# A CONVENTIONALIST PERSPECTIVE ON INFORMATION SECURITY POLICIES IN ORGANISATIONS

*Research in Progress*

Zellhofer, Dominik, WU (Vienna University of Economics and Business), Vienna, Austria, dominik.zellhofer@wu.ac.at

## Abstract

*Concern for information security is a major driver for policy implementation, and with new regulations like the General Data Protection Regulation, almost all types of organisations face the challenge of implementing and applying information security policies. Information security standards guide these processes, but the challenge of ensuring compliance is still a major issue, despite extensive information security research in this aspect. The lack of versatility in theoretical approaches led to 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, providing a pragmatic and contextualized perspective and a strong theoretical foundation from sociology. By adopting a conventionalist view of information security policies, attention is focused on issues of legitimacy without limiting the analysis to a solely structuralist perspective. This research in progress tries to take first steps in building a conventionalist framework for case-based research by introducing some of the main concepts of convention theory and illustrates possible implications for information security research and practice.*

*Keywords: Information Security Policy, Convention Theory, Compliance, Legitimacy.*

# 1 Introduction

Because of the growing availability of big data, organisations rely heavily on large amount 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 to not only customers but other stakeholders as well, organisations need to ensure data security from outside and inside threats. Media attention is typically centred on big cases of data theft, like in 2014, when a substantial security breach caused a leak of account information of 145 million eBay-users (Briegleb, 2014), drawing major public scrutiny. The cost of such a breach of information security is of special interest to organisations and is used to argue for better industry standards, tighter policies and bulletproof technological solutions. An international, IBM-sponsored study supports the ever-rising relevance of the cost-aspect, reporting that the average cost of a data breach in 2016 was four million dollars, with the cost per incident having increased by 30 percent since 2013 (Institute, 2016). However, because more data that is personal is used to provide tailored services to customers, these incidents are now also a matter of public legitimacy that can lead to public scrutiny of organisational practices beyond the data breach, like the prominent data theft at Ashley Madison recently showed (Mansfield-Devine, 2015). Although hackers are frequently the culprits in such incidences, the threat does not exclusively stem from external factors. In fact, Stanton et al. (2005) report that between 50 and 75 percent 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 (Bulgurcu et al., 2010), the lack thereof leading to (non-malicious) non-compliance. In addition, recent literature in information security policies identified issues of legitimacy to be important when considering compliance to policies (Hu et al., 2012), showing that legitimization is not only an issue in regard to external stakeholders of the organisation.

Attempts to minimize inherent risks of information processing lead to the development of standardized information safety procedures, reflected through information security guidelines and standards like CobiT, GMITS or BS7799, which in turn are implemented through organisation policies. These policies target issues concerning the organisational environment and intra-organisational 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 organisational hierarchy, whereas today organisations rely on information systems in every aspect of their business (McFadzean et al., 2006). The consequence is that IT experts no longer act as the sole “gatekeepers” responsible to ensure security in information systems, but every employee involved in business processes of an organisation needs to have knowledge about and adhere to information security policies. To address non-compliance, several measures are proposed in literature, recently there is also a focus on information security awareness, facilitated through training programs (Bauer et al., 2017). This is an example showing not only the variety of stakeholders impacted “on the receiving end” of information security policies, but that the responsibility to enforce policies is distributed to different organisational stakeholders, as training is one of the core responsibilities of HR departments. The obvious challenge therefore is to ensure acceptance and compliance of good security practices in organisations, guided through the implementation of security policies.

Zafar and Clark (2009) note that the term “information security” has a plurality of definitions, depending on the perspective, seeing a progression from mere technological viewpoints to behavioural, managerial, philosophical, and organisational 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 (2001) gives a similar de-

scription, grouping tasks of information security in availability, confidentiality, integrity, authenticity and non-repudiation of information systems.

