An explorative approach on the impact of external and organizational events on information security

Ilirjana Ajazaj[1], Sebastian Kurowski[2]

Abstract: This contribution aims at the research question on which observable organizational events occur prior to an information security incident, and how these may relate to the organization. It therefore uses a dataset that was built using Google News, and the list of data breaches from [Mc17] to analyse which organizational events occur most often. It provides a categorization of these events, which were built by using a grounded theory approach. On the other hand, causal chains are constructed by using the sociologic system theory and constructivism. Both, the causal chains and the organizational event categories are applied together within this contribution to discuss, the likelihood of the causalities of the occurred events. However, events, such as financial gains also exhibit a higher occurrence prior to an information security incident. This contribution is a speculative, yet first approach on this question. Further research will focus on refining the constructed causalities.

Keywords: information security management, security culture, constructivism

1 Introduction

Externalities of the information security subsystem and its environment are rarely considered within the literature. Existing research, such as [No12], [No14a], [No14b], find small but significant impacts of data breaches on the stock market. [Ku14], [Ku16], [Ro14] identify business model as an important prerequisite for sustainable information security services, and [An01] clearly find that the available information security budget impacts the quality of information security within the organization. However, all these contributions regard the organizations' information security system as a holistic, clearly separated system. Even system dynamics contributions only indicate external threats as information security system external influence factors [DR08]. However, the same system dynamics model regards the information security budget as an additional influence factor [DR08], which we assume to be different, e.g. during a financial crisis, and thus influenced by external factors as well.

This contribution focuses on the impact of externally observable inter- (inside), inter-

[1] Institute for Labour Science and Technology Management, University of Stuttgart, Competence Team Identity Management, Allmandring 35, Stuttgart, 70565, ilirjana.ajazaj@iat.uni-stuttgart.de

[2] Institute for Labour Science and Technology Management, University of Stuttgart, Competence Team Identity Management, Allmandring 35, Stuttgart, 70565, sebastian.kurowski@iat.uni-stuttgart.de
The Annex is available at:
https://www.researchgate.net/publication/318209375_On_the_impact_of_external_and_organizational_events_on_organizational_information_security_-_Annex

(between), and extra-organizational (in the relevant environment) events. More specifically, we want to know if, and which events regularly occur before a data breach. In order to approach this research question, we acquired news events with Google News up to 6 years prior to a data breach, of organizations listed in [Mc17]. Following a grounded theory approach [Ra15], the data was categorized and used to construct causal relationships between observable events and assumed resulting failures of the information security system of the organization. Hereby, sociologic system theory [Lu84], and its' applications to organizations [Lu11] and risk [Lu90] were used for structuring the construction. Constructivism [Jo91] was used as underlying philosophy. We assume that any data breach that is reported in [Mc17] is not subject to chance, but rather the result of failures of the information security management system. We define information security system as an information security management system with all technical, organizational, and socio-technical information security controls as defined in [IS05], [IS13a], [IS13b]. Additionally, this contribution introduces descriptive statistics indicating the commonness of observed categorized events prior to an information security incident. Both the causal relationship between observed events and the commonness events together should provide enough insight to draw first conclusions.

This contribution is structured as follows. Section 2introduces the research subject and methodology. Section 3 introduces the categories of observed news events which occurred prior to an event, along with the construction of causal relationships of these events to the assumed failures of the organizations' information security system. Finally, Section 4 provides an analysis of the commonness of news events prior to information security incidents. Our findings are briefly discussed in concluded in Section 5.

2 Methodology

As mentioned throughout the introduction, the research that is presented in this contribution aims to shed light at previously not discussed relationships. Therefore, the research subject is briefly introduced throughout the following section.

2.1 Research Subject

The following Fig. 1 provides an overview on the research subject of the contribution.

