoption of the balanced scorecard and statistical testing of performance indicators in the area of IT-security
Iheagwara (2004)	USA	Conceptual	Measurement concepts	Quantification of the ROI of intrusion detection systems, based on economic indexes
Khansa and Liginlal (2009)	USA	Conceptual	Measurement concepts	Mathematical decision model for investments in IT-security process innovations
Martin et al. (2011)	Germany	Conceptual	Measurement concepts	Adoption of the Total Quality Management approach and the use of quality standards in the area of IT-security
Patriciu et al. (2006)	Romania	Conceptual	Specific metrics	Framework for ranking vulnerabilities and metrics for the measurement of IT-security
Purser (2004)	Belgium	Conceptual	Specific metrics	Improvement of the ROI of IT-security
Tallau et al. (2010)	USA	Conceptual	Measurement concepts	Adoption of the balanced scorecard for the evaluation of technology investments in the area of IT-security
Tsiakis and Stephanides (2005)	Greece	Conceptual	Specific metrics	Different approaches for the evaluation of investments in the area of IT-security



Interviews with 12 security experts

Expert's focus and affiliation	Public firm	Private firm
Security management	2	2
Security governance		1
Crisis management	1	
Event protection	1	
Site protection	1	1
Personal protection		1
Information protection		1
Project security		1

semi-structured interviews with 20 security experts (DAX-30)

standardized survey completed by 19 security experts (DAX-30)

Industry	number of firms
Financial intermediation	7
Computer and related activities	6
Manufacture of chemical products and man-made fibres	5
Other services	3
Research and development	3
Transport and storage	3
Wholesale and retail trade	3
Manufacture of motor vehicles	3
Mining and quarrying	3
Water supply /disposal	2
Energy supply	2
Other manufacturing	2
Manufacture of pharmaceutical products	2
Other business activities	1
Real estate	1
Hotels and restaurants	1
Construction	1
Manufacture of machinery	1
Manufacture of electrical equipment	1
Manufacture of electronical and optical equipment	1
Manufacture of rubber and plastic products	1
Manufacture of food products, beverages and tobacco	1

Fig. 1 Empirical study—data and breakdown of the sample

preparing our main empirical study. We applied a purposeful sampling approach and included the views of experts from different areas activity, both from public and private organizations (Fig. 1). The rationale behind this was the insight we gained during our literature review, that emergency rescue services, police, military and private enterprises face common security threats like violence, organized crime and terrorism. The pre-study sample comprises one executive emergency physician, one executive police officer, three executive military officers including two generals and seven security managers including two chief security officers. In addition to a variation in their areas of activity, the selection criterion for the interviewees was proven experience of working in ES (Fig. 1).

We interviewed these twelve security experts discussing the following guiding question: “How is enterprise security and its value contribution currently measured in practice?” All interviews were conducted personally and lasted between 30 and 60 minutes. Most of the interviewees explained that there are no systematic, quantitative measurement approaches in their companies. Organizations rather apply a rough estimation, which is delivered formally by the security-providing experts and—often with significant impact on the perception of ES—in informal ways by the protection-receiving laypersons. We further considered this information in our empirical study by paying special attention to informal controls.

We also asked about the information requirement of their top executives regarding security work. Especially representatives of private organizations reported that executive directors typically ask about how “secure” their organization currently is, thereby alluding to the quality of protection and the resulting security level. The interviewees also described a growing frequency of queries for security’s value contribution to justify the high spending. Based on the results of the literature review and the pre-study, we prepared the main study.

4 Research design

The empirical data of our study includes both, qualitative and qualitative data. The pre-study as well as the main study include qualitative interview data which in the main study was complemented by quantitative data. Figure 1 shows the different steps of the empirical study, the data and the breakdown of the sample.

We chose a convergent semi-parallel mixed-method design for our main study. We started with an exploration, based on semi-structured interviews, and supplemented and triangulated the findings with a standardized survey (Creswell and Plano Clark 2011). The interviews mainly served to generate insights into central security processes, results of protection activities and measurement approaches, whereas the survey aimed at confirming these insights and supplementing them with figures concerning the frequency of use of evaluation approaches to security production, security implementation, and security’s value contribution.

4.1 Sample selection

The sample consists of companies that are included in the DAX-30, the leading German stock index as these companies globally expose their assets to internal and external local threats and we expected a high maturity of their security functions. Furthermore, we believe that findings gained with this sample are highly representative of large and globally operating firms. We decided to carry out a complete survey, asked all members of the DAX-30 to take part and were invited to interview the security experts of 20 corporations. Most of these corporations do business in more than one industry. Taken together there are 22 different industries represented in our sample (Fig. 1).

We compared the regional presence of the sample with the list of countries that have an above-average risk-profile (Control Risks 2015) and found that more than 60 % of the enterprises expose their assets to local threats in Latin America, Middle East, Africa and Asia.

4.2 Qualitative data

The pre-study revealed that many security measurement and evaluation activities are done implicitly and informally. We therefore encouraged the interviewees in our main study to report examples of protective activities that took place during the last ten years. These “stories” helped us to discover unconscious and informal patterns of evaluation.

Based on our research questions we developed an interview guide that comprised 11 guiding questions and focused on the following topics:

- Illustration of the protection of human, tangible and intangible assets
- Different perspectives on the achieved level of security
- Current experience with security measurement and control

We pre-tested the interview guide with the help of six security experts with an academic and practical background and revised our tool. Then we used it in 20 interviews that were conducted personally, lasted 80 minutes on average and were recorded. The sample of our main study included 15 chief security officers and 5 subordinated security managers. During all the interviews the interviewer wrote field notes and composed a field-visit protocol after every interview (Patton 2002). Finally, we sent the finished transcripts to the interlocutors for quality check and approval.

4.3 Coding and analysis

For the coding we used the software MAXQDA. We started inductively with open coding of the raw data following a well-established approach in grounded theory (Glaser 1992; Strauss and Corbin 1990). We extracted first order categories and assigned sentences from our transcripts to these categories. After all the interviews had been coded, we re-examined our initial codes and moved to axial coding i.e. identifying relationships among the open codes and developing new and more abstract categories. Figure 2 shows the different steps of the coding process.