## 2 Information Security Policies

Form the aforementioned multitude of aspects, I focus on information security policies to depict 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 organisational members' day-to-day practices. In general, a policy is simply a general rule to limit the discretion of subordinates in an organisation (Simon, 1957). Similarly, management information systems research defines policies as a control instrument to establish limits of acceptable behaviour, guide and restrict decisions and serve as standards (Davis and Olson, 1985). While the formulation of such documents, including the exact wording, is important, the generation and implementation process itself is important to ensure acceptance within an organisation. Knapp et al. (2009) 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 organisational context. They base their framework on the account of practitioners, thereby providing an overview that is based on actual practices in organisations. When comparing their framework with the lists 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. Practitioners are aware of continuous tasks like awareness trainings, monitoring, and policy enforcement, while also acknowledging influences of organisation culture and institutional pressures of industry standards and legislation. Measures to increase information security awareness are considered an important step in achieving compliance (Bauer et al., 2017). These measures serve to make employees aware of their "security mission" (Siponen, 2000) and therefore foster compliance with security policies. This hints at the need for (constant) dialogue and the insufficiency of just writing up a policy (Warkentin and Willison, 2009). The focus on individual behaviour is reflected in information security research, Warkentin and Willison (2009) state that much of the focus within the behavioural security research community has been on information security policy non-compliance by employees. On the other hand, Orlikowski and Barley (2001) argue that, while information technology research occasionally references organisation studies, it is still underrepresented and call for a stronger focus on the institutional context. Interestingly, they find that the reverse is also true; organisation studies often carelessly neglect how technologies shape organisations.

Clearly, the problem of information security is an inherently complex one, combining technical issues with social, psychological and organisational aspects, thus a holistic approach to tackle these problems requires interdisciplinary efforts (Siponen and Oinas-Kukkonen, 2007). Earlier calls for sociology to provide a strong theoretical foundation to enrich information security research were made but only partly addressed (Dhillon and Backhouse, 2001) and the framework of convention theory proposed in this paper is a sociological perspective that attempts to integrate these 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. Emile Durkheim (1982) was the most prominent proponent of the "old social sciences" (Wagner, 2001). In the late 1960s, Pierre Bourdieu moved the focus to the structural, hence his description as "philosophy without subject" (Bourdieu and Passeron, 1967). 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 (Wagner, 2001). In this new interpretation of human action, "convention" does not only address traditions, rituals or customs in a Weberian (1922) sense of the word, but as culturally established logics of coordination (Diaz-Bone, 2015). 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 (McFadzean et al., 2006), although there is some research that finds goals to be dependent of the actor's subjective views (e.g., Sadok et al., 2014). This mainstream leads to a neglect of the essential role of legitimation of said goals (Hirschheim and Klein, 1989) 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 with regard to some kind of worth. Boltanski and Thévenot (2006) 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 organisations maintain their legitimacy regarding relevant stakeholders. For the organisation to maintain its legitimacy, it has to sustain the harmonious arrangement of things and persons in a state of general agreement (Patriotta et al., 2011). 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 (Thévenot, 2001; Boltanski and Thévenot, 2006). 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 a "normal" 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 organisation. 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. Table 1 gives an overview of the initial six orders of worth and their attributes. 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 (Patriotta et al., 2011). Once an agreement on orders of worth (there can be multiple orders at play at once), a legitimate conventions that serve coordination based upon them are established. Conventions "convene" qualified objects and human beings, they give a sense of what dimension of time and space is relevant.

| | Market | Industrial | Civic | Domestic | Inspired | Opinion |
|---|---|---|---|---|---|---|
| Mode of evaluation (worth) | Price, cost | Technical efficiency | Collective welfare | Esteem, reputation | Grace singularity creativeness | Renown, fame |
| Test[b] | 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 & 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 |

*Table 1. Schematic summary of orders of worth (Thévenot et al., 2000) (adapted)*

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 common 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 (Thévenot, 2009), 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 (Thévenot, 1984). 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 (2007) 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 (Thévenot, 2001).

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 (Thévenot, 2002).

## 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* (Thévenot, 2001; Thévenot, 2010). 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 (Thévenot, 2006). 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* cap-

tures 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 (Thévenot, 2001)). With this view of the environment, convention theory avoids the critique mentioned by Orlikowski and Barley (2001) and the proposed framework follows suit with other, socio-material approaches in information security research (e.g., Hedström et al., 2010).

