In Cloud We Trust?
Coopting Occupational Gatekeepers to Produce Normalized Trust
in Platform-mediated Interorganizational Relationships

Abstract

Interorganizational trust plays an important role in facilitating business relationships, especially for the organizational adoption of new services. Prior research suggests that interorganizational trust develops when the trustor has adequate confidence in the reliability of the trustee's services. Nevertheless, reliability breakdowns are also an inevitable part of service provisioning. Such breakdowns are especially prominent and visible in the context of platform-based services. Yet, platform-based services continue to be adopted and used by organizational customers. This increased adoption and use of such services despite its inconsistent reliability pose the following question: how is trust produced in platform-mediated interorganizational relationships? To examine this question, I conduct a 20-month field study of a cloud computing platform provider and its customers, focusing on the practices of trust production in the wake of reliability breakdowns. I describe customer concerns about the platform's inconsistent reliability that hampered the development of interorganizational trust. I then identify four practices of *trust work* enacted by the platform provider to address some of these concerns and to coopt the occupational gatekeepers in customer organizations who are responsible for technology adoption decisions. Following this, I describe how and why these occupational gatekeepers performed *justification work* to rationalize the continued use of the platform despite its inconsistent reliability. Together, trust work and justification work facilitate the co-production of interorganizational trust through normalizing reliability breakdowns as "business-as-usual" events. Synthesizing these findings, I develop a normalization model of trust production and discuss the implications of *normalized trust* for platform-mediated interorganizational relationships in the digital economy.

Forthcoming in *Organization Science*

Author:

Arvind Karunakaran

Assistant Professor, Strategy and Organization,

Desautels Faculty of Management, McGill University, Montreal, Quebec, Canada, H3A 1G5

Contact: arvind.karunakaran@mcgill.ca

Keywords: Trust, Occupations and Professions, Interorganizational Relationships, Economic Sociology, Platforms, Cloud Computing, Digital Innovation.

Acknowledgements:

I would like to sincerely thank the senior editor, Pamela Hinds, and four anonymous reviewers for their time and generative feedback throughout the review process. I am deeply grateful to my advisor, Wanda Orlikowski, for her invaluable guidance, support, and generous comments. I would also like to thank Grace Augustine, Lindsey Cameron, Lisa Cohen, Diana Dakhlallah, Daphne Demetry, Kate Kellogg, Ann Langley, John Van Maanen, Siobhan O'Mahony, Paola Perez-Aleman, Leslie Perlow, Mike Pratt, Jean-François Soublière, Emily Truelove, JoAnne Yates, Chris Yenkey, and Ezra Zuckerman for their helpful comments on earlier drafts of this paper, to the participants in Harvard's Craft of Qualitative Inductive Research seminar, Montreal Organizations Writing Workshop, AOM PDW on Trust, ASA Annual Conference, and to seminar attendees at Boston University, MIT, and University of Virginia.

Interorganizational trust plays an important role in the formation and sustenance of business relationships (Dirks and Ferrin 2001, Graebner 2009, McEvily, Zaheer and Kamal 2017, Schilke and Cook 2013). Various conceptualizations of trust as “the expectation that the other [party] will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party” (Mayer et al. 1995), or as the “extent of trust placed in the partner organization by the members of a focal organization” (Zaheer, McEvily, and Perrone 1998, p.142), interorganizational trust is considered critical for the adoption and use of new services by organizational customers (Bailey and Bakos 1997). Conceptual and empirical works in this area of research suggest that interorganizational trust develops when the trustor has adequate confidence in the reliability of the trustee’s services (Dyer and Chu 2000, Lewis and Weigert 1995, Schilke and Cook 2015, Schumann et al. 2000). Reliability not only signals the trustee’s technical competence but also indicates its commitment to maintaining internal quality control processes (MacDuffie 2011).

Nevertheless, breakdowns in reliability are also an inevitable part of service provisioning (Gutierrez 1995, Kramer and Lewicki 2010). Scholars have documented various internal (e.g., human errors, quality control failures) and external (e.g., natural disasters) reasons for how and why such reliability breakdowns happen (Dirks et al. 2011, Gillespie and Dietz 2009, see also Perrow 1984, Vaughan 1997). In the digital economy, reliability breakdowns are especially prominent in the context of platform-based services i.e., services that are delivered to thousands of organizational customers in a parallel manner via online platforms (Gillespie 2010, Gawer 2014)¹. Prior research and multiple news reports have documented the inconsistent reliability of platform-based services (Bezemer and Zaidman 2010, Groucutt 2019). These reliability breakdowns range from service outages and unscheduled downtime (Ranger 2018, Raphael 2019) to security failures and even the abrupt discontinuation of the service with little notice to customers (Marshall 2013). Moreover, since reliability breakdowns in platform-based services are characterized by

¹ I use the term “platform” to refer to “platform-as-a-service [PaaS]” — the specific configuration of hardware infrastructure (e.g., servers, storage, networks) and software deployment environment that supports the building and execution of various business functions — as opposed to other invocations of the term such as “industry platform” or “two-sided platform” (Gawer 2014). Platforms are becoming more prevalent in the business-to-business (B2B) domain, especially in functions such as customer relationship management, human resource management, accounting, supply chain management, and payroll processing.

high visibility, they remain not as privately-held beliefs amongst a select few customers, but rather as public information that is common knowledge to customers (Chwe 2001).

In addition, there is also a relative lack of institutional safeguards such as service level agreements (SLAs), professional codes of conduct, and industry associations in the context of platform-based services. These institutional safeguards would otherwise provide the guard rails needed to limit a firm's unreliable behavior by specifying monetary penalties and/or social sanctions (Heimer 1985, Zucker 1986). However, as Cochran and Witman (2011) describe, several platform providers avoid instituting SLAs for “platform downtime,” “service outage,” and “access speed” with their customers to preempt significant financial penalties that they might need to incur if in case the platform experiences downtime or service outage for a substantial time period.

Yet, these platform-based services are increasingly being adopted and used by organizational customers across multiple industries (BVP CloudIndex 2015, Gartner 2018). Even firms in sensitive industries such as pharma, healthcare, and financial services are adopting and using platform-based services (NorthBridge Report 2017). Therefore, this increased organizational adoption and use of platform-based services despite its inconsistent reliability pose the following question: *how is trust produced in platform-mediated interorganizational relationships?* Examining this question will help address the broader theoretical issue regarding the production of interorganizational trust in the face of reliability breakdowns that are difficult to anticipate fully, and therefore, cannot be guaranteed by the provider from happening again in the future.

To examine this research question, I conducted a 20-month field study of SigmaCloud – a business-to-business (B2B) cloud computing platform provided by Sigma Inc., – and its two customer organizations (Energy Corp and CommHousing). Sigma grew from a few thousand customers in the early 2000s to 150,000 customers in 2017, generating over USD 2 billion in annual revenues. In the same time period, the company also encountered —and continues to confront— several reliability breakdowns, including service outages, denial-of-service attacks, database failures, and data center power shut down that made their platform unavailable to users for a significant time period. In addition, there is also a relative lack of

institutional safeguards (e.g., SLAs) in this context, posing further challenges to ensuring reliability. Therefore, the SigmaCloud platform served as a useful research site to examine my research question.

Through this field study, I identified several customer concerns about the inconsistent reliability of the SigmaCloud platform that hampered the development of interorganizational trust. I then elaborate on the four practices that Sigma enacted to address these customer concerns: governing through code, creating and circulating trust rhetoric, establishing trust indicators, and convening an occupational community. Together, these practices constitute the *trust work* performed by Sigma, aimed at (a) signaling that good faith efforts are being taken by the company to prevent reliability breakdowns as much as possible and therefore these breakdowns should not be taken to reflect the “true nature” (Dirks et al. 2009) of the company; (b) indicating that such reliability breakdowns are nevertheless inevitable, and not just one-off incidents, due to the “radically innovative” nature of the platform, but will be eventually repaired by Sigma in an ongoing manner; (c) crafting a renewed “innovation narrative” for the occupational gatekeepers — the corporate information technology (IT) professionals — who are responsible for technology adoption decisions in customer organizations; such an innovation narrative includes the construction and dissemination of aspirational labels (e.g., change agents, agile) that these professionals could in turn use to counter the negative labels historically associated with them (e.g., roadblocks, naysayers) in their respective companies. Collectively, through trust work Sigma not only attempted to coopt the occupational gatekeepers, but also generate *accounts of trustworthiness* that portrayed the company as an earnest one that is acting in good faith while also simultaneously trying to “disrupt” the status quo in the entrenched enterprise software industry. In that sense, these accounts sought to implicitly contrast the conventional dimensions of economic worth (such as reliability and consistency in service delivery) against the new dimensions of economic worth (such as innovation and disruption) that Sigma is purportedly bringing to the enterprise software industry and its customers.

However, these trustworthiness accounts alone did not beget interorganizational trust, because they were not uncritically accepted by the service users (i.e., sales managers, sales representatives) in customer organizations. Rather, an elaborate *justification work* was performed by the occupational gatekeepers (i.e., corporate IT professionals) in customer organizations to rationalize the continued use of the platform

despite its reliability issues. Specifically, I discuss how these occupational gatekeepers, in their efforts to retain jurisdictional control over IT procurement, repurposed Sigma's trustworthiness accounts to justify the platform's continued use to the sales managers and sales representatives in their respective companies. Finally, I discuss how trust work and justification work together facilitate the co-production of interorganizational trust via normalizing reliability breakdowns as "business-as-usual" events, and in the process, reorienting service user's expectations about reliability.

This study advances our understanding of the processes through which trust is produced in platform-mediated interorganizational relationships, despite the platform's inconsistent reliability. In doing so, this research makes the following contributions to the literature on interorganizational trust. First, this research makes a theoretical contribution by explicating a model of *normalization* that highlights the processes through which interorganizational trust is co-produced in the wake of reliability breakdowns. Second, this research unpacks and analytically characterizes the outcome of the normalization process: *normalized trust*. As compared to particularized trust (where trust is a function of the trustee's consistent reliability and is rooted in personal relations between members of the trustee and trustor organizations) and generalized trust (where trust between parties is shaped by institutional safeguards that limit unreliable behavior), normalized trust is an "emergent social effect" (Leslie 2015, p.31) that gets produced through reorienting trustor's expectations about reliability. Consequently, normalized trust reduces customer vigilance about platform governance (e.g., quality control processes, reliability standards) and instead structures an environment whereby precarious reliability becomes the de-facto norm (cf. Kollock 1994). Third, this study brings the backstage processes of trust production in platform-mediated relationships to the foreground. In doing so, this research contributes to the emerging stream of work on trust in platforms by highlighting the role of occupational gatekeepers as well as technology – and sociotechnical practices, more broadly – in trust production. Finally, this study makes an empirical contribution by moving beyond the "reliance on single-sided data collection" (Graebner et al., 2020, p.365) that characterizes prior research on interorganizational trust. By collecting and analyzing "data from both sides of the interorganizational relationship" (p.369), this study unpacks the distributed processes of trust co-production happening across both the provider and customer organizations.

Theoretical Background

Reliability and Interorganizational Trust

Interorganizational trust is important to the sustenance of business relationships (Adler 2001, Blois 1999, Child and Möllering 2003, Gulati and Nickerson 2008, McEvily 2011), and plays an especially important role in facilitating the organizational adoption and use of new services (Bradach and Eccles 1989, Bailey and Bakos 1997, Barrett and Gendron 2006). One of the key factors that shape the development of interorganizational trust is reliability (MacDuffie 2011, Schumann et al. 2000). Organizational scholars have examined why customers' (hereafter trustor) confidence in the reliability of providers' (hereafter trustee) services is vital for trust development (Dyer and Chu 2000, Schilke et al. 2017, Zaheer et al. 1998). Reliability – conceptualized as the ability to generate results in a consistent manner with little to no variance in quality (Selznick 1957) – signifies both the technical competence and commitment of the trustee (Sako and Helper 1998). For instance, Dyer and Chu's (2000) study on the determinants of interorganizational trust in automaker-supplier relationships found that reliability of the suppliers' products/services directly influenced the development of interorganizational trust. While the trustee's reputation might shape initial expectations of reliability (Abraham et al. 2017), firsthand experiences that the trustor gained by using the trustee's services is a more direct assessment of trustee's reliability (Dyer and Chu 2003, Schilke and Cook 2013).

Particularized Trust. Prior research has documented how repeated interactions and concrete personal relations between boundary-spanning members of the trustee and the trustor organizations can play a key role in assessing reliability (e.g., Currall and Judge 1995, Perrone et al. 2003). Such assessments, in turn, can strengthen or weaken interorganizational trust (Ring and Van de Ven 1994). For example, Gulati (1995) examined the importance of repeated interactions for assessing the reliability of trustee's services, which in turn gradually facilitates the development of interorganizational trust between firms. Similarly, Schumann et al. (2010) found that individual members' (i.e., trustors) experience of inconsistent reliability and lack of predictability in the trustee's services significantly undermines the development of interorganizational trust (see MacDuffie 2011 for a review).

Although reliability is critical to the development of interorganizational trust, breakdowns in reliability are an inescapable part of service provisioning (Guttek 1995, Kramer and Lewicki 2010). Prior research has described the reasons for how and why such reliability breakdowns happen, including human errors, design flaws, quality control failures to detect anomalies, as well as exogenous events such as natural disasters (Dirks et al. 2011, Gillespie and Dietz 2009, see also Perrow 1984, Vaughan 1997). These breakdown incidents trigger members of the trustor organization to revisit their “preliminary judgments” (Schilke and Cook 2013, p.288) and update their beliefs about the reliability of trustee’s services. This, in turn, could put the “trust relationship in jeopardy” (Jones and George 1998, p. 538; Schilke et al. 2013).

Scholars have also documented the various types of repair activities performed by members of the trustor organization to fix these reliability breakdowns and regain the trust that was breached (Gillespie and Dietz 2009, Heaphy 2013, Kuwabara et al. 2014). These repair activities include offering an apology, admitting culpability, fixing the issue, and shouldering responsibility (Scott and Walsham 2005).

Overall, the nature of trust that emerges in this process is *particularized trust* (Delhey et al. 2011, Kollock 1994, Schilke, Reimann, and Cook 2021, Uslaner 2002), where “concrete personal relations” (Granovetter 1985, p.490) to assess the trustee’s reliability play a central role (Van Hoorn 2014). Particularized trust, therefore, is rooted in personal relationships between members of the trustee and trustor organizations and is largely a function of trustee’s consistent reliability.

Generalized Trust. Scholars have also examined how institutional safeguards – in the form of legal provisions, codes of conduct, and industry/professional associations – play an important role in acting as guard rails to limit unreliable behavior (Bachmann and Inkpen 2011, Zucker 1986). The broader institutional arrangements, including its legal and political regime, structures the business environment by explicitly specifying monetary penalties for inconsistent reliability and/or implicitly suggesting social sanctions for breaches (Rothstein and Stolle 2008, Shapiro 1987). Together, these arrangements provide safeguards to the trustor against opportunistic or unreliable behavior by the trustee (Bradach and Eccles 1989, Cook et al. 2005, Mollering 2006).

