Knowledge protection in firms: A conceptual framework and evidence from HP Labs

July 20, 2018

Abstract

This paper proposes a simple framework to examine organizational methods of knowledge protection. The framework highlights a basic trade-off between improving decision-making and innovation through communication and mitigating security risks by imposing restrictions on communication flows. The trade-off is mediated by factors such as the sensitivity of information, the degree to which employees can be trusted to handle sensitive information appropriately, and firms' investments in legal protection mechanisms. Evidence from HP Labs supports the basic predictions of the model, in particular the importance of employee trustworthiness and internalized codes of behavior in promoting open communication. Our interviews also suggest a potential conflict between two of the most important appropriability mechanisms: secrecy and lead-time advantage.

Keywords: Secrecy, information security, organization design, trust, innovation, appropriability mechanisms.

JEL Classification: L14, L23, M10, M14.

Apple's obsession for secrecy is legendary. Big projects are divided into small teams and employees are told not to fraternize with members of other groups, lest someone gain access to the bigger picture (New York Times, July 10, 2008).[1]

1 Introduction

What advantages do firms, as a nexus of contracts, have over markets, as a nexus of firms? A widespread view, usually associated with the knowledge-based view of the firm, is that firms have superior capabilities in managing knowledge assets (Kogut and Zander, 1992; Grant, 1996; Nahapiet and Ghoshal, 1998). One particular capability that firms may have developed is the ability to protect valuable information (Liebeskind, 1996; Rajan and Zingales, 2001). Client lists, customer information, non-patented technical

[1] See `http://bits.blogs.nytimes.com/2008/07/10/apple-imposes-gag-rule` (accessed 26/08/2011).

knowledge are examples of information that, if leaked, may compromise a firm's source of competitive advantage and reputation. To protect this information, firms employ a variety of methods including the use of secure IT infrastructure, the screening and monitoring of employees, restrictions to communication flows, and requirements that employees and contractors sign nondisclosure agreements.

In this paper we explore a fundamental trade-off. On the one hand, firms often encourage interactions and knowledge sharing among employees to improve decision-making and foster innovation. On the other hand, firms also sometimes restrict employees' access to information to prevent information leakage (Liebeskind, 1996; Hannah, 2005). We propose a simple framework that highlights a number of factors that are likely to influence whether communication flows should be restricted or kept open. These include the sensitivity of information, employee trustworthiness, and various legal instruments such as patents and non-disclosure agreements that organizations can use to mitigate the risk of information leakage.

Then we examine how HP Labs—the research unit of Hewlett-Packard Company (HP)—internally protects its knowledge in practice. Previous research on the management of R&D labs (e.g., Tushman and Katz, 1980; Katz and Tushman, 1981; Chesbrough, 2002; Von Zedtwitz, 2004) and science-based businesses (e.g., Gambardella, 1995; Pisano, 2006) has paid scant attention to organizational (as opposed to patent-based) methods of knowledge protection. Exceptions are Zhao (2006) and Quan and Chesbrough (2010), who examine how the geographical segmentation of the R&D process can be used to protect intellectual property (IP) rights. Our evidence complements this limited body of work by providing a more comprehensive analysis of organizational knowledge protection methods.

Supporting the idea that information items are heterogeneous in security requirements, we find that, while managers and researchers at HP Labs all emphasize the importance of open communication in facilitating their work, sometimes restrictions are imposed on the communication of certain kinds of sensitive information. Auditing who has access to what information is also an important element of HP Lab's knowledge protection policy. For instance, as part of a software development project, special software tags were used to provide a clearer audit trail for the distribution within HP Labs of sensitive source code. Geographical separation can hinder interactions among partners, especially when other restrictions to communication are also present. In one case, difficulties occurred because of rules related to the encryption of electronic messages, which could not easily be overcome via informal communication.

Consistent with our framework, we also find that open communication at HP Labs is supported by internalized codes of behavior. HP Labs delegates many decisions concerning security to employees and trusts them, by and large, to behave appropriately. Training and mentoring are important tools for establishing the appropriate norms and standards of behavior regarding security. One reason why internalization of norms may be emphasized is that many types of communication may be very difficult if not impossible to monitor or audit. Relational contracts also appear to be important (Baker, Gibbons and Murphy, 2002; Gibbons and Henderson, 2012; Baldwin and Henkel, 2015). HP Labs researchers understand that failure to behave appropriately regarding security will be detrimental to their career prospects, not just at HP but at similar organizations as well.