Each of the regime of engagement implies a distinct cognitive format related to a different kind of access to the human environment of nature and artefacts (Thévenot, 2001). Cognitive formats characterize the actor's access to reality and thereby how he coordinates his behaviour within a certain apprehension frame (Thévenot, 2007). 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 (2006) identified them. The format of information is also more conventional, e.g. reports are much more conventional than everyday language use (Thévenot, 2001). 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 (Thévenot, 2006). 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. Therefore, 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 behaviour and criticizing this new standard, because this kind of customization will mostly likely not rank high in common orders of worth that 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" (Thévenot, 2001). 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 co-workers 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 organisations: 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 visible the functional aspect of a convention. 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 or reasons of dispute and non-compliance.

## 3.3 Organisations as Compromising Devices

While other theories often grant organisations a reality on their own, convention theory is not interested in a concept of organisation as a mode of coordination on its own (Diaz-Bone, 2015). Thévenot (2001) defines an organisation 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 that are seen as constraints, which Thévenot defines as "over-socialized" representations of this idea. He argues for a no-

tion of coordination more open to uncertainty, critical tensions and creative arrangements. As a result, this conception of organisation 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 organisations.

Conceptualizing organisations as compromising devices appreciates the tension created in organisations by different orders of worth governing coordination. For example, an organisation 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 A preliminary model of an applied conventional approach

Standards in organisations are already of interest in sociological research, but they were largely tackled from an institutionalist approach, and convention theory is in this regard always compared with institutional theory (Thévenot, 2015). Recent applications of convention theory in organisational research show the advantages of adopting this perspective compared to the more prominent institutional approach (Cloutier and Langley, 2013; Brandl et al., 2014). But most research currently focuses on legitimation issues concerned with external stakeholders of organizations, as for example a recent Austrian publication which focuses on educational reforms and its implications for schools and teachers (Graß, 2018), making models that depict the inner workings of the concepts described above a rarity. Figure 1 shows a preliminary model depicting the implementation and application of policies as a revolving process of three steps corresponding to the regimes of engagement (on the y-axis), with each step being characterized by the prevalent theoretical concepts at play. Step one corresponds with finding a compromise between different orders of worth, leading to step two where investment in forms determine the spatial and temporal validity of the policy and functionality is evaluated. Finally, step three corresponds to the application of these new practices in the work routine, where critical moments will appear due to reality tests showing insufficiencies and leading to critique and justification, forcing actors to engagement in justification. The reciprocal arrows at each step emphasize that not only the whole process is reiterated over time and space, but that each step is a revolving process.

