# Information Security Policies in Organizations

## How Convention Theory Can Serve as a Framework to Inform Information Security Research and HR Practice

**Dominik Zellhofer**

**Abstract** The increased use of information technology throughout organizations led to a surge in concern for information security. Information security standards guide information security policy implementation, but the challenge of ensuring compliance is still a major issue, despite extensive information security research. The lack of versatility in theoretical approaches spurred calls for sociological approaches to contribute to the literature, but they were only partly addressed. The proposed framework of convention theory can serve as a fruitful approach by providing a holistic perspective and a strong theoretical foundation. The use of human resource information systems (HRIS) und electronic human resource management (e-HRM) extends the concern for information security to human resource (HR) practices and data privacy is no longer an issue solely for external stakeholders but for employees alike. At the same time, the role of HR practices in contributing to compliance with information security policies seems to be underestimated in existing literature. This paper introduces main concepts of a convention theory-based framework and illustrates implications for information security research and suggests that HR practices can contribute to ensuring information security in organizations.

**Keywords** Information security policy · HR practice · Convention theory

D. Zellhofer (✉)
Interdisciplinary Institute for Management & Organizational Behaviour,
WU Vienna (Vienna University of Economics and Business), Welthandelsplatz 1,
1020 Vienna, Austria
e-mail: dominik.zellhofer@wu.ac.at

F. Cabitza et al. (eds.), *Organizing for the Digital World*, Lecture Notes in Information
Systems and Organisation 28, https://doi.org/10.1007/978-3-319-90503-7_5

## 1 Introduction

In 2013, the New Yorker published an article titled "Steamrolled by Big Data" [1], depicting the triumph of this buzzword in the recent years. Indeed, there is a sense of gold fever regarding data in many sectors of the economy, fueled by the advances in information technology. As a consequence of the growing availability of big data, organizations rely heavily on large amounts of data in almost aspects of their business, from supply chain management to marketing. As data processing is based on modern information technology, with interfaces not only to customers but other stakeholders as well, organizations need to ensure data security from outside and inside threats. In 2014, a substantial security breach caused a leak of account information of 145 million eBay-users [2], drawing major media scrutiny. An international, IBM-sponsored study finds that the average cost of a data breach in 2016 was four million dollars, with the cost per incident having increased by 30% since 2013 [3]. Although hackers are frequently the culprits in such incidences as mentioned above, the threat does not exclusively stem from external factors. In fact, Stanton et al. [4] report that between 50 and 75% of all data security violations are caused by internal stakeholders. Despite of the obvious image of a disgruntled employee, non-compliance to security standards is often unintentional, a problem of awareness [5], the lack thereof leading to (non-malicious) non-compliance.

Attempts to minimize these inherent risks of information processing led to the development of standardized information safety procedures, reflected through information security standards like ISO27000, COBIT or ITIL, which in turn are implemented through organization policies. These policies target issues concerning the organizational environment and intra-organizational processes alike.

In the past, technology-focused research on information systems security was successful because information technology was largely an issue of a single function in the organizational hierarchy, whereas today organizations rely on information systems in every aspect of their business [6]. This trend also directly impacts HR practice, not only because of the need for proper training, e.g. concerning information security awareness [7]. HR departments increasingly rely on human resource information systems (HRIS) and electronic human resource management (e-HRM) [8]. Beadles et al. [9] found in their study that 80% of HR-directors reported that HRIS increased the usefulness of information and their ability to disseminate it, while 90% thought that HRIS added value to the organization. The intent of use of HRIS is not limited to improving efficiency and cutting costs of information processing. As Kovach et al. [10] note, it is not restricted to maintaining employee records anymore, but is used as decision support systems, communication systems, transaction processing systems and more. While there is no unique definition of e-HRM [11], it generally denotes the interface to other stakeholders in the organization, making the HR department internal HRIS accessible to employees while both HRIS and e-HRM are now often embedded in organization-wide information systems [8]. Besides efficiency and cost benefits of these systems, the privacy of employee and customer data alike must be guaranteed or organizations face a loss of legitimacy, not only in the legal context, but in the broader societal context. The obvious challenge therefore is to ensure acceptance and compliance of good security practices in organizations, guided through the implementation of security policies.