We discussed our intermediate results with security executives from three participating corporations to ensure the reliability of our analyses. Based on the feedback received we continued with axial coding and re-clustered our codes. Then we started selective coding and developed a first multi-order data structure that comprises first-order categories, second-order themes and aggregate dimensions, which displayed the main elements of Enterprise Security.

To challenge our results (Miles and Huberman 1994) we went back to the literature, reviewed specific concepts and questioned rival interpretations. We recognized distinct opportunities for improvement and started a second coding approach. This time we

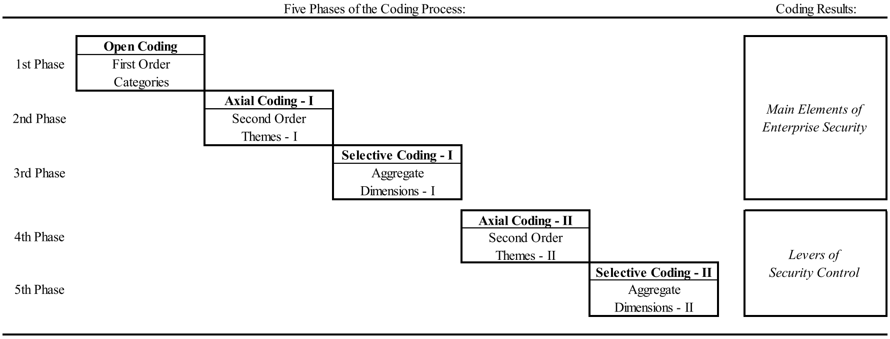


Fig. 2 Coding process

Sample Quotes	First-Order Categories	Second-Order Themes
# "Networking is one of our success factors. We constantly stay in contact with law enforcement authorities and the foreign office" (#26_A) # "We have a command and situation center that provides up-to-date situational information" (#11_B) # "Internal and external security experts work hand in hand to create a common operational picture" (#8_A)	Continuous situational awareness	Interactive Control Systems
# "We always analyze our past protection activities to improve our performance" (#19_B) # "Often unforeseen challenges require effective responses within a very short time. Afterwards it´s time for our *lessons learned* and to strengthen our preventive skills" (#7_A) # "Continuous dialog with my subordinates and with our business partners is a main aspect of continuous improvement" (#22_A)	Continous improvement: From successful reactive protection to preventive activities	
# "Meanwhile we get involved in business case development more early and can help to prevent unnecessary costs" (#11_A) # "When we support e.g. location decisions … nobody calculates the follow-up security costs that would arise, when we would not have been involved and the company would have chosen an insecure location…" (#12_A) # "Most of our business managers appreciate our advice during the planning phase of business activities in high risk areas" (#2_A)	Supporting business case development	
# "Location decisions in high risk areas mostly have impact on business resilience" (#4_A) # "Resilience requires an alignment of business processes and security processes" (#13_B) # "We ask uncomfortable questions to remind our business managers of our joint responsibility for business resilience" (#5_A)	Advocating business resillience management	

Fig. 3 Coding example

worked deductively using Simons' LOC framework for axial and selective coding. The rationale behind was, that we wanted to enrich the structure of the existing categories and relate our data to the theoretical framework (Strauss and Corbin 1990; Kelle 2005). Thus we developed a second multi-order data structure which displays both the main elements of enterprise security and the levers of security control. Figure 3 provides an example of the coding results.

4.4 Quantitative data and data triangulation

After the first ten interviews we analyzed the transcripts, field notes and field-visit protocols. Based on evolving patterns (Corbin and Strauss 2008) we developed a standardized questionnaire comprising 13 variables that focus on identified measurement approaches and variables regarding the processes and results of ES. We invited five security experts with an academic and practical background and conducted a pre-test that led to a slight revision of the questionnaire. After completion of the remaining ten interviews we sent the questionnaires to all 20 interviewees and received back 19 answers. Following a standard for data analysis in convergent mixed method designs (Creswell and Plano Clark 2011) we initially analyzed the information from the interviews and survey separately. Then we merged both qualitative and quantitative results for combined interpretation. We found that the qualitative results were confirmed, enriched and specified by quantitative data. On the other hand our survey results draw a picture of an extensive, regular and explicit measurement practice that is not always supported by our interview data. This finding will be discussed in the next chapter.

5 Levers of enterprise security control

For business operations enterprises utilize three main categories of assets: human assets (e.g. employees, customers), tangible assets (e.g. equipment) and intangible assets (e.g. intellectual property). Security management comprises two main elements -production and implementation. The production phase primarily generates protection plans and the implementation phase subsequently puts these plans into practice. The result of successful security production and implementation work is asset security. This means that despite current threats the protected assets remain intact and in a sound condition so that they are available for the intended purposes. Thus asset security works as an enabler for business operations, firstly by supporting business continuity and business generation and secondly by protecting corporate reputation. Provided that all steps are carried out successfully, security is an important support for business targets like contract compliance and revenue generation and therefore contributes to business success.

We identified several distinct practices of management control that CSOs use to steer the development and implementation of their security strategies. We found that performance and value creation in the area of enterprise security depend on both intended and emergent strategies. The interviews provided data that describe different approaches to the development and implementation of security strategies. We found numerous examples for existing formal and informal control mechanisms that can be assigned to all of the four levers of control. Figure 4 shows the adaptation of the LOC framework to enterprise security management.