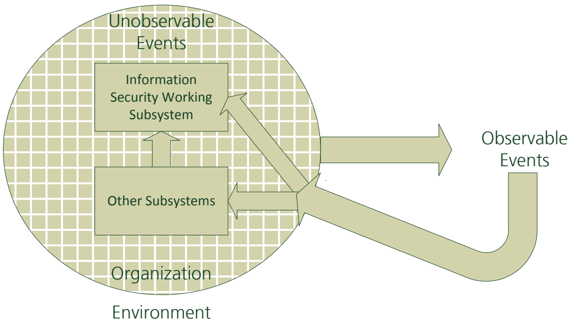

Fig. 1: Research Subject of the contribution

Our analysis tries to shed light on the question, whether, and how events that occur prior to a data breach may result in failure of the information security system of the organization. Observable events are hereby events that can be generated by an organization (for instance mergers), and/or impact the organization (for instance the loss of a customer). We assume that the observable environment impacts the information security working system, whereas a working system is defined as the consolidation of all interacting parties that collaborate on information security tasks. In information security systems that align with current information security management standards, such as [IS13a], [IS13b], this can include security specialists and non-security users. We assume that externally observable events may be the result of, or impact the information security working system directly, or via other subsystems of the organization that are at first glimpse not involved in information security tasks (e.g. corporate management).

2.2 Used construction scheme

In order to construct the information security working system, we use the sociologic system theory [Lu11], [Lu84], [Lu90]. In this theory, any interaction is regarded as communication between two subsystems, whereas any system can be divided into numerous subsystem, and any subsystem can be divided into subsystems itself. System theory assumes that individuals are characterized by a psychologic black box [Lu84] which allows us to disregard psychological constraints, as e.g. dispositional factors [Jo16]. Any action within the system, e.g. collaboration during deprovisioning of access rights, or classification of assets, is regarded as communication between actors of the (sub-)system. The system hereby differentiates itself from its environment by these structures. Every communication is based upon basic elements, which in the information security working system we assume to be the sense of acting in the information security system in the first place, and the perceived risk of the participating actors. Risk is hereby regarded as anticipation upon an observation by an individual [Lu90], and thus as subject to not further defined constraints, such as knowledge, by the psychological black boxes of the actors. Finally, the communication between the actors is characterized by double contingency [Lu11], [Lu84], meaning that either side cannot securely predetermine the actions of the other side upon an act. This may influence the act of either side, e.g. by abandoning the act altogether. Double contingency is clearly influenced by trust, which reduces the asymmetry of information and allows the communication between the parties (e.g executing the act), to be more smoothly [Lu11], as less controlling is required. A system in sociologic system theory only prevails, if it is capable of autopoiesis [Lu84], meaning that it reproduces its structures, and the basic elements that these structures are based on in the next iteration of its' existence. If this is not the case, the system will diminish, or fail.

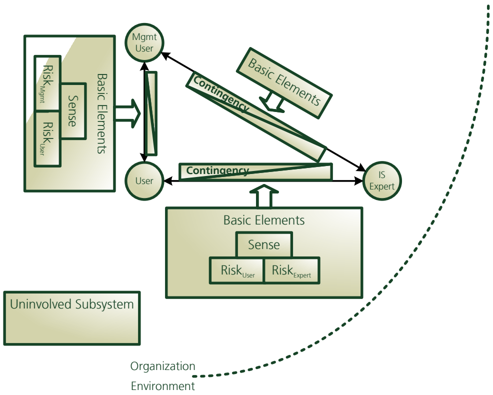

Fig. 2: Constructed relationships within the research subject

2.3 Used construction methodology

[Ur09] define guidelines for grounded theory studies in information systems. These guidelines include the constant comparison of data instances within a particular category with other instances of data in the same categories, '...exposing the analytic properties of the codes and categories to rigorous scrutiny.' [Ur09]. The level of abstraction should be iteratively increased, and categories should be related to each other by 'a process of iterative conceptualization' [Ur09]. Theoretical sampling should be applied to analytically decide which data is sampled. Higher-level categories should be scaled up into broader themes in order to contribute to the generalizability, and thus to the comparability of the theory with the broader literature. Finally, the study should compare a substantive theory to other developed theories, which contributes to 'theoretical integration' of the generated theory [Ur09]. Constant comparison was addressed by involving three different persons in different steps of the data acquisition and synthesis process that led up to the causal relationships of this contribution. Person A conducted the data acquisition, Person B categorized the data, and Person C developed the categories of causal relationships based upon the categories. Throughout development of the categories and development of the causal relationships constant comparison of the categories with the data was necessary. Furthermore, this process provides an iterative conceptualization, as Person B first provided first-order categories, which were than consolidated towards second-order categories, and finally related towards broader causal relationships by Person C. As this process also involves scaling up of the applied categories towards broader causal relationships, does also satisfy the guideline for scaling the grouping up. The constructed causal relationships have not been systematically compared with the broader literature, however existing but not systematically acquired literature on information security policy compliance, and information security management systems has been used, satisfying the theoretical integration. Finally, theoretical sampling does not apply to this contribution, as no further data samples, than the one used in this contribution have been acquired. In this issue, it should be noted, that the philosophical foundation of the sociologic system theory is constructivism [Jo91], which means that it can only be used to create one of many competing realities. The indications of Section 3.2 are thus rather speculative, as no objective truth can be assumed.