Zafar and Clark [12] note that the term “information security” has a plurality of definitions, depending on the perspective, seeing a progression from mere technological viewpoints to behavioral, managerial, philosophical, and organizational perspectives. In an attempt to provide a holistic view of information security, they derive a definition that includes the identification and assessment of risks and associated threats, training of personnel in security awareness and best practices, the implementation and monitoring of technologies to prevent security breaches, the implementation of policies and procedures to prevent misuse and loss in the event of a security breach, and lastly the incorporation of information security governance as part of corporate governance. Williams [13] gives a similar description, grouping tasks of information security in availability, confidentiality, integrity, authenticity and non-repudiation of information systems. In an attempt to provide a model of factors that contribute towards information security specifically in HRIS and e-HRM, Zafar [8] provides a similar account of significant aspects, including policies.

## 2 Information Security Policies

I focus on information security policies to depict the perspective of a convention theory-based framework as they show the conventional nature of coordination in a very material way, a document that describes “good” practices, guided by international industry standards and implemented with the intent to shape the organizational members’ day-to-day practices. In general, a policy is simply a general rule to limit the discretion of subordinates in an organization [14]. Similarly, management information systems research defines policies as a control instrument to establish limits of acceptable behavior, guide and restrict decisions and serve as standards [15]. While the formulation of such documents, including the exact wording, is important, the generation and implementation process itself is also important, because it must aim to ensure acceptance within an organization. Knapp et al. [16] acknowledge that there is a plethora of frameworks and guidelines in literature concerning the formulation and implementation of security policies, but they did not find a framework illustrating the overall process of developing and managing information security policies within the organizational context. Their framework is based on the account of practitioners, thereby providing an overview that is based on actual practices in organizations. When comparing their framework with the list of what information security entails given above, it is clear that the process of applying information security policies entails all these aspects. I intentionally chose the word application over implementation, as the latter does not sufficiently convey the dynamics of policy use (see Fig. 1). Practitioners are aware of continuous tasks like awareness trainings, monitoring and policy enforcement, while also acknowledging influences of organization culture and institutional pressures of industry standards and legislation.