Two unexpected findings emerged from our interviews. The first was about the type of information that was most likely to be protected. Within a leading research lab, we expected technical information to be very closely guarded. We found instead that protecting client confidentiality was always deemed to be of the utmost importance. While technical information was sometimes classified as sensitive, in general other leading technology firms were not expected to engage in espionage activities or stimulate a market for stolen information. HP Labs employees were much more strongly concerned about protecting client information and confidentiality. This may partly reflect the needs of HP Labs' customers, which include government agencies and financial institutions.

A second unexpected finding related to the reasons for preferring open communication modes to more secure/restricted communication modes. We expected restrictions to communication to potentially reduce the quality of decision-making or hinder creativity. By contrast, HP Labs employees emphasized more frequently the issue of delays. Security protocols were sometimes a problem because they tended to slow down new product development. This finding has interesting implications for managers. The innovation literature finds that secrecy and lead-time advantage are two of the most important methods that firms can use to appropriate the returns from their R&D efforts (Cohen, Nelson and Walsh, 2000; Arundel, 2001; Thomä and Bizer, 2013). Our evidence indicates that there may be a conflict between these two appropriability mechanisms. Security protocols help protect intellectual property, but they may also introduce delays, thus compromising lead-time advantage.

The remainder of this paper is organized as follows. Section 2 reviews existing research on knowledge

protection in organizations. Section 3 provides a simple framework to understand when organizations should restrict access to information, and when instead should keep it open. Section 4 describes and analyzes our interview data. Section 5 discusses our findings and highlights potential avenues for future research.

2 Related literature

The literature on knowledge protection in firms is scattered through economics, management and engineering. In an important paper, Liebeskind (1996) argues that firms possess specific capabilities that allow them to protect their knowledge from expropriation and imitation more effectively than market contracting. Protecting knowledge is difficult because knowledge resides in the heads of individuals and is thus inherently mobile. Moreover, the creation of new knowledge frequently requires interaction. As a result, organizations involved in innovative activities may be concerned that several people get access to valuable or sensitive information.

Liebeskind (1996, 1997) describes a number of methods that firms can use to protect their knowledge. These methods include employee participation in share ownership schemes, the design of long-term compensation packages, and the compartmentalization of organizational knowledge. By sharing ownership, firms can provide powerful incentives that can induce key individuals to commit to a particular organization. Deferred rewards also reduce employee mobility by imposing exit costs on employees. Examples of deferred rewards include staggering promotions over time, deferred stock options and pension plans with delayed vesting. Contractual clauses such as the exclusivity of the employment relationship and 'non-compete' and confidentiality clauses also tend to reduce the value of employment elsewhere, and therefore tend to make employees more loyal to their organization.

Quite distinct from these methods are features of job design and communication structures that tend to compartmentalize organizational knowledge. Hannah (2005) classifies restrictions to communication flows into two groups: *access restrictions*—rules that restrict employees' rights to access certain areas of an organization or documents—and *handling procedures*—rules that specify what employees can and cannot do with sensitive information once they gain access to it. Examples of communication restrictions include rules that require an employee to "conduct her work in a particular place within its premises (and

not enter other areas of its premises), and that the employee communicate with, and report to, particular other employees (and not communicate with other specific employees)" (Liebeskind, 1996: 98-99).

A concern with open communication in firms is that it may facilitate unwanted knowledge spillovers or spin-offs. For instance, Bhide (2000) finds that the vast majority of the founders of 1989 Inc. 500 fastest growing private companies adapted ideas they had encountered in their previous jobs. Moreover, about ninety percent of entrepreneurs in high-tech and professional service industries were previously employed in established firms in the same sector (Burton, Sorensen and Beckman, 2002; Gompers, Lerner and Scharfstein, 2005). Knowledge protection issues are especially prominent when evaluating outsourcing opportunities to countries like China, where the potential for information leakage and competition from local firms is high (Newhouse, 2007).

A number of formal models examine organizational strategies for knowledge protection. Demski, Lewis, Yao and Yildirim (1999) find that market forces are typically insufficient alone to induce firms to protect customer information. However, firms may be able to signal their intention to protect customer information, for instance by providing specific client contracts or by erecting internal security systems. Rønde (2001) examines how restricting information sharing between employees affects firm profits. In his model, information sharing improves operational efficiency but makes information leakage more likely. He focuses on how this trade-off is affected by the degree of competition in the market. Fosfuri and Rønde (2004) study how firms' incentives to cluster together are affected by stronger trade secrets laws. Rajan and Zingales (2001) focus on hierarchy and staggered firm growth as methods to protect a firm's source of competitive advantage. Baldwin and Henkel (2015) compare different knowledge protection mechanisms (doing nothing, licensing, and relational contracts), and evaluate how these options are affected by the modularity of the system and the degree of employee trustworthiness.