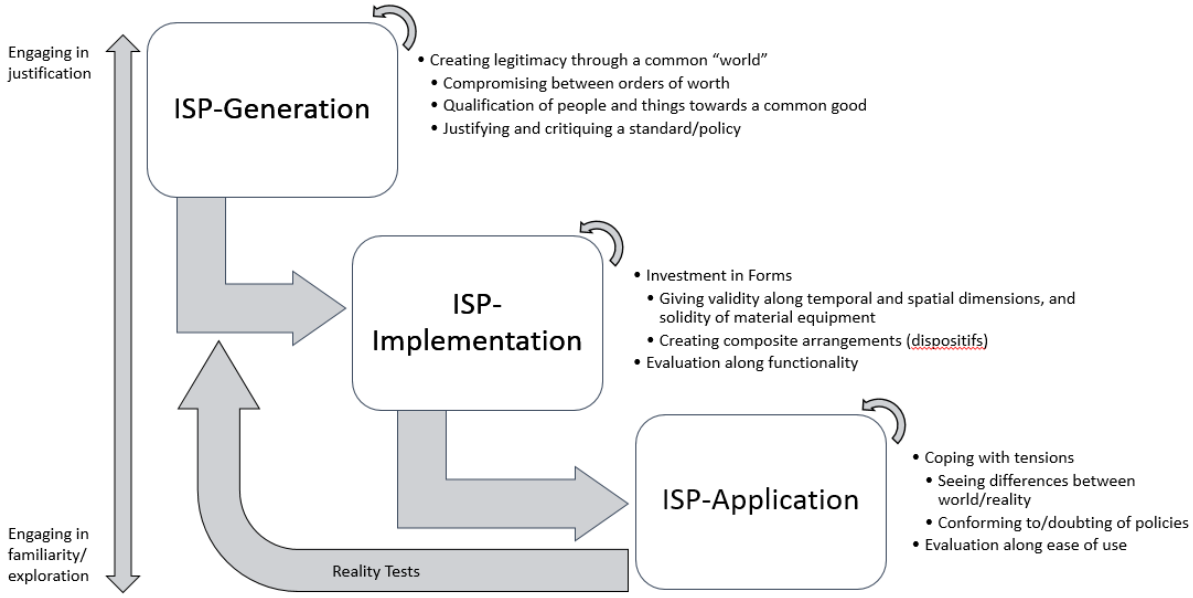


*Figure 1. Model of Co-ordination through Information Security Policies*

# 5 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 can integrate aspects of multiple alternative approaches already existing in literature under a common theoretical framework. First, I also delineate some expected results when applying this framework to critical incidents regarding information security policies.

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, but also on its embeddedness in the situation and its relations to other actors and objects in it. Legitimization plays an important role in establishing and maintaining compliance to conventions like information security policies and if inadequate, it can lead to non-compliance. Balozian and Leidner (2017) address the implementation of security policies without adequate legitimization by using the term "information system security menace" and in its essence, this is a story of justification and critique of a convention with individual and situational aspects.

Similarly to the findings of Richards, Zellweger & Gond (2017) when examining organizations and the way they manage moral legitimation, I expect to find that organizational actors use (multiple) distinct orders of worth which shape their security compliance and critique or support of information security policies. In particular, I assume that orders of worth connected to the "domestic" and "industrial" world will be prevalent in the organizational discourse about policies. On a smaller scale, workarounds of employees to stick to the traditional ways of doing things could be a symptom of conflicting worlds. When critical incidents arise, organizational actors can be forced into the realm of public engagement. These are typical reality tests and these situations are opportunities from a managerial point of view to intervene and readjust conventions based on policies. Management commitment, which has been deemed especially important (e.g. Knapp et al., 2009), can be investigated in terms of conflicting orders of worth or in terms of investment in forms, as management as an organizational actor has high capabilities to stabilize new modes of coordination through investments. I expect that investing in objects that foster new conventions like information security behaviours can promote the shift from an engagement in the regime of justification into the regime of planned action, the more unambiguous the arrangement of objects in a workplace (i.e. technology, but also architecture etc.), the faster conflicts should resolve. Growing digitalization in organizations leads to a need to address wider circle of organizational actors. Digitalization also changes the relevant coordination situation, as the material environment plays an inherently important role in convention theory. Therefore, I expect that a higher degree of information technology involved in organizational coordination alters the way people engage with their environment and how they evaluate security policies, acknowledging the importance of interactions of material and human agency (Leonardi, 2012). On an organizational level, I expect to be able to classify or relate an organization's identity (Brickson, 2007) with principles of different worlds, which can be distinctly expressed by organizational practices and their justifications. This can be seen by inspecting how an organization deals with uncertainty, critical tensions and creative arrangements, thereby addressing Thévenot's critique that we need to characterize modes of coordination by their dynamics and not the resulting order (Thévenot, 2001). To address the individual aspect, 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 considered 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" (Diaz-Bone, 2011; Diaz-Bone, 2015). As a consequence, the concept of rationality is altered and shifted towards a "situated rationality" (Simon, 1957; Thévenot, 2002). This makes seemingly paradox irrational behaviour interpretable and leaves the outdated perceptions of consistent rational decisions behind. A convention theory-based

framework also integrates power relations in the actor's capabilities of form investment and their ability to utter critique and legitimizing conventions. This conforms to existing literature identifying power as important factor in compliance beyond the mere punitive aspect that follows from a deterrence theory perspective. For example, Kolkowska and Dhillon (2013) formulate implications from their case study on power and compliance that closely resemble acts of investment in forms: The need for structural changes and their dependence on different power bases. A conventionalist framework helps identify positions of all relevant actors at play, and besides the IT department and the "general" employee body, the top management plays an important role in legitimizing security policies (Hu et al., 2012).