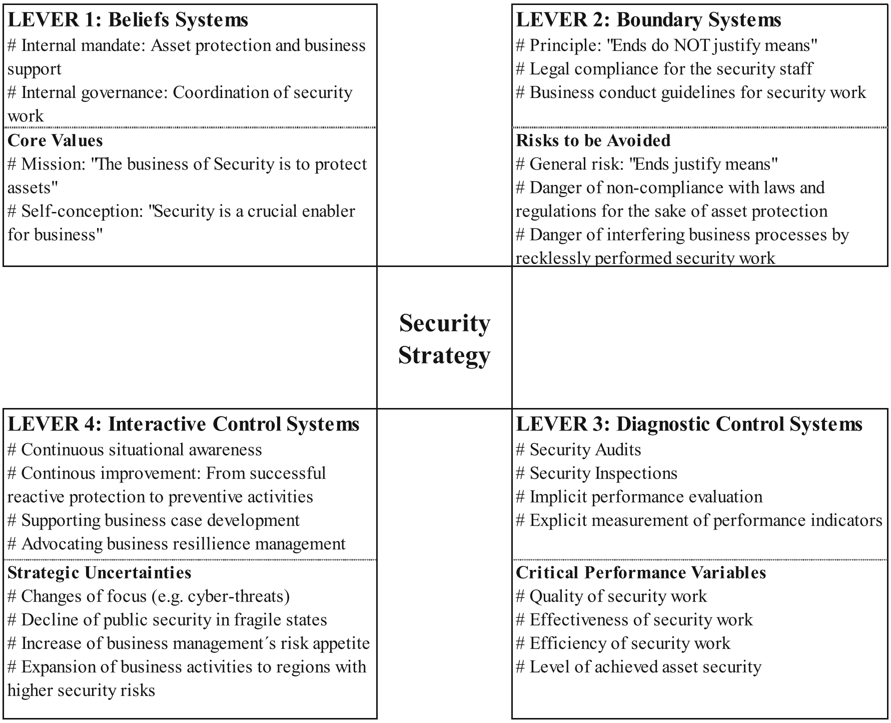
In the area of *core values* we identified official mission statements and common self-conceptions of the security experts. Among the *risks to be avoided* we found recurring warnings about the danger of "doing wrong things with best intentions". Regarding the *critical performance variables* we collected extensive data that document the use of process-oriented and result-oriented measures. Finally, we also analyzed several *strategic uncertainties* that are caused by changes in the security situation and by decisions of business managers that lead to a higher risk exposure of assets. Although we achieved substantial results after clustering our data according to Simons' framework, we realized that the current use of the four levers is neither balanced, nor integrated. The following sections are each dedicated to one LOC and explain our findings.

5.1 Lever #1: beliefs systems—the security mission

In most enterprises we found mission statements like "the business of security is to protect assets" (Dalton 1995: 93). As the executive directors usually supports these statements, most security organizations have an official internal mandate. Typically these mandates comprise the responsibility for asset protection and the duty to support business operations. Thus, the CSO is responsible for the enterprise-wide coordination of security work in predefined areas of activity.

Quotation: *"The mandate of corporate security comprises protection of persons, objects and business operations … there is a global governance for security issues." (#3_B)*

In the majority of cases the security experts consider security to be crucial for business success and define themselves as business enablers. Consequently the inter-



LEVER 1: Beliefs Systems
Internal mandate: Asset protection and business support
Internal governance: Coordination of security work

Core Values
Mission: "The business of Security is to protect assets"
Self-conception: "Security is a crucial enabler for business"

LEVER 2: Boundary Systems
Principle: "Ends do NOT justify means"
Legal compliance for the security staff
Business conduct guidelines for security work

Risks to be Avoided
General risk: "Ends justify means"
Danger of non-compliance with laws and regulations for the sake of asset protection
Danger of interfering business processes by recklessly performed security work

Security Strategy

LEVER 4: Interactive Control Systems
Continuous situational awareness
Continous improvement: From successful reactive protection to preventive activities
Supporting business case development
Advocating business resillience management

Strategic Uncertainties
Changes of focus (e.g. cyber-threats)
Decline of public security in fragile states
Increase of business management´s risk appetite
Expansion of business activities to regions with higher security risks

LEVER 3: Diagnostic Control Systems
Security Audits
Security Inspections
Implicit performance evaluation
Explicit measurement of performance indicators

Critical Performance Variables
Quality of security work
Effectiveness of security work
Efficiency of security work
Level of achieved asset security

Fig. 4 Levers of enterprise security control

nal security organization is often focused on business continuity. Some security departments show this dedication in their organizational chart by defining specific (sub-)departments for business continuity.

Quotation: *"To ensure uninterrupted business and create value for the company by the three major functions … Business Continuity has a global governance and responsibility … and therefore a clear mandate for business enabling"*. (#4_A)

Thus, certain beliefs systems (Lever #1) for the control of security strategies in our sample are already in use although there were also several enterprises that had an internal mandate that was fuzzy or not officially communicated. Most interviewees regarded this situation as a weakening of the security function.

5.2 Lever #2: boundary systems—codes of conduct and legal compliance

The pursuit of asset protection and business continuity incorporates the risk of behavior that is non-compliant with laws and regulations. Therefore, several organizations advocated the doctrine that the "ends do not justify means" and resolved to deploy a principle of "zero tolerance". This means that legal compliance is required for the security staff and if, for example, security investigations should require additional competencies, the official law enforcement authorities have to be involved.

Quotation: *"This means we take care that our systems are compliant to fulfill legal requirements … and avoid legal violations."* (#4_A)

Another risk lies in the danger of interfering with business processes by recklessly performed security work. This seems to be an issue that frequently causes trouble and regularly leads to internal discussions and complaints. The reasons for these conflicts are manifold. Sometimes there is indeed a lack of business understanding that results in the establishment of security policies that unnecessarily constrain business operations. In other situations it is the behavior of individual security experts that is regarded as too rigorous and thereby provokes resistance within the company.

Quotation: *"It's not difficult, to provide *total protection* - just let your employees work inside a huge safe. But this would disable certain business processes. Instead we prefer approaches that are smarter and more intelligent."* (#10_A)

Quotation: "*Therefore security managers strive to provide maximum protection with minimal expense ... discrete and ... inaudible, invisible ... so that security can nearly not be perceived"* (#10_A)

But often there is also a lack of information or a low risk awareness among business managers and their employees who tend to regard every policy and every protective measure as an unreasonable burden on their job. Security managers counteract the latent danger of business interference in two ways. Firstly, they decree and monitor business conduct guidelines for all security professionals. Secondly, they stay in dialog with business managers to both avoid misperceptions and understand criteria for the evaluation of security service delivery.

To sum up, our results indicate that certain boundary systems (Lever #2) for the control of security strategies are in use in all enterprises of our sample.

5.3 Lever #3: diagnostic control systems—performance measures and evaluation

Most enterprises identified critical performance variables for the implementation of security strategies. These variables focus on aspects of service quality, effectiveness and efficiency and on the level of achieved asset security. To monitor these variables, CSOs initiate periodical security audits and inspections and utilize both implicit and explicit approaches to performance measurement and evaluation.

Having discovered the different steps in the ES process we identified three main elements. In the following we will explain these elements in more depth and illustrate the related measurement approaches that are part of diagnostic control systems.

