Toward Uncovering Patterns of Certification Internalization

Short Paper

Malte Greulich
Karlsruhe Institute of Technology
76133 Karlsruhe, Germany
greulich@kit.edu

Sebastian Lins
Karlsruhe Institute of Technology
76133 Karlsruhe, Germany
lins@kit.edu

Ali Sunyaev
Karlsruhe Institute of Technology
76133 Karlsruhe, Germany
sunyaev@kit.edu

Abstract

The number and variety of information systems (IS) certifications have increased continuously as the use of information technology has diversified and expanded. IS certifications are neutral third-party attestations of specific system characteristics and management principles to prove compliance with requirements. The reasons for organizations to adopt IS certifications are diverse, such as fostering learning and improvement, or demonstrating regulatory compliance. However, because of organizations' diverse motivations to adopt certifications, organizations also differ in their degree of internalizing the certification. In particular, superficial, ceremonial adoption and a lack of internalization of certifications become critical issues harming the certification's reputation and effectiveness. This short paper reports on preliminary findings from a qualitative study on the development of a data protection certification. Based on unique access to case companies throughout the certification attestation process, our research will provide insights into how motivations for adoption impact the internalization processes of organizations.

Keywords: Data protection, certification, seals, adoption, internalization

Introduction

Information systems (IS) certifications are an important mechanism for policymakers and organizations alike (Lansing et al. 2018; Löbbers and Benlian 2019). IS certifications are neutral third-party attestations of specific system characteristics, operations, and management principles to prove compliance with regulatory or industry requirements (Lansing et al. 2018). The number and variety of IS certifications have increased continuously as the use of information technology (IT) has diversified and expanded. Nowadays, well-known certifications include *"Certified Privacy"* for webshops, *"CSA STAR"* for cloud services, and management standards such as "*ISO/IEC 27001—Information security management systems"* for security. Recently, the EU General Data Protection Regulation (GDPR) has foreseen certification as the primary mechanism for organizations to demonstrate compliance with GDPR requirements across industries and legislative regions. Likewise, the EU Cybersecurity Act introduces an EU-wide cybersecurity certification framework to harmonize existing security certifications and foster the development of novel security certifications in emerging domains, such as distributed ledger technology or artificial intelligence.

The reasons for organizations, who are responsible for system operations, to adopt IS certifications are diverse (Lins et al. 2020). Some organizations adopt certifications to achieve organizational learning and improvements (Prajogo 2011), some are eager to demonstrate regulatory compliance and to gain legitimacy

(Heras-Saizarbitoria and Boiral 2013), whereas others use certifications as a marketing tool to attract consumers (King et al. 2005). The diversified use of certifications, however, comes with its downsides: organizations also differ in their degree of internalizing the certification. *Internalization* refers to the process of absorbing both tacit and explicit information underlying the certification (e.g., best practices, attestation results, and third-party feedback) into the organization and translating it into knowledge, routines, and procedures (Knight and Liesch 2002).

Some organizations may thoroughly internalize feedback gained during the certification attestation about, for example, security vulnerabilities to foster internal improvements (Prajogo 2011). Other organizations may internalize certifications only "*superficially so that the organization could pass the certification audit without posing serious questions that were seen to be unnecessary and undesirable"* (Boiral 2003, p. 732). Such ceremonial adoption without the appropriate internalization of stated practices (Meyer and Rowan 1977) threatens the effectiveness of certifications. Revealing internalization failures can also damage the certification's reputation in the market and might harm the certification mechanism altogether.

The diverse types of adopters and resulting internalization variations put substantial pressure on policymakers and certification authorities issuing certifications: they must ensure that the certification is thoroughly internalized by an organization to ensure conformity with the certification requirements and to ensure that the certification upholds the intended standards. This is especially true for IS certifications concerning data protection because they must guarantee effective protection of personal data—a considerable challenge owing to the recent drastic increase in cyberattacks. History shows that policymakers can fail with such efforts, like the case of an information security certification in the UK vividly describes that failed because of organizations' resistance to adopt the novel certification (Silva et al. 2016). Further knowledge is required on how to ensure internalization for specific certification adopter types.