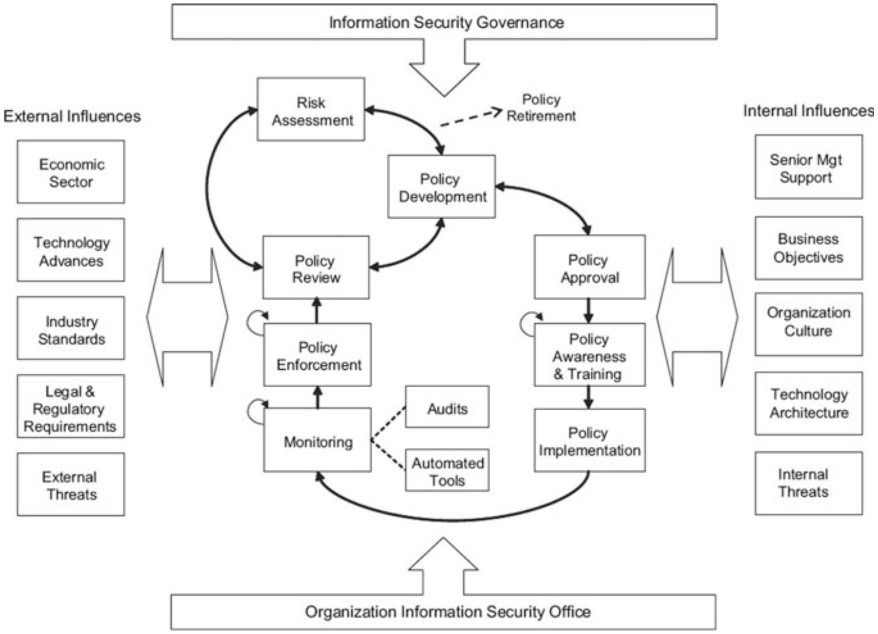

**Fig. 1** Comprehensive information security policy process model [16]

Measures to increase information security awareness are considered an important step in achieving compliance [7]. These measures serve to make employees aware of their “security mission” [17] and therefore foster compliance with security policies. This hints at the need for (constant) dialogue and the insufficiency of just writing up a policy [18]. The focus on individual behavior is reflected in information security research, Warkentin and Willison [18] state that much of the focus within the behavioral security research community has been on information security policy non-compliance by employees. On the other hand, Orlikowski and Barley [19] argue that, while information technology research occasionally references organization studies, it is still underrepresented and call for a stronger focus on the institutional context. Interestingly, they find that the reverse is also true, organization studies often carelessly neglect how technologies shape organizations.

Clearly, the problem of information security is an inherently complex one, combining technical issues with social, psychological, and organizational aspects, therefore a holistic approach to tackle these problems requires interdisciplinary efforts [20]. Earlier calls for sociology to provide a strong theoretical foundation to enrich information security research were made but only partly addressed [21] and the framework of convention theory proposed in this paper is a sociological perspective that attempts to integrate the aforementioned aspects.

Institutions play an important role in the coordination of persons and objects but at the same time, the capabilities of the individuals to shape the situations he or she is in are extremely relevant too. Focusing the analysis on the level of the situation instead of the collective or the individual, convention theory also acknowledges that the materiality of the environment is a fundamental aspect of its framework, as coordination is not only necessary between human agents, but also with material objects, which in turn shape the view of the world of the actors. In the following, I will introduce essential concepts of the theoretical framework after briefly situating convention theory in the history of sociology.

## 3 Convention Theory—A Pragmatist Approach

In the first half of the twentieth century, collectivism seemed to be the only alternative to the individualism proposed by the economic model of man. Durkheim et al. [22] was the most prominent proponent of the "old social sciences" [23]. In the late 1960s, Pierre Bourdieu moved the focus to the structural, hence his description as "philosophy without subject" [24]. Some twenty years later, a new French sociology, a movement consisting of sociologists, economists, political philosophers, and historians combined the Durkheimian notion of collective practices with individual action, thereby shifting the focus on the genesis of institutions or conventions [23]. In this new interpretation of human action, "convention" does not only address traditions, rituals or customs in a Weberian [25] sense of the word, but as culturally established logics of coordination [26]. The notion that conventions are essential for coordination stresses the aspect of legitimacy, a concept that is also inherent to institutions, although institutionalism has a more stable view of legitimacy. This is important because information security research mainly focuses on practices aiming to ensure regularities, like checklists and protocols, which shows that it is implicitly assumed that the goals of information security are commonly agreed on [6]. This leads to a neglect of the essential role of legitimation of said goals [27] and therefore to an underestimation of the relevance of legitimizing information security governance practices.

### *3.1 Orders of Worth—Defining Qualities of People and Things*

For coordination, it is necessary to agree on what is "good." This means that for coordination to be successful, people have to reduce the uncertainty about persons and objects by qualifying them, which means ranking them in regard to some kind of worth. Boltanski and Thévenot [28] initially identified the six most common *orders of worth*, but they argue there are many more left to discover. To understand how those orders of worth are relevant to coordination, one may consider the question how organizations maintain their legitimacy regarding relevant stakeholders. For the organization to maintain its legitimacy, it has to sustain the harmonious arrangement of things and persons in a state of general agreement [29]. To reach that agreement, one has to objectively qualify or classify things and people. This evaluation and qualification process is guided by orders of worth, which people refer to in disputes and which have to meet certain political and moral requirements [28, 30]. One example in the context of information security would be using the standard category of a Chief Security Officer (CSO) to convey responsibilities and power to a person and she would rank higher in terms of governing information security than the average employee. This would be a qualification along the *industrial worth*, where standardization is of value, because some kind of certification (along a standard), governing what a CSO is, would form that category. Important is that one has to refer to common orders of worth, because this negotiation happens in a public arena and referring to some very personal order of worth would not have legitimacy with other persons. Another example is the argument about how to apply technical equipment to produce a product or service in an organization. A security policy may change the use of a computer in another way than the employees traditionally used to, their argument would be based on the *domestic worth*, where tradition ranks high in importance. An overview of the initial six orders of worth and their attributes is given in Table 1. This requirement for justification in discourse and action with reference to more objective orders of evaluation is a clear distinction to traditional institutionalist approaches and requires actors to have specific competencies [29]. Once an agreement or compromise on orders of worth (there can be multiple orders at play at once) is reached, legitimate conventions that serve coordination based upon them can be established. Conventions "convene" qualified objects and human beings, they give a sense of what dimension of time and space is relevant.