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 (Richards et al., 2017). The focus on the situation as a level of analysis also highlight the importance of the role of temporality and space, which also has implications on the methodological approach and provides venues for possible quantified qualitative approaches (Hamann and Suckert, 2018). 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 (Latour, 2005; Orlikowski and Scott, 2008). The concept of regimes of engagement extends the framework beyond evaluation and dispute to the application of conventions and does not only focus on the situational embeddedness of actors, but their engagement with the world around them. It can show how standards are applied (Thévenot, 2009) and make tensions between the most public and most intimate engagement with the world visible. It can also differentiate 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 that need to be considered when conducting research, but issues of importance remain which cannot be discussed here in full length. The relevance of the concept of regimes of engagement for information systems in organisations is exemplified when considering the case of BYOT (Bring Your Own Technology), which constitutes new challenging security issues (Miller et al., 2012). With the spread of devices and software that are attached both to the private and corporate realm (e.g. smartphones, learning software, productivity and time management apps used in private and working life), ambiguity of conventional use is likely and the reach of information security policies extends beyond organisational borders. The resulting conflicts when different "worlds of worth" and regimes of engagements collide (e.g., using devices in the way the planned action regime presumes in an inherently personal environment of your home) can be solved by searching for compromise between differing orders of worth. As private use is inherently subjective and only very loosely convention-bound, it is clear that policies that address this issue have to consider the employee perspective. Employee participation in the formulation and implementation process is also deemed important by other research (Siponen et al., 2014). 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. Existing research show the results, e.g., Spears and Barki (2010) found that user participation did improve security control performance by fostering awareness, alignment with the business environment and improved control development. IT specialists often prefer solely technical solutions, putting much effort in restrictions of possible actions of employees with means within their realm of expertise, but research on tools like information security awareness trainings hint at a social dimension of the problem. As the authors note, there is a strong focus of organisations on the technological aspect of information security, while at the same time there is a neglect of other vulnerabilities stemming from people, policies, processes, and culture (Spears and Barki, 2010). The importance of the latter aspect is also pointed out by research on information security culture (Schlienger and Teufel, 2002). 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 behaviour" must be considered too. The concept of reality tests entails this notion; it also underlines the revolving nature of accepting and disputing standards. Existing practices in organisations like perfor-

mance 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" suggested by Knapp et al. (2009). External audits are a standard practice for information security policies, but they often fail to detect workarounds in actual practice, institutionalists would denote this disparity of official practice and actual routine as decoupling (Meyer and Rowan, 1977). This "decoupling" from practices suggested by guidelines is often caused by their generic and universal scope and as Siponen and Willison (2009) note, guidelines should be company-specific and methods should be tailored to their environment and operations. The validation of standards by appeal to common practice and authority is a justification by values of the industrial world in terms of convention theory, and as already described, employees do not necessarily evaluate policies with that particular order of worth in mind. With regard to risk analysis, Sadok et al. (2014) identify the importance of context and exceptional situations, with an emphasis on the different perceptions regarding information security of different stakeholders. Convention theory similarly argues that conventions, like those contained in information security policies, are viewed and evaluated differently by actors in a particular situation. This integrates a multi-actor, contextualized perspective into the implementation and application of said policies.

## 5.1 Limitations

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. 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 difficult too considering the wide-ranging implications of the concepts. As Jagd (2011) noted, the relevance of the framework for organisational 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 in organisation research; an overview of this research can be found in Knoll (2015). 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. This paper cannot provide a comprehensive account of convention theory and its application to the topic at hand, but should serve as a stepping-stone in formulating and applying a convention theory-based framework to information security policy research.

## References

Balozian, P. and D. Leidner (2017). "Review of IS Security Policy Compliance: Toward the Building Blocks of an IS Security Theory." *SIGMIS Database* 48(3), 11-43.

Bauer, S., E. W. Bernroider and K. Chudzikowski (2017). "Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks." *Computers & Security* 68, 145-159.

Boltanski, L. and L. Thévenot (2006). *On Justification: Economies of Worth*. Princeton: Princeton University Press.

Bourdieu, P. and J.-C. Passeron (1967). "Sociology and Philosophy in France since 1945: Death and Resurrection of a Philosophy without Subject." *Social Research*, 162-212.

Brandl, J., T. Daudigeos, T. Edwards and K. Pernkopf-Konhäusner (2014). "Why French pragmatism matters to organizational institutionalism." *Journal of Management Inquiry* 23(3), 314-318.

Brickson, S. L. (2007). "Organizational identity orientation: The genesis of the role of the firm and distinct forms of social value." *Academy of Management Review* 32(3), 864-888.