5.3.1 Security management

The task of security management is to protect threatened assets that are needed for business operations. The processes of security management can be split into a production phase and an implementation phase.

The production phase is completely controlled by security experts. It mainly produces protection plans that have to be put into practice in the subsequent phase of implementation. Within the concept of security management production we distinguished three sub-concepts:

- *Situational awareness and reporting:* In most of the enterprises security experts continuously observe security-relevant news and developments all over the world, conduct security risk analyses, compile an operational security picture and hereby enable their organization to maintain situational awareness.
- *Specification of protection targets:* Other security experts prepare business impact analyses where they support business managers to identify and classify those assets that are crucial for business operations and the achievement of business targets and therefore need particular protection.
- *Security management cycle:* We also found a concept we call the security management cycle. It has conceptual similarities with the Deming-Cycle (Tang 2008), a classical model in quality management, and helps to organize overall protection work. Additionally many corporations optimize their standard protection processes according to the classic Plan-Do-Check-Act-logic. Although every organization developed its own specific set of security activities (see Table 1), the security management cycle is completely or partly adapted to every area of administrative, physical or operational security.

Despite significant differences between the enterprises, e.g. regarding their organizational design, we identified common patterns of evaluation. Table 3 shows the frequency (percentage of cases) of the different approaches to the evaluation of security work in the "production phase" that are used by more than 50 % of our sample.

These results, however, need some additional comments. For instance, in Table 3 the "satisfaction of internal customers" approach appears three times. However, this does not imply that security experts always send out questionnaires as soon as they have finished a certain deliverable. In practice it is rather informal feedback received through phone calls, e-mails or personal conversations.

Quotation: *"When we meet our internal clients, we ask for oral feedback - but only once a year we have an official satisfaction survey"* (#6_A)

The majority of these evaluations are carried out qualitatively and event-driven, and most enterprises in our sample conduct individual satisfaction inquiries for internal customers.

The production phase is succeeded by the implementation phase. This phase is only partially controlled by security experts but it requires coordinated cooperation by three kinds of actors: security experts, functional actors and individual actors.

- *Security experts:* These are members of internal security departments as well as staff from external security providers (e.g. personnel protection services). They implement protection plans as a central task of their job profile.
- *Functional actors:* These are the executives and business managers as well as the members of support processes that are usually represented among the corporate functions. In some enterprises it is an explicit task of their job to play a distinct role in the implementation of protection plans in cooperation with the security experts.
- *Individual actors:* Individual actors are all the remaining employees of an enterprise who are neither part of the security organization, nor *explicitly* integrated into security work. Despite they are *implicitly* engaged in the implementation of protection concepts. This category contains the largest number of people and several interviewees pointed out that protection plans cannot be implemented without

Table 3 Main evaluation approaches to security production

Production activities	Focus of work	Evaluation approach	Frequency of use (%)
Situation Awareness and Report	Developing an operational security picture based on various security risk analyses and compile an evaluated report to provide situational awareness	Timeliness of used information	95
		Considered sources of information	79
		Completeness of situational picture	68
Specification of Protection Targets	Analyzing the business impact of a potential damage/loss of an asset to assess its importance for business	Degree of detail of analysis	61
		Compliance with internal standards	56
		Quality according to other internal criteria	56
	Identifying and outlining critical assets to focus protection efforts	Frequency of security incidents	84
		Number of protection targets accordig to asset category (e.g. people, tangibles, intangibles)	84
		Appropriateness of selection criteria	63
		Satisfaction of internal customers	58
Planning Phase of Security Production	Analyzing specific threats to corporate assets to provide a base for the determination of counter measures	Degree of detail of analysis	79
		Satisfaction of internal customers	58
		Number of analyses according to threat category (e.g. crime, terrorism, desaster)	53
	Developing specific protection plans to prevent security incidents	Degree of detail of planning	63
		Satisfaction of internal customers	63
		Compliance with internal standards	53

the contribution of individual actors—which often are unaware of the necessity of their contribution.

An example will illustrate the cooperation of these three categories of actors. A technical expert needs to visit a construction site somewhere in the Middle East. The security experts deliver standard protective measures including protected transportation and a security briefing with “dos and don’ts” for that particular region. The occupational health department provides medical services including revaccination and the human resource department takes care of travel documents and travel arrangements. The tech-

Table 4 Main evaluation approaches of security implementation

Evaluation approach	Frequency of use (%)
Effectiveness of implementation	79
Satisfaction of internal customers	79
Acceptance of security services by recipients	63
Compliance with internal standards	63
Costs of implementation	63
Efficiency of implementation	58

nical expert receives all these services, travels to the site and starts working. Everything is just fine until one evening when he decides to take photographs of armed insurgents while he is on a sightseeing trip in a nearby village. As expected the insurgents capture him and it causes the security experts a lot of work to secure his release. Therefore protection activities initially fail due to the poor implementation work on the part of an individual actor—despite good implementation work by security experts and functional actors.

Exploring the interplay of roles and persons during security implementation we asked our interviewees to describe the contribution of different actors. We found that security experts do only 34 % of the complete implementation work in our sample. Functional actors perform 50 % and the "ordinary" employees carry out 16 % of the implementation work. This reveals two problem areas: First, the dependency of protection success from the implementation efforts of the individual actors. Although their individual share in the implementation is only small, security experts regard the involvement of employees as vital for enterprise security.

Quotation: *"Without the cooperation of the normal employee, every protection program will collapse!"* (#3_B)

Second, our results show that security experts only control 34 % of the implementation part, whilst the largest share (66 %) is not centrally managed. Instead responsibility for two-thirds of security implementation is widely spread among all functional and individual actors. We estimate that this is a latent discrepancy to the official internal mandate of the security function and its governance (Lever #1) that can have a crucial impact on the ability of the security executives to implement the planned strategies (Lever #3) and therefore requires strategic flexibility (Lever #4).

Notwithstanding the implementation share of different actors, we found common patterns for the overall evaluation of implementation. Table 4 shows the frequency (percentage of cases) of the different approaches to the evaluations of security work in the "implementation phase" that are used by more than 50 % of the sample.