Contrary to classic notion of institutions as being relatively stable, conventions are frequently put to a *reality test*. For example, established standards guide actions, they give security on what is good practice and thereby serve as a common logic of coordination. But these moments of "being at ease" with them are interrupted with moments of doubt, where the standard is unmasked as arbitrary, conformist, formulaic and inauthentic [32], where proof of legitimacy has to be given and the standard has to be justified. To be able to argue about the quality of things and people, one has to engage in discourse, but to be able to do so, information has to be put in a general form [33]. Convention theorists call this process *investment in form,* with the term "investment" hinting that this is a costly effort and depend on the capabilities of the actor. One may consider how programmers translate ideas into functions and methods, guided by the syntax of a programming language. A device does not know how to process an idea, but the compiler knows how to handle code. Note that there is a common understanding of what "good" code is, but there is also dispute about what good programming style is. It is important to keep in mind that when convention theorists talk about information transmission, they do not focus on the content but on the form of it, as Thévenot [34] notes: "*Information here refers to [...] coordination, with the understanding that coordination is always problematic.*" This notion reveals that different forms generate different "forms of the probable", which defines what can be proved and offered as evidence [30].

**Table 1** Schematic summary of orders of worth [31] (adapted)

| | Market | Industrial | Civic | Domestic | Inspired | Opinion |
|---|---|---|---|---|---|---|
| Mode of evaluation (worth) | Price, cost | Technical efficiency | Collective welfare | Esteem, reputation | Grace singularity creativeness | Renown, fame |
| Test | Market competitiveness | Competence, reliability, planning | Equality and solidarity | Trustworthiness | Passion, enthusiasm | Popularity, audience, recognition |
| Form of relevant proof | Monetary | Measurable: criteria, statistics | Formal, official | Oral, exemplary, personally warranted | Emotional involvement and expression | Semiotic |
| Qualified objects | Freely circulating market good or service | Infrastructure, project, technical object, method, plan | Rules and regulations, fundamental rights, welfare policies | Patrimony, locale, heritage | Emotionally invested body or item: the sublime | Sign, media |
| Qualified human beings | Customer, consumer, merchant, seller | Engineer, professional, expert | Equal citizens, solidarity unions | Authority | Creative being | Celebrity |
| Time formation | Short-term, flexibility | Long-term planned future | Perennial | Customary past | Eschatological, revolutionary, visionary moment | Vogue, trend |
| Space formation | Globalization | Cartesian space | Detachment | Local, proximal anchoring | Presence | Communication network |

The concepts of orders of worth, tests, and investing in forms make it possible to understand the implementation and functioning of a firm or other conventional resources like standards, rules and policies, all oriented towards specific values or worth, e.g. in the case of standards usually towards efficiency [35].