In her classic historical analysis of the U.S. economy between the 1840s and the 1920s, Zucker (1986) showed how institutional arrangements such as the law and legal services, the banking and insurance

system, and industry associations were critical in providing safeguards that helped trustors mitigate uncertainties. These institutional safeguards created an enabling environment for the development of interorganizational trust. Legal provisions – in the form of contracts and service level agreements – are also a central aspect of the fabric that constitutes institutional safeguards. These provisions assert the power of the “shadow of the law,” reassuring the trustor organization that uncertainties inherent in interorganizational relationships could be transformed into “manageable [legal] risks” (Bachmann and Inkpen 2011). This encourages the trustor to engage in the relationship without obsessing over the technicalities of detecting misconduct (Bachmann 2001, Dasgupta 1988). Although scholars have debated whether contracts and SLAs are complements or substitutes to trust, they nevertheless agree that the *willingness* to contract and the *inclination* to specify SLAs are positive signals of commitment toward reliability that, in turn, could facilitate interorganizational trust (Poppo and Zenger 2002)

The nature of trust that emerges in this process is *generalized trust* (Carruthers 2009, Nannestad 2008, Paxton 2007, Paxton and Glanville 2015, Schilke et al. 2021, Uslaner, 2002), where the institutional environment plays a central role in limiting unreliable behavior. Compared to particularized trust where personal relations play a central role, the qualities of the broader institutional environment - including its legal regime - are fundamental to the emergence and sustenance of generalized trust.

Inconsistent Reliability and the Production of Interorganizational Trust

These lines of work have produced important insights on interorganizational trust, including the mechanisms for assessing and guaranteeing reliability in the trustee’s services (Gambetta 1988, Gefen and Pavlou 2012). However, what happens in situations where the trustee’s services are characterized by inconsistent reliability, and when institutional safeguards to limit unreliable behavior are limited?

Indeed, situations such as these are becoming prevalent in the digital economy where services are developed by a provider organization and delivered to thousands of customer organizations in a parallel manner via online platforms (Gillespie 2010, Vaquero et al. 2008). Such platform-based services (Gawer 2010) confront reliability breakdowns that are prominent and highly visible to customers (Ranger 2018, Willcocks et al. 2013). These breakdowns range from service outages, unscheduled downtime, response delays, security failures such as phishing attacks and denial-of-service attacks, login failures (Groucutt

2019, Raphael 2019) to even the sudden discontinuation of the service by the platform provider with little notice to customers (Marshall 2013). Moreover, since these reliability breakdowns in platform-based services are characterized by high visibility, they remain not as privately-held beliefs amongst a few customers that ensue in pluralistic ignorance, but rather as public information that is common knowledge to customers (Chwe 2001). In addition, institutional safeguards are relatively weak in this context. For one, to preempt financial penalties, platform providers avoid instituting safeguards such as SLAs with their customers that specify and guarantee reliability standards (e.g., access speed, platform downtime, service outage) (Cochran and Witman 2011). This, in turn, signals a lack of commitment toward providing consistently reliable services to customers. Moreover, the norms and codes of conduct about platform governance are also unclear in this context (NorthBridge Report 2018).

Yet, these platform-based services are increasingly adopted and used by organizational customers (Gartner 2018). Given that interorganizational trust is considered critical for the adoption and use of new services by organizational customers (Bailey and Bakos 1997), and prior research identifying reliability as a critical component in the development of interorganizational trust (Dyer and Chu 2000), this increased organizational adoption and use of platform-based services despite its inconsistent reliability poses the following question: how is trust produced in platform-mediated interorganizational relationships? Before discussing the findings, I elaborate on the research setting and methods.

Research Methods

I used qualitative, ethnographic methods to examine my research question. This approach is aligned with the nature of my research question and the phenomenon that I seek to understand (Edmondson and McManus 2007). This research espouses the tenets of relational ethnography (Desmond 2012) to follow the phenomenon of interest across multiple field sites – for instance, the platform provider firm, customer organizations, and platform conferences. My primary sources of data included field-based observations, interviews, and archival materials. In the subsections below, I describe the research setting and elaborate on the procedures followed for data collection and analysis.

Research Context and Setting

Enterprise cloud computing served as the research context for this study. In the enterprise cloud computing model, a platform provider develops and maintains a business-to-business (B2B) platform through which services (e.g., customer relationship management [CRM], payroll processing) are delivered to organizational customers via the Internet. This model is distinct from the traditional “packaged software” model, offered by vendors such as SAP and Oracle, where a software package is licensed and installed within the customer’s premises (Pollock and Williams 2008).

The SigmaCloud platform — a Platform-as-a-Service (PaaS) in the enterprise cloud computing industry, developed by Sigma Inc., — served as the research setting for this study. Through the platform, services such as SigmaCRM are delivered to customer organizations. These services are primarily used by sales professionals within firms to manage sales-related processes (e.g., tracking and updating of sales lead and associated information) and marketing managers to manage promotional campaigns. SigmaCloud provided an appropriate research setting to examine my research question for the following reasons. First, since SigmaCloud is a B2B platform used by organizational customers, this setting helped me to understand and better explicate the phenomenon of platform-mediated *interorganizational* relationships. Second, this setting enabled me to observe the process of trust production at a granular level unfolding at both the platform provider and customer sites.

Data Collection

Data collection spanned multiple sites: the platform provider’s headquarters and local offices, customer organizations, their IT and sales department offices, and platform conferences. These research sites were located across three cities (2 in the Northeast and 1 in the West Coast) in the United States. Table 1 presents a summary of the data sources. I collected and analyzed three types of data: archival, interviews, and observations. I elaborate on the data collection process below.

--- Insert Table 1 about here ---

Archival materials. I employed historical methods to collect and analyze considerable amounts of archival data and publicly available materials on the enterprise cloud computing industry, Sigma, and the SigmaCloud platform. These archival data sources were particularly helpful in developing a contextual and longitudinal understanding of trust production in platform-mediated interorganizational relationships

(Please refer to Appendix A1 for an elaboration on the archival data sources and processes followed for data collection). I synthesized these materials to create a chronology of events (Van de Ven and Poole 1990) relating to Sigma and its platform. This step enabled me to understand (a) the various concerns that customers reported over time (e.g., Will this new model of service provisioning be reliable? Will data be safe and not compromised? What will happen to customer data and applications if the platform provider goes bankrupt and/or discontinues its service?); (b) how Sigma responded to those concerns.

Interviews and Observations. My primary data were drawn from interviews and observations that unfolded over two phases. The first phase of primary data collection happened during an 18-month period (from May 2012 to November 2014) at multiple sites. The second phase of data collection happened during a 2-month period (from mid-June 2018 to August 2018), primarily at the platform provider and customer sites. During the first phase, I started data collection at the platform provider's site. I visited Sigma's headquarters and conducted multiple interviews with their senior executives and employees. These interviews helped me understand the various practices of trust production espoused by Sigma during the online provisioning of its platform. I also observed the ongoing practices enacted by Sigma in addressing the concerns faced by customers. Specifically, I collected data on 31 "reliability breakdown" events (e.g., service outages, platform downtime, security issues) that I observed during the time period of this field study, and analyzed how Sigma's customers responded to those incidents. Events such as conferences (CloudConf) also became important venues to observe in real-time the practices enacted by Sigma to manage customer concerns. I also viewed and analyzed 83 videos in the Sigma YouTube channel – including live product demos, conference presentations, and Q&A sessions between Sigma and its customers (Please refer to Appendix A2 for details on the data collection process).

To understand the perspective of customer organizations, I conducted semi-structured interviews with 24 senior executives and IT decision-makers from five companies who were Sigma's customers and belonged to different industries (banking, insurance, telecom, consumer products, healthcare). These interviews helped me examine the various trust-related concerns experienced by customers during platform adoption and deployment. I selected two of these customer companies – Energy Corp and CommHousing – for a more in-depth study. Energy Corp, a specialist in energy management, has over

100,000 employees and operates in nearly 100 countries. CommHousing is a mid-sized company with around 500 employees and 1,000 partners. It is in the business of lending funds and equity to partners for building and managing housing properties. At the time this study was initiated, both organizations were in the process of decommissioning their existing on-premise packaged software and deploying SigmaCloud across their organizations. This shift allowed for a depth of access to not just their senior managers but also the middle-managers, IT developers, and end-users of the platform. Moreover, examining these two organizations allowed me to identify similarities and differences in the reliability-related concerns experienced by customers of different sizes and structures during their efforts to decommission packaged software and transition to SigmaCloud. For instance, EnergyCorp had a separate legal team to assess vendor risks and a well-established internal structure for performing due diligence. By contrast, CommHousing did not have a separate legal team, and due diligence was performed by the IT department. This research design helped me address alternative explanations (e.g., Does proper due diligence alone, performed by the IT department and/or specialist legal teams, help alleviate trust-related concerns?) pertaining to the development of interorganizational trust.

Across these two companies, I conducted interviews with IT executives as well as sales/marketing managers and end-users of the platform. I was able to observe in real-time how middle managers (e.g., sales managers, marketing managers) and end-users (e.g., business development executives, sales representatives) were using the SigmaCloud platform, the accounts, justifications, and skepticisms offered by these actors about SigmaCloud, and how they reacted to reliability breakdowns such as service outages. These multiple sources of data enabled me to triangulate (Jick 1979) and understand the phenomenon of platform-mediated interorganizational relationships from different vantage points.

The second phase of data collection was conducted to examine the extent to which reliability breakdowns, and other related concerns about Sigma and its platform, were normalized by the customer organizations, and its consequential outcomes. These outcomes were manifested in both the rhetoric and explicit actions of the customer organizations (e.g., continuing to store and update sensitive data such as the master client list on SigmaCloud as opposed to their local server). During this phase, I conducted

additional interviews and observations at Sigma headquarters and at the customer sites (Please refer to Table 1 for a summary of data sources, and Appendix B for the semi-structured interview protocol.)

Data Analysis

Data collection and analysis unfolded in an iterative manner (Langley et al. 2013). I used qualitative data analysis methods, including writing descriptive memos, data coding, analytical memo-ing, writing case histories, identifying empirical puzzles, and abstracting convergent themes into theoretical concepts.

I did not begin this research project with a focus on interorganizational trust. Instead, the focus of the study emerged during the iterative process of data collection and analysis. I started this research with orienting questions such as how interorganizational relationships are managed in platform-mediated contexts. During the first phase of data analysis, I synthesized my field notes into weekly descriptive memos detailing how Sigma remotely delivers its platform to a heterogeneous set of customers distributed across the world. In parallel, I did “initial coding” (Charmaz 2006) of the field notes, interview transcripts, and archival materials (especially the forums) to identify the different concerns raised by customers, prospects, and technology journalists. Responses were coded on the basis of “in vivo” codes — phrases and terms offered by the informants (e.g., “trust revolution,” “cloud computing is trust-based computing,” “lack of SLAs,” “we’re the disruptors”). Through this process of synthesizing field notes, writing memos, and initial coding, several interesting observations and puzzles emerged. For instance, I noticed several instances where issues related to reliability were confronted by Sigma, and by extension, its customers. I also repeatedly encountered advertisement slogans, banners, and conference videos about “trust” and realized its prominence in this context. This awareness prompted me to probe further how trust was developed between Sigma and its customers, despite the persistent concerns on reliability.

In the second phase of data analysis, I did “focused coding” (Charmaz 2006) of field notes, interview transcripts, and archival data to understand the various activities enacted by Sigma to manage the customer concerns on reliability that were detrimental to the development of interorganizational trust. For example, this phase highlighted the active role played by Sigma in creating and circulating trust rhetoric, instituting the Chief Trust Officer role, and establishing trust indicators such as the Trust dashboard and Trust seals. At this stage, I expanded the list of people to interview, including the trust officer and

members of the “customer engineering” team at Sigma, and analyzed the transcripts from these interviews. I also coded for how members across different levels of the customer organization (CIO/IT managers vs. business users) reacted to reliability breakdowns.

In the third phase, I wrote detailed case histories of Sigma and the two customer organizations to perform within-case analysis. When writing these case histories, I focused on reliability breakdowns (e.g., service outages, platform downtime, security failures) encountered by customers, and how Sigma addressed the customer concerns around reliability. The individual cases ranged from 25 to 40 pages in length. I then conducted cross-case analysis to identify variations and similarities in themes observed across the two customer organizations. Iterative rounds of memo-ing and focused coding uncovered that the activities enacted by Sigma converged onto four overarching practices. I synthesized those practices as constituting the “trust work” performed by Sigma.

Data analysis of field notes and interview transcripts from the customer organizations strongly indicated that the service users at the customer organizations did not merely accept the trustworthiness accounts generated by Sigma. The service end-users at these companies did express several concerns to the IT managers (occupational gatekeepers responsible for technology adoption decisions) about the reliability of SigmaCloud. I noticed the rationalization provided in response by the senior IT executives on the continued use of the platform, how these actors repurposed Sigma’s trust rhetoric inside their companies, and why they attempted to do so in the manner they did. For example, the IT managers used language such as “service interruptions...are part of the game,” and “they [sales managers] should not be regressive.” As data analysis progressed, I carried out further focused coding to make sense of these puzzling observations. I wrote memos to synthesize and abstract these processes as “justification work.”

In the fourth phase, I sought to understand what my findings meant theoretically. In this task, I engaged with the literature on interorganizational trust (e.g., Bachmann and Inkpen 2011, Schilke and Cook 2013) and reliability breakdowns (e.g., Gillespie and Dietz 2009, Kramer and Lewicki 2010). In parallel, I also wrote theoretical memos to interpret my findings on trust work and justification work in light of the processes and mechanisms discussed in prior research on interorganizational trust. While this literature was useful in explaining some of the findings, it offered few insights about how

interorganizational trust was produced despite the inconsistent reliability of the services provided by the trustee. At this stage, I engaged with the literature on “normalization” (Vaughan 1997, see also Perrow 1984). This literature enabled me to make better make sense of how trust work and justification work normalize reliability breakdowns as business-as-usual events, and in the process, reorient user expectations about the reliability. Finally, I did “theoretical coding” (Charmaz 2004) to strengthen emergent findings and contrast them with prior research on trust. For example, I re-coded statements such as “We worry less about service disruptions,” and “As the CIO, I don’t want to be that annoying guy who always says ‘no-you-can’t-do-that’” and abstracted them as “normalization.” Similarly, I coded actions such as “master client data uploaded to SigmaCloud,” and “increased use of SigmaCloud platform by sales reps” as evidence for normalized trust. This iterative process culminated in a model of normalization that illustrates how interorganizational trust is co-produced in the wake of reliability breakdowns.

Findings

In this section, I start by highlighting the customer concerns about reliability breakdowns in the SigmaCloud platform that hampered the development of interorganizational trust. Following this, I elaborate on the four practices of *trust work* enacted by Sigma to address these reliability concerns. I show how trust work was aimed at coopting the occupational gatekeepers in customer organizations as well as to generate “accounts of trustworthiness” about Sigma and its platform. In the final sub-section, I describe the skepticism expressed by service users (sales managers and reps) in customer organizations about Sigma’s trustworthiness accounts. I then explain and why the occupational gatekeepers in these customer organizations performed *justification work* to rationalize the continued use of the platform despite its reliability issues. I conclude by discussing how trust work and justification work together shaped the co-production of interorganizational trust.