2.4 Data Acquisition and Synthesis

In order to acquire the data, news events for the 30 organizations listed in [Mc17] up to 6 years prior to the reported data breach, have been acquired by using Google News. Hereby, only news reports that were referring to an event that could be exactly located in time were used. This excluded any marketing reports, or general descriptions of organizations. Unfortunately, not all organizations were reported on equally in the time span of 6 years. Thus, some organizations did not include news coverage over 6 years. Additionally, some organizations had reported data breaches prior to the ones referred to in [Mc17]. Therefore, to retrieve an internally consistent sample, only 10 events prior to the data breach were considered. Additionally, only those organizations were considered that did not include a reported data breach, prior to the one referred to in [Mc17]. This resulted in news events from the following organizations: Zappos, Yahoo Japan, Vodafone, UbiSoft, South Africa police, Scribd, Nintendo, Living Social, Kirkwood Community College, Indiana University, Evernote, Citygroup, Apple, Advocate Medical Group, and Adobe. Therefore, the used sample included 15 organizations. For comparison purposes, the amount of relevant information was limited to 10 events before the IT security incident. These 10 events constitute the relevant period of investigation for the impact of the events on a subsequent IT security incident.

3 Observable Events and their causal chain towards information security system failure

3.1 Categorization of events

In order to systematically determine the causal effect of the observation on a data breach, the contents of news events were coded and first partitioned into categories (first-order codes). Using the news events and the first-order categories, all first-order codes were then aggregated towards second-order categories. Those second-order categories were then aggregated into broader third-order categories. During coding, the contents of the selected announcements, reports and articles were broken up and reduced to elementary, event-related information. This stepwise increase of abstraction is well-aligned with the guidelines of [Ur09] (see Section 2.4). It tries to construct valid and efficient means for conceiving events of different kinds (with potential similar effects on organizations) through an inductive procedure.

In total, 22 1st order codes and 9 2nd order codes were identified. Tab. 1 shows the generated categories.

The category ‘Divergence’ refers to conflicts of interest between business partners. ‘Information disclosure’ means the disclosure of organizational information by an organizational partner. The two categories constitute the 2nd order category ‘Conflict between trading partners’ and are assigned to the first category ‘Disturbances of external relationship of the organization’. If an organization is taken over by or takes over another organization, the categories ‘Organization takeover of’ or ‘Organization takeover by’ are used. The category ‘Cooperation/Partnership’ is used when organizations start a new cooperation or partnership with a specific strategic aim. For this purpose, the category ‘Structural coupling’ is used as a 2nd order category and means the (un-)specific cooperation, consolidation or a stable, reciprocal influence of organizations. The categories ‘Value gain’ or ‘Value loss’ mean the increase in (financial) resources or the loss of an organizations value or resources. These two categories are summarized as the 2nd order category ‘Function’. Function means the performance factor (e.g. tasks/goals, interests, responsibilities) in organization and occurs when the organization is fulfilling this function in a salient way. The ‘New orientation’ category means a new direction of action or a new cultural style, which could lead to such a change within the organization. The category ‘Expansion’ means the growth of an organization, such as domestic or abroad business expansion. The category ‘Improving the product range’ means, an improved version of existing products. The category ‘Changing the product range’ means a further development of the products or product displacement. The category ‘New offering’ means the diversity of offering. With these categories the 2nd order category ‘Restructuring’ can be formed. The categories ‘Hiring’, ‘Layoff’ and ‘Changes of leadership’ are summarized into ‘Changes in Personal’ as a 2nd order category. All these categories are assigned to the second order category ‘Structural changes of the organization’. The 2nd order Category ‘Reputation’ includes the categories ‘Positive’ and ‘Negative-Headline’ and means the public perception of a company in the organizations’ environment. In total, these categories are assigned to the third category ‘Changes of the organizations’ environment’. The 2nd order Category ‘Rivalry’ reports on the competing organizations in the organizations’ environment and includes the categories ‘Competition’, which means an increase in competitors, and ‘Merger of competitive companies’. The categories ‘Legal proceedings between organizations’ and ‘Legal violation’ are assigned to the 2nd order category ‘Legal proceedings’ and mean any legal proceedings between organizations. The category ‘Hacker attack’ means the reporting of externally forced data outflows in an organization. These categories are assigned to the fourth category ‘External pressure on the organization’.