The findings reported in this paragraph show *how protection activities are currently measured*. All participating enterprises have a strong orientation towards quality management, have established a kind of security management cycle and measure and manage the security work done in the production phase by adopting partially sophisticated approaches. The activities and results of the implementation phase, however, are not measured and managed to this extent.

For instance, all companies count and report the number of employees that attend their security awareness programs (production phase). These are educational events aimed at raising awareness of security issues and promoting responsible behavior. Nevertheless, only two interviewees referred to a kind of “live testing”, where they explore whether the employees manage the knowing-doing-gap and actually show the “correct” behavior in their workplace environment (implementation phase).

Quotation: *“Amongst other things we measure the delivery of protection services by our subcontractors. (...) By doing tests we are able to measure fairly precisely whether certain key operation procedures are compiled” ... “We constantly do live testing”* (#28_A)

5.3.2 Asset security

Asset security is the result of successful security work in the two phases of security management. Our results suggest that asset security should be understood as a concept that comprises two dimensions of the achieved security level in a current situation:

- *Objective security:* Objective asset security equals the state of the risk-exposed assets and considers official reporting, the expert’s assessments of risks and threats, delivered protective measures and—most important—reported incidents.
- *Subjective security:* Subjective asset security equals the “feeling of security” and considers the individual evaluation of employees, their personal assessments, perceived protective measures and—most important—perceived incidents.

This distinction is particularly important when the evaluations of objective and subjective security differ from each other. For instance, when a business traveler needs to visit a high-risk area in the Middle East, security experts have to provide expensive protection services. When everything goes according to plan, he will return unscathed, which equals an objective asset security of 100 %. Nevertheless the subjective asset security might be considerably lower, according to a poor “security feeling” because of the riots he saw and the gunfire he heard when he crossed the city in a protected convoy.

Most interviewees emphasized that for overall evaluations and public opinion, subjective security or, at least, the selective perceptions of laypersons are normally more important than comprehensible estimations and measurements of qualified security experts. These findings show *how the level of the achieved security is currently measured and controlled.* Although the participating enterprises describe an elaborated two-dimensional concept, they only measure individual aspects of objective and subjective asset security. Qualitative estimation dominates here over quantitative measurement, mostly due to a lack of practical instruments. Surprisingly, objective security attracts more attention than subjective security although the subjective phenomenon is considered to have a greater relevance.

Quotation: *“A worst case scenario of employee satisfaction is the feeling of fear and insecurity ... and this can lead to a situation, where the company is no longer attractive for certain groups of people.”* (#28_A)

Therefore, the answer to the recurring question of executive officers on the state of security is only partly based on systematic performance measurement systems.

5.3.3 Business enabling and business success

The results of our interviews also provide empirical evidence for the concept of business enabling. Business enabling means providing and maintaining the necessary conditions for conducting business activities, accomplishing business targets and thereby achieving business success. We identified three sub-concepts of business enabling:

- *Business generation support:* In some industries the precondition for licenses to operate is compliance with specific security standards. Here security experts establish appropriate security programs and support the business during the auditing process. In addition, if the deployment of growth strategies in emerging countries leads to a higher risk exposure of corporate assets, security experts take care of travel security and provide secure storage, logistics and working environments to make the start of new business activities possible.
- *Business continuity support:* Continuous implementation and adjustment of security programs is a precondition for perpetual compliance with specific standards and their re-auditing. Here security experts enable the maintenance of licenses to operate. Moreover, situational changes like civil unrest or natural disasters often endanger business continuity in certain areas of the world. When security experts succeed in protecting business operations or at least limiting business interruptions, they enable contract fulfillment and help to avoid contractual penalties.
- *Corporate reputation support:* Successful protection activities build and maintain corporate reputation in two ways. Firstly, the avoidance of critical security incidents is an effective way to avoid negative press coverage. For instance, violence against business travelers, robbery or kidnapping often causes negative publicity. If security experts successfully protect the organization's assets, they also protect corporate reputation and thereby support all future business activities. Secondly, the successful protection of people is a very practical way to put corporate values into action and to integrate corporate responsibility into everyday life.

With regard to the value contribution of ES, business enabling is the intermediate of asset security and business success. Therefore its measurement is important for the assessment of security's value contribution. However, our results show that this evaluation is predominantly done implicitly and qualitatively. Security experts report persuasive examples about successful practices of the past and their impact on business success, but they do not usually apply quantitative measurements except in cases of business continuity issues.

Quotation: *"Initially there is a latent commercial interest for a region. Partially we have existing contacts … to provide good estimates of the markets. To some extent we completely opened markets - right up to the establishment of necessary political contacts."* (#22_A)

Quotation: *"We act as business enablers … and we are respected for that – but we have no explicit metrics for it."* (#22_A)

Table 5 shows how frequently certain (percentage of cases) approaches for the evaluation of security's value contribution are used.

Table 5 Evaluation approaches of security's value contribution

Evaluation approach	Frequency of use (%)
Decrease of incidents—resulting from prevention	89
Business support—achievement of strategic targets	79
Business support—maintenance of reputation / brand equity	74
Business support—implementation of corporate values	68
Decrease of incident impact—resulting from prevention	68
Decrease of incident impact—resulting from reaction to threats	58
Decrease of costs—resulting from increased efficiency	53
Decrease of costs—resulting from increased effectivenes	53
Revenue by externally payed security services	5

Our results suggest that there are two dimensions for the recognition of value contribution: the decrease of costs and the increase of "success" in terms of target achievement.

These findings show *how the value contribution of the achieved security level is currently measured*: The participating enterprises do not apply a consistent approach to the measurement of value contribution. Nevertheless there are individual initiatives using particular cases to describe causal chains that show the impact and benefit of the achieved asset security. However, this is based more on qualitative estimation than on quantitative measurement.

In summary, our results indicate intensive efforts regarding the use of diagnostic control systems (Lever #3) for the control of security strategies. The focus of the current diagnostic control is the phase of security production where common approaches from quality management are applied. Compared to this, the use of diagnostic control in all other phases of security management is less prevalent. Our interviewees expressed a need for learning about additional measurement options. In particular, they called for a more quantitative measurement that is supposed to be less biased than the prevalent qualitative estimations.