Prior research already offers rich descriptions about why organizations adopt certifications (e.g., Heras-Saizarbitoria and Boiral 2013; Lins et al. 2020; Prajogo 2011) and sparse insights into the internalization process (e.g., Hsu et al. 2012; Niemimaa and Niemimaa 2019). While these two research streams offer valuable insights for itself, the literature lacks an integrated view of both research streams, and thus we still lack an understanding of the patterns that underly the internalization processes for each adopter type. To facilitate a better understanding of how adoption motivations inform the organization's internalization of certifications, we seek to answer two research questions (RQ):

RQ1: *How does the internalization of certifications differ across adopter types?*

RQ2: *How can certification mechanisms ensure thorough internalization?*

In this short paper, we report on preliminary findings from a multi-year research project that shed light on the internalization of IS certifications across different adopter types. We use a multi-phase research approach that includes a thorough literature review, semi-structured interviews, and field observations with three case companies throughout the development and pilot implementation of a data protection certification in Europe from 2017 to 2021. Thereby, we identified preliminary patterns of internalization that explain internalization differences across adopter types. For example, organizations might '*wait and observe'* by upholding established organizational practices and only seeking to change these practices after a careful cost-benefit assessment following the certification attestation. We also identified improvements of the certification mechanism that support policymakers in the certification development process.

We expect valuable contributions to research and practice. First, our research will provide insights into the internalization process of (future) adopters of data protection certifications, thereby addressing recent calls in IS research (e.g., Hsu et al. 2012; Nielsen et al. 2014; Niemimaa and Niemimaa 2019). Second, we bridge two so far distinct research streams (i.e., adoption and internalization), which enables us to advance prevalent research discussions on superficial or failed internalization. In particular, our research seeks to explain how internalization processes (Hsu et al. 2012; Niemimaa and Niemimaa 2019) differ across adopter types and associated motivations (Lins et al. 2020; Prajogo 2011). Finally, our unique access to the case companies before, during, and after the adoption of a novel data protection certification allows us to derive valuable insights into the internalization process of organizations.

Adoption and Internalization of Information System Certifications

Information System Certifications

The certification process involves three actors: certification authorities, organizations, and users (Lins et al. 2020). Certification authorities are independent, neutral intermediaries between users and organizations that provide forms of oversight to deter or punish inappropriate behavior by the organization (Lansing et al. 2018). The oversight covers, among other things: assessing the system documentation about its security and data protection measures, interviewing organizations' employees, or conducting on-site assessments or penetration tests to evaluate the system's compliance. If the target system for a certification adheres to specified requirements, the certification authority awards a formal certificate. The organization is then permitted to present the certification information in their communications to users and outside stakeholders. In the context of IS use, organizations typically signal the possession of such certifications by placing certification seals on their websites or in their system interfaces.

While a wide variety of IS certifications exist, three types of IS certifications prevail, addressing (1) privacy, (2) security, or (3) business-integrity concerns of users (Löbbers et al. 2020). First, certifications addressing users' privacy concerns seek to alleviate users' perceived risks in terms of, for example, inappropriate usage of personal data. Second, certifications addressing users' security concerns (e.g., unauthorized access, malicious programs, or malware) are used to reassure users that an organization uses appropriate countermeasures (i.e., intrusion detection software, firewalls, or antivirus software and anti-spyware software). Finally, certifications addressing business integrity concerns guarantee fair business practices and reliable management processes (e.g., reliable system administration).

The literature on IS certifications and related web seals grew constantly in recent decades, predominantly in three research streams. First, various scholars have examined how to develop and design (e.g., Lansing et al. 2018) or innovate certifications and underlying attestation processes (e.g., Lins et al. 2019). Second, research adopting a user perspective seeks to explain how certifications affect users, why these effects occur, and how to predict these effects (e.g., Löbbers et al. 2020; Löbbers and Benlian 2019). In particular, user-related studies have focused on increasing users' trust perceptions, purchase intentions, and perceived assurances. Finally, research taking an organizational perspective analyzes the motivations of organizations to adopt certifications, how organizations internalize certifications, and whether organizations can harness the benefits of certifications (e.g., Heras-Saizarbitoria and Boiral 2013; Hsu 2009; Lins et al. 2020). In this paper, we adopt an organizational perspective to examine the adoption and internalization of data protection certifications to prove GDPR compliance. While this breadth of research has led to varying terminology (e.g., web seals, assurance services, certifications), we follow recent conceptualizations of certifications in the IS discipline (e.g., Lansing et al. 2018; Lins et al. 2020; Löbbers and Benlian 2019) that attest qualities of IS (e.g., security and data protection) and related management practices.