### *3.2 Regimes of Engagement*

The process of investing in forms hints at a second main concept of convention theory, the idea that these most legitimate orders of worth (also *regimes of coordination*) are fabricated on more basic *regimes of engagement* [30, 36]. As already mentioned, the evaluation and justification as described above happens in a public arena, but action or agency happens in another kind of engagement with the world. This engagement is associated with a different kind of confidence, and this confidence in turn is dependent on the power or capacity attributed to the agent and the support he or she recognizes in the environment [37]. Thévenot consciously avoids the terms action or practice, as these focus attention on the human agent, but neglects the person's dependence on the environment and the different conceptions of what is "good" (the French term *engagement* captures not only the very mechanical conception of engaging with something in the English sense of the term, but the notion of engagement with moral and political commitments as well [38]). Each regime of engagement implies a distinct cognitive format related to a different kind of access to the human environment of nature and artifacts [30]. Cognitive formats characterize the actor's access to reality and thereby how he coordinates his behavior within a certain apprehension frame [34]. The mechanisms previously described happen in the *regime of justification*, where confidence in politics and institutions are relevant. This regime demands the highest degree of legitimacy, the actor cannot rely on personal convenience as a way of qualification, but must rely on more common orders of worth as Boltanski and Thévenot [28] identified them. The format of information is also more conventional, e.g. reports are much more conventional than everyday language use [38]. On the other hand, the *regime of familiar engagement* describes an engagement with the world where the immediate material and human surroundings are deeply personal and the individual accommodated himself in them [37]. As already described, each engagement has its own format of information, and in this regime of engagement, information cannot easily be transferred by discourse, it is formatted in the language of the body. So the "good" which governs coordination of herself with her environment is a deeply personal good. An obvious example in the context of the topic at hand would be the employee's customization of his or her computer. A desktop wallpaper with pictures of family has no functional use, but it generates a kind of good that is hard to make obvious. It serves to making the work environment your own, just as the habit of suspending your coat on your chair, although it is against its original function and makes the chair less efficient to sit on. New information security policies might prevent the worker from changing desktop wallpaper, but in this case, he will have a hard time justifying this behavior and criticizing this new standard, because this kind of customization will mostly likely not rank high in common orders of worth which are at play in this situation. In contrast to the familiar engagement, the *regime of planned action* describes a more functional orientation with the environment, also to facilitate coordinated action with other actors. The good with which one grasps their environment is not entirely focused on the functional nature, but, as the name suggests, on successfully realizing a plan. The difference of this regime to the most public regime of justification is that the notion of what is good is loosely reliant on everyday narratives, on common knowledge, one is supposed to know what counts as "good working order" [38]. To illustrate, imagine the scenario of a shared workplace, where planned action is necessary to achieve a common goal of being productive. Conventions of how a workstation ought to be arranged to be suitable for coworkers may lead the worker to removing the very convenient post-it with handwritten passwords from the monitor.

The concept of regimes of engagement proves to be important when considering the process of applying information security policies in organizations: Establishing and maintaining legitimacy of said policies as a common mode of coordination is only one (nevertheless important) aspect. The coordination via planned action makes the functional aspect of a convention visible. The most intimate form of engagement with the world may hint at why employees' actual practices deviate from planned action based upon policy and could serve as a starting point when looking for potential sources of or reasons for dispute and non-compliance.

### *3.3 Organizations as Compromising Devices*

While other theories often grant organizations a reality on their own, convention theory is not interested in a concept of organization as a mode of coordination on its own [26]. Thévenot [30] defines an organization as a compromising device. He criticizes the common notion of a stable and collective order. Aspects of this idea are rules, hierarchical prescriptions, rationalizing and bureaucratic methods, social structures, shared representations and common culture which are seen as constraints, which Thévenot defines as "over-socialized" representations of this idea. He argues for a notion of coordination more open to uncertainty, critical tensions and creative arrangements. As a result, this conception of organization explicitly appreciates informal and personal practices, which could be an important piece of the puzzle regarding non-compliance to formal policies, without necessarily interpreting it as a pathology of organizations.

Conceptualizing organizations as compromising devices appreciates the tension created in organizations by different orders of worth governing coordination. For example, an organization must deal with the tension brought on by the need to standardize processes to ensure survival on the economic market. Driven by the value of efficiency, this may undercut practices that are based on trust and tradition, values that characterize the domestic world, leading to dispute and critique.

## 4 Contributions for Research and Practice

I will briefly illustrate a selection of aspects of how a conventionalist approach can inform information security research and argue that this perspective shows the relevance of HR practices in this matter, which seems to be neglected in both research and practice.