5.4 Lever #4: interactive control systems—emerging strategies to manage the unexpected

All enterprises in our sample are familiar with the strategic uncertainties that often and repeatedly inhibit the deployment and execution of planned strategies and therefore require the use of emergent strategies. These uncertainties can be explained by two reasons: changes in the security situation and changes in business operations. Both can lead to a higher or lower risk exposure of the corporate assets. Most interviewees reported that asset risk exposure rose steadily during the last ten years with severe peaks, for example, during the Arab Spring and the Fukushima disaster.

Quotation: *"Today our company is represented in more regions at risk than 10 years before. But this is not due to a planned expansion into high-risk areas. Instead the security situation suddenly deteriorated in countries where we had been for a* *long time. Moreover new assets were added after mergers and along with them came additional risks." (#13_B)*

Negative changes in the security situation are either caused by the appearance of new threats (e.g. cyber-crime, internal information leaks), or by an increase in threats in existing business environments (e.g. riots, deterioration in public security). The change of business operations results either from an increase in business management's appetite for risks or from business opportunities in emerging markets that mainly comprise regions with higher security risks.

Most security executives counteract these strategic uncertainties by intensive internal and external networking and strategic flexibility. Here the explicit and implicit expectations of the executive directors are the main drivers. Due to the global activities of the enterprises we visited and the fact that unforeseen incidences significantly impact asset security almost on a weekly basis, top executives require the ability to provide relevant information and appropriate security strategies at any time. Therefore, CSOs must stay in close contact with external partners (e.g. foreign office, law enforcement authorities) and internal partners. It is the continued and systematic exchange of information and views with the internal situation and risk analysts and the core experts for all areas of security work, in particular, that is the precondition for constant updating of the situational awareness and the adjustment and development of effective security strategies. Moreover, a close dialog with subordinates enables the security executive to steer continuous improvement. In addition, the regular information exchange with business managers provides a base for the support of business case development, when, for example, decisions regarding the location of a new site can be influenced in a way that reduces the level of previously estimated investments in protection measures.

Quotation: *"When we support, for example, location decisions … nobody calculates the follow-up security costs that would arise, if we had not been involved and the company had chosen an insecure location…"* (#12_A)

Consequently, our results indicate that specific interactive control systems (Lever #4) for the control of security strategies are already in use in all enterprises in our sample. In particular, the flexible management of unexpected challenges is a pronounced characteristic of the security business.

6 Discussion

We provide a first empirical analysis of the use of management control, measurement practice and of the value contribution of ES. Our results show the application of all four LOC, although there are significant differences regarding their elaboration and measurement practice. The motivation put forward by an internal mandate for asset protection and business support and the self-perception of being a business partner who enables business success (Lever #1) is checked and balanced by specific business conduct guidelines and the demand for business empathy (Lever #2). We identified a wide range of measurement approaches to security production, security implementation, and value contribution with a clear focus on diagnostic control systems (Lever #3). As security executives know that the implementation of planned strategies is very often disrupted by certain types of changes, they participate in internal and external networks to enhance performance and value contribution of their main department by emergent security strategies (Lever #4).

Although in most cases the four LOC could be identified in ES, we rarely observed an integrated and balanced use of the levers. The enterprises in our sample use the different elements of management control rather as a package than as an integrated and coherent system of complementary elements (Grabner and Moers 2013). The development and application of management control of ES emerged mainly throughout the last decade, reflecting a growing maturity of the internal security function. The individual levers were introduced when there was an immediate need and the utilization of the four levers of control still mostly occurs in isolated cases. Due to a lack of consistency existing potentials are often neither identified nor exploited. Nevertheless, some enterprises strive for further development and integration of the existing control systems to form a complete framework for security management control. In the literature on MCS, several authors argued that the design and MCS should consider potential interdependencies and complementarities of the different elements (Chenhall 2003; Malmi and Brown 2008; Grabner and Moers 2013). Likewise, Simon (2000) called for an integrated use of the LOC and Henri (2006) and Mundy (2010) have empirically shown that a balanced use of control systems can enhance performance. Further research could therefore investigate how MCS of ES can be designed and used in a coherent way and how the degree of coherence affects the effectiveness and efficiency of the MCS. These findings could be helpful for ES practice and support security managers during the development process of MCS.

Our research showed that measurement of protection activities predominantly uses methods from quality management. This corresponds to the work of Martin et al. (2011) regarding security measurement in the field of IT Security (Dalton 1995). In contrast, the level of objectively achieved security is only partly measured, a finding which corresponds to research where only particular aspects of IT security were considered (Iheagwara 2004; Khansa and Liginlal 2009). The concept of subjective security emerged as especially important for the overall evaluation of the security work although it is hardly measured systematically. We believe that a more coherent and quantitative validation of the concept of asset security would be supportive here. Our data represent the perspective of the security providing experts and allowed us to gain an understanding of the objective part of asset security that mainly focuses on the number and severity of security incidents. One way to clarify the subjective part of asset security could be a series of interviews with employees who received protection services to further explore different aspects of subjective security. This could be followed up by a survey based on a larger sample. This would allow for the use of statistical methods for identifying the most important determinants of subjective security. In an ideal case, this research would be conducted in an area like project security. Project delegates who worked in high risk areas could provide valuable insights into the establishment and the changes of the phenomenon of subjective security and its impact on their willingness to contribute to security implementation.

We introduced the concept of business enabling and its implications on an empirical basis but we found no measurement concept that goes beyond the casual description of potential causal chains. A formalized measurement of security's value contribution has neither been discussed in the literature nor is it applied in practice. The literature does not usually consider the challenges of security control in non-IT areas (Bojanc and Jerman-Blazie 2008; Iheagwara 2004; Purser 2004). Furthermore it does not address the link between a certain security level and the achievement of business targets. We recommend more research to further explore the relation between security performance and business success.

Although our study provides first insights on the use of management control, measurement practice and of the value contribution of ES, it involves two major limitations which must be considered when interpreting the results and should be addressed by future research. First, our study is based on a rather limited sample size. Interviewing 20 out of 30 representatives of the largest German corporations draws a fairly representative picture for large firms in this particular country, but future research should investigate management control of ES in different national settings. This particularly applies to firms originating from regions where security is a major concern. Being constantly confronted with high security risks in the home country may lead to a different organization of ES management and corresponding MCS. Those firms may either have a more developed security function due to their long experience, or they may have developed a higher degree of risk tolerance and therefore have lower security standards. Likewise, research on management control of ES should look at firms of different size such as small and medium-sized enterprises (SME). We assume that in smaller firms, MCS of ES can be even more informal than in large firms. However, the different elements of MCS may be better integrated and harmonized as the small size can reduce coordination costs. Second, due to its exploratory character, our study design was primarily qualitative and quantitative data was only added to supplement the qualitative information. Future research should seek to expand the empirical basis by collecting standardized data from a large sample and to test the hypothesis on the effectiveness and efficiency of the use of different elements of MCS of ES and of the combined use.