Distinguishing Adoption and Internalization of Certifications

The motivations to adopt IS certifications are diverse because adopting certifications is voluntary and not legally binding (Heras-Saizarbitoria and Boiral 2013; Lins et al. 2020). Adoption, in our context, refers to the attainment of a certificate after the successful completion of the certification process in which a certification authority assesses the system's fulfillment of certification requirements. Synthesizing prior research on certification adoption reveals three major adopter types, namely ***functionalists***, ***institutionalists***, and ***signalers*** (Table 1; Lins et al. 2020). Different motivations characterize these adopter types, originating from three competing theoretical perspectives that are commonly used to understand certification adoption (Heras-Saizarbitoria and Boiral 2013; Lins et al. 2020), namely, the *resource-based view* (Barney 1991), the *institutional theory* (DiMaggio and Powell 1983), and the *signaling theory* (Spence 1973). *Functionalists* leverage and implement certifications as an organizational resource to achieve organizational benefits, reflecting the resource-based view. *Institutionalists* adopt a certification to conform with institutional pressures and seek legitimacy, in accordance with the institutional theory. *Signalers* use a certification predominately as a marketing tool to convey information regarding their unobservable characteristics and actions, in line with the principles of signaling theory. While this typology illustrates extremes and multiple types can coexist, it offers a frame for examining and classifying differences in internalization efforts.

Table 1. Typology of Certification Adopters (Lins et al. 2020)		
Adopter type	**Key objectives for adoption**	**Example motivations**
Functionalist (resource-based view)	Leverage and implement IS certifications as an organizational resource to achieve organizational benefits.	Improve quality, productivity, customer satisfaction, IT security, and legal conformity; access expert knowledge; achieve a competitive advantage and realize cost savings
Institutionalist (institutional theory)	Conform to institutional pressures and seek to achieve legitimacy.	Satisfy coercive pressures (e.g., pressures from regulatory, suppliers, or customers), mimetic pressures (e.g., match level of certification of competitors), normative pressures (e.g., public opinion, industry associations, internal norms)
Signaler (signaling theory)	Convey information regarding organizations' unobservable characteristics and actions.	Convey hidden information (e.g., integrity, data protection), use as a marketing tool (e.g., certification as a unique selling proposition), increase trust into the organization

In general, certifications provide guidelines and best practices that must be internalized into the organization and used as daily practices (Naveh and Marcus 2004). The internalization process is inherently a sense-making process that involves understanding the prescribed requirements, assessing the status quo of the organization, and taking necessary actions to fulfill the certification requirements. Prior research has identified mechanisms that help to explain how this internalization process shapes organizational practices. Such mechanisms include, for instance, "(1) translating global to local, (2) disrupting and reconstructing local non-canonical practices, and (3) reconstructing and enacting local canonical practices" (Niemimaa and Niemimaa 2017, p. 1). The internalization process can uncover discrepancies between the certification requirements and organizational practices that can spur innovations resolving these discrepancies (Hsu et al. 2012; Niemimaa and Niemimaa 2019). In particular, a certification internalization process will produce a set of routines and procedures (tacit and explicit) for internal operations, which cannot be easily imitated by other organizations (Prajogo 2011). Hence, certifications can help organizations build and improve internal operational capabilities, which may produce variability in performance against their competitors in the market (Prajogo 2011). Thorough internalization of certifications is a key requirement for certification effectiveness and ensures that the organizational practices suffice the prerequisites for attaining the certification (Lins et al. 2020).

Nevertheless, the adoption of a certification does not mean that the organization has thoroughly internalized the certification (Boiral 2003). Prior research already concluded that some organizations tend to adopt a minimalist approach in implementing the certification, meet the minimum requirements, and take a short-cut approach in attaining the certification (Boiral 2003; Lins et al. 2020; Power 2019; Prajogo 2011). Besides, several challenges can disrupt the internalization process. For instance, the resistance of organizational stakeholders can cause the process to fail or to be slowed down (Hsu 2009; Silva et al. 2016). Also, organizations can willingly decouple "stated practices from actual behaviors" (Terlaak 2007, p. 981), thereby actively inhibiting internalization. In addition, many organizational aspects relevant to the certification cannot be fully grasped within the scope of a certification attestation because certification authorities typically apply sampling techniques to get an understanding of how the organization addresses the certification requirements (Power 2019). Finally, recent research highlights that ever-changing technologies threaten certification reliability and that (malicious) organizations may deliberately stop adhering to certification requirements to achieve benefits (e.g., reducing required incident response staff to save costs), once the certificate is issued (Lins et al. 2019). Consequently, there is a clear difference between adoption and internalization, and the organizational efforts to internalize and maintain certification practices can vary.