3.2 The causal chain towards information security system failure

By applying the scheme introduced in Section 2.2 along with the acquired data categories (see Section 3.1), we are able to provide causalities by arguing that organizational events may result in (a) an increase of double contingency between the subsystems, (b) a differentiation of senses in the communication, or (c) a differentiation of risks in the communication. An overview on the causalities along with the categories can be found in the Annex. **An increase of double contingency** can occur out of the extension of a business unit (e.g. new hiring), the introduction of new management roles, or by pressure that results out of newly created competing business units, and internal or external pressure on the employees (e.g. in the case of financial losses). The increase of double contingency is essentially driven by a loss of trust between the users of the system. As indicated in Fig. 2 the communication processes that can be negatively affected by an increase of double contingency are between the user and the management of the user, between the user and the information security expert, and between the management of the user and the information security expert. Both, the relationship between the management of the user, or the user, and the information security expert are characterized by different perceptions of their role in information security [AH09]. This means, that security experts may expect users to act against the organizations’ information security goals, whereas the user, and the management of the user may expect the security experts to act against their own business, value-driven goals. Analogously, the relationship between the management of the user and the user may be driven by different goals. The management of the user may expect the user to act, e.g. more efficient, whereas the user may want to increase its own utility, e.g. by reducing his/her own workload. This ultimately results in a situation, where managements actions are driven by the expectation, that the user may want to avoid work, whereas the users actions are driven by the expectation that his/her management want to increase his/her workload, against his/her will. Such a setting is usually observed in studies that build upon the principal-agent theory [LM01]. This lack of trust however, may lead to information security tasks not being executed[3]. For instance, if the user expects its management to reduce the staff, he/she may start to tend to concentrate less on security-oriented tasks over business-oriented tasks. If management or the user tends to perceive the information security experts to not act in their favor, they may fail to execute fully, or adequately security-oriented tasks, hiding this lack of security task quality towards the information security experts. As a consequence of both situations, security controls such as access rights deprovisioning, correct application of security classifications, return or

[3] For instance [Li14] find that the perceived organization justice by individuals influences internet use policy compliance intentions, and fosters ethical objections against internet abuses. More generally, [CS01] show in their meta study that perceived procedural justice, organizational justice, and distributive justice were related to satisfaction measures including trust and organizational commitment.