7 Conclusion

Although ES is becoming increasingly important for many firms and security costs are constantly rising, the literature on management control of ES is scarce. We therefore presented a first empirical study focusing on the measurement of security performance and the value contribution of security. We also introduced fundamental concepts and processes of enterprise security management such as security production, security implementation, asset security and business enabling by security. This allowed for a systematic analysis of management control of ES. We applied Simons' LOC framework to ES and showed how and to what extent beliefs systems, boundary systems, diagnostic control systems and interactive control systems are currently used for the development and implementation of security strategies.

This paper contributes to existing research in three ways: Firstly, we provided first empirical insights that allow us to identify main elements and causal chains of ES and understand ES as an important support function and its (potential) implications on corporate performance. Secondly, we adapted the LOC framework to gain a holistic understanding of the practices of security management control. Thirdly, we discovered current practices and the limitations of security measurement and the recognition of security's value contribution. Thereby we provided the first empirical insight into performance measurement in the area of ES that goes beyond IT-systems security and information protection. These results may serve as starting points for the development of management control systems in ES and for future research aiming at a better understanding of the interrelationship of the identified concepts as well as the effects and consequences of security control. This will enhance the effectiveness and efficiency of asset protection and thereby increase business success in risky environments.

References

Akroyd, C., Narayan, S., & Sridharan, V. (2009). The use of control systems in new product development innovation: advancing the 'Help or Hinder' debate. *Journal of Knowledge Management*, *7*, 70–90.

Allianz (2015) Allianz Risk Barometer. Die 10 größten Geschäftsrisiken 2015. Allianz Global Corporate & Specialty. Munich.

Anthony, R. J., & Govindarajan, V. (2007). Management control systems. Boston, McGraw-Hill.

Ast, S. A. (2010). *Managing security overseas: protecting employees and assets in volatile regions*. Boca Raton: CRC Press.

Bader, B., & Berg, N. (2013). An empirical investigation of terrorism-induced stress on expatriate attitudes and performance. *Journal of International Management*, *19*, 163–175.

BASF (2015): Responsible Care. (https://www.basf.com/de/company/sustainability/management-and-instruments/responsible-care.html). Retrieved March 20, 2015

Beiersdorf (2015) Gesundheit & Sicherheit unserer Mitarbeiter. (http://www.beiersdorf.de/nachhaltigkeit/people/gesundheit-sicherheit-mitarbeiter). Retrieved March 08, 2015

Bernroider, E. W. N., & Ivanov, M. (2011). IT project management control and the Control Objectives for IT and related Technology (CobiT) framework. *International Journal of Project Management*, *29*, 325–336.

Berry, A. J., Coad, A. F., Harris, E. P., Otley, D. T., & Stringer, C. (2009). Emerging themes in management control: a review of recent literature. *British Accounting Review*, *41*, 2–20.

Blyth, M. (2008). *Risk and security management. Protecting people and sites worldwide*. Hoboken: John Wiley & Sons.

Bojanc, R., & Jerman-Blažiè, B. (2008). Towards a standard approach for quantifying an ICT security investment. *Computer Standards & Interfaces*, *30*, 216–222.

Broadbent, J., & Laughlin, R. (2009). Performance management systems: a conceptual model. *Management Accounting Research*, *20*, 283–295.

Burrill, D., & Green, K. (2011). *Value from security*. Bloomington: AuthorHouse.

Chenhall, R. H. (2003). Management control system design within its organizational context: findings from contingency-based research and directions for the future. *Accounting, Organizations and Society*, *28*, 127–168.

Cokins, C. (2009). *Performance management. Integrating strategy, execution, methodologies, risk, and analytics*. Hoboken: John Wiley & Sons.

Contos, B. T., Crowell, W. P., DeRodeff, C., Dunke, D., & Cole, E. (2007). *Physical and logical security convergence: powered by enterprise security management*. Burlington: Syngress.

Control Risks (2015). *RiskMap Report 2015*. London: Control Risks.

Corbin, J. M., & Strauss, A. L. (2008). *Basics of qualitative research: techniques and procedures for developing grounded theory*. Los Angeles: Sage.

COSO (2004). Enterprise Risk Management. Integrated framework. Executive summary. Jersey: Committee of Sponsoring Organizations of the Treadway Commission.

Creswell, J. W., & Plano Clark, V. L. (2011). *Designing and conducting mixed methods research*. Thousand Oaks: Sage.

Czinkota, M. R., Knight, G., Liesch, P. W., & Steen, J. (2010). Terrorism and international business: a research agenda. *Journal of International Business Studies*, *41*, 826–843.

Dalton, D. R. (1995). *Security management: business strategies for success*. Boston: Butterworth-Heinemann.

Dalton, D. R. (2003). *Rethinking corporate security in the post-9/11 era*. Amsterdam: Butterworth-Heinemann.

De Waal, A., & Kourtit, K. (2013). Performance measurement and management in practice. Advantages, disadvantages and reasons for use. *International Journal of Productivity and Performance Management*, *62*, 446–473.

Entorf H (2013) Der Wert der Sicherheit. Anmerkungen zur Ökonomie der Sicherheit. Conference paper. BMBF-Conference “Sichere Zeiten”. June 2013. Berlin.

Fay, J. (2007). *Encyclopedia of security management*. Burlington: Butterworth-Heinemann.

Ferreira, A., & Otley, D. T. (2009). The design and use of performance management systems: an extended framework for analysis. *Management Accounting Research*, *20*, 263–282.

Fullerton, R. R., Kennedy, F. A., & Widener, S. K. (2013). Management accounting and control practices in a lean manufacturing environment. *Accounting, Organizations and Society*, *38*, 50–71.

Fumy, W., & Sauerbrey, J. (2006). *Enterprise security: IT security solutions: concepts, practical experiences, technologies*. Erlangen: Publicis Corporate Publishing.