Prior research provides initial insights that this variation depends on the motivations for certification adoption (e.g., Boiral 2003; Lins et al. 2020; Prajogo 2011; Terlaak 2007). For instance, a functionalist may deliberately internalize the tacit and explicit certification information to improve internal processes and increase user satisfaction. In contrast, an institutionalist who seeks to conform with the regulations as the primary goal may try to invest as little as possible effort in the internalization process. While these examples highlight how different adoption motivations can influence the internalization process, we still lack an understanding of the patterns that underly the internalization processes for each adopter type. Understanding these patterns will help policymakers to better prevent superficial or insufficient internalization of certifications during certification design. In particular, ensuring the internalization of data protection certifications is crucial because of the ever-increasing frequency and severity of data breaches and cyberattacks.

Research Approach

We use an exploratory, qualitative multi-case study research approach to uncover patterns of certification internalization for different adopter types. The research is divided into a conceptualization and two data gathering and analyzing phases (Figure 1).

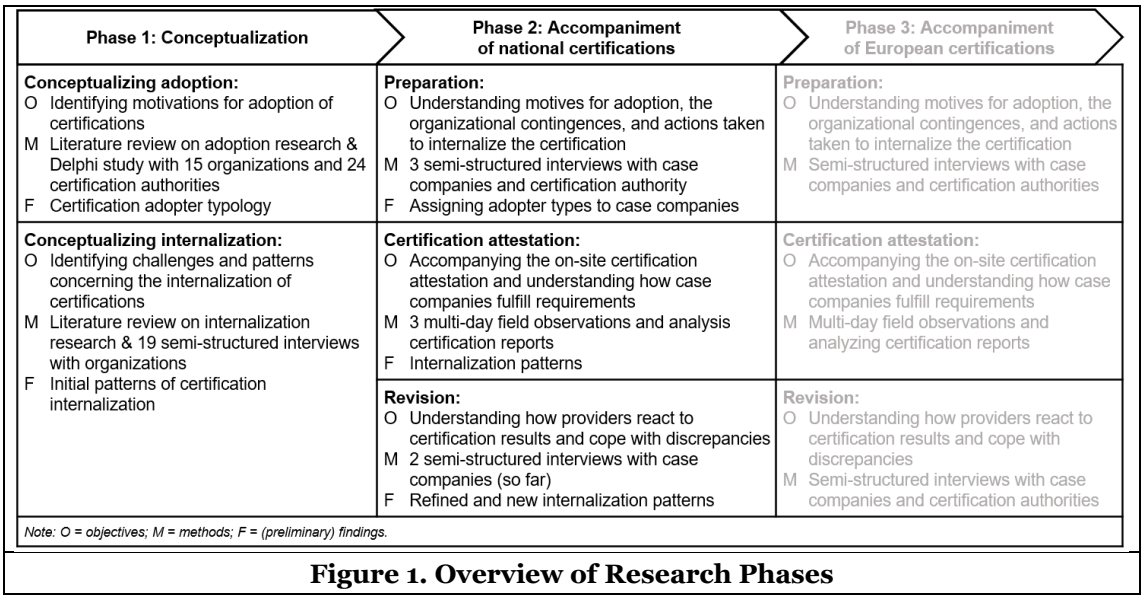

Figure 1. Overview of Research Phases

Research Context: Data Protection Certification for Cloud Services

The context of the study is a data protection certification for cloud services to prove GDPR compliance in Europe, which is currently under development. First, we chose this context because cloud services are now widely used and have become a critical element of many IT infrastructures and related services (e.g., ecommerce, storage services) (Benlian et al. 2018). Further, cloud service markets are characterized by a high degree of uncertainty because users largely depend on the organization for ensuring the security and privacy of their data. Consequently, users find it difficult to determine in advance which cloud providers can be trusted to provide reliable and secure services.