Concerns about Reliability that Hampered Interorganizational Trust

Customers expressed several concerns pertaining to breakdowns in the reliability of the SigmaCloud platform. These concerns, in turn, hampered the development of interorganizational trust. Third-party watchdog websites (such as the now-defunct SigmaWatch.com) tracked and reported over 150 incidents of reliability breakdowns in the SigmaCloud platform between 2007 and 2015. During the duration of my

fieldwork (from May 2012 to November 2014, and from mid-June to August 2018), I noted 31 incidents of reliability breakdowns, major and minor, in the SigmaCloud platform. Appendix C provides a timeline and description of these reliability breakdowns. Such breakdowns were manifested in terms of the following categories: *access* (i.e., how reliably can the customer login and access the various functionalities of the platform without any outage or downtime issues), *safeguards* (i.e., lack of SLAs to mitigate reliability issues), and *security* (i.e., protecting the platform from security breaches). I elaborate on these customer concerns throughout the rest of this section. Please refer to Table 2 for illustrative quotes about these reliability concerns. The puzzle, therefore, is on how interorganizational trust is produced between Sigma and its customers, despite the platform's inconsistent reliability. This puzzle is especially intriguing considering that the SigmaCloud platform is not necessarily cost-effective compared to the incumbent, on-premise CRM packages in the enterprise software industry. Neither is SigmaCloud's subscription fee lower than that of the other cloud-based CRM platforms offered by its competitors. Therefore, it is neither due to cost savings nor due to a lack of alternative solutions that customers were willing to "put up with" the SigmaCloud platform despite its reliability issues. In the below subsections, I elaborate on the practices of trust work and justification work that facilitated the co-production of interorganizational trust, despite the inconsistent reliability of the SigmaCloud platform.

--- Insert Table 2 here ---

Trust Work Enacted by Sigma

I identified four practices — governing through code, creating and circulating trust rhetoric, establishing trust indicators, and convening an occupational community — that collectively constitute the *trust work* enacted by Sigma. Individually, these four practices attempted to address customer concerns on reliability. Collectively, they coopted the occupational gatekeepers and generated accounts of trustworthiness about Sigma and its platform. Appendix D offers supporting evidence for these practices.

Governing through Code. The SigmaCRM application is delivered through the SigmaCloud platform to thousands of customer organizations in a parallel manner. Therefore, the ability to reliably access the platform is an important issue for customers. End-users encountered reliability issues with respect to service outages, platform downtime, and access speed. Coding errors and software bugs were common

causes for such breakdowns in reliability. Exogenous events, such as power shutdown in data centers due to hurricanes, also played a role. However, one of the prominent reasons for these breakdowns, especially for service outages and reduced access speed, was the excessive usage of the platform by some customers. As the infrastructure of the SigmaCloud platform is shared by all customers, Sigma had to manage these “commons” resources in a manner that the heavy use of the platform by one customer does not affect other customers, and/or bring down the platform’s overall performance.

One way to address such concerns around reliability is through safeguards such as SLAs, where usage guidelines are clearly articulated, agreed upon, and signed-off with the customers. However, signing such SLAs with customers is a double-edged sword for Sigma. If the SigmaCloud platform falls below certain uptime and access speed requirements as pre-specified in the SLA, then it will lead to a significant financial loss for Sigma because of the way the platform is structured and provisioned. Specifically, when the platform experiences downtime and fails to meet reliability standards, the entire customer base is affected. Consequently, signing SLAs with customers will involve substantial financial risks for Sigma.

Therefore, instead of SLAs, Sigma’s senior management decided on an alternative approach: to monitor and govern customers’ usage through software code. To achieve this, Sigma created and disseminated a set of rules –referred to as “platform community rules” – and enforced those rules through software code. As a senior software engineer at Sigma remarked:

It is too risky for us, imagine if there is a tornado that shuts down our data center? These are beyond our control, and it is so risky that we might even go out of business if three or four of these incidents happen. Remember, we are offering tens of thousands of seats of open-ended capability for large customers... But for this model to work, we need to enforce some governance limits on customers [Interview]

These community rules were aimed at policing the heavy usage of the SigmaCloud platform to ensure that one customer does not monopolize the common resources of the platform to the extent that it slows down access to the platform – or worse, brings the platform to a halt. Sigma operationalized these community rules into what the company refers to as “governance limits” and engineered those into software code in three distinct steps: (a) keeping track of the number of API [Application Programming Interface] calls made by a customer organization within a 60-second period, (b) monitoring the level of customizations made by customers to their instantiation of the SigmaCRM application, and (c)

implementing alert systems that monitor heavy usage of the platform and enforce penalties for rule-breakers. As a manager in the Customer Engineering team at Sigma described:

... Improper or heavy usage by customers is always a problem for us. Sometimes, this happens by mistake. For example, you [customer] write infinite loops... Other times, it is intentional. We enforce these things with governance limits... that lets us automatically restrict the level of usage... This really helps us in keeping up the quality and performance of the platform [Interview]

Another major reliability concern that hampered the development of trust is related to the security of customer data. Given that all customer data are located in shared servers, Sigma has to ensure data security so that external hackers and/or another customer could not gain access to client-specific data and applications. One way to address such customer concerns is by being transparent about the security features of the platform, including the measures taken by Sigma to implement those features in practice. However, the dilemma that Sigma faced was that by being transparent about the measures taken to ensure security, it also potentially exposed the platform to hackers, phishers, and other third-party security attacks. Paradoxically, this could decrease the platform's reliability and increase the security threats that Sigma sought to avoid.

To address this issue, Sigma instituted further forms of safeguards through software code. To manage internal security threats, it architected the platform in such a way that boundaries between one customers' data are programmatically demarcated 'by-design' from another customer's data. This demarcation was done through what Sigma referred to as its "multi-tenant" architecture. Details of the design and implementation of the architecture were held as a trade secret. However, Sigma provided high-level details about their multi-tenant architecture and how it guaranteed "data property rights" by virtually separating one customer's data ("the tenants") from another, while physically keeping them together in shared servers. Customers subscribed to a "tenancy" within Sigma's platform, an arrangement similar to renting a room in an apartment building where many tenants share the building's common facilities but are separated from one another by walls and doors. The enactment of this multi-tenant architecture through software code enabled the data and applications of one customer to remain secure and insulated from those of other customers. In this way, data property rights were materialized through software code without a formal SLA. As a senior Sigma executive described:

We take a very pure approach and take special pride in the multi-tenancy environment. That means we only have one version of our system, and every single customer - whether they're a single user in Japan, a 100 user

company in Italy or India, or a 10,000 user company in North America - are all running on the exact same version [of our platform] and the exact same infrastructure. Also, in this way, the customer data - and also their applications and the customizations they make to those applications - are completely isolated from other customer data and applications...So we completely secure... [Interview]

In summary, this practice of governing through code helped Sigma minimize reliability breakdowns via instituting *local safeguards*. This was achieved by creating community rules about platform usage, and enforcing those rules in software code (cf. Lessig 1999). Through this practice, the commons resources were managed, and network externalities such as congestion were avoided in an ongoing manner. This practice accomplished distributed governance and signaled to the customers that “good faith” efforts were being taken by Sigma to prevent reliability breakdowns.

Creating and Circulating Trust Rhetoric. While the above practice of governing through code helped Sigma address concerns about reliability to some extent, it was not able to fully prevent breakdowns in reliability. Reliability breakdowns continued to happen due to software bugs, quality assurance failures, and exogenous events such as data center power shutdowns. Consequently, in the face of these breakdowns, customers were hesitant about uploading their sensitive sales- and client-related data to SigmaCloud. As an IT executive from a medical devices firm remarked:

Well, this is all good, but how the heck would I know that no one is snooping around my data? And I am also extremely uncomfortable with the idea that my client data will reside on the same server as my competitor, and even with some goddamn mom-and-pop shop owner... How could I trust them [Sigma] with all my data and customer contact info? Things could happen, you know, and I just want to be sure. [Interview]

Similar concerns emerged from executives across different industries. End-users (such as sales reps and sales managers) in customer organizations continued to experience service outages, downtime, and access speed issues. Therefore, they were reluctant to use SigmaCloud for their critical sales operations and to upload sensitive business data, such as the “master client list” that has the contact information of all their clients, prospects, and prospective sales deals, onto the platform.

Sigma’s senior engineers and system architects – a politically powerful group within the company – believed that customer concerns about reliability breakdowns were primarily related to service outages, access speed, and security. They believed that while these breakdowns cannot be fully prevented from happening again in the future, they could be addressed “by design” through software code and platform architecture. However, the marketing executives at Sigma argued that given the eventuality of breakdowns and the nature of cloud platforms, where “100% reliability” cannot be guaranteed to

customers, Sigma needed to invest in a marketing campaign that could complement the engineering group's technical solutions. These marketers understood that customer concerns were fundamentally about the lack of trust in Sigma and its platform. Therefore, they advocated for a large-scale campaign aimed at reimagining Sigma's brand around trust. As a senior marketing manager at Sigma reflected:

So the real issue I think is trust.... They're [customers and prospects] trusting us with their data, and they're trusting us to run them in our servers. And so, we needed to prove that, regardless of whether we had single-tenant architectures or multi-tenant architectures or hybrid architectures, or whatever it was – that we have their trust. So I think **trust is the essence of the cloud question**. [Interview, emphasis added]

Sigma's co-founders and senior executives took active steps in rhetorically articulating trust as its “number one value.” In particular, the company inscribed the notion of trust as the centerpiece of its platform positioning and external messaging. Its rhetoric around Trust (always capitalized) was materialized in marketing collaterals, banner advertisements, product release announcements, demo videos, sales pitches, and annual reports. Sigma also appointed a “Chief Trust Officer” who was responsible for inculcating Trust as a foundational value within the company. Sigma continually emphasized Trust as a core value and guiding principle in its stakeholder meetings and product release events. Beyond external messaging, Sigma's trust rhetoric also became a central part of its internal training programs. As a Sales executive at Sigma reflected:

We place a lot of emphasis on Trust... in fact that is central to our training here...Can you imagine pitching to someone, “Hey, give us all your data and applications, we will host it for you in our Cloud, and you pay a monthly fee for it?” So it is all about building deep trust... Our Chief Trust Officer, for example, is often used in the sales process. ... And I think it's important for many, they [prospect] start to understand not all clouds are created equal, and some [like Sigma] really focus on things like Trust. [Interview transcript]

Sigma's emphasis on trust did not stop with that campaign but became an ongoing endeavor. Even in its recent marketing pamphlets and product announcements, Sigma continued to stress Trust as core to its values. In its annual reports, Sigma likewise listed Trust in the same vein as its core service offerings. In addition, Sigma wanted to establish Trust as a core aspect of enterprise cloud computing. It produced a number of white papers and reports on topics related to “Trust in Cloud Computing” and used slogans such as “Cloud Computing is Trust-based Computing” and “SigmaCloud: Your Trusted Cloud Computing Platform.” In these documents, Sigma elaborated on how trust has become an intrinsic part of cloud computing, and on the various governance measures it uses to “engineer” trust into the platform. These white papers were circulated to industry analysts (from firms such as Gartner), who then used these

documents as springboards to generate industry-wide rhetoric about trust in cloud computing. The rhetoric around Trust was widely circulated in each of Sigma's roadshows and conferences. For instance, during a product demo to thousands of customers at their annual conference, the CEO of Sigma invoked the central importance of Trust, placing it on the same footing as the company's core service offerings.

There's all these trends that are happening out there -- social, mobile, big data, community, applications, cloud, and of course trust, super important. It gets down to when we're making that connection with that customer, with that partner, with that product - what is the level of trust that we're able to deliver as a vendor to that customer - **it's a Trust Revolution**...the people that you're connecting with, you're going to need another level of trust... *The Customer Revolution is truly a Trust revolution.* [Presentation by Sigma's CEO at CloudConf, italics added]

As part of the Trust rhetoric, Sigma advertised its "extensive efforts" to detect the breakdowns and repair them in a timely manner. For instance, in conferences and demo events, Sigma highlighted the early-warning tools used by its "reliability engineering" team to detect issues and repair them quickly by re-enforcing governance limits. Sigma did so without revealing the technical know-how behind the design of those tools. As the VP of Customer Engineering described:

Our programming languages, they are incredibly powerful languages and they can allow you to do great things on the platform, but they can also allow you write infinite loops, they can allow you to write code that takes up large amounts of memory. We are trying to catch all these things with governance limits... **We have a reliability team [to do that] and then the top 20 customers** - the ones that we need to focus on...and understand what they are doing [Conference Presentation, emphasis added]

Likewise, Sigma advertised its "disaster management plan" by highlighting its strategy for data backups and recovery in case of a data center shut down. In addition to creating automated backups of customer data at regular intervals, the data are also saved in multiple locations to build redundancy in the event of an unexpected power shutdown in a data center. In this way, customers were ensured that they would be able to recover their data at any point in time. As the EVP of Technology at Sigma described at a conference presentation, "So how many times do we save the data? ... It's six times - that's a lot...we store it six times because we want to make sure that it's there when you really need it." At these conferences, Sigma also highlighted its approach for detecting and fixing bugs (that may have caused the breakdowns in the previous release cycle) via automated scripts. These scripts supposedly run over 200,000 different scenarios and approximately 60 million tests to "catch" the bugs in an efficient manner, which in turn will be "patched" by the software engineering team at Sigma.

To sum up, through the practice of creating and circulating trust rhetoric, Sigma was able to infuse the notion of trust as central to its brand and image, and project this image to its customers. Underlying the

Trust rhetoric was the message that Sigma is trying its best to continuously monitor, detect, and preempt breakdowns as much as possible; however, trust rhetoric also signaled that if such breakdowns eventually happen, then the company has thought such scenarios through and prepared to repair those breakdowns in an ongoing manner.

Establishing Trust Indicators. Although the creation and circulation of the trust rhetoric helped Sigma establish a trust-centric image and signal its commitment to customers, the reliability breakdowns continued to happen. Moreover, due to the networked nature of the SigmaCloud platform, these breakdowns became visible to all the customers. Customer concerns around reliability intensified even further after SigmaCloud experienced a multi-hour service outage that prevented end-users from logging-in and accessing their data during a critical pre-holiday period. A technology journalist writing for a popular tech magazine raised questions about the reliability of Sigma's services, and challenged Sigma to formulate, sign, and honor SLAs with its customers. Several other customers supported the journalist's arguments and demanded that Sigma establish SLAs as a credible signal of its commitment to reliability. Another platform outage a few months later raised more questions about the SigmaCloud platform's inconsistent reliability. Disgruntled end-users and system administrators at customer organizations formed a coalition and started a website, SigmaWatch.com, to post downtime log files and disseminate counter-narratives about Sigma's reliability. These counter-narratives further led many customers to insist that Sigma come up with SLAs to warrant adequate levels of uptime for its platform. They also demanded that Sigma specify credits and penalties if the company is not able to honor the uptime levels specified in the SLAs. Despite such mounting pressures, Sigma resisted specifying SLAs because of the potential financial costs it would incur if adequate performance levels were not achieved as specified in the SLAs.