Gladen, W. (2011). *Performance Measurement*. Wiesbaden, Gabler.

Glaser, B. (1992). *Emergence vs forcing: basics of grounded theory analysis*. Mill Valley: Sociology Press.

Goel, S., & Chen, V. (2008). Can business process reengineering lead to security vulnerabilities: analyzing the reengineered process. *International Journal of Production Economics*, *115*, 104–112.

Grabner, I., & Moers, F. (2013). Management control as a system or a package? Conceptual and empirical issues. *Accounting, Organizations and Society*, *38*, 407–419.

Gummer, S. C., Skrzypietz, T., & Stuchtey, T. (2013). *Die Sicherheitswirtschaft in Deutschland*. Brandenburgisches Institut für Gesellschaft und Sicherheit, Potsdam: Ergebnisbericht.

Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, *16*, 377–397.

Herath, T., Herath, H., & Bremser, W. G. (2010). Balanced scorecard implementation of security strategies: a framework for IT security performance management. *Information Systems Management*, *27*, 72–81.

Henri, J.-F. (2006). Management control systems and strategy: a resource-based perspective. *Accounting, Organizations, and Society*, *31*, 529–558.

HSE (2014). *Cost to Britain of workplace fatalities and self-reported injuries and ill health*. Merseyside: Health and Safety Executive.

Huang, S.-M., Lee, C.-L., & Kao, A.-C. (2006). Balancing performance measures for information security management: a balanced scorecard framework. *Industrial Management & Data Systems*, *106*, 242–255.

Iheagwara, C. (2004). The effect of intrusion detection management methods on the return on investment. *Computers & Security*, *23*, 213–228.

Kelle U (2005) “Emergence” vs. “Forcing” of Empirical Data? A Crucial Problem of “Grounded Theory” Reconsidered. Forum: Qualitative Social Research 6: Art. 27.

Khansa, L., & Liginlal, D. (2009). Valuing the flexibility of investing in security process innovations. *European Journal of Operational Research*, *192*, 216–235.

Kotabe, M. (2005). Global security risks and international competitiveness. *Journal of International Management*, *11*, 453–455.

Kovacich, G. L., & Halibozek, E. P. (2006). *Security metrics management: how to measure the costs and benefits of security*. Burlington: Butterworth-Heinemann.

Liao, Y.-S. (2006). Human resource management control system and firm performance: a contingency model of corporate control. *International Journal of Human Resource Management*, *17*, 716–733.

Malmi, T., & Brown, D. A. (2008). Management control systems as a package: opportunities, challenges and research directions. *Management Accounting Research*, *19*, 287–300.

Martin, C. A., Bulkan, A. B., & Klempt, P. K. (2011). Security excellence from a total quality management approach. *Total quality management & business excellence*, *22*, 345–371.

McCarthy, I. P., & Gordon, B. R. (2011). Achieving contextual ambidexterity in R&D organizations: a management control system approach. *R&D Management*, *41*, 240–258.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: an expanded sourcebook*. Thousand Oaks: Sage.

Mundy, J. (2010). Creating dynamic tensions through a balanced use of management control systems. *Accounting, Organizations and Society*, *35*, 499–523.

Otley, D. (2003). Management control and performance management: whence and whither? *British Accounting Review*, *35*, 309–326.

Patriciu, V. P., Priescu, I. P., & Nicolaescu, S. N. (2006). Security metrics for enterprise information systems. *Journal of Applied Quantitative Methods*, *1*, 151–159.

Patton, M. Q. (2002). *Qualitative research and evaluation methods*. Thousand Oaks: Sage.

Pondeville, S., Swaen, V., & De Rongé, Y. (2013). Environmental management control systems: The role of contextual and strategic factors. *Management Accounting Research*, *24*, 317–332.

Purser, S. A. (2004). Improving the ROI of the security management process. *Computers & Security*, *23*, 542–546.

Ramos, M. A., & Ashby, N. J. (2013). Heterogeneous firm response to organized crime: evidence from FDI in Mexico. *Journal of International Management*, *19*, 176–194.

Sennewald, C. A. (2011). *Effective security management*. Burlington: Butterworth-Heinemann.

Siemens (2015) Zero Harm Culture @ Siemens. (http://www.siemens.com/about/sustainability/de/themenfelder/sicherheit/zero-harm-culture-at-siemens.php). Retrieved March 08, 2015

Simons, R. (1995). *Levers of control: how managers use innovative control systems to drive strategic renewal*. Boston: Harvard Business School Press.

Simons, R. (2000). *Performance measurement and control systems for implementing strategy*. Upper Saddle River: Pearson.

Smith, C. L., & Brooks, D. J. (2013). *Security science. The theory and practice of security*. Waltham: Butterworth-Heinemann.

Spich, R., & Grosse, R. (2005). How does homeland security affect US firms' international competitiveness? *Journal of International Management*, *11*, 457–478.

Strauss, A. L., & Corbin, J. (1990). *Basics of qualitative research. Grounded theory procedures and techniques*. Newbury Park: Sage.

Strauß, E., & Zecher, C. (2013). Management control systems: a review. *Journal of Management Control*, *23*, 233–268.

Tallau, L. T., Gupta, M. G., & Sharman, R. S. (2010). Information security investment decisions: evaluating the Balanced Scorecard method. *International Journal of Business Information Systems*, *5*, 34–57.

Talbot, J., & Jakeman, M. G. (2009). *Security risk management body of knowledge*. Hoboken: Wiley.

Tang, J. (2008). The implementation of Deming's system model to improve security management: a case study. *International Journal of Management*, *25*, 54–68.

Tsiakis, T., & Stephanides, G. (2005). The economic approach of information security. *Computers & Security*, *24*, 105–108.

UNODC (2015) United Nations Office on Drugs and Crime. Crime and criminal justice statistics. http://www.unodc.org/unodc/en/data-and-analysis/statistics/crime.html. Retrieved March 08, 2015

Watts, T., & McNair-Connolly, C. J. (2012). New performance measurement and management control systems. *Journal of Applied Accounting Research*, *13*, 226–241.

Widener, S. K. (2007). An empirical analysis of the levers of control framework. *Accounting, Organizations and Society*, *32*, 757–788.