Second, more than two years after the enactment of the GDPR in mid of 2018, many organizations in the European economic area are still uncertain about how to interpret the regulation and to fulfill its data protection requirements to avoid substantial GDPR fines. Just recently, the data protection authority in the UK intended to fine British Airways 183.39 million pounds because customer data was breached through a cyberattack in 2018. The GDPR has foreseen certifications to cope with this uncertainty and to allow organizations to demonstrate compliance with GDPR requirements. In particular, the GDPR not only demands European member states to initiate certification development projects to tackle prevalent uncertainty and to provide guidance on how to implement GDPR requirements but also defines strict requirements on how to perform data protection certifications in articles 42 and 43 GDPR (European Parliament and Council of the European Union 2016). For instance, article 42 mandates the approval of certification criteria, and article 43 demands the accreditation, independence, and subject-matter expertise of certification authorities. Given prevalent uncertainty about GDPR compliance and initiatives to develop novel data protection certifications, we deem this context as appropriate to understand internalization patterns and derive recommendations on how to ensure thorough internalization.

Phase 1: Understanding the Problem and the Theory Domain (Conceptualization)

To understand the problem and the theory domain, that is, to gain insights into why organizations are adopting and internalizing IS certifications, we first conducted a literature review (*N=60*) on IS certification adoption research, and a ranking-type Delphi study with two unique panels comprising certified organizations (*N=15*) and certification authorities (*N=24*) (Lins et al. 2020). Second, we reviewed the existing literature on the internalization of certifications to ground our work in prior research. In the upcoming phases we not only aim to empirically validate extant internalization patterns from prior research

but are also eager to gather additional in-depth data about these patterns and understand how extant patterns relate to the diverse adopter types. Finally, we conducted 19 semi-structured interviews with small and medium-sized cloud service providers headquartered in Germany to refine internalization patterns and matching adopter types to these patterns, providing a first basic framework for the upcoming phases.

Phase 2: Identifying Internalization Patterns (National Certification)

In phase 2, we accompany the development of a national data protection certification for cloud services to prove GDPR compliance. During the development process, one certification authority performs the certification attestation at three pilot case companies to evaluate the certification's effectiveness and reliability. The three pilot case companies include small and mid-sized cloud providers headquartered in Germany. We will refer to the three pilot case companies as Alpha, Beta, and Zeta. Owing to confidentiality, we are unable to provide more detailed descriptions of the case companies.

At the current research stage, we have conducted two semi-structured interviews with the case companies Alpha (2 participants) and Beta (2 participants) before the certification attestation, and additionally, one interview with the certification authority performing the attestation, to understand motivations for adopting the GDPR certification and actions taken to internalize the certification. More importantly, we were able to accompany the on-site attestations for each case company. During each attestation, the certification authority interviewed employees and inspected physical facilities to assess the adherence to certification requirements. While each attestation lasted for two days, we were able to make various field observations about how Alpha, Beta, and Zeta internalized the certification and complied with the requirements. Afterward, we also gained privileged access to the certification reports summarizing compliance for each requirement. We also conducted two interviews with Alpha (1 participant) and Beta (1 participant) to discuss how they interpreted and reacted to the certification results. Scheduled interviews with Zeta were canceled due to organization's internal reasons.

To analyze transcribed interviews, field notes, and supplementary documents (e.g., certification reports), we apply a multi-coding approach. First, we use selective coding to match internalization patterns derived from prior literature during the conceptualization phase, thereby comparing our data with findings from extant research; second, open coding to identify novel internalization patterns that have been neglected in prior research; third, axial coding to understand causes and consequences of patterns; forth, selective coding to assign adopter types to each pattern to join the research streams on internalization and adoption; and finally, theoretical coding to reflect the theoretical perspectives underlying the adopter type (i.e., resource-based view, institutional theory, and signaling theory) on the patterns.

Phase 3: Validating and Refining Internalization Patterns (European Certification)

The upcoming phase 3 also concerns the accompaniment of the same data protection certification. While the certification is currently piloted for Germany, it will be further developed to be accepted as a *European Data Protection Seal* in 2021. As part of this advancement, the certification will be tested at four to six cloud service providers operating on a European and international level in the beginning of 2021. Similar to phase 2, we planned to conduct interviews before, during, and after the certification attestation and also planned to accompany the on-site attestations. By extending our sample of case companies and by incorporating global case companies, we aim to refine derived internalization patterns and increase their generalizability.