Such dynamics are illustrated below in the response given by a senior executive of Sigma to a customer:

Ok, I am going to be quite frank with you. [Vendor Name], they have SLAs. [Another vendor name], they also do. But seriously, do you really think they care about their customers? It [SLA] doesn't mean a thing to them, really. They are like a factory and you folks are just an ID to them. Compared to them, we are quite new and small. And we care about you, we REALLY do, and we are desperately trying to change how things are done in the enterprise software world, which is so stuck in the past. [Recorded video of the Q&A]

Nevertheless, customer pressures to improve the platform's reliability continued. To address these customer concerns, Sigma needed to move beyond its trust rhetoric to credibly signal that it was indeed

taking customer concerns about reliability seriously. One way to accomplish such credible signaling is through transparency, that is, to further open-up and detail the internal governance and quality control processes implemented internally within Sigma to increase its platform reliability. However, as described before, the dilemma that Sigma faced was that by being transparent and opening-up its internal governance processes, it also risked exposing its platform to security threats and external attacks, potentially decreasing the platform's reliability. To circumvent this problem, Sigma objectivized² the notion of reliability by developing a set of quantified measures that publicly display *indicators* of trust in the form of a "Trust dashboard." Trust dashboard included statistics related to operational (e.g., uptime, downtime, maintenance, access speed) as well as strategic reliability issues (e.g., security threats in the form of denial-of-service attacks, worm attacks, phishing attacks) faced by its platform. It also displayed live and historical data on the platform's reliability, including up-to-the-minute information about downtime and planned maintenance. This dashboard was made available through a public website that customers and the general public could access. Trust dashboard was promoted as an automated display of real-time data about the platform, captured directly from data center sensors and tracking response times of data packets, without any human intervention, and therefore depicted as a credible, objective indicator of the platform's reliability. A senior executive from Sigma explained:

We put Trust as the number one priority for the company, right? And there's a great site, Trust.sigma.com, which is a totally transparent view into how our systems are running, issues we're having, all that sort of thing, so that customers are never in the dark about what it is that we're doing... [We] really do put Trust as our number one priority. And that we walk the talk, we don't just talk the talk. [Conference presentation]

In addition, Sigma obtained external certifications (e.g., ISO 27002) and received a number of "Trust" seals (e.g., Verisign, TRUSTe, and AICPA) from third-party auditors attesting to the various internal measures and processes taken by Sigma to increase its platform reliability. These seals were uploaded to Sigma's Trust website and became part of Sigma's marketing collaterals. As this VP of Engineering at Sigma described:

We delivered [a few] billion transactions last year. And they are coming faster than ever, at a current average of approximately a quarter of a second. It's all there for the world to see every day on our Trust website... customers always go away feeling very comfortable that we really do put trust as our number one...It really is,

² I differentiate the term "objectivize" – the process of making a subjective phenomenon and/or experience into an objective one – from the more well-known concept of "objectify," which is commonly defined as "the act of degrading someone to the status of a mere object" (Oxford English Dictionary 2014).

it's demonstrated in how we think about our systems from a security and trust perspective every day. So, many [customers] get comfortable with that. [Conference Presentation]

This practice enabled Sigma to objectivize reliability through its Trust dashboard and have its processes assessed by external auditors. In this way, Sigma signaled to its customers that the company was indeed trying to “walk the talk” and stay true to its trust rhetoric about commitment to reliability.

Convening an Occupational Community. In addition to its trust rhetoric and trust indicators, Sigma also attempted to convene the occupational community of corporate Information Technology (IT) professionals. These IT professionals — ranging from the CIOs and senior IT executives to IT managers and corporate IT developers — act as gatekeepers inside customer organizations for decisions pertaining to the procurement and adoption of information technologies of various kinds, including cloud computing platforms. Sigma, therefore, convened these IT professionals under a single roof through the conferences it organized. While the stated purpose of these conferences was to provide training to IT professionals so that they could better understand the features of the SigmaCloud platform, the implicit purpose was to elicit their identification with Sigma and its platform. Towards that end, Sigma crafted a renewed innovation narrative for the IT professionals, providing them with aspirational labels centered around “change” and “agility” as opposed to the negative labels, such as “roadblocks,” “naysayers,” and “obstructionists,” that were historically associated with these corporate IT professionals.

To elaborate, Sigma hosts multiple conferences and events each year, including its yearly CloudConf conference that attracts thousands of attendees. Sigma designed CloudConf to mimic a carnival, with foosball tables and gaming consoles located across the conference center, and open-mic events happening on the lawn outside the center. CloudConf features top government executives, Hollywood celebrities, motivational speakers, and even spiritual gurus as part of their keynote events. CloudConf typically culminates in an exclusive music concert featuring popular rock bands, with free beer, over 50 food stalls, and shuttle service back and forth from the city center to the concert venue. Throughout the four-day conference, multiple workshops are organized by Sigma's employees. At some of these sessions, IT executives and IT managers from customer organizations share their experiences about transitioning to SigmaCloud. Moreover, Sigma's trust indicators such as the Trust Dashboard, Trust Seals, and ISO certifications, were visibly displayed and demo'ed at CloudConf. In addition, the word “community” was

frequently used by the senior executives of Sigma during their keynote presentations and by the Sigma employees when they interacted with the IT professionals (e.g., “platform community,” “developer community,” “customer community”). Interviews with IT professionals indicated how CloudConf freed them from the bureaucratic confines of their workplace. As this IT manager of a telecom firm described:

Every year I look forward to attending CloudConf... I'm 44 now and it is the closest thing to Burning Man that I can ever get to [laughs]. It's a lot of fun... You know how these “Enterprise IT”-type people are. The grey suit-and-tie-wearing, spreadsheet-and-due-diligence types. I'm one of them, so I shouldn't be so condescending, but they are just boring types. But CloudConf is different, because you get to meet cool people. Even the boring ones, when they come to CloudConf, they become cool... It is good to meet and mingle with people from other companies who are just like me, who used to use [package software name] but now use SigmaCloud. It's good to connect with them, grab a beer or three [laughs], attend the [concert by band name] and just have a good time.

As this quote suggests, because CloudConf created a carnivalesque atmosphere, it “liberate[d] participants from routine activities” (Turner 1986). Although conference attendees need to pay over 800 USD as registration fee, there was increasing interest among IT managers and developers to attend CloudConf. Sigma also publicized a series of articles, variously titled “How to Convince Your Boss to Send You to Sigma's CloudConf” and “Justify Your Trip to CloudConf,” to encourage IT professionals to attend the conference. In this regard, Sigma provided a URL link to an email template (Justify-your-Trip-to-your-Boss.doc) that IT professionals within customer organizations could download, modify, and send to their supervisors for approval (Please refer to Appendix E for the email template).

Nevertheless, the Q&A sessions at CloudConf became a venue for these IT professionals to express their concerns about the platform's reliability. Although Sigma's executives acknowledged the issues, they also rhetorically downplayed the legitimacy and seriousness of these concerns by using phrases such as “we strive towards near-zero downtime, but still it [downtime] happens,” “such things [platform outage and downtime] happen,” “we also believe in ‘move fast and break things,’ but with minimal damage,” and “all tech platforms do that.” Similarly, Sigma's executives emphasized how their platform is “radically innovative” with a “disruptive” potential, which will in turn help the IT executives - and IT departments in general - to become more innovative and shed their legacy negative labels such as “roadblocks,” “buzzkills,” and “naysayers” within their own company. As Sigma's VP of Sales described:

We value two things at Sigma. Well, first and foremost, absolutely, it is Trust... **Even if we did go down, even if there was a glitch... the fact that we were there, it was all hands-on deck, and they [customers] didn't have to worry about it.** They knew we were going to come back up and running. That was a huge, it was a leap of faith for them. Right? Trust, [that is] Number one. Number two, they [CIOs] love the innovation that we bring to their businesses... So yeah, there are some organizations that are kind of fine with the status quo,

they deploy an application. It's out there for two or three years. Users know how to use it. **But there's very little innovation. They're just kind of stuck in a rut...** They [CIOs] loved that we're constantly pushing the envelope and kind of pushing their businesses, so when the CIO wants to consume that innovation and bring that to their business, it really makes them a change agent – a true innovator within their company – as opposed to being THAT person who just struggles to “keep the lights on.” [Interview, emphasis added]

As indicated in the above quote, Sigma acknowledged the reliability issues (“even if there was a glitch”) and signaled its commitment to repair those breakdowns in a timely manner (“The fact that we were there, it was all hands on deck, and they [customers] didn't have to worry about it. They knew we were going to come back up and running”). At the same time, the quote also suggests how Sigma provided the IT professionals with aspirational labels (e.g., “innovators,” “change agents,” “agility”) that they could in turn use to counter the negative labels (e.g., “naysayers,” “roadblocks,” “buzzkills,” “obstructionists”) that were historically associated with them, especially within their own respective companies. All of these, in turn, elicited the IT professionals' identification with Sigma and its platform.

To sum up, conferences such as CloudConf enabled Sigma to convene the corporate IT professionals, who are the occupational gatekeepers for technology adoption decisions, under a single roof. At these conferences, Sigma crafted a renewed innovation narrative for these IT professionals, filled with aspirational labels around change and agility. In this process, Sigma was able to probe and elicit the IT professionals' identification with the company and its platform.

Viewed together, through the four practices of trust work, Sigma aimed to address some (but not all) of the customer concerns about the platform's reliability. But more importantly, through trust work Sigma aimed to coopt the occupational gatekeepers with the expectation that they could potentially become champions – or “trust ambassadors” – for Sigma within their respective companies. Collectively, these practices generated “accounts of trustworthiness” about Sigma and its platform. Such accounts signaled that “good faith” efforts are being taken by Sigma to address reliability breakdowns as much as possible; nevertheless, such breakdowns are inevitable and would nevertheless happen due to the radically innovative nature of the platform but will be eventually repaired by Sigma in an ongoing manner.

Justification Work Unfolding within Customer Organizations

Having examined the practices of trust work enacted by Sigma, I now focus on how customers responded to Sigma's accounts and shaped the co-production of interorganizational trust. In particular, I

examine why and how the occupational gatekeepers – senior IT executives and IT managers – in customer organizations rationalize the continued use of the SigmaCloud platform via *justification work*. To accomplish this, I focus on two customer organizations (Energy Corp and CommHousing) that were decommissioning their existing on-premise software and moving to the SigmaCloud platform. Appendix F offers supporting evidence for the justification work unfolding in these two customer organizations.

During the early stages of my fieldwork at these organizations, I observed initial skepticisms expressed by the service users (such as sales reps, sales managers, marketing managers) about the reliability of SigmaCloud. When the sales department experienced service outages and access speed issues, the sales reps and managers were reluctant to use SigmaCloud for their critical sales operations and to upload sensitive business data — the “master client list” that has contact information of all their clients and prospects, existing sales deals, and prospective projects — onto the platform.

As I followed the deployment of SigmaCloud in these two organizations, I observed how such skepticisms increased with every reliability breakdown the service users encountered. At one point, the sales managers escalated the issues they faced to the mid-level IT managers, and then to the senior IT executives such as the IT director and the CIO. However, as the champions of Sigma within their company, these senior IT executives urged the sales managers to “give it [SigmaCloud] some more time.” Such platform outages and downtime issues were recurring, but the IT executives were still supporting the continued use of the platform. Therefore, the service users – specifically the senior sales managers at EnergyCorp and the marketing managers at CommHousing – decided to confront the issue by exploring alternatives to SigmaCloud. Since the procurement of cloud-based platforms falls under the category of operational, and not capital, expenditures, sales executives at EnergyCorp learned that such expenditures could come from their department’s discretionary budget and did not need approval from the IT

department. The VP of Sales at EnergyCorp decided to pilot a platform that was a competitor to Sigma:

... At one point, I decided, enough is enough. I can’t keep my guys on-the-road waiting when that darn thing [SigmaCloud] is down again. So I went ahead with the pilot idea that Jim [one of the sales managers] proposed. I asked my guys to keep it under the radar for sometime, till we figure out how [the new platform name] performs as compared to SigmaCloud. Under the radar, because if Henri [CIO] finds out what we were doing, he won’t be happy and then I got to deal with that [Interview]

Similarly, at CommHousing, the Head of Marketing gave the “go ahead” for her team to subscribe to the cloud version of a CRM application they had used before to run marketing campaigns. Eventually, when the CIOs and IT directors at the companies found out how they were getting bypassed, it led to a contestation, followed by occupational jurisdictional conflicts over who was in-charge of IT procurement. As a consequence of such occupational jurisdictional conflicts, senior IT executives formalized an approval process for “cloud pilot projects.” They used these approval processes to block ongoing pilot projects that the sales and marketing departments were pursuing.

More importantly, this occupational jurisdictional conflict between the IT and the Sales/Marketing departments triggered the CIOs to justify the continued use of SigmaCloud within their companies. I observed that in order to retain jurisdictional control over IT procurement, the CIO and other senior IT executives at these two customer organizations began to mimic, with some variation, the trust rhetoric of Sigma. For instance, the CIO of CommHousing prepared a position paper for his Board of Directors, requesting the Board and the governing council to approve migrating a significant portion of their data and applications to SigmaCloud. This position paper significantly mirrored Sigma’s trust rhetoric, including phrases such as “true multi-tenant platform,” “hundreds of millions of dollars of investment that Sigma has made for infrastructure improvements and efficiencies for quality, performance and security,” and “SigmaCloud is... secure, with SAS70, ISO 270001 and SysTrust certifications.” Similarly, I observed several other instances where the CIO, VP, and Director of IT in these companies reused Sigma’s trustworthiness accounts internally when communicating with their service users, including the sales and marketing. For example, the VP of IT at EnergyCorp asked the mid-level IT project managers to “go talk to the sales guys” and tell them that they are “sorry about the [SigmaCloud] service disruption and feel terrible that they got to take long coffee breaks” but that such service disruptions they encountered are “nothing out of the ordinary.” These IT executives repurposed the trustworthiness accounts to counter the concerns that end-users had about SigmaCloud. In doing this, they rationalized the continued use of the platform despite its reliability issues. For example, a senior IT executive at EnergyCorp noted the following:

We worry less about that [platform downtime and service disruptions]. It doesn’t mean we say nothing will ever happen... And yes, as my boss said, it is an act of faith. One day you say, “OK I trust [CEO of Sigma]. **I trust**

that I can put my data on the same server as my competitor and OK, this is a new world... I would not say that there is no risk but I would say what happens tomorrow if the [in-house] DNS server collapses? [Interview]

To understand this further, I probed the IT executives more and asked them how, as people responsible for IT, they were planning to address issues around Sigma's downtime and the consequent loss of business incurred by their company? One of the executives gave the following answer:

[Moving to SigmaCloud] is actually a **bold and radical move**, considering the history of this company. **It is true that service interruptions and system outages happen**, like the one we had last month and also the month before, **but that is part of the game**. We got to work around it and move ahead, **not be regressive and move backward...** [Interview transcript; Senior IT executive from CommHousing, emphasis added]

These findings suggest how the IT executives rationalized the continued use of SigmaCloud as a way to retain jurisdictional control over IT procurement. In that task, they also reused the aspirational labels disseminated by Sigma at CloufConf, such as "radical," "innovative," "change agents," and "forward-looking." These justifications for the use of SigmaCloud by senior IT executives shaped the sales reps' continued platform usage. Over time, these sales reps (and other end-users) got accustomed to the reliability breakdowns in SigmaCloud to the extent that they considered them as commonplace occurrences. As this sales representative at EnergyCorp described:

I used to be super annoyed by these [service] outages, especially when I am trying to see my [sales] dashboard and update my deals-in-progress, or just pull up some info before a prospect meeting. But I guess I am more used to it now, and kinda get that these things happen especially for cloud [platforms]. I am not a techie, but was told that SigmaCloud is cutting-edge... and from my experiences so far, yeah it [SigmaCloud] goes down but also comes back up again, and things do get resolved. [Interview, Business development executive, EnergyCorp]

With increased usage, more and more CRM transactions flowed through the SigmaCloud platform. Consequently, the habituated end-users became more dependent on the platform to accomplish their work. The business managers too decided to move the master client list to SigmaCloud to have all their "client, prospect, and lead" data in one place.