An extensive empirical literature examines how firms appropriate the returns from their R&D activities (Cohen et al., 2000; Arundel, 2001; de Faria and Sofka, 2010; Gallié and Legros, 2012; Thomä and Bizer, 2013; Sofka et al., 2014; Belenzon and Patacconi, 2014). This literature distinguishes between "formal" or "legal" appropriability mechanisms such as patenting, trademarks and copyrights, and "informal" appropriability mechanisms such as secrecy, lead-time advantage, and complementary assets. A common finding is that, except in a few sectors such as chemicals and pharmaceuticals, patenting is often *not*

the most important appropriability mechanism. Other mechanisms, most notably secrecy (especially for process innovation) and lead-time advantage, are more effective. For instance, based on a 1994 survey of 1478 R&D labs in the U.S. manufacturing sector, Cohen et al. (2000: 1) find that, among appropriability mechanisms, "patents tend to be the least emphasized by firms in the majority of manufacturing industries, and secrecy and lead time tend to be emphasized most heavily". Using data from the 1993 European Community Innovation Survey, Arundel (2001) finds that secrecy is rated as more valuable than patents by a higher percentage of firms in all size classes. Thomä and Bizer (2013) show that, among innovative small firms in Germany that choose to protect their innovations at all, informal protection mechanisms (lead time, secrecy, complexity of design) tend to be the most heavily emphasized.

While this literature underscores the importance of secrecy as an appropriability mechanism, very little is known about how secrecy is implemented in practice. As mentioned above, Zhao (2006) and Quan and Chesbrough (2010) are notable exceptions. These papers show that multinational companies counter weak IP rights protection in host countries by geographically segmenting the R&D process. Labs in countries with weak IP rights protection tend to perform tasks whose full value emerges only when combined with other internal resources, thus mitigating the risk of knowledge spillovers. Png also finds that stronger legal protection of trade secrets is associated with greater R&D spending (Png, 2017a) and, conditional on R&D spending, a decline in patenting especially in complex product industries (Png, 2017b).

3 Conceptual framework

Building on the body of research discussed above, this section proposes a simple framework to inform our analysis of knowledge protection practices at HP Labs. The framework is summarized in Figure 1. In the online appendix, we also provide a mathematical model where some of the key ideas discussed here are formalized.

FIGURE 1 ABOUT HERE

Our analysis is motivated by a chasm in the innovation literature. On the one hand, communication, information sharing and interactions among employees are widely regarded as essential features of innov-

ative organizations. Open communication is believed to improve decision-making, facilitate coordination and foster creativity and innovation inside organizations (Brown and Duguid, 1991; Rønde, 2001). On the other hand, when employees have access to a substantial portion of a firm's knowledge, leakage of information is more likely to occur (Liebeskind, 1996; Rønde, 2001). Some employees, for instance, may leave the firm and set up competing firms using their former employer's trade secrets. A solution could be compartmentalizing a firm's knowledge and restricting communication flows. Secrecy has consistently been found a very effective mechanisms to appropriate the returns from R&D (e.g., Cohen et al., 2000; Arundel, 2001).

Google provides a nice illustration of the risks that wide access to corporate information can bring about. According to former Google executives Eric Schmidt and Jonathan Rosenberg, the default mode at Google is "to share virtually everything. The company's intranet, Moma, includes information on just about every upcoming product, for example [...] We trust our employees with all sorts of vital information" (Schmidt and Rosenberg, 2015: 176-177). Yet, not all Google's employees may deserved that level of trust. In February 2017, Waymo, the self-driving-car division that spun out of Google in December 2016, filed a lawsuit against Uber alleging that Google's former employee Anthony Levandowski stole more than 14,000 documents (9.7 gigabytes of data) from Google. Just weeks after Levandowski downloaded this documents from Google's servers, Levandowski left the company to start Otto, a self-driving-truck company, which six months later was acquired by Uber for an estimated 680 million dollars. Waymo claims that Uber and Levandowski used the stolen information to jump-start Uber's self-driving car program.[2]

In this paper we argue that organizations must strike a balance between sharing information internally, which improves decision-making and innovation, and restricting communication flows, which reduces information leakage. Thus, in practice organizations will put systems and procedures in place so as to balance the benefits of open communication against the risks of information leakage.