Convention theory moves the focus to the dynamic process of how coordination is established. The introduced concepts have several implications for research: The concept of orders of worth suggests that research should pay attention to justification and evaluation as an ongoing process, as described by reality tests. As this is done in a public arena, the level of analysis cannot solely focus on the individual. At the same time, the capabilities of the actor (e.g. his ability to invest in forms and bring arguments to the dispute) and how he or she perceives the world (which is again dependent on hints of objects in the coordination situation) are relevant too, which means that a mere focus on the collective level underappreciates the complexity of the situation. This is reflected in the methodological stance of convention theory, which can be seen as a "complex pragmatic situationalism" [26, 39]. The reference to particular orders of worth shape the cognitive format, as do the different engagements with the world. As a consequence, the concept of rationality is altered and shifted towards a "situated rationality" [14, 35]. This makes seemingly paradox irrational behavior interpretable. Because of the strong emphasis on the influence of the particularities of the situation, qualitative research approaches are at an advantage, although there are examples of the successful application of quantitative or mixed methods [40]. By valuing the influence of materiality, the proposed framework is particularly potent for providing insights in technology-rich contexts and appreciating the implications of socio-technical systems [41, 42]. The concept of regimes of engagement extends the framework beyond evaluation and dispute to the application of conventions. It can show how standards are applied [32] and make tensions between the most public and most intimate engagement with the world visible, while also differentiating a mode of coordination that is concentrated on following a plan, thereby it is possible to integrate into the analysis the aspect of legitimacy, functional use, and the role of familiarity and personal aspects, without drawing on theoretically separated models for each engagement. The examples I provided throughout the text highlighted some of details needed to be considered when conducting research, but issues of high importance remain which cannot be discussed here in full length.

Although much of information security research is behavioral, there is a lack of literature that stresses the role of HR practices. Information technology seems to be relevant for HR when thinking about e-HRM or HRIS, but existing literature would suggest that there is no relationship vice versa. Recently, a literature review on information security management [43] called for a holistic approach in information security management, explicitly including human resource management. This call should go far beyond mere employee training in awareness and IT literacy. Policymaking should be approached in a holistic way, especially if it directly impacts the way employees conduct their work. With the spread of digital devices that are attached both to private and working life (e.g. smartphones), ambiguity of conventional use is likely. Convention theory can shed light on this matter via the concept of regimes of engagement. Flexible working time arrangements are inherently connected to this issue and HR practice can address the resulting tension (e.g. using devices in the way the planned action regime supposes in an inherently personal environment of your home) by searching for compromise between differing orders of worth. This could speed up the process of setting up an information security policy by facilitating the shift from a regime of justificatory action to the application in the planned action regime. IT specialists usually prefer solely technical solutions, putting much effort in restrictions of possible actions of employees, but the effectiveness of tools like information security awareness trainings hint at a social dimension of the problem. This is also pointed out by research on information security culture [44]. Informing employees via training is only part of the solution, the aspect of personal engagement with the functional environment, implicitly addressed by the term "user behavior" must be considered too. This notion is entailed in the concept of reality tests, which also underlines the revolving nature of accepting and disputing standards. HR practices like performance evaluations or appraisal interviews could be used to investigate this aspect on a regular basis, without relying on solely technical instruments (as for example "automated tools" suggest in Fig. 1). External audits are a standard practice for information security policies, but they often fail to detect workarounds in actual practice, institutionalists would denote a systematic disparity of official practice and actual routine as decoupling [45]. Lastly, e-HRM could be a promising way to foster security behavior by "formatting" learning routines with services like e-learning. With respect to gathering data with HRIS, convention theory may provide a new perspective on resistance against these instruments by employees. While these instruments provide value in terms of efficiency and standardization (industrial worth), trust and privacy are important values in the domestic worth, as well as tradition. When a company decides to introduce HRIS, the extended use of these instruments may be seen as a breach of trust, because the system does not qualify within the domestic order of worth. Therefore, legitimacy is an important issue and HR practitioners have to be aware that compromising between those orders may be more fruitful way of solving dispute than relying solely on arguments of efficiency.