handling of assets, or reporting of security relevant observations, or even incident reporting may be jeopardized: The organization becomes vulnerable. A **differentiation of senses** refers to the basic element of sense being jeopardized. This means, that communication between the participants of the affected structure may be jeopardized and thus ultimately abandoned. If for instance, the user does loses the perception of sense in notifying the information security expert, or his/her management that access rights are no longer required, he/she may ultimately abandon the task altogether. Without sense as a basic element, the reproduction of the structure is not possible, and the system will start to dissolve [Lu84]. Communication partners may start to perceive different senses of doing something. For instance, while the information security subsystem **may** perceive the sense of policy compliance to be the protection of the organization from existing and real threats, the user may not perceive the behavior required to be policy compliant to be backed by sense. As a consequence the user may abandon being policy compliant altogether. The differentiation of sense can be subject to changes in priorities of either side. For instance, in the case of mergers & acquisitions, competing business units, or even on a smaller level competing employees may be introduced, which may switch the focus of the employees away from security-oriented tasks towards business-goal-oriented tasks (e.g. increasing the working efficiency). The same holds if pressure is introduced either on the subsystem as a whole (e.g. in the case of financial losses, or rising market competition). Also, if new management is introduced in the system, users may perceive the mentioned pressure. The consequences of pressure in any case are that the sense of information security is overshadowed by the sense for other more important tasks, and ultimately forgotten - the information security subsystem dissolves. Differentiation of sense can also be the tipping point that results out of newly composed subsystems. In the case of restructuration for instance, employees that are already in the organization are introduced in new business units. As the sense of information security is not perceived equally [AH09], the newly composed system already starts off with different senses of information security. This can lead to processes being hindered or ultimately abandoned either until the next restructuration, or until the sense between the systems participants has been unified. Analog to the differentiation of sense, results **the differentiation of risks** in the absence of an important basic element for information security tasks. If risk is considered as an element that has been individually anticipated out of an observed threat [Lu11], [Lu90], both communication partners in our scheme must anticipate the same risk in order to provide a basic element for the information security tasks. However, along with the users illusion of control [La75], [Mc93], [Rh05] that is required for smooth operation of the organizational system [Lu11] it is likely that the basic element of risk is different. Even if the risks perceived by either participant of the system is equal, it may be argued that due to the mention precondition of risk anticipation this basic element is highly vulnerable to impacts by the causal chains described for the differentiation of senses. In this case, the system participants would be only left with the sense of information security. If one argues that the sense of information security, is the mitigation of risks, the differentiation of these risks between the participants also damages the unified sense of information security.

4 Observable Events prior to information security system failure

While the previous Section provides a short overview on the possible causalities that can be drawn from the observable organizational events, the following focuses on which events occur more frequently, and more often before a reported incident.

4.1 Second Order Codes and Incidents

Tab. 4 first off shows the findings within the identified categories of events by the point of time before the IT security incident. The first category of events ('Disturbance of external relationship of the organization' or 'Conflict between business Partners') only shows one event of fifteen possible events, directly before the security incident. Therefore, it was only possible to identify one organization, which was exposed to an event within the relationship to its business partners. The second category of events ('Structural changes of the organization'), indicates an amount of nine, the third category ('Changes of the organizations' environment') an amount of five and the fourth category ('External pressure on the organization') an amount of two events immediately before the IT security incident. Overall, the means of the categories are 1.2 in the first category, 10.5 in 2nd, 3.6 in the 3rd and 3.3 in the 4th. It becomes clear that the second category contains the most relevant events at every point in time. When combined or observed separately, the third and fourth categories seem to hold an importance for the number of events within the organization or its environment before an IT security incident. With a mean of 1.2, the first category is clearly underrepresented and therefore it will be excluded from further analysis. For this reason, it is assumed that events like divergences within the relationship to business partners or the disclosure of information by such partners exert no relevant impact on the occurrence of IT security incidents.

4.2 First Order Codes and Incidents

To sort out the occurrence of the specific events in each category, the categories need to be split up in their components. This allows examining their specific impact on the entirety of categories. Therefore the 1st order codes will be focused. The 1st order codes, shown in Tab.2 represent the second category ('Structural changes of the organization'). Among these codes it is noticeable, that the 1st order code 'New offerings' shows a high mean of 2.7 for those points in time in which it occurred at all. 'New offerings' occurred at all points of time which were observed. This is followed by the code 'New orientation', which shows a mean of 1.9 for eight of ten points of time, in which it occurred at all. According to the same logic the code 'Cooperation' shows a mean of 2.0 for four out of ten points of time. At the point of time, immediately before the IT security incident the codes 'Organization takeover by' (1), 'New orientation' (2), 'New offerings' (3), 'Hiring' (1) and 'Change of leadership' (1) appear. It is noticeable that nine out of thirteen codes occur at the fifth point of time before the IT security incident. Also important seems to be the fact that the code 'New offerings' is present throughout the whole observed span of time with a high occurrence. The codes ‘Changing of the product range’ and ‘Expansion’ all occur only once. Therefore, it can be said that among the second category ‘Structural changes of the organization’, the code ‘New offerings’ plays a dominant role. The third category of events (‘Changes of the organizations’ environment’) contains the two codes ‘Positive Headline’ and ‘Negative Headline’. The dominant code among the types of events is ‘Negative headlines’ with a mean of 2.6 and a minim of one occurrence at each observed point of time before an IT security incident. The code ‘Positive headline’ follows with a mean of 1.7 over six out of ten points of time.