Preliminary Findings

Our preliminary analysis revealed four important findings. First, the conceptualization phase revealed a rank-order list of 24 motivators and 17 demotivators impacting organizations' intentions to adopt IS certifications (Lins et al. 2020). Comparing our findings to three competing theoretical perspectives enabled us to derive a typology of distinctive certification adopters: functionalists, institutionalists, and signalers (Table 1; Lins et al. 2020). We further identified initial internalization patterns that guide the analysis of future phases, for example, discursive resistance (i.e., the organizational resistance against the adoption of a certification; Silva et al. 2016) or abductive innovation (i.e., a process that facilitates the development of innovative information security policy through reconciling tensions between best practices and organizational practices; Niemimaa and Niemimaa 2019). In particular, we seek to relate extant and novel patterns with the diverse adopter types.

Second, the data gathered in phase 2 lend support for the three adopter types and that the internalization efforts differ across the adopter types. For example, with a clear focus on adopting the certification to improve the firm's market position, Alpha showed predominant characteristics of the signaler adopter type. The CEO notes "*Data protection is one of our core areas where we can provide our customers with added value. Certifications help us to substantiate this claim*." In contrast, the CISO of Beta emphasized that a GDPR certification must offer "*tangible benefits for us or our customers"* otherwise the investment into a certification may be unreasonable because "*we must fulfill data protection anyway*". This view suggests that institutional pressures, such as customer pressures, are a key driver for adopting the certification, thus mostly matching the institutionalist adopter type for Beta.

Third, we noted a difference between Alpha (signaler) and Beta (institutionalist) in that the predisposition to change is different. While Alpha has a clear motivation upfront and seems to embrace necessary changes to fulfill the certification requirements, Beta is more reluctant and cautious when it comes to implementing changes. Beta seems to regard the certification as an incremental process in which the potential benefits are continuously assessed against the effort. Through accompanying the attestation process, we found Beta to follow a minimalistic approach that involved preparing mandatory documents for the attestation, yet not implementing any changes to processes or technologies beforehand. They revealed internal processes cautiously to the certification authority, letting them identify and assess deviations from certification requirements. Afterward, they carefully elaborated, if the benefits obtained from internalizing the certification to resolve requirement deviations exceed the costs (i.e., fewer resources for value-adding tasks such as product development). We characterize this internalization process as the '*wait and observe*' pattern, which involves upholding established organizational practices and merely seeking to change these practices after a careful cost-benefit assessment following the certification attestation. To this end, Beta is more cautious and hesitant to internalize the certification practices with relates to the pattern of discursive resistance from prior research (Silva et al. 2016).

Alpha was more long-term oriented concerning realizing benefits from the certification. Alpha's handling of the certification process involved a close assessment of organizational circumstances and a dialectic process with certification authorities and researchers. We also recognized a reasonable level of experience on how to deal with IS certifications because Alpha had a mature information security management and has already internalized best practices from a related IS certification. In particular, the post-attestation interview suggests that the previous experiences with IS certifications have helped Alpha to internalize requirements of the data protection certification. As a result, the novel data protection certification requirements could be more easily embedded in the existing frame of already established organizational security practices. We characterize this internalization process as the '*embedment*' pattern, which involves the organization to embed novel certification practices into already established and substantiated information security practices. This pattern seems to expand the abductive innovation pattern from prior research (Niemimaa and Niemimaa 2019) because it suggests that previous experiences with the development of information security practices can ease future certification internalization processes.

Finally, analyzing the certification and internalization processes revealed ambiguity of the certification requirements that resulted in likewise ambiguous interpretations and varying degrees of internalization of organizations. For instance, uncertainties concerning the fulfillment of certification requirements were evident at all case companies. Our cases reveal that missing guidance on how to interpret and implement ambiguous certification requirements was a potential reason for differences in the internalization of certain certification requirements at the case companies. We thus can derive important recommendations for policymakers on how to improve the certification mechanisms by improving the description and guidance of certification requirements.