## *4.1 Limitations and Future Research Agenda*

Due to the scope of convention theory to cover a range of societal issues, grasping an understanding of the framework can seem daunting, which may stunt the spread to narrower fields like information security research or research on digitalization of HRM. The methodological standpoint can prove challenging when research traditions in some fields are purely quantitatively oriented and qualitative research is less common. Operationalization of constructs can seem daunting too considering the wide-ranging implications of the concepts. As Jagd [46] noted, the relevance of the framework for organizational processes has only been partly explored. The full potential of this framework can only be explored if future research applies it to a variety of topics, information security research is one promising direction that can add to a growing body of literature (for an overview of this research see [47]). The extension of the body of applied research may also strengthen the repertoire of implications for practitioners, and case-based formatting of research findings may help to make contributions visible for non-sociologists. The intent of this paper is not to provide a comprehensive account of convention theory and its application to the topic at hand, but should serve to foster discussion of the potential benefits for information security research and HR practice alike.

## References

1. The New Yorker. http://www.newyorker.com/tech/elements/steamrolled-by-big-data
2. Heise Medien GmbH & Co.KG: https://www.heise.de/security/meldung/145-Millionen-Kunden-von-eBay-Hack-betroffen-2195974.html
3. Cost of Data Breach Study: Global Analysis. Ponemon Institute (2016)
4. Stanton, J.M., Stam, K.R., Mastrangelo, P., Jolton, J.: Analysis of end user security behaviors. Comput. Secur. **24**, 124–133 (2005)
5. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q. **34**, 523–548 (2010)
6. McFadzean, E., Ezingeard, J.-N., Birchall, D.: Anchoring information security governance research: sociological groundings and future directions. J. Inf. Syst. Secur. **2**, 3–48 (2006)
7. Bauer, S., Bernroider, E.W., Chudzikowski, K.: Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. Comput. Secur. **68**, 145–159 (2017)
8. Zafar, H.: Human resource information systems: information security concerns for organizations. Human Resour. Manag. Rev. **23**, 105–113 (2013)
9. Beadles, I., Aston, N., Lowery, C.M., Johns, K.: The impact of human resource information systems: an exploratory study in the public sector. Commun. IIMA **5**, 6 (2005)
10. Kovach, K.A., Hughes, A.A., Fagan, P., Maggitti, P.G.: Administrative and strategic advantages of HRIS. Employ. Relat. Today **29**, 43–48 (2002)
11. Strohmeier, S.: Research in e-HRM: review and implications. Human Resour. Manag. Rev. **17**, 19–37 (2007)
12. Zafar, H., Clark, J.G.: Current state of information security research in IS. Commun. Assoc. Inf. Syst. **24**, 572–596 (2009)
13. Williams, P.: Information security governance. Inf. Secur. Tech. Rep. **6**, 60–70 (2001)
14. Simon, H.A.: Models of Man; Social and Rational. Wiley, New York (1957)
15. Davis, G., Olson, M.: Management Information Systems: Conceptual Foundations, Methods and Development. McGraw-Hill, New York (1985)
16. Knapp, K.J., Franklin Morris Jr, R., Marshall, T.E., Byrd, T.A.: Information security policy: an organizational-level process model. Comput. Secur. **28**, 493–508 (2009)
17. Siponen, M.: A conceptual foundation for organizational information security awareness. Inf. Manag. Comput. Secur. **8**, 31–41 (2000)
18. Warkentin, M., Willison, R.: Behavioral and policy issues in information systems security: the insider threat. Eur. J. Inf. Syst. **18**, 101 (2009)
19. Orlikowski, W.J., Barley, S.R.: Technology and institutions: what can research on information technology and research on organizations learn from each other? MIS Q. **25**, 145–165 (2001)
20. Siponen, M., Oinas-Kukkonen, H.: A review of information security issues and respective research contributions. SIGMIS Database **38**, 60–80 (2007)