Briegleb, V. (2014). *145 Millionen Kunden von eBay-Hack betroffen*. https://www.heise.de/security/meldung/145-Millionen-Kunden-von-eBay-Hack-betroffen-2195974.html (visited on 02.02.2016).

Bulgurcu, B., H. Cavusoglu and I. Benbasat (2010). "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness." *MIS quarterly* 34(3), 523-548.

Cloutier, C. and A. Langley (2013). "The logic of institutional logics: Insights from French pragmatist sociology." *Journal of Management Inquiry* 22(4), 360-380.

Davis, G. and M. Olson (1985). "Management information systems: Conceptual foundations, methods and development." *McGraw-Hill, New York*.

Dhillon, G. and J. Backhouse (2001). "Current directions in IS security research: towards socio-organizational perspectives." *Information Systems Journal* 11(2), 127-153.

Diaz-Bone, R. (2011). "The methodological standpoint of the "économie des conventions"." *Historical Social Research/Historische Sozialforschung*, 43-63.

Diaz-Bone, R. (2015). *Die" Economie des conventions": Grundlagen und Entwicklungen der neuen französischen Wirtschaftssoziologie*. Wiesbaden: Springer VS.

Durkheim, E., S. A. Solovay, J. H. Mueller and S. G. E. G. Catlin (1982). *The Rules of Sociological Method, by Emile Durkheim... Translated by Sarah A. Solovay and John H. Mueller and Edited by George EG Catlin*. New York: Free Press.

Graß, D. (2018). "Justification and Critique of Educational Reforms in Austria: How Teachers and Head Teachers (Re-) Frame New Governance." *JSSE-Journal of Social Science Education* 16(4), 60-74.

Hamann, J. and L. Suckert (2018). "Temporality in Discourse: Methodological Challenges and a Suggestion for a Quantified Qualitative Approach." In: *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*.

Hedström, K., G. Dhillon and F. Karlsson (2010). "Using actor network theory to understand information security management." *Security and Privacy–Silver Linings in the Cloud*, 43-54.

Hirschheim, R. and H. K. Klein (1989). "Four paradigms of information systems development." *Communications of the ACM* 32(10), 1199-1216.

Hu, Q., T. Dinev, P. Hart and D. Cooke (2012). "Managing employee compliance with information security policies: The critical role of top management and organizational culture." *Decision Sciences* 43(4), 615-660.

Institute, P. (2016). *Cost of Data Breach Study: Global Analysis.*

Jagd, S. (2011). "Pragmatic sociology and competing orders of worth in organizations." *European Journal of Social Theory* 14(3), 343-359.

Knapp, K. J., R. Franklin Morris Jr, T. E. Marshall and T. A. Byrd (2009). "Information security policy: An organizational-level process model." *Computers & Security* 28(7), 493-508.

Kolkowska, E. and G. Dhillon (2013). "Organizational power and information security rule compliance." *Computers & Security* 33, 3-11.

Latour, B. (2005). *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford: Oxford university press.

Leonardi, P. M. (2012). "Materiality, sociomateriality, and socio-technical systems: what do these terms mean? How are they related? Do we need them?".

Mansfield-Devine, S. (2015). "The Ashley Madison affair." *Network Security* 2015(9), 8-16.

McFadzean, E., J.-N. Ezingeard and D. Birchall (2006). "Anchoring information security governance research: sociological groundings and future directions." *Journal of Information System Security* 2(3), 3-48.

Meyer, J. W. and B. Rowan (1977). "Institutionalized organizations: formal structure as myth and ceremony." *American Journal of Sociology* 83(2), 340-363.

Miller, K. W., J. Voas and G. F. Hurlburt (2012). "BYOD: Security and privacy considerations." *It Professional* 14(5), 53-55.

Orlikowski, W. J. and S. R. Barley (2001). "Technology and institutions: What can research on information technology and research on organizations learn from each other?" *MIS quarterly* 25(2), 145-165.

Orlikowski, W. J. and S. V. Scott (2008). "Sociomateriality: challenging the separation of technology, work and organization." *The Academy of Management Annals* 2(1), 433-474.

Patriotta, G., J.-P. Gond and F. Schultz (2011). "Maintaining legitimacy: controversies, orders of worth, and public justifications." *Journal of Management Studies* 48(8), 1804-1836.