I also found additional evidence on the effects of Sigma's trust work on customer organizations by observing 31 reliability breakdowns that happened during my fieldwork. Specifically, I observed the responses of customers (as well as that of Sigma) after these breakdown events, and noticed how and to what extent senior executives in customer organizations continued to mimic (or not) Sigma's trustworthiness accounts to rationalize the continued use of the platform. I describe one such event – and the subsequent responses by customers and Sigma – below.

This particular breakdown event was a major service outage that prevented customers from logging into the SigmaCloud platform for over 12 hours. By happenstance, I was visiting the Sigma headquarters when this event happened and was able to observe firsthand the various repair activities undertaken by Sigma. These efforts included the creation of an “emergency” technical team to address the problem as soon as possible through temporary fixes so that the platform could be up-and-running quickly, as well as a separate cross-functional team composed of engineers, testers, and architects to isolate the problem and perform “root cause” analysis to develop long-term solutions. Additionally, the customer service team provided periodic updates through Twitter, and Sigma’s PR team handled questions from tech journalists and industry analysts. Shortly after this breakdown event, I interviewed the IT executives, managers, and end-users in EnergyCorp and CommHousing to understand their reactions to this major service outage. Specifically, I used this event as an opportunity to formulate a set of critical-incident questions. Although the end-users expressed some frustration for being unable to login and access the platform, they nevertheless mentioned that they have “come to terms” with such breakdowns. On the other hand, the senior IT executives continued to view this service outage as a ‘business as usual’ event, providing further evidence for the justification work and its consequences:

I know that the business users were complaining of not being able to login. And worried whether they will never be able to login or that their data is permanently lost. I sort of understand their concerns, but I think they are misplaced... So I think, moving to Cloud, we are becoming more agile and innovative. Of course, outages happen there too. And we hope Sigma reduces them in the future. But that doesn’t mean we should give up on the Cloud... Yes, it would be nice to have SLAs, but it is really a matter of trust. [IT Director from EnergyCorp]

In the summer of 2018, I visited the two customer organizations again to examine (a) if there were any changes to their use of the platform, (b) the extent to which customer concerns about Sigma and its platform were normalized (or not), and (c) the continued impact of normalization on interorganizational trust, as manifested in both rhetoric used within these companies and their explicit actions (e.g., continuing to store and update the master client list on SigmaCloud as opposed to storing it in their local server). I found that both companies had expanded their use of SigmaCloud to several departments beyond just sales and marketing. They also continued to keep their master client data on SigmaCloud.

I remember [that time] when people were groaning and grunting, they still do, and we do face login issues [downtime] from time to time, but I will say that we are in a steady-state now. We are moving more data to SigmaCloud and even thinking of building an add-on that will directly interface with our ERP. It was a lot of work, lot of convincing lot of running around and a lot of political stuff that I had to personally get involved in. I’m glad I did, and as you can see, we are now doing very well. [Interview transcript; CIO of EnergyCorp]

The IT budget spent on SigmaCloud was increased by ~52% in the case of EnergyCorp and ~35% in the case of CommHousing. These dynamics highlight the role of justification work in rationalizing the continued use of the platform despite its reliability issues.

Co-Production of Interorganizational Trust in the Wake of Reliability Breakdowns:

Towards a Model of Normalization

I began this paper by asking how trust is produced in platform-mediated interorganizational relationships, despite the platform's inconsistent reliability. Synthesizing the findings from my field study, I propose a model of normalization that illustrates the processes through which interorganizational trust is co-produced in the wake of reliability breakdowns (Figure 1).

--- Insert Figure 1 here ---

Processes of Normalization

As illustrated in Figure 1, reliability breakdowns hamper the development of interorganizational trust between the trustee (i.e., provider) and trustor (i.e., customer) organizations. Interorganizational trust is co-produced despite these reliability breakdowns via the processes of normalization. At the center of these processes are trust work and justification work. Through trust work, the provider organization aims to signal that good faith efforts are taken by them to prevent reliability breakdowns as much as possible and therefore such breakdowns should not be taken to reflect the “true nature” (Dirks et al. 2009) of the company. At the same time, trust work is also used to underscore the inevitability of reliability breakdowns and by extension, the difficulty in completely preempting such breakdowns ex-ante (as opposed to repairing such breakdowns ex-post in an ongoing manner). And finally, trust work is used to craft a renewed “innovation narrative” for the occupational gatekeepers in customer organizations who are responsible for technology adoption decisions. Such an innovation narrative includes the construction and dissemination of aspirational labels (e.g., change agents, agile) for these occupational gatekeepers that they in turn use as a scaffold to further their own professional projects, especially in countering the negative labels (e.g., roadblocks) that are associated with them in their respective companies.

Viewed together, trust work is used to coopt the occupational gatekeepers in customer organizations as well as to generate *accounts of trustworthiness* about the provider organization (cf. Elsbach 2004,

Sonenshein et al. 2010). Such accounts portray the provider organization as a “new kid on the block” that is trying to “disrupt” the status quo in an entrenched industry made up of large corporations, but also earnestly trying to repair the reliability breakdowns in its services in an ongoing manner. In summary, these accounts rhetorically signal to the customers, prospects, and external audiences at large that the provider organization is worthy of their trust, thereby urging them to stick with the company and its platform despite its reliability issues.

However, such trustworthiness accounts alone do not generate interorganizational trust, as these accounts are not uncritically accepted by the service users in customer organizations. As these service users encounter the platform’s inconsistent reliability, they express skepticism about the provider’s trustworthiness accounts. Such skepticism is escalated to the occupational gatekeepers, but the need to retain jurisdictional control triggered these gatekeepers to engage in justification work. Indeed, occupational gatekeepers seek to actively guard their jurisdiction from outsiders (Abbott 1988, p.823). Although some of the individual members might have been privately unsure of the trustworthiness accounts, they nevertheless maintained a different public posture to retain jurisdictional control. In that task, these gatekeepers rationalize the continued use of platform despite its reliability issues through repurposing and circulating the trustworthiness accounts inside their company. In due course, the service users’ concerns regarding reliability breakdowns were normalized and rendered as commonplace issues.

Together, trust work and justification work facilitate the co-production of interorganizational trust through normalizing breakdowns as “business-as-usual” events (Vaughan 1997, see also Perrow 1984), and in the process, reorienting user expectations about reliability (Buell, Kim, and Tsay 2017). A normalization model, thus, views interorganizational trust as occurring neither through a passive process of development whereby the trustor deciphers the inner properties of the trustee nor through ascribing a set of attributes upon the trustee, but rather as co-produced – a dynamic accomplishment as opposed to a static attribute – in sociotechnical practice.

The two underlying mechanisms of normalization are (a) objectivizing reliability into metrics, visual indicators, dashboards, and other quantitative representations, and (b) contrasting the old/conventional

dimensions of economic worth (e.g., reliability and consistency) with new dimensions of economic worth (e.g., innovation and disruption) that the provider firm is purportedly bringing to the entrenched industry.

To elaborate, objectivizing happens when customer concerns about reliability (e.g., the legal and pecuniary rights that customers have to access the platform at a particular speed and with limited downtime) are managed through the construction and visual display of quantitative facts. Through objectivizing, reliability is transformed into a set of quantitative facts, and thereafter, categorized as technical issues handled by experts such as software architects and third-party auditors (Smith et al. 2011). In due course, many of these concerns around reliability have come to be viewed as purely technical issues better left to the purview of experts³. In addition, contrasting conventional dimensions of economic worth (e.g., “reliability,” “consistency”) with new dimensions (e.g., “innovation,” “disruption,” “novel functionality”) of economic worth enables the provider to downplay the legitimacy and seriousness of customer concerns. While these new dimensions are projected as “sacred” (Healy 2016, Wherry 2010) in the digital economy, and therefore as something to be embraced – and not resisted – by “forward-looking” customers, the old dimensions of economic worth are said to be embraced by “regressive” customers who are “outdated” and “ossified.” For instance, concerns related to reliability (e.g., service outage, platform downtime) are contrasted against the innovativeness that the platform brings to customers and to the industry at large. By extension, anyone who excessively “cribs and complains” about service outage or downtime is framed as going against the spirit of innovation and, therefore, as a regressive old-guard.

Through these processes of normalization, reliability breakdowns are cumulatively rendered as commonplace, business-as-usual events that customers should tolerate and accept, especially considering the innovation that is brought to the table by the provider organization.

Outcome: The Emergence of Normalized Trust

Having described the processes of normalization, I now turn to theorizing the outcome of these processes: *normalized trust*. Unlike particularized trust, which is based on “concrete personal relations”

³ Even the meaning of trust is now viewed as a technical feature of that platform, which is made up of five properties (authentication, authorization, integrity, privacy, and non-repudiability). As long as these five technical properties are satisfied, the platform is certified as a “trusted platform” (e.g., TRUSTe and SysTrust).

(Granovetter 1985, p.490) between a trustee and a trustor and is a function of the trustee's consistent reliability (Dyer and Chu 2000, Uslaner 2002), normalized trust is produced despite the trustee's inconsistent reliability. Similarly, in contrast to generalized trust, where trust and cooperation between parties are shaped by institutional safeguards that mitigate unreliable behavior (Bachmann and Inkpen 2011, Zucker 1986), normalized trust is a function of the trustor implicitly accepting the criteria set by the trustee on what constitutes reliability within a specific milieu. In other words, normalized trust is generated through reorienting trustor's expectations about the reliability of the trustee's services, accomplished via shaping the beliefs and meanings in an environment whereby "a trustee appears to others as trustworthy" (Leslie 2015, p.28). The analytical gaze, thus, is shifted from the question of "Why did the customers trust the provider organization?" to "How and from whom did the provider organization gain the advantage of being deemed trustworthy" (p.27) i.e., from *underlying characteristics* that engender trust to *reorienting* expectations that shape trustworthiness (cf. Van Maanen, 1991).

Moreover, both particularized and generalized trust are characterized by transforming customer concerns and uncertainties "inherent in interorganizational relationships... into manageable risks" (Bachmann and Inkpen 2011). In the case of particularized trust, customer concerns about reliability breakdowns are transformed into relational risks that are manageable. With generalized trust, these concerns are transformed into legal risks. In the case of normalized trust, however, customer concerns about reliability breakdowns are transformed not into "manageable risks" per se, but rather as commonplace, business-as-usual incidents. Please refer to Table 3 for a comparison of particularized, generalized, and normalized trust.

--- Insert Table 3 here ---

In summary, this concept of normalized trust helps advance our understanding of the co-production of trust between organizations in the wake of reliability breakdowns, and their consequential outcomes. The most significant of these consequences is that through rendering reliability breakdowns as business-as-usual incidents, normalized trust reorients the service users' expectations on what constitutes the meaning and boundary of reliability within a specific milieu. This, in turn, shapes the usage of the platform (and technology, more broadly) inside customer organizations. As more and more transactions flow through

the platform, the service users and business managers within customer organizations are more dependent on the platform to perform their everyday work. As a result, normalized trust impacts what issues these business managers and occupational gatekeepers in customer organizations pay attention to and what issues they tend to justify/rationalize or even ignore. Viewed together, normalized trust undermines the scope and intensity of governance measures taken by managers and occupational gatekeepers to pressurize the platform provider toward delivering a consistently reliable service.

Discussion and Implications

This study advances our understanding of trust production in platform-mediated interorganizational relationships and contributes to the literature on interorganizational trust in the following ways.

First, this research proposes a model of normalization to explicate the processes through which interorganizational trust is co-produced in the face of reliability breakdowns. While prior research has identified the importance of consistent reliability for the development of interorganizational trust (Dyer and Chu 2000, MacDuffie 2011), this research highlights how interorganizational trust is produced despite the inconsistent reliability of trustee's services. Through normalization, reliability breakdowns are rendered as business-as-usual events, and the repair activities needed to “patch” these breakdowns (as opposed to resolving them permanently) are also rendered as ongoing work-in-progress. In this process, the expectations that service users have about the platform’s reliability – including the very meaning and boundary of reliability – are reoriented. A normalization model, therefore, views interorganizational trust as occurring neither solely due to the inner characteristics of the trustee nor entirely due to the attributes that a trustor ascribes upon the trustee, but rather as co-produced in sociotechnical practice.

Second, this research unpacks and analytically characterizes the outcome of the normalization process: *normalized trust*. In contrast to particularized trust and generalized trust theorized in prior research (Schilke et al. 2021), normalized trust is an “emergent social effect” (Leslie 2015, p.31, Heimer 2001). This is accomplished in part through signaling to the trustor that “good faith” efforts are being taken by the trustee to prevent reliability breakdowns from happening as much as possible, while at the same time implicitly conveying the message that some breakdowns will inevitably happen due to the innovative nature of the platform but will be eventually repaired by the provider. Future research could examine the

social-structural conditions needed for the sustenance of normalized trust. It is also important to note that normalized trust has its downsides. For instance, instead of demanding that the platform provider institute robust quality control and platform governance practices to avoid breakdowns, normalized trust reduces customer pressure and vigilance on platform governance practices. In other words, normalized trust structures an environment whereby *precarious reliability becomes the de-facto norm*. Future work could explore the sociotechnical arrangements needed to bring more operational transparency, reliability, and accountability back into the governance of these platforms (Bernstein 2017, Buell et al. 2017)

Third, this study contributes to the emerging stream of work on trust in platforms by shedding light on the backstage dynamics that underlie the production of interorganizational trust in platform-mediated contexts. In describing the practices of trust work and justification work, this study highlights the role of occupational gatekeepers as well as technology such as software code and APIs – and sociotechnical practices, more broadly – in the production of interorganizational trust, something that prior research has overlooked. This is a significant oversight considering the critical gatekeeping function that occupational communities (Van Maanen and Barley 1982) inside organizations play in the adoption and use of new products/services as well as the role that technology itself plays in mediating interorganizational relationships in the digital economy (Orlikowski and Scott 2014). Departing from prior views of technology as conduits, this study views technology as constitutive of trust production (cf. Kipnis 1996). In other words, trust gets materialized in practice, in part through technologies such as software code, APIs, dashboards, and automated scripts/trackers for monitoring customer behavior. Relatedly, this study shows that in platform-mediated contexts, customers can also be a source of reliability breakdowns through their excessive usage of the platform “commons.” Such excessive usage by any single customer creates congestion externalities, which in turn can undermine trust in the platform. This research, therefore, highlights how a distributed customer base can be governed through software code where usage limits are continually monitored and enforced.

Fourth, this study overcomes the “reliance on single-sided data collection” (Graebner, Lumineau, and Kamal 2020, p.365) that is typical of prior research on interorganizational trust. Indeed, “most (if not all) recent trust papers” are based on data collected from “only one side of the partnership” (Graebner et al.,

2020 p.363). By collecting and analyzing “data from both sides of the interorganizational relationship” (Graebner et al. 2020, p.369), this study moves beyond the “single party blind spot” that characterizes much of prior research on interorganizational trust (p.2). In doing so, this study empirically disentangles the distributed processes of trust co-production happening across provider and customer organizations. Relatedly, prior research has largely “overlooked the supply-side rhetoric” (Pollock and Williams 2008) undertaken by provider organizations in the production of interorganizational trust. Part of the reason for this is the reliance upon single-sided data, especially data collected through surveys. Through this study, I show the importance of supply-side trust rhetoric that is constructed and disseminated by the provider organization to generate accounts of trustworthiness about the company and its platform.