Discussion and Contributions

With this research, we aim to contribute to IS research in three important ways. First, we address calls in IS research (e.g., Hsu et al. 2012; Nielsen et al. 2014; Niemimaa and Niemimaa 2019) and management science (e.g., Heras-Saizarbitoria and Boiral 2013; King et al. 2005) for a deeper understanding of the "microfoundations" (Powell and Rerup 2017, p. 311) that shape how IS certifications are enacted within organizations. We thereby help to understand "why firms choose to certify, [and] how certification influences behavior" (King et al. 2005, p. 1091). With our study, we thus advance existing research by revealing the internalization patterns that explain how organization internalize certifications. In addition,

the focus of our study on data protection certifications also provides a relevant and timely context (e.g., Hsu et al. 2012; Niemimaa and Niemimaa 2019) that goes beyond prior research on quality management (e.g., ISO 9001) or environmental management (e.g., ISO 14001) (Heras-Saizarbitoria and Boiral 2013; Prajogo 2011). However, our focus on data protection certifications may limit our findings' generalizability to other types of certifications, such as those focusing on quality management.

Second, while prior research often draws attention to the issue of ceremonial, insufficient adoption of certification practices (e.g., Boiral 2003; Power 2019; Prajogo 2011), we know less about the motivations and patterns that underly such lack of internalization (Niemimaa and Niemimaa 2019). With our research, we bridge two so far distinct research streams (i.e., adoption and internalization), which enables us to advance prevalent research discussions of internalization and to unravel underlying internalization patterns for different adopter types. To this end, our preliminary findings already suggest two patterns, namely '*wait and observe'* and '*embedment'* that have been neglected in prior research and originate from different adopter types.

Third, our unique access to empirical data throughout the certification development process as well as the adoption process of organizations provides a unique opportunity for IS research. We can gather nuanced insights into the complex development process of IS certifications and derive implications for policymakers and organizations that allow for more effective IS certifications (Silva et al. 2016). The possibility to take part in the holistic process not only allows us to embrace important principles of qualitative IS research, including situating ourselves as actors, minimizing social dissonance, and integrating various voices (e.g., organizations, certification authorities, policymakers) across the adoption and internalization process. But also allows us to provide the insights necessary to strengthen certification mechanisms, thereby avoiding that the path from certification adoption to internalization becomes one of trial and tribulation. In particular, we are eager to advance the researcher's understanding of how certification mechanisms can ensure thorough internalization and prevent superficial internalization.

This research has important implications for policymakers and organizations alike. First, our insights on the internalization of different adopter types provide valuable guidance for policymakers that addresses an important issue for the effectiveness of IS certifications and thus informs the development of IS future certifications. The more IS certifications are developed to address pressing challenges in IS (e.g., the protection of personal information), the more valuable these insights become. Our preliminary findings already emphasize that policymakers must find a balance between describing requirements in neutral, abstract terms that apply to a wide range of organizations and providing useful descriptions and guidance for certification requirements. This challenge of IS certifications creates uncertainty for organizations on how to interpret certification requirements and derive necessary changes. For organizations, the understanding of internalization challenges can help to better prepare the certification process so as to maximize the benefits obtained (e.g., understanding and learning). However, a mere focus on immediate benefits warrants caution because the adoption of IS certification usually takes a substantial amount of time and effort from organizations (Hsu 2009).

Conclusion

The objective of this research is to uncover internalization patterns of IS certifications, thereby supporting policymakers with the development of reliable and trusted IS certifications. The heightened use of IS certifications as trusted signals for data protection and IT security of organizations makes it necessary for researchers and policymakers to better understand the certification adoption and internalization processes. A lack of such knowledge can lead to superficial adoption and, eventually, ineffective IS certifications. To support this endeavor, we aim to attain a better understanding of what is happening "behind the curtain" of adopting organizations by deriving patterns of certification internalization for different certification adopter types. Otherwise, we risk the effectiveness of certifications as a means to ensure the protection of sensitive information, which is a crucial good in today's digitally enabled and interconnected world.

Acknowledgements

We are grateful to Carol Hsu, Tongji University for a helpful discussion on an early version of this paper.

References

Barney, J. 1991. "Firm Resources and Sustained Competitive Advantage," *Journal of Management* (17:1), pp. 99-120.

Benlian, A., Kettinger, W. J., Sunyaev, A., and Winkler, T. J. 2018. "Special Section: The Transformative Value of Cloud Computing: A Decoupling, Platformization, and Recombination Theoretical Framework," *Journal of Management Information Systems* (35:3), pp. 719-739.

Boiral, O. 2003. "ISO 9000: Outside the Iron Cage," *Organization Science* (14:6), pp. 720-737.

DiMaggio, P. J., and Powell, W. W. 1983. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields," *American Sociological Review* (48:2), p. 147.