In striking this balance, organizations must take several factors into account. One key factor is the nature of information. Information that is sensitive and imposes very large costs if leaked will be handled securely by the organization. Information that is less sensitive and is deemed critical for decision-making

[2] See, e.g., https://en.wikipedia.org/wiki/Otto_(company) and the references therein for more information. Accessed 20/10/2017.

and new product development will be shared more widely. The idea that information is heterogeneous in terms of security risk is captured by the common practice of classifying documents based on their sensitivity, for instance "confidential" or "private". Studies have found that knowledge tends to be most closely guarded when it is highly tacit and core (Norman, 2002), and that external information leakage is especially detrimental when knowledge is related to radical innovations (Li, Eden, Hitt and Ireland, 2008; Ritala, Husted, Olander and Michailova, 2018).

A second factor that can influence how freely organizations will share information internally is the degree to which they trust their employees to handle sensitive information appropriately. As highlighted in Schmidt and Rosenberg's quote above, Google trusts its employees with all sorts of vital information. Google has experienced leaks, but does its best to track down the source of leaks and, when the leaks come from Googlers, those Googlers get fired (Schmidt and Rosenberg, 2015: 177). Indeed, severe penalties in case of misconduct may support trust of the calculative type because violations of trust will tend not to benefit the untrustworthy partner. An extensive body of research supports the notion that trusting relationships are conducive to information sharing (e.g., Uzzi, 1996, 1997; Dirks and Ferrin, 2001; Dyer and Chu, 2003), for instance in the context of knowledge-intensive work such as research and development (Norman, 2002; Levin and Cross, 2004).

Third, organizations may be more willing to share information internally if they invest significant resources in legal protection mechanisms such as patents, employee non-compete clauses and non-disclosure agreements. Patents, by establishing temporary monopoly rights over the use of inventions, mitigate the risks of imitation and expropriation of intellectual property. Non-compete clauses reduce the risk that an employee, upon termination or resignation, may start a competing business or begin working for a competitor. The concern is that workers may gain undue competitive advantage from their exposure to their former employer's confidential information (e.g., client lists, trade secrets). Non-disclosure agreements are contracts where parties agree not to disclose information covered by the agreement. Arguably, the more organizations invest in protecting their knowledge through legal mechanisms, the less they will have to rely on "informal" appropriability mechanisms such as restricting communication flows and compartmentalizing information.

To summarize, we propose that restrictions to internal communication flows are less likely to be imposed when: (i) information is important for decision-making and innovation and the cost of information leakage is low (that is, the information is not sensitive); (ii) firms trust their employees to handle sensitive information appropriately; (iii) firms invest resources in legal protection mechanisms such as patents, employee non-compete clauses and non-disclosure agreements.

Often information is shared not just internally among firm employees, but also externally with business partners, suppliers and customers. A large literature examines the "paradox of openness", whereby firms collaborate with external partners to innovate and commercialize their inventions, but at the same time must also prevent harmful knowledge spillovers and capture sufficient returns from innovation (e.g., Hamel, 1991; Laursen and Salter, 2014; Ritala, Olander, Michailova and Husted, 2015; Arora, Belenzon and Patacconi, 2017).

Compared to information sharing within the firm, external information sharing is regarded to be more prone to hazards. This is especially true when external partners are competitors or may become one after absorbing the firm's distinctive competencies (Khanna, Gulati and Nohria, 1998). The ability of a focal firm to control how information is used across the organizational boundary may also be limited. Compared to markets, firms are believed to have superior capabilities in managing knowledge assets and protecting information (Kogut and Zander, 1992; Grant, 1996; Liebeskind, 1996; Nahapiet and Ghoshal, 1998). These capabilities derive from firms' abilities to compartmentalize information and incentivize good security practices, for instance through deferred compensation or ownership shares (Liebeskind, 1996). They may also derive from socialization mechanisms that engender trust among employees and allow them to internalize social norms (Ouchi, 1980; Bowles, 1998; Adler, 2001; Ramalingam and Rauh, 2010). Thus, the context in which information sharing occurs (whether within the firm or across organizations) can influence the cost-benefit analysis of information restrictions not only directly by affecting for instance the magnitude of security risks, but also indirectly by affecting moderators such as the trustworthiness of the information recipient.

If agency problems are typically more severe across firms than within, and firms are able to handle information more securely than markets, then we would expect restrictions to communication flows to be more common across organizational boundaries than within organizational boundaries.