Finally, this research highlights the prevalence of trust work in the digital economy. In particular, this study describes the carefully orchestrated trust work performed by platform providers. While prior research has largely focused on B2C platforms such as Apple iOS, eBay, Amazon and Facebook, this research highlights the practices of trust work in B2B platforms. Academic and industry research reports strongly suggest how platform providers aim for the successful “commercialization of trust” (Jeacle and Carter 2011; see also Silverman and Mac 2021 on the recent controversy about the Aspen/Facebook-funded “Weave” project aimed at “building trust through online communities.”) This includes employing columnists, cultural/political commentators, and social scientists in roles such as Trust Researchers and Chief Trust Scientists to “engineer trust” (Abrahao et al. 2017, Bolton et al. 2013, Parigi and Cook 2015) into platforms via “applying theory and knowledge about trust into concrete product recommendations” (Parigi 2017). Likewise, recent research also suggests that justification work is also happening in customer organizations that are adopting and using platform-based services (Corporaal and Lehdonvirta 2018). For instance, sales and engineering departments in firms are increasingly using online labor market platforms such as UpWork and TaskRabbit to directly hire temporary workers to fulfill their project needs. By using these platforms, business managers often bypass the hiring processes set by the company’s HR department. This, in turn, triggers occupational jurisdictional conflicts between HR executives and business managers, prompting these HR executives to officially adopt and justify the use of a single platform for “temp worker hiring” across the company, despite the platform’s multitude issues

(e.g., quality control, reliability). All of these suggest that findings from this study could be analytically generalizable to different settings involving platform-mediated interorganizational relationships.

Limitations

This research is not free of limitations. First, this research is based on a single case study of Sigma and its cloud platform that uses a multi-tenant architecture. In other types of platforms that use a single-tenant architecture, customer concerns around reliability might be different. Although the specific practices to address customer concerns on reliability might vary from one type of platform to another, the broader process of normalization to render these reliability breakdowns as “business-as-usual” events could be analytically generalizable. Future studies could examine the extent to which processes of normalization are prevalent (or not) in other types of platforms. A second limitation of this study is related to a lack of data on how the practices of trust work emerged in the first place. However, given that those practices were ongoing, I did observe them in action during field visits and at platform conferences. I also tried to address this issue by conducting retrospective interviews with Sigma’s senior executives and engineers, as well as by analyzing archival materials on Sigma and its platform.

Conclusion

Platform-based services are increasingly adopted and used by organizational customers. This field study examined the processes of normalization that underlie the co-production of trust in platform-mediated interorganizational relationships, especially in the wake of reliability breakdowns. Through examining the processes of normalization, we can further understand which customer concerns are downplayed, which ones are dealt with, and which dimensions of economic worth (e.g., reliability, consistency, innovation, agility) are valued more by firms in the digital economy. Moreover, as platforms take on a prominent role in mediating interorganizational relationships, examining how and why occupational groups in customer organizations trust and adopt these platforms despite their inconsistent reliability is critical to not only understanding the nature of “trust blind spots” in these relationships, but also toward instituting mechanisms that could overcome such blind spots and bring forth more reliability and accountability into the governance of platforms.

References

- Abbott, A. D. 1988. *The System of the Professions: An Essay on the Division of Expert Labor*: University of Chicago.
- Abrahao, B., Parigi, P., Gupta, A., & Cook, K. S. 2017. Reputation offsets trust judgments based on social biases among Airbnb users. *Proceedings of the National Academy of Sciences* **114**(37), 9848-9853.
- Adler, P. S. 2001. Market, hierarchy, and trust: The knowledge economy and the future of capitalism. *Organization Science* **12**(2), 215-234.
- Bachmann, R. 2001. Trust, power and control in trans-organizational relations. *Organization Studies* **22**(2), 337-365.
- Bachmann, R., A. C. Inkpen. 2011. Understanding institutional-based trust building processes in interorganizational relationships. *Organization Studies* **32**(2) 281–301.
- Bailey, J. P., & Bakos, Y. 1997. An exploratory study of the emerging role of electronic intermediaries. *International Journal of Electronic Commerce* **1**(3), 7-20.
- Bernstein, E. S. 2017. Making transparency transparent: The evolution of observation in management theory. *Academy of Management Annals* **11**(1), 217-266.
- Barrett, M., & Gendron, Y. 2006. WebTrust and the “commercialistic auditor” The unrealized vision of developing auditor trustworthiness in cyberspace. *Accounting, Auditing & Accountability Journal* **19**(5), 631-662.
- Bezemer, C.P., A. Zaidman. 2010. Multi-tenant SaaS applications: maintenance dream or nightmare? *Communications of the ACM*, 88–92.
- Blois, K. J. 1999. Trust in Business to Business Relationships: An Evaluation of Its Status. *Journal of Management Studies* 36(2): 197–215.
- Boltanski, L., & Thévenot, L. 2006. *On Justification: Economies of Worth*. Princeton University Press.
- Bolton, G., Greiner, B., & Ockenfels, A. 2013. Engineering trust: reciprocity in the production of reputation information. *Management Science* **59**(2), 265-285.
- Bradach, J. L., & Eccles, R. G. 1989. Price, authority, and trust: From ideal types to plural forms. *Annual Review of Sociology* 15(1), 97-118.
- Buell, R. W., Kim, T., & Tsay, C. J. 2017. Creating reciprocal value through operational transparency. *Management Science*, 63(6), 1673-1695.
- BVP Cloud Index. 2015. Bessemer Venture Partners’ Cloud Computing Index. Accessed from <http://www.bvp.com/cloud/comps>
- Carruthers, BG. 2009. Trust and credit. In *Whom Can We Trust? How Groups, Networks, and Institutions Make Trust Possible*, edited by Karen S Cook, Margaret Levi. Russell Sage Foundation.
- Cook, K. S., Hardin, R., & Levi, M. 2005. *Cooperation without Trust?*. Russell Sage Foundation.
- Corporaal, G.F. and Lehdonvirta, V. 2017. Platform Sourcing: How Fortune 500 Firms are Adopting Online Freelancing Platforms. Oxford Internet Institute: Oxford
- Charmaz, K. 2006. Constructing grounded theory: A practical guide through qualitative research. *Sage Publications Ltd, London*.
- Child, J., Möllering, G. 2003. Contextual Confidence and Active Trust Development in the Chinese Business Environment. *Organization Science* **14**(1): 69–80.
- Chwe, M. 2001. *Rational ritual: Culture, Coordination, and Common Knowledge*. Princeton University Press.
- Cochran, M., P.D. Witman. 2011. Governance and Service Level Agreement Issues in a Cloud Computing Environment. *Journal of Information Technology Management*, **22** (2) 41-55
- Currall, S. C., Judge, T. A. 1995. Measuring Trust between Organizational Boundary Role Persons. *Organizational Behavior and Human Decision Processes* **64**(2): 151–70.
- Das, T. K., & Teng, B. S. 2001. Trust, control, and risk in strategic alliances: An integrated framework. *Organization studies*, **22**(2), 251-283.
- Dasgupta, P. 1988. Trust as a commodity. In *Trust: Making and breaking of cooperative relations*, edited by Diego Gambetta. New York: Basil Blackwell.
- Delhey, J., Newton, K., & Welzel, C. 2011. How general is trust in “most people”? Solving the radius of trust problem. *American Sociological Review*, **76**(5), 786-807.
- Desmond, M. 2014. Relational ethnography. *Theory and Society* **43**(5), 547-579.

- Dirks, K. T., Ferrin, D. L. 2001. The role of trust in organizational settings. *Organization Science* **12** (3): 450–467.
- Dyer, J. H., & Chu, W. 2000. The determinants of trust in supplier-automaker relationships in the US, Japan and Korea. *Journal of International Business Studies* **31**(2), 259-285.
- Dyer, JH, Chu, W. 2003. The role of trustworthiness in reducing transaction costs and improving performance: Empirical evidence from the United States, Japan, and Korea. *Organization Science* **14**(1): 57–68.
- Edmondson, A. C., & McManus, S. E. 2007. Methodological fit in management field research. *Academy of Management Review* **32**(4), 1246-1264.
- Elsbach, KD. 2004. Managing images of trustworthiness in organizations. Pp. 275-292 in *Trust and distrust in organizations: Dilemmas and approaches*, edited by Roderick M. Kramer and Karen S. Cook. New York: Russell Sage.
- Espeland, W. N., M. L. Stevens. 2008. A sociology of quantification. *European Journal of Sociology* **49**(03) 401–436.
- Fulmer, C. A., Gelfand, M. J. 2012. At What Level (and in Whom) We Trust: Trust across Multiple Organizational Levels. *Journal of Management* **38**(4): 1167–230.
- Gambetta, D. 1988. *Trust: Making and breaking cooperative relations*. New York: Basil Blackwell.
- Gartner. 2018. Gartner Forecasts on Cloud Computing. Gartner Global Research, Stamford, Connecticut.
- Gawer, A. 2014. Bridging differing perspectives on technological platforms: Toward an integrative framework. *Research Policy*, 43(7), 1239-1249.
- Gefen, D., & Pavlou, P. A. 2012. The boundaries of trust and risk: The quadratic moderating role of institutional structures. *Information Systems Research* **23**(3), 940-959.
- Gillespie T. 2010. The politics of “platforms.” *New Media & Society*. **12**(3):347–64
- Gillespie, N., & Dietz, G. 2009. Trust repair after an organization-level failure. *Academy of Management Review* **34**(1), 127-145.
- Graebner, M.E., 2009. Caveat venditor: Trust asymmetries in acquisitions of entrepreneurial firms. *Academy of Management Journal* **52**(3): 435–472.
- Graebner, M. E., Lumineau, F., & Kamal, D. F. 2020. Unrequited: Asymmetry in interorganizational trust. *Strategic Organization*. **18**(2): 362-374.
- Granovetter, M. 1985. Economic action and social structure: The problem of embeddedness. *American journal of sociology*, **91**(3), 481-510.
- Groucutt, P. 2019. Cloud risk, cloud outages and cloud security — human error is the cause. <https://www.information-age.com/cloud-outages-cloud-security-123483558/>
- Gulati, R. 1995. Social structure and alliance formation patterns: A longitudinal analysis. *Administrative science quarterly* **40**(4), 619–652.
- Gulati, R., Nickerson, J. A. 2008. Interorganizational Trust, Governance Choice, and Exchange Performance. *Organization Science* **19**(5): 688–708.
- Gutek, B. A. 1995. *The dynamics of service: Reflections on the changing nature of customer/provider interactions*. Jossey-Bass.
- Hardin, R. 2002. *Trust and trustworthiness*. New York: Russell Sage Foundation.
- Healy, K. 2016. The Moral Economy of Technology. SASE Meeting Panel, Berkeley, CA.
- Heaphy, E. D. 2013. Repairing breaches with rules: Maintaining institutions in the face of everyday disruptions. *Organization Science* **24**(5), 1291-1315.
- Heimer, C.A. 2001. "Solving the problem of trust." Pp. 40-88 in *Trust in society*, edited by Karen S Cook. New York: Russell Sage Foundation.
- Jeacle, I., C. Carter. 2011. In TripAdvisor we trust: Rankings, calculative regimes and abstract systems. *Accounting, Organizations and Society* **36**(4) 293–309.
- Jick, T. D. 1979. Mixing qualitative and quantitative methods: Triangulation in action. *Administrative science quarterly* **24**(4), 602-611.
- Jones, G. R., George, J. M. 1998 The experience and evolution of trust: Implications for cooperation and teamwork. *Academy of Management Review*, **23**: 531–546.
- Kipnis, D. 1996. Trust and technology. In R. M. Kramer & T. R. Tyler (Eds.), *Trust in organizations: Frontiers of theory and research* (pp. 39-50). Thousand Oaks, CA: Sage.
- Kollock, P. 1994. The emergence of exchange structures: An experimental study of uncertainty, commitment,

- and trust. *American Journal of Sociology*, **100**(2) 313-345.
- Kollock, P. 1999. The production of trust in online markets. *Advances in Group Processes* **16**(1), 99-123.
- Kramer, R. M., & Tyler, T. R. 1996. *Trust in organizations: Frontiers of theory and research*. Thousand Oaks, CA: Sage.
- Kuwabara K, Vogt S, Watabe M, Komiya A. 2014. Trust, cohesion, and cooperation after early versus late trust violations in two-person exchange: the role of generalized trust in the United States and Japan. *Social Psychology Quarterly* **77**: 344-60
- Langley, A. N. N., Smallman, C., Tsoukas, H., & Van de Ven, A. H. 2013. Process studies of change in organization and management: Unveiling temporality, activity, and flow. *Academy of management journal*, **56**(1), 1-13.
- Lepore, J. 2014. The disruption machine. *The New Yorker*, 23, 30-6.
- Leslie, C, A. 2015. Trustworthiness and Jurisdiction in the Stanford Financial Group Fraud. Unpublished Dissertation, University of Michigan.
- Lessig, L. 1999. *Code: and Other Laws of Cyberspace*, Basic Books, New York, NY.
- Lewis, J. D., A. Weigert. 1985. Trust as a social reality. *Social forces* **63**(4) 967-985.
- Lui, SS, Ngo, H-Y. 2004. The role of trust and contractual safeguards on cooperation in non-equity alliances. *Journal of Management* **30**(4): 471-485.
- Malhotra, D., & Lumineau, F. 2011. Trust and collaboration in the aftermath of conflict: The effects of contract structure. *Academy of Management Journal*, **54**(5), 981-998.
- MacDuffie, J. P. 2011. Interorganizational Trust and the Dynamics of Distrust. *Journal of International Business Studies* **42**(1): 35-47.
- Marshall, D. 2013. Cloud storage provider Nirvanix is closing its doors. Accessed from <https://www.infoworld.com/article/2612299/cloud-storage-provider-nirvanix-is-closing-its-doors.html>
- Mayer, R. C., J. H. Davis, F. D. Schoorman. 1995. An integrative model of organizational trust. *Academy of management review* **20**(3) 709-734.
- McEvily, B, Zaheer, A, Kamal, DK. 2017. Mutual and exclusive: Dyadic sources of trust in interorganizational exchange. *Organization Science* **28**(1): 74-92.
- Mizrachi, N., Drori, I., & Anspach, R. R. 2007. Repertoires of trust: The practice of trust in a multinational organization amid political conflict. *American Sociological Review*, **72**(1), 143-165.
- Nannestad, P. 2008. What have we learned about generalized trust, if anything? *Annual Review of Political Science* **11**, 413-436.
- NIST 2011. NIST Definition of Cloud Computing. Accessed from <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>
- NorthBridge Report. 2017. Future of Cloud Computing Report. Accessed from <http://futureofcloud.drupalgardens.com/>
- Parigi, P. 2017. The AirBnB – Stanford Project. <https://web.stanford.edu/~pparigi/projects.html>
- Parigi, P., & Cook, K. 2015. Trust and relationships in the sharing economy. *Contexts: Understanding People in Their Social Worlds* **14**(1), 18-19
- Palmer, J. W., Bailey, J. P., & Faraj, S. 2000. The role of intermediaries in the development of trust on the WWW: The use and prominence of trusted third parties and privacy statements. *Journal of Computer-Mediated Communication* **5**(3), 532.
- Perrow, C. 1984. Normal accidents: Living with high risk technologies-Updated edition. *Princeton university press*, New Jersey.
- Pavlou, P. A. 2002. Institution-based trust in interorganizational exchange relationships: The role of online B2B marketplaces on trust formation. *The Journal of Strategic Information Systems* **11**(3) 215-243.
- Paxton, P. 2007. Association memberships and generalized trust: A multilevel model across 31 countries. *Social Forces* **86**(1), 47-76.
- Paxton, P., & Glanville, J. L. 2015. Is trust rigid or malleable? A laboratory experiment. *Social Psychology Quarterly* **78**(2), 194-204.
- Perrone, V, Zaheer, A, McEvily, B. 2003. Free to be trusted? Organizational constraints on trust in boundary spanners. *Organization Science* **14**(4): 422-439.
- Pollock, N., R. Williams. 2008. *Software and organisations: The biography of the enterprise-wide system or how SAP conquered the world*. Routledge.