European Parliament, and Council of the European Union 2016. *General Data Protection Regulation*.

Heras-Saizarbitoria, I., and Boiral, O. 2013. "ISO 9001 and ISO 14001: Towards a Research Agenda on Management System Standards*," *International Journal of Management Reviews* (15:1), pp. 47-65.

Hsu, C., Lee, J.-N., and Straub, D. W. 2012. "Institutional Influences on Information Systems Security Innovations," *Information Systems Research* (23:3-part-2), pp. 918-939.

Hsu, C. W. 2009. "Frame misalignment: interpreting the implementation of information systems security certification in an organization," *European Journal of Information Systems* (18:2), pp. 140-150.

King, A. A., Lenox, M., and Terlaak, A. 2005. "The Strategic Use of Decentralized Institutions: Exploring Certification with ISO 14001 Management Standard," *Academy of Management Journal* (48:6), pp. 1091-1106.

Knight, G. A., and Liesch, P. W. 2002. "Information internalisation in internationalising the firm," *Journal of Business Research* (55:12), pp. 981-995.

Lansing, J., Benlian, A., and Sunyaev, A. 2018. ""Unblackboxing" Decision Makers' Interpretations of IS Certifications in the Context of Cloud Service Certifications," *Journal of the AIS* (19), pp. 1064-1096.

Lins, S., Kromat, T., Löbbers, J., Benlian, A., and Sunyaev, A. 2020. "Why Don't You Join In? A Typology of Information System Certification Adopters," (forthcoming).

Lins, S., Schneider, S., Szefer, J., Ibraheem, S., and Ali, A. 2019. "Designing Monitoring Systems for Continuous Certification of Cloud Services," *Communications of the AIS*, pp. 406-510.

Löbbers, J., and Benlian, A. 2019. "The effectiveness of IS certification in E-commerce: does personality matter?" *Journal of Decision Systems* (28:3), pp. 233-259.

Löbbers, J., Lins, S., Kromat, T., Benlian, A., and Sunyaev, A. 2020. "A multi-perspective lens on web assurance seals: contrasting vendors' intended and consumers' perceived effects," *Electronic Commerce Research* (forthcoming).

Meyer, J. W., and Rowan, B. 1977. "Institutionalized Organizations: Formal Structure as Myth and Ceremony," *American Journal of Sociology* (83:2), pp. 340-363.

Naveh, E., and Marcus, A. 2004. "When Does the ISO 9000 Quality Assurance Standard Lead to Performance Improvement?" *IEEE Transactions on Engineering Management* (51:3), pp. 352-363.

Nielsen, J. A., Mathiassen, L., and Newell, S. 2014. "Theorization and Translation in Information Technology Institutionalization," *MIS Quarterly* (38:1), pp. 165-186.

Niemimaa, E., and Niemimaa, M. 2017. "Information systems security policy implementation in practice: from best practices to situated practices," *European Journal of Information Systems* (26:1), pp. 1-20.

Niemimaa, M., and Niemimaa, E. 2019. "Abductive innovations in information security policy development: an ethnographic study," *European Journal of Information Systems* (28:5), pp. 566-589.

Powell, W. W., and Rerup, C. 2017. "Opening the Black Box: The Microfoundations of Institutions," in *The SAGE Handbook of Organizational Institutionalism*, R. Greenwood, C. Oliver, T. B. Lawrence and R. Meyer (eds.), Thousand Oaks, CA: SAGE, pp. 311-337.

Power, M. 2019. "Modelling the Microfoundations of the Audit Society: Organizations and the Logic of the Audit Trail," *Academy of Management Review (In-Press)*.

Prajogo, D. I. 2011. "The roles of firms' motives in affecting the outcomes of ISO 9000 adoption," *International Journal of Operations & Production Management* (31:1), pp. 78-100.

Silva, L., Hsu, C., Backhouse, J., and McDonnell, A. 2016. "Resistance and power in a security certification scheme: The case of c:cure," *Decision Support Systems* (92), pp. 68-78.

Spence, M. 1973. "Job Market Signaling," *The Quarterly Journal of Economics* (87:3), pp. 355-375.

Terlaak, A. 2007. "Order without Law? The Role of Certified Management Standards in Shaping Socially Desired Firm Behaviors," *Academy of Management Review* (32:3), pp. 968-985.