4 Knowledge protection at HP Labs

In this section, we examine knowledge protection strategies in a specific but important context—the large corporate lab. Our evidence comes from HP Labs. HP Labs has two major research facilities, one in Palo Alto in the U.S. and one in Bristol in the U.K. From its inception in 1966, HP Labs's stated objectives have been "to carry on basic and applied research studies, to assist the operating divisions in finding solutions to their technical problems, and, if necessary, to develop prototype products in new and promising fields" (WR Hewlett, quoted from House and Price, 2009: 105). Important discoveries attributable to HP Labs include the pocket calculator, the RISC architecture for computer chips, cordless pointing devices, and the 64 bit Itanium chipsets developed jointly with Intel. The objectives of HP Labs have not changed materially in over four decades.[3]

The normal operating procedure for a development phase at HP Labs is to conduct a research project, often in collaboration with universities. The research project may result in tools or solutions with commercial potential being developed. If this happens, the tools or solutions are then normally shipped to the relevant business unit within HP for further development and possibly commercialization, or a new unit is spun out with external partners such as other firms or a government department (this is particularly the case for defence related activities).

We chose HP Labs for this study for a number of reasons. First, HP Labs is one of the largest private research labs in the world. Issues related to knowledge protection are likely to be particularly important for such a concern. Moreover, the lab has operated successfully for more than half a century, suggesting that its knowledge protection practices are of the highest standard.

Second, HP Labs is a very interesting organization in its own right. There is significant variation in how the research function in major technology companies is carried out,[4] but most would agree that

[3] On October 6, 2014, HP initiated a plan to split the PC and printers business from its enterprise products and services business resulting in two publicly traded companies: HP Inc. and Hewlett Packard Enterprise. This does not effect our analysis as the component of HP Labs we have spoken to has solely been in the enterprise services division for many years and there was little impact of this restructuring on the individuals involved.

[4] Apple, for example, has tended to embed small research groups directly into the product teams for various business units (Apple 2010 Quarterly Report). By contrast, HP and IBM have established large standalone research units charged with conducting basic and applied research and developing integrated proofs of concept packaged for existing and/or new product units (HP Labs Annual Report 2010 and IBM Research, Annual Report 2010). Somewhere between these models is the Microsoft approach, where basic research is conducted by a standalone research group and applied research is integrated into the various business units (Microsoft Research 2010).

the major research labs are an important part of the mix. Research suggests that many leading firms in developed countries are withdrawing from science (Arora, Belenzon and Patacconi, 2018). Hence, there is a need to better understand the strengths and weaknesses of large research labs, for instance with respect to knowledge protection.

Lastly, and most importantly for research purposes, we had very good access to key personnel in HP Labs. For studies focusing on security issues, access to key personnel is often a major roadblock. The present case study developed during the conduct of a research project on information security in a cloud environment. The authors suggested, and HP Labs agreed, to conduct interviews to establish a baseline for a cloud ecosystem, as a collaborative development tool within and across organizations. The trust and knowledge built up by the research team over several years of interactions with personnel in HP Labs was fundamental both for carrying out the study and for the interpretation of the data.[5]

4.1 Methodology and data collection

We began our investigation by gathering extensive secondary data and performing documentary analysis of the available resources on HP and HP Labs, including the HP Labs library and archive at Bristol, in addition we looked extensively at similar organizations, from multiple archival sources. These include: (i) books, published case studies and articles on HP and similar organizations, with special focus on the management of innovation and large labs (e.g., House and Price, 2009; Lashinsky, 2012; Gertner, 2012; Schmidt and Rosenberg, 2015). We also consulted (ii) HP and HP Labs websites, and other online sources, through extensive Google searches (e.g., Annual Reports, HP Labs publications, news articles). In particular, we read and in many cases discussed with the authors several HP Labs working papers on issues related to information security, innovation and privacy management. HP Labs staff produce large numbers of internal and external publications; from these, we selected several (about 30) that we most relevant for our study. Attention was paid to ensure the authenticity, credibility, representativeness and meaning of the documentary sources (Bryman, 2004). Attention was also directed towards consciously recognizing that in re-reading text it may become interpreted within the current context and thus reconstructed outside the original meaning of the author (Hodder, 2003).

[5] Yin (2011) identifies gatekeepers who provide access and facilitation for qualitative research. In our study the lab director performed this role and allowed us access to a cross section of roles within the lab.