- Ranger, S. 2018. Cloud computing: Here's how much a huge outage could cost you. Accessed from <https://www.zdnet.com/article/cloud-computing-heres-how-much-a-huge-outage-could-cost-you/>
- Raphael, J.R. 2019. The 10 worst cloud outages (and what we can learn from them). <https://www.infoworld.com/article/2622201/the-10-worst-cloud-outages--and-what-we-can-learn-from-them-.html>
- Ring, P. S., Van De Ven, A. H. 1994. Developmental Processes of Cooperative Interorganizational Relationships. *Academy of Management Review* **19**(1): 90–118.
- Sako, M., & Helper, S. 1998. Determinants of trust in supplier relations: Evidence from the automotive industry in Japan and United States. *Journal of Economic Behavior & Organization* **34**(3), 387–417.
- Schilke, O., & Cook, K. S. 2013. A cross-level process theory of trust development in interorganizational relationships. *Strategic Organization* **11**(3), 281–303.
- Schilke O, Cook KS. 2015. Sources of alliance partner trustworthiness: Integrating calculative and relational perspectives. *Strategic Management Journal* **36**(2), 276–97
- Schilke O, Reimann M, Cook KS. 2013. Effect of relationship experience on trust recovery following a breach. *Proceedings of the National Academy of Sciences* **110**(38), 15236–41
- Schilke, O., Reimann, M., & Cook, K. S. 2021. Trust in Social Relations. *Annual Review of Sociology*, 1–46
- Schilke O, Wiedenfels G, Brettel M, Zucker LG. 2017. Interorganizational trust production contingent on product and performance uncertainty. *Socio-Economic Review* **15**(2), 307–30
- Selznick, P. 1957. *Leadership in Administration*. Berkeley: University of California Press.
- Schumann, J. H., Wangenheim, F. V., Stringfellow, A., Yang, Z., Praxmarer, S., Jimenez, F. R., ... & Komor, M. 2010. Drivers of trust in relational service exchange: understanding the importance of cross-cultural differences. *Journal of Service Research* **13**(4), 453–468.
- Scott, S. V., & Walsham, G. 2005. Reconceptualizing and managing reputation risk in the knowledge economy: Toward reputable action. *Organization Science*, **16**(3), 308–322.
- Shapiro, S.P., 1987. The social control of impersonal trust. *American Journal of Sociology* **93**, 623–658.
- Silverman, C & Mac, R. 2021. NYT Columnist David Brooks Resigns From Nonprofit After More Evidence Of Conflicts Emerges. BuzzFeedNews. <https://www.buzzfeednews.com/article/craigsilverman/times-columnist-david-brooks-told-people-to-join-nextdoor>
- Sonenshein, S., Herzenstein, M., Dholakia, U. M. 2011. How accounts shape lending decisions through fostering perceived trustworthiness. *Organizational Behavior and Human Decision Processes*, **115**: 69–84.
- Sztompka, P. 1999. *Trust: A Sociological Theory*. Cambridge University Press.
- Turner V.W. 1986. Dewey, Dilthey, and drama: An essay in the anthropology of experience. In Turner VW and Bruner EM (eds) *The Anthropology of Experience*. Champaign, IL: University of Illinois Press.
- Van Hoorn, A. 2014. Trust radius versus trust level: Radius of trust as a distinct trust construct. *American Sociological Review*, **79**(6), 1256–1259.
- Van de Ven, A. H., & Poole, M. S. 1990. Methods for studying innovation development in the Minnesota Innovation Research Program. *Organization Science* **1**(3), 313–335.
- Van Maanen, J. 1991. The Smile Factory. In P. Frost et al. (eds) *Reframing Organizational Culture*, pp. 58–76. Newbury Park, CA: Sage.
- Vaughan, D. 1997. *The Challenger launch decision: Risky technology, culture, and deviance at NASA*. University of Chicago Press, Chicago, IL.
- Uslaner, E. M. 2002. *The moral foundations of trust*. Cambridge University Press.
- Wherry, F. F. 2010. The Sacred and the Profane in the Marketplace. In *Handbook of the Sociology of Morality* (pp. 147–161). Springer, New York, NY.
- Willcocks, L.P., Venters, W Whitley, E.A. 2012. Cloud and the future of business: From costs to innovation: Accenture, In association with The Outsourcing Unit London School of Economics and Political Science, London, UK.
- Zaheer, A., B. McEvily, V. Perrone. 1998. Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance. *Organization science* **9**(2) 141–159.
- Zucker, L. G. 1986. Production of trust: Institutional sources of economic structure, 1840–1920. *Research in organizational behavior*. **8**, 53–111.

Table 1. Data Sources

Type	Number	Description
PHASE 1		
Platform provider (Sigma)		
Semi-structured Interviews	36 interviews	In-depth interviews with senior executives, product and technology managers, account managers, operations managers, sales executives, pre-sales engineers, service support executives, and developers.
Observations	350 hours (approximately)	Attended five conferences hosted by the Sigma; Participated in a number of developer-group and user-group meetings.
Archival materials	850 documents (approximately)	Press reports, company press reports, analyst reports, popular press articles, external audit reports, independent accountant reports, privacy and security statements, policy documents, master subscription agreements and contracts.
Conference Videos	83 videos	Demos, Talks, Keynote presentations, Customer Q&A discussions, Webinars.
Customer discussion forums	120 threads and 2500+ messages (approximately)	Discussions and complaints around a variety of concerns such as performance, security, privacy, latency, and more.
Customers of Sigma (In-depth case study of 2 customer organizations)		
<u>Energy Corp</u>		
Semi-structured interviews	28 interviews	Senior executives (CEO, CIO etc.), Senior IT leaders, Project Managers, Software developers, Implementation specialists, Business managers, and Users.
Archival materials	45 documents	Project plans, Contracts and Service Agreements, Governance structure, Status reports, Implementation report, Power point slides, Technology-related issue log.
<u>CommHousing</u>		
Semi-structured Interviews	26 interviews	Senior executives (CEO, CIO etc.), Senior IT leaders, Infrastructure managers, Project Managers, Software developers, Business managers, and Users.
Observations	30 hours (approximately)	Project meetings, Vendor interactions, and Technology usage.
Archival materials	23 documents	Project plans, Contracts and Service Agreements, Governance structure, Meeting notes, Implementation report, Power point slides, Issue log.
<u>Other customers of Sigma</u>		
Semi-structured Interviews	24 interviews, 5 companies (multiple rounds)	Senior executives, managers, IT-related decision makers from firms in various industries
Customers of other Enterprise Cloud Computing Platforms		
Semi-structured interviews	32 interviews, 6 companies (multiple rounds)	Senior executives, managers, IT-related decision makers from firms in various industries
Total	146 interviews + 370 hours of observation + 918 documents + 83 videos + 2500 forum messages	

Type	Number	Description
PHASE 2		
Platform provider (Sigma)		
Semi-structured Interviews	10 interviews	Follow-up interviews with senior executives, technology managers, customer engineering team, trust officers, and customer support executives.
Observations	~15 hours	Sigma headquarters meetings; Attended a customer conference hosted by the Sigma; Participated in two user-group meetings.
Customers of Sigma		
<u>Energy Corp</u>		
Semi-structured interviews	14 interviews	CIO, Senior IT executives, IT Project Managers, Marketing Managers, Sales managers, and End Users.
Observations	~22 hours	IT department meeting, SigmaCloud-related project meetings, End user technology usage.
<u>CommHousing</u>		
Semi-structured Interviews	16 interviews	CIO, Senior IT executives, IT Project Managers, Marketing Managers, Sales managers, Developers, and End Users.
Observations	~25 hours	IT department meeting, SigmaCloud-related project meetings, End user technology usage.
Total	40 interviews + 62 hours of observations	

Table 2. Customer Concerns about Reliability

Concerns about Reliability	Description	Illustrative Quotes
Access (e.g., outage, speed)	How reliably can customers access the various functionalities of the platform without any downtime or delays?	“The issue with cloud is speed. You know, salespeople are impatient. I need to push them to even work with Excel, which they feel is slow. So if SigmaCloud is slow and if it takes more than 30 seconds to enter data in a field, then they will not use it.” [Interview Transcript]
Safeguards	Whether there are any service level agreements pertaining to platform reliability? What are the terms and penalties for decreased reliability?	“We are here at the mid-west, thousands of miles away... Unlike other services we use, we’ve hardly met those [Sigma] folks, so that is a concern for us...And they don’t do SLAs either, so if something goes wrong, what happens then? Who is going to be held accountable for it when there are no SLAs? Frankly, we are quite worried about this and we have been raising this issue with Sigma” [Interview Transcript]
Security	Can one customer access the data and applications of another customer? Whether the platform is protected against external hackers?	“We keep reading about the hacking attempts at cloud services, which frankly worries me ... And also the multi-hour downtime due to some power issues two weeks back... We heard there was even some data loss due to that... We want the data to be backed-up every minute we add more data. We can’t function otherwise” [Interview Transcript]

Table 3. Generalized Trust, Particularized Trust, and Normalized Trust: A Comparison

Characteristics	Particularized Trust	Generalized Trust	Normalized Trust
Foundational elements	Function of the trustee’s consistent reliability, and is based on concrete personal relations between a trustee and a trustor.	Function of established institutional safeguards such as the legal environment, contracts/SLA enforceability, regulations, and industry/professional associations.	Emerges despite the trustee’s inconsistent reliability. Normalized trust is a function of the trustor implicitly accepting the criteria set by the trustee on what constitutes reliability.
Production of Trust	Concrete, personal relations play a central role in the production of trust. Through such personal relations, the trustee’s reliability is assessed by the trustor.	Institutional safeguards, including the legal regime, provide the enabling environment for trust to flourish. These institutional safeguards provide the guard rails needed to limit unreliable behavior and mitigate uncertainties.	Co-production via the processes of normalization. Reliability breakdowns are rendered as business-as-usual events. Underlying mechanisms are <i>objectivizing reliability</i> and <i>contrasting old- and new- dimensions of economic worth</i> .
Customer Concerns	Concerns about reliability breakdowns are transformed into relational risks.	Concerns about reliability breakdowns are transformed into legal risks.	Concerns about reliability breakdowns are normalized into commonplace, business-as-usual incidents.

Figure 1. Co-Production of Interorganizational Trust in the Wake of Reliability Breakdowns: Towards a Model of Normalization

APPENDIX

Appendix A1: Data Collection – Archival Materials

Following archival methods, I collected publicly available data about the company (Sigma), the platform (SigmaCloud), and the industry (enterprise cloud computing). For data on the industry, I used several keywords ("cloud computing," "enterprise cloud computing," "on-demand" etc.) to search different databases (ABI Inform, EBSCO Business Source Premier, Lexis-Nexis Academic) for press articles related to enterprise cloud computing platforms. I also gathered reports on enterprise cloud computing from industry analyst firms such as Gartner, Forrester, IBIS World, International Data Corporation (IDC), and S&P's NetAdvantage. I subscribed to news feeds from websites (such as Businesscloudnews.com, Cloudtimes.org, and Cloudcomputing-news.net) and newsletters that tracked industry events related to cloud computing. I looked for information that helped me understand the emergence of enterprise cloud computing, the different players within the industry, and how incumbents (such as the packaged software providers) reacted to enterprise cloud computing. I then filtered this data to narrow down on a corpus of articles, essays, reports, and press releases (from different stakeholders such as industry analysts, packaged software providers, and customers) that mentioned concerns related to "trust" in enterprise cloud computing platforms. Specifically, I collected materials to understand the various category of reliability concerns expressed about enterprise cloud computing by various parties (e.g., industry analysts, technology journalists, packaged software providers, CIOs, and business users) that were detrimental to the development of trust. I also tracked the responses offered by platform providers.

For data about Sigma, I used company-related keywords to search the aforementioned databases for relevant press articles. I also collected numerous documents about Sigma over time (e.g., press releases, annual reports, analyst reports, employee blog posts, online videos, technology-related release notes). I collected different versions of artifacts at Sigma related to reliability and the challenges of building trust with customers. These artifacts include external audit reports, privacy and security statements, policy documents, advertisement campaigns, and third-party secured seals (e.g., Verisign, TRUSTe). These

materials about Sigma and the SigmaCloud platform helped me construct a timeline about the reliability-related concerns that Sigma faced from customers (as well as from prospects, industry analysts, and technology journalists). While some of these concerns were reported in news articles and industry watchdog websites, others were reported and discussed in the Sigma Online Discussion Forum for customers. I systematically parsed the Sigma online discussion forum using a specific set of keywords (e.g., "service disruption," "outage," "downtime," "system down," "performance issues," "unable to login," "fail," "error," "bug," "trust," "privacy," "reliability," "security," etc.) to track the specific reliability breakdowns and the customer concerns reported over time at a fine-granular level. I also recorded Sigma's response to the specific concerns reported by customers. These materials helped me to create a chronology of events relating to Sigma (Van de Ven and Poole 1990), which in turn enabled me to chronicle the SigmaCloud platform's reliability breakdowns and the associated concerns that customers reported.

Appendix A2: Data Collection – Additional Information

To examine the concerns about reliability breakdowns expressed by customers, especially the end-users, I signed up for a SigmaCRM "free trial" account, which allowed me to attend Sigma-related events (such as SigmaCloud customer group meetings, user group meetings, administrator, and developer group meetings) as an observer. These events highlighted various issues, tensions, and questions pertaining to the reliability of SigmaCloud — some widely known and others simmering beneath the surface.

At the two customer organizations, I took detailed field notes about the concerns expressed by end-users to business managers, how business managers escalated those concerns to senior IT executives (such as the VP of IT and the CIO) during quarterly meetings, and how the senior IT executives responded to those concerns. When I was unable to attend some of these meetings, I obtained the meeting minutes and used the issues discussed during the meeting to structure my follow-up interviews. Across these two companies, I conducted formal interviews (28 at Energy Corp and 26 at CommHousing) with senior-level executives, IT Directors, and budgetary decision-makers as well as with mid-level IT project managers and IT developers involved in the deployment of the platform. I collated field notes from my

real-time observations at customer sites and compared it with the transcripts from retrospective interviews to examine both the immediate reactions (to platform-related reliability issues such as outages, downtime, response time, etc.) expressed by actors at different levels of the organizational hierarchy as well as the various forms of justification that got circulated within the customer organizations. In total, during Phase 1, I conducted 146 interviews, performed around 370+ hours of observation, and collected 918 documents and 2500+ forum messages. All formal interviews lasted between 45 and 100 minutes, with an average of 55 minutes per interview. Most of the interviews recorded and transcribed. During phase II of data collection, I conducted an additional 40 interviews (10 interviews with Sigma executives and middle managers, 14 interviews with senior IT executives, IT managers, and end-users of EnergyCorp, and 16 interviews with senior executives, IT managers, and end-users of CommHousing) and did ~62 hours of observations at Sigma headquarters and at the customer sites to examine the extent to which reliability concerns about Sigma and its platform were normalized, and with what consequential outcomes.