The category ‘External pressure on the organization’ contains the codes ‘Competition’, ‘Merger of competitive organizations’, ‘Legal proceedings between organizations’, and ‘Legal violations’. In this category of events it is salient that from the fifth point of time on to the security incident there seems to be hardly any occurrence of the basic event types at all. The period of time directly before an IT security incident therefore doesn't give any reason to believe that external pressure on the organization plays a major role in the following security incident. Only the code ‘Legal violations’ at the third point of time before the incident could be indicating an influence of external pressure on the organisation and its IT security. Overall the means are: 1.5 for ‘Competition’, 1.0 for ‘Merger of competitive companies’ and ‘Legal proceedings between organizations’ and 1.8 for the code ‘Legal violations’.

Our findings show that structural changes of the organization occurs the most often, and the most frequent among all events that occurred prior to an incident. 10 of 15 organizations have indicated a structural change. However, the frequency of structural changes in the sample is relatively high (10.5), which shows, that these changes occurred in any random order prior to an incident. If structural changes are considered more closely, New Offerings occur most often (10 of 15 organizations), and more closely to the incident (mean frequency 2.7). This is followed by change of leadership (8/15, f=1.1), new orientation (8/15, f=1.9), and value gain (7/15, f=1.6). Along with our previous construction of three different causalities (see Section 3), this could indicate that the loss of the basic elements of sense and risk (new orientation, change of leadership), along with the increase of double contingency (change of leadership) due to structural changes, hinders the information security tasks in the organization. However, the indication of value gain before an information security incident can neither be explained by pressure, nor by differentiation of sense and risk. Changes in the organizations environment partially support the previous statement: When looking at the changes of the organizations environment, negative headlines that induce pressure on the system occur more often (10/15, f=2.6), and especially very often just before an incident than positive headlines (6/15, f=1.7). Also for external pressures on the organization, rising competition on the market, (6/15, f=1.5) and reported legal violations (6/15, f=1.8) by the organization, which both increase the pressure on the organizations’ subsystem (see Section 3).

5 Conclusion

This contribution provides a construction of possible causal chains that lead from observable organizational events to information security incidents. Due to the complexity of the observed system, and the large amount of unobservable variables, this research is in nature highly speculational due to the application of a theory that is founded in the philosophy of constructivism. Whether Google news events are in any way an expression about the actual behaviour of an organization, its structures or communications remains open for further analysis. It should also be mentioned that certain news are published by the company itself and therefore a further differentiation would be necessary. In summary it can be said, that the most important findings of the data evaluation are based on three types of news events, namely ‘New offerings’, ‘New orientation’ and ‘Changes of leadership’. These categories may be taken together as ‘Structural changes of the organization’. In fact there is a high coincidence between these categories. So these three types of news are probably the most frequent organizations produce, in this case, this analyse shows a close correlation.

We highlight the role of basic elements and double contingency within the information security subsystem. Our explorative analysis indicated that the majority of events that occur at most organizations are associated with one or more of our causal chains. However, not all events support the causal chains. For instance, legal violations occur frequently before an information security incident, but legal proceedings between organizations do not. Also, the frequent occurrence of structural changes to an organization prior to an information security incident, while being a good match for the causal chains, may also only be subject to the larger amount of data points within this category. Future research will thus approach this subject both by using qualitative content analysis, and time series analysis (e.g. by creating markov chains). This will be used to further refine, and critically discuss the causal chains that are introduced within this contribution.

6 Bibliography

[AH09] Albrechtsen, E.; Hovden, J.: The information security digital divide between information security managers and users. Comput. Secur. 28, 6, 476–490 (2009).