Richards, M., T. Zellweger and J. P. Gond (2017). "Maintaining moral legitimacy through worlds and words: An explanation of firms' investment in sustainability certification." *Journal of Management Studies* 54(5), 676-710.

Sadok, M., V. Katos and P. M. Bednar (2014). "Developing contextual understanding of information security risks." In: *HAISA*. 1-10.

Schlienger, T. and S. Teufel (2002). Information Security Culture. In: M. A. Ghonaimy, M. T. El-Hadidi and H. K. Aslan (Eds.), *Security in the Information Society: Visions and Perspectives*, p. 191-201. Boston, MA: Springer US.

Simon, H. A. (1957). *Models of Man; Social and Rational*. 1st. New York: John WIley and Sons, Inc.

Siponen, M. (2000). "A conceptual foundation for organizational information security awareness." *Information Management & Computer Security* 8(1), 31-41.

Siponen, M., M. A. Mahmood and S. Pahnila (2014). "Employees' adherence to information security policies: An exploratory field study." *Information & management* 51(2), 217-224.

Siponen, M. and H. Oinas-Kukkonen (2007). "A review of information security issues and respective research contributions." *SIGMIS Database* 38(1), 60-80.

Siponen, M. and R. Willison (2009). "Information security management standards: Problems and solutions." *Information & management* 46(5), 267-270.

Spears, J. L. and H. Barki (2010). "User Participation in Information Systems Security Risk Management." *MIS quarterly* 34(3), 503-522.

Stanton, J. M., K. R. Stam, P. Mastrangelo and J. Jolton (2005). "Analysis of end user security behaviors." *Computers & Security* 24(2), 124-133.

Thévenot, L. (1984). "Rules and implements: investment in forms." *Social Science Information* 23(1), 1-45.

Thévenot, L. (2001). "Organized complexity: conventions of coordination and the composition of economic arrangements." *European Journal of Social Theory* 4(4), 405-425.

Thévenot, L. (2001). Pragmatic regimes governing the engagement with the world. In: K. Knorr-Cetina, T. Schatzki and E. v. Savigny (Eds.), *The Practice Turn in Contemporary Theory*, p. 56-73. London: Routledge.

Thévenot, L. (2002). Conventions of co-ordination and the framing of uncertainty. In: (Eds.), *Intersubjectivity in Economics: Agents and Structures*, p. 181-197. London: Routledge.

Thévenot, L. (2006). "Institutions and agency: differentiating regimes of engagement." In: *Conference on Economy and Society*. Italy.

Thévenot, L. (2007). "The plurality of cognitive formats and engagements moving between the familiar and the public." *European Journal of Social Theory* 10(3), 409-423.

Thévenot, L. (2009). "Postscript to the Special Issue: Governing Life by Standards A View from Engagements." *Social Studies of Science* 39(5), 793-813.

Thévenot, L. (2010). "Die Person in ihrem vielfachen Engagiertsein." *Trivium. Revue franco-allemande de sciences humaines et sociales - Deutsch-französische Zeitschrift für Geistes-und Sozialwissenschaften*(5).

Thévenot, L. (2015). "Certifying the world." *Reimagining economic sociology. Oxford: Oxford University Press, S*, 195-223.

Thévenot, L., M. Moody and C. Lafaye (2000). "Forms of valuing nature: arguments and modes of justification in French and American environmental disputes." *Rethinking comparative cultural sociology: Repertoires of evaluation in France and the United States*, 229-272.

Wagner, P. (2001). *A History and Theory of the Social Sciences*. London: Sage Publications Ltd.

Warkentin, M. and R. Willison (2009). "Behavioral and policy issues in information systems security: the insider threat." *European Journal of Information Systems* 18(2), 101.

Weber, M. (1922). *Wirtschaft und Gesellschaft: Grundriss der verstehenden Soziologie*. Tübingen: Mohr.

Williams, P. (2001). "Information Security Governance." *Information Security Technical Report* 6(3), 60-70.

Zafar, H. (2013). "Human resource information systems: Information security concerns for organizations." *Human Resource Management Review* 23(1), 105-113.

Zafar, H. and J. G. Clark (2009). "Current state of information security research in IS." *Communications of the Association for Information Systems* 24(1), 572-596.