Appendix B: Protocol for Semi-Structured Interviews

Platform Provider

1. Could you describe your role in Sigma? How long have you been with Sigma?
2. Can you talk for a few minutes about your daily work schedule? What are the different tasks and activities you do?
3. How do you learn about what your customer expectations are?
4. How often do you communicate with individual customers?
5. How do you support your customers with respect to the issues they face is using SigmaCloud and/or integrating SigmaCloud with their in-house products?
6. How do you manage the relationship with customers? What are some of the challenges you have faced?
7. Why is trust emphasized repeatedly in Sigma's conference presentations and marketing materials?
8. What are some of the challenges that you have observed in building trust with customers?
9. What does your team specifically do with respect to developing trust with customers?
10. What do you mean by "Trust as Sigma's Core Value"? Can you elaborate?
11. Can you elaborate on what does Sigma mean when it refers to "trust engineering" and "customer engineering"?

12. What is the role of the Chief Trust Officer (and his team) in Sigma?
13. Can you recollect an instance where trust broke down between Sigma and one of its customers?
 - a. Why and how did it happen?
 - b. How did the customer react?
 - c. What did Sigma do?
14. Is there anyone else that you think I should talk to as part of this study?

Customer Organizations

1. How long have you been with <customer organization name>?
2. Could you describe your role in <customer organization name>?
3. What products were your organization using before the transition to SigmaCloud?
4. What was the motivation to move from <existing product> to SigmaCloud?
 - a. What goals were guiding your organization to adopt SigmaCloud?
 - b. Who is pushing the adoption agenda, business (i.e., Sales team) or IT?
 - c. What is the funding model being used to cover the adoption of SigmaCloud? Is this different than the traditional IT funding model used in your organization? If so, why?
 - d. Who is responsible for the decisions pertaining to the adoption (e.g., business case) and ongoing use (e.g., service-level monitoring and vendor management) of SigmaCloud
5. Do you use SigmaCloud? If yes, how often do you use it? If not, why?
6. Have you faced any challenges in using SigmaCloud? If so, can you elaborate upon them?
7. What are some of the concerns or issues you have with Sigma as a platform provider?
8. To whom do you typically go to when you face such challenges?
9. Can you recollect what happened during the recent SigmaCloud service outage?
 - a. What was your reaction?
 - b. Was your work affected? If so, how?
 - c. How did your team react?
10. Do you Trust Sigma as a vendor? If so, why? If not, why not?
11. How supportive is Sigma when responding to your queries and service requests?
12. Where do you keep the "master client list"? And why?
13. What are your continuing concerns about the use of SigmaCloud?
14. Is there anyone else that you think I should talk to as part of this study

Appendix C. Reliability Breakdowns in SigmaCloud

#	Month/Year	Category	Description
1	July 2012	Access	Multi-hour service outage due to data center power failure
2	July 2012	Access	Reduced transaction speed
3	August 2012	Safeguards	Customer escalations about the lack of SLAs for platform uptime
4	September 2012	Security	Denial-of-service attack
5	October 2012	Security	API vulnerability and data exposure
6	November 2012	Safeguards	Media coverage about the lack of SLAs for SigmaCloud
7	November 2012	Access	Minor service outage
8	January 2013	Safeguards	Prominent industry analyst coverage about the lack of SLAs
9	March 2013	Security	Worm attack
10	April 2013	Access	Performance degradation
11	June 2013	Access	Performance degradation
12	July 2013	Access	Multi-day service outage due to database failure
13	September 2013	Security	Sigma themed phishing attack
14	October 2013	Security	Malware targeting Sigma users
15	November 2013	Safeguards	Customer pushback to establish SLAs for platform uptime
16	November 2013	Access	Multi-hour service outage due to undisclosed reasons
17	January 2014	Safeguards	Tech journalist's report about the lack of SLAs
18	March 2014	Access	Performance degradation
19	March 2014	Access	Multi-hour service outage due to file integrity issues
20	April 2014	Access	Performance degradation
21	May 2014	Security	Remote code execution incident
22	May 2014	Access	Performance degradation
23	May 2014	Safeguards	Customer pushback to establish SLAs for platform uptime
24	June 2014	Security	Denial-of-service attack
25	June 2014	Access	Performance degradation
26	July 2014	Access	Multi-day service outage due to database and file storage failure
27	September 2014	Access	Performance degradation
28	October 2014	Access	Minor service outage
29	November 2014	Security	Remote code execution incident
30	June 2018	Access	Performance degradation
31	August 2018	Security	API vulnerability

Appendix D. Practices of Trust Work – Additional Evidence

Practices	Quotes
<i>Governing through Code</i>	<p>"Because the initial technical concept was a globally shared service, we architected the application rigorously to that. Anything below the line is the shared resource which we maintain and you as a customer cannot access. Any customizations that you perform are not done in that space. That means we can upgrade things down in that space any way we want to without breaking anything you've done. Nothing down there is yours. Everything above the line we handle as metadata, which looks and behaves the way you want it to when you are using it, but leaves your customization completely free from what we do in the basement. We guarantee that certain aspects across that boundary will not be disrupted, so you are free to keep using your customizations no matter what we do in the basement." (Interview, VP of Platform Architecture, Sigma)</p> <p>"... in a cloud-based environment infrastructure upgrades as well as applications upgrades are seamless... When it comes to upgrading, the multi-tenancy model means all users have the exact same version and infrastructure. So our developers don't have to worry about the particular effect of upgraded software on any particular customer. We can have a lean environment, focus the customer gets upgrades that are seamless, and they don't have to do anything for them. It is the Sigma competitive advantage over hosted outsourcing and with respect to enterprise software vendors." (Interview, Director of Software Engineering, Sigma)</p>
<i>Creating and Circulating Trust Rhetoric</i>	<p>"... Once you get clear about what you really want, then the second thing is what is really important about it? What are the values that are going to guide you? In our world, the most important value at Sigma today is Trust. Our customers -- we are stewards of their data... you [customers] have to have a Trust relationship with us or you are not going to provide us that business, so Trust is the most important thing." (Conference presentation, CEO, Sigma)</p> <p>"Something that I'm very proud of with Sigma on what we've created is -- yes, we created a new technology model, yes, we created a new financial revenue model of recurring revenue... But what's most important is not all of that. It's the connective tissue we have with our customers. It means so much. We talk about customer success within Sigma, and it's part of who we are. We live and breathe it. And it's part of what makes us successful... And the customer actually expects it now. They don't care how big the company is. They don't care how many customers we have. They expect to be treated as the most important customer. And it's a trust revolution. It's a customer revolution... Everyone needs an application, and it's running in the cloud, and it's trusted. [Sigma's CEO during an industry analyst event]</p> <p>"Ok, I am going to be quite frank with you. [Vendor Name], they have SLAs. [Another vendor name], they also do. But seriously, do you really think they care about their customers? It [SLA] doesn't mean a thing to them, really. They are like a factory and you folks are just an ID to them. Compared to them, we are quite new and small. And we care about you, we REALLY do, and we are desperately trying to change how things are done in the enterprise software world, which is so stuck in the past." [Senior Executive of Sigma, Conference Q&A video]</p> <p>"Well, first and foremost, absolutely, it was trust... And even if we did go down, even if there was a glitch, and we took a customer down for whatever period of time, the fact that we were there, it was all-hands on deck, and they didn't have to worry about it. They knew we were going to come back up and running... Right? [Trust] number one." (Interview, VP of Customer Engineering, Sigma)</p>

Practices	Quotes
<i>Establishing Trust Indicators</i>	<p>"Trust starts with transparency. That's why Sigma displays real-time information on system performance and security on the Trust site. This site provides live data on system performance, alerts for current and recent phishing and malware attempts, and tips on best security practices for your organization." (Conference presentation, CEO, Sigma)</p> <p>"We have obtained a number of these third-party audit reports and Trust seals. We have put those audit reports on our corporate website as well as on our Trust site for anyone to see. We have also undergone some formal certifications on various aspects of our platform – on how secure and reliable it is, performance aspects and so on. And we have undergone all of these voluntarily, not because some customer asked us to. That's the difference between us and many of the other cloud vendors. We are more voluntary and transparent." (Interview, EVP, Sigma)</p> <p>"I don't know how many customers these competitors have, because they won't say. They won't say how many net subscribers they have... they're making these broad generalizations without the facts. Where are the numbers? And specific to this point, where's the quality of service? ... Of course, we don't know any of these things, because there's no transparency. There is no Trust site for any of these competitors. There are no performance benchmarks; it's all a kind of strange hearsay." (Conference presentation, CEO, Sigma)</p>
<i>Convening an Occupational Community</i>	<p>"We have a lot of customers. And even more number of end-users. As a cloud vendor, it is not really possible for us to know what each customer or each end-user wants. We have only very little face-to-face interactions. But there needs to be some way for us to figure out what the customer wants so that we can prioritize internally. We don't have infinite resources, so we need to exactly know where to move the product forward, what additional feature or what new toolkit that we need to provide to the customers to make their job easy. That's where ... our approach toward mining customer usage is extremely insightful... In addition to that, we organize a lot of events. CloudConf is the largest of them all... That's where we bring our customers together, put them inside the sprawling [conference center name] and make them chat with each other. And then, magic happens" (Interview, VP of Customer Engineering, Sigma)</p> <p>"We believe a lot in events. And so I remember, for, in the 18 months period, we had what we called the [anonymized], which was basically global event – where we had event after event after event... we talked about technology but also about business models and things like that. We did a lot of these events... And also a lot, a lot of, developer marketing... We'd invite IT professionals... We'd invite technical people and business people and marketing people... The idea is to create a customer community... And not just a customer community, but also sub-communities within them like an administrator community, a developer community, a user community... We try hard to create a sense of community anchored around our platform. And let me tell you, it costs us quite a bit [to organize these conferences], but it also pays us back a pretty good dividend [Presentation, Co-founder of Sigma]</p> <p>"I don't know how many customers these [competitor companies] have because they won't say... They won't say how many net subscribers they have... But we do, because we know our customers... Our Customer Community, we bring them here every year, to CloudConf, what an amazing event it is. Amazing, amazing, don't you think [looking at the audience]?... I don't do much at CloudConf. It is a busy time for sure, but more than us [i.e., Sigma employees] we make the customers busy by ensuring that they bump into each other and learn from each other. That's what CloudConf is all about" (Presentation, CEO of Sigma)</p>

Appendix E. Email Template Provided by Sigma to Employees working in Customer Organizations

CloudConf Conference Proposal

To:

From:

Subject: Conference Proposal Approval

I'm writing to ask for approval to attend Sigma's annual conference, on [date] and [location]. The entire community of Sigma's experts will be on hand to learn and share best practices, hands-on training, new innovations and a lot more.

CloudConf is in its tenth year, and post-event surveys of past attendees have shown substantially increased return on their Sigma investment, which you can see here ([URL link to ROI Calculator](#)). Many of the customers who have experienced these successes will be featured as guest speakers.

In particular, I'd like to focus on finding solutions or best practices that could benefit these projects:

- [add project or initiative]
- [add project or initiative]
- [add project or initiative]

In addition to 650+ breakout sessions with Sigma.com customer and partner speakers, the conference offers the chance to problem solve with Sigma.com employees and technology partners. The Sigma Expo, which features Sigma solutions plus 300+ partners and 1,000+ integrated solutions, is an ideal place to pick up new ideas to drive more productivity from our implementation and maximize your Sigma investment.

Here's an approximate breakdown of conference costs:

Airfare:	\$ xxx
Transportation (between airport and hotel):	\$ 90
Hotel: (3 nights at \$200)	\$ 600
Meals: (3 days at \$50)	\$ 150
Registration Fee:	<u>\$ xxx</u> [check for current price]
Total:	\$ X,XXX

I'm currently working on ways to reduce expenses, including hotel discounts, ride sharing, and meals with vendors. ***Also, the earlier I can register, the cheaper it will be.*** I'll also submit a post-conference report that will include an executive summary, major takeaways, tips, and a set of recommendations to maximize our current investments in Sigma. I can also share relevant information with key personnel throughout the company.

Thank you for considering this request. I look forward to your reply.

Regards,

Appendix F. Justification Work in Customer Organizations – Additional Evidence

Themes	Quotes
<i>Service users experiencing the platform's inconsistent reliability, leading to initial skepticism about the platform providers' accounts</i>	<p>“When I’m meeting a prospect who is almost ready to sign on the dotted line... and as I’m trying to set him up through our portal that uses SigmaCRM... and at that precise moment, I’m unable to login and the system hangs up. Or it’s super slow. Not because of some WiFi issue or anything, but it’s just slow and takes forever to load. I’m sitting there, awkwardly apologizing to him. It’s embarrassing, really. It just sucks... I can’t close a deal if shit like this keeps happening. I mean, it’s already hard to get a major client in our geography, but these kinds of things make it more difficult for us” [Business development executive, Sales department, EnergyCorp]</p> <p>“I’m in-charge of campaign management... and run a lot of campaigns. If I mess up the campaign rollout or even the launch date by a little bit, then the whole campaign becomes ineffective. Because campaigns work only if they are perfectly designed and executed at a precise moment. If you miss that moment, you may very well not run that campaign... So when I am trying to launch a campaign at a specific date, and I can’t do that because the platform [SigmaCloud] we use is down, then I just get cranky. It’s so annoying, and I keep raising this to [marketing manager], so let’s see what she will do about it” [Marketing executive, CommHousing]</p>
<i>Business managers (e.g., sales managers) exploring alternative options, triggering jurisdictional contestation</i>	<p>“My guys [sales reps] escalated these issues [service outage, access speed] to me a few months back, and I did drop a note to him [VP of IT]... I also mentioned it to him at our meeting, and he said he will talk to [CIO] about it, but I didn’t hear back anything... And all this while, my guys were still upset and they were complaining to me that they can’t get stuff done fast enough with all these issues and close the damn deal. It was creating a lot of friction internally, and also between us [sales] and IT... At one point, I realized that it is really affecting our work and hindering our sales process, so I asked [Director of Sales] to do the thinking and give me some [alternative] options [for SigmaCloud]” [VP of Sales, EnergyCorp]</p> <p>“And if we don’t do it, the marketing department will bypass IT and subscribe to some cloud-based platform using their credit card. It is just OpEx for them, and not CapEx that requires approval from us... So we want to be at the top of our game to avoid such “Shadow IT” stuff” [Interview transcript; Senior IT executive from CommHousing, emphasis added]</p>
<i>Occupational gatekeepers (e.g., IT managers) rationalizing the continued use of the platform despite its reliability issues</i>	<p>“SigmaCloud provides a trusted source of information for [our] operations. We propose using SigmaCloud...to implement the foundation of the integrated operations platform. Because SigmaCloud is a true multi-tenant platform, we will be able to leverage part of their entire infrastructure specifically for our corporate needs. We will benefit from the hundreds of millions of dollars of investment that Sigma has made for infrastructure improvements and efficiencies for quality, performance and security. SigmaCloud is also secure, with SAS70, ISO 270001 and SysTrust certifications.” [Position Paper prepared by the CIO of CommHousing, and presented to the Board of Directors]</p> <p>“CommHousing is not an IT or software company... and the IT department’s role is to deliver the most useful, usable IT solutions as cost-effectively... In the past, the approach has been to custom-build solutions to serve our operations... all this creating additional integration challenges... Moving to Cloud and Sigma helps us to avoid these challenges.” [Interview, Senior IT executive, CommHousing]</p>