[An01] Anderson, R.: Why information security is hard - an economic perspective. In: Proceedings of the 17th Annual Computer Security Applications Conference, 2001. IEEE (2001).

[CS01] Cohen-Charash, Y.; Spector, P.E.: The role of justice in organizations: A meta-analysis. Organ. Behav. Hum. Decis. Process. 86, 2, 278–321 (2001).

[DR08] Dutta, A.; Roy, R.: Dynamics of organizational information security. Syst. Dyn. Rev. 24, 3, 349–375 (2008).

[IS05] ISO: Information technology - Security techniques - Code of practice for information security management. , Geneva, CH (2005).

[IS13a] ISO/IEC: Information technology - Security techniques - Entity authentication assurance framework. ISO/IEC, Geneva, CH (2013).

[IS13b] ISO/IEC: Information technology - Security techniques - Information security management systems - Requirements. ISO/IEC, Geneva, CH (2013).

[Jo16] Johnston, A.C. et al.: Dispositional and situational factors: Influences on information security policy violations. Eur. J. Inf. Syst. 25, 3, 231–251 (2016).

[Jo91] Jonassen, D.H.: Objectivism versus constructivism: Do we need a new philosophical paradigm? Educ. Technol. Res. Dev. 39, 3, 5–14 (1991).

[Ku14] Kubach, M.: Effektives Identitätsmanagement in der Cloud. Forsch. Kompakt. 08, 17–18 (2014).

[Ku16] Kubach, M. et al.: Non-technical Challenges of Building Ecosystems for Trustable Smart Assistants in the Internet of Things: A Socioeconomic and Legal Perspective. In: Hühnlein, D. et al. (eds.) Open Identity Summit 2016, Lecture Notes in Informatics – Proceedings. pp. 105–116 Köllen, Bonn (2016).

[La75] Langer, E.J.: The illusion of control. J. Pers. Soc. Psychol. 32, 2, 311 (1975).

[Li14] Li, H. et al.: Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. Inf. Syst. J. 24, 6, 479–502 (2014).

[LM01] Laffont, J.-J.; Martimort, D.: The Theory of Incentives: The Principal-Agent Model. Princeton University Press (2001).

[Lu11] Luhmann, N.: Organisation und Entscheidung. VS Verlag, Wiesbaden (2011).

[Lu84] Luhmann, N.: Soziale systeme. Suhrkamp Frankfurt am Main (1984).

[Lu90] Luhmann, N.: Technology, environment and social risk: a systems perspective. Organ. Environ. 4, 3, 223–231 (1990).

[Mc17] McCandless, D.: World’s Biggest Data Breaches & Hacks, http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/, accessed: 20/07/(2017).

[Mc93] McKenna, F.P.: It won’t happen to me: Unrealistic optimism or illusion of control? Br. J. Psychol. 84, 1, 39–50 (1993).

[No12] Nofer, M. et al.: The Economic Impact of Privacy Violations and Security Breaches - A Laboratory Experiment. (2012).

[No14a] Nofer, M. et al.: Der ökonomische Einfluss von Privacyverletzungen und Securityvorfällen. Wirtschaftsinformatik. 56, 6, 369–380 (2014).

[No14b] Nofer, M. et al.: The Economic Impact of Privacy Violations and Security Breaches: A Laboratory Experiment. Bus. Inf. Syst. Eng. 6, 6, 339–348 (2014).

[Ra15] Ramalho, R. et al.: Literature Review and Constructivist Grounded Theory Methodology. Forum Qual. Sozialforschung Forum Qual. Soc. Res. 16, 3, (2015).

[Rh05] Rhee, H.-S. et al.: I am fine but you are not: Optimistic bias and illusion of control on information security. ICIS 2005 Proc. 32 (2005).

[Ro14] Roßnagel, H. et al.: What is wrong with Supply and Demand of Federated

Identity Management Systems? Eur. J. Inf. Syst. forthcoming, (2014).

[Ur09] Urquhart, C. et al.: Putting the “theory” back into grounded theory: guidelines for grounded theory studies in information systems: Guidelines for grounded theory studies in information systems. Inf. Syst. J. 20, 4, 357–381 (2009).