21. Dhillon, G., Backhouse, J.: Current directions in IS security research: towards socio-organizational perspectives. Inf. Syst. J. **11**, 127–153 (2001)
22. Durkheim, E., Solovay, S.A., Mueller, J.H., Catlin, S.G.E.G.: The Rules of Sociological Method, by Emile Durkheim (trans: Solovay, S.A., Mueller, J.H. and Ed: Catlin, G.E.G.). Free Press, New York (1982)
23. Wagner, P.: A History and Theory of the Social Sciences. Sage Publications Ltd., London (2001)
24. Bourdieu, P., Passeron, J.-C.: Sociology and philosophy in France since 1945: death and resurrection of a philosophy without subject. Soc. Res. 162–212 (1967)
25. Weber, M.: Wirtschaft und Gesellschaft: Grundriss der verstehenden Soziologie. Mohr, Tübingen (1922)
26. Diaz-Bone, R.: Die "Economie des conventions": Grundlagen und Entwicklungen der neuen französischen Wirtschaftssoziologie. Springer VS, Wiesbaden (2015)
27. Hirschheim, R., Klein, H.K.: Four paradigms of information systems development. Commun. ACM **32**, 1199–1216 (1989)
28. Boltanski, L., Thévenot, L.: On Justification: Economies of Worth. Princeton University Press, Princeton (2006)
29. Patriotta, G., Gond, J.-P., Schultz, F.: Maintaining legitimacy: controversies, orders of worth, and public justifications. J. Manag. Stud. **48**, 1804–1836 (2011)
30. Thévenot, L.: Organized complexity: conventions of coordination and the composition of economic arrangements. Eur. J. Soc. Theory **4**, 405–425 (2001)
31. Thévenot, L., Moody, M., Lafaye, C.: Forms of valuing nature: arguments and modes of justification in French and American environmental disputes. In: Rethinking Comparative Cultural Sociology: Repertoires of Evaluation in France and the United States, pp. 229–272 (2000)
32. Thévenot, L.: Postscript to the special issue: governing life by standards a view from engagements. Social Stud. Sci. **39**, 793–813 (2009)
33. Thévenot, L.: Rules and implements: investment in forms. Soc. Sci. Inf. **23**, 1–45 (1984)
34. Thévenot, L.: The plurality of cognitive formats and engagements moving between the familiar and the public. Eur. J. Soc. Theory **10**, 409–423 (2007)
35. Thévenot, L.: Conventions of co-ordination and the framing of uncertainty. In: Intersubjectivity in Economics: Agents and Structures, pp. 181–197. Routledge, London (2002)
36. Thévenot, L.: Die Person in ihrem vielfachen Engagiertsein. Trivium. Revue franco-allemande de sciences humaines et sociales—Deutsch-französische Zeitschrift für Geistes-und Sozialwissenschaften (2010)
37. Thévenot, L.: Institutions and agency: differentiating regimes of engagement. In: Conference on Economy and Society
38. Thévenot, L.: Pragmatic regimes governing the engagement with the world. In: Knorr-Cetina, K., Schatzki, T., von Savigny, E. (eds.) The Practice Turn in Contemporary Theory, pp. 56–73. Routledge, London (2001)
39. Diaz-Bone, R.: The methodological standpoint of the "économie des conventions". Hist. Soc. Res./Historische Sozialforschung 43–63 (2011)
40. Richards, M., Zellweger, T., Gond, J.P.: Maintaining moral legitimacy through worlds and words: an explanation of firms' investment in sustainability certification. J. Manag. Stud. **54**, 676–710 (2017)
41. Latour, B.: Reassembling the Social: An Introduction to Actor-Network-Theory. Oxford University Press, Oxford (2005)
42. Orlikowski, W.J., Scott, S.V.: Sociomateriality: challenging the separation of technology, work and organization. Acad. Manag. Ann. **2**, 433–474 (2008)
43. Soomro, Z.A., Shah, M.H., Ahmed, J.: Information security management needs more holistic approach: a literature review. Int. J. Inf. Manag. **36**, 215–225 (2016)

44. Schlienger, T., Teufel, S.: Information Security Culture. In: Ghonaimy, M.A., El-Hadidi, M.T., Aslan, H.K. (eds.) Security in the Information Society: Visions and Perspectives, pp. 191–201. Springer, US, Boston, MA (2002)
45. Meyer, J.W., Rowan, B.: Institutionalized organizations: formal structure as myth and ceremony. Am. J. Sociol. **83**, 340–363 (1977)
46. Jagd, S.: Pragmatic sociology and competing orders of worth in organizations. Eur. J. Soc. Theory **14**, 343–359 (2011)
47. Knoll, L. (ed.): Organisationen und Konventionen. Die Soziologie der Konventionen in der Organisationsforschung. Springer VS, Wiesbaden (2015)