In addition to archival sources, we conducted (iii) semi-structured recorded interviews with representative participants from the various levels of the hierarchy in HP Labs, as suggested by Denis, Lamothe and Langley (2001). We had access to over 60 engineers, researchers and commercial managers based on a single research site. For availability and confidentiality reasons, we focused on five members of staff. Specifically, we interviewed the lab director (LD), a senior research manager (SRM), a research engineer who works on multiple projects (RE1), a second more senior research engineer with expertise in security policy (RE2), and an external liaison officer with another business unit in Hewlett Packard (EL).[6] These five members of HP Labs were selected to be broadly representative of the complete organizational structure of the individual lab site examined in this study. Indeed, the sample covers all levels of staff from frontline engineers to the most senior lab manager, just below board level. They are themselves experts in the information technology aspects of security and intimately involved in key HP Labs' business processes. Appendix 1 provides a brief description of their roles.

Each interview lasted for approximately one and one-half hours with some variation.[7] We recorded approximately 50 minutes of each interview. The remaining time was used before the interview to discuss the question sheet and after the recorded interview to engage in further discussion. For the post-interview session, notes were taken. In one case (EL), we asked that part of this discussion also be recorded as we felt that the discussion contained valuable ancillary information. The interviews were then transcribed and merged with the set of extra notes taken during the unrecorded part of the conversation. The objective was to provide the participants with maximum control over their information while collecting as much data as possible. In total this resulted in just under 10 hours of interviews, about 5 hours of recordings, and about 45 pages of transcripts (including some extra notes from the interviewer). We have anonymized parts of the interviews to ensure that specific individuals cannot be identified from the data presented.[8]

Interviews were conducted 'on-site' over a period of two days and were structured as follows. A question sheet was circulated to the participants two weeks prior to the interview dates. The first three

[6] The external liaison officer (EL) acts as an intermediary between the research unit and the commercial part of the business. The EL provides insight to the research team regarding current customer requirements and feeds back to the research unit on the response of customers to prototypes of tools and solutions tested by them.

[7] Two interviews lasted more than two hours.

[8] For each quote from the interviews, we identify the quote by the designation of the interviewee who made the comment in square brackets. Within the text we follow the standard convention and add missing subjects, pronouns and conjunctives, in square brackets. Significant grammatical or logical errors are tagged with the sic erat scriptum [sic] identifier.

interviews were conducted on day one and the second two interviews were conducted on day two. Despite the fact that interviews were conducted on-site, each was conducted in private and interviewees were explicitly given autonomy to answer questions as they preferred. All interviews were conducted by the principal investigator of the research team.

We started our interviews by requesting participants to describe their position within HP Labs. This provided some background for the following discussion. The subsequent questions focused on identifying methods for knowledge protection and the costs and benefits associated with them. We were also interested in understanding whether the use of knowledge protection methods was contingent on the identity of the parties involved in knowledge exchange (i.e., collaboration with other HP Labs' employees, or other HP units, or external organizations). The complete set of questions is provided in Appendix 2. Data coding and analysis concerning procedures for knowledge sharing and protection, both within and between organizational boundaries, were manually conducted (see Appendix 3).

Following Strauss (1987) and Corbin and Strauss (2015), we analyzed the data using a 'process' coding approach. This is a cyclical approach where the general meaning of the discussions conducted within the semi-structured interviews is initially categorized (initiation), structured around specific themes (focus) and then reviewed and encoded (axial coding). All the material was reviewed to check that we had grasped what was significant to the interviewee (respondent validation; see also Charmaz, 2014). Subsequently, items were reduced into a more manageable form of themes or 'sets' and triangulated via inter-researcher verification and with interviewees (Gioia, Corley and Hamilton, 2013).

To further enhance the validity of our findings, we include in the discussion below extensive verbatim descriptions of the participants' views, to reduce the impact of our own biases. We confirmed through internal written records that the views of our participants regarding security practices were more widely shared within HP Labs. Descriptions of security practices in other leading U.S. technology firms (e.g., Lashinsky, 2012; Schmidt and Rosenberg, 2015) suggest that our findings also have some external validity, at least in a developed country context. Nevertheless, given that our study includes only a single site and a small number of interviews, concerns about validity remain justified and further work is certainly needed.

4.2 Information flows and security risk

As mentioned above, HP Labs's main role is in conducting basic and applied research that develops new technology and supports business processes. Since knowledge generation is the lab's main objective, a policy of openness and collaboration within the organization is considered to be the norm. For instance, the Lab Director noted that:

> "HP Labs consciously decided several years ago to try to keep as much information in the open between employees inside [the] lab so that you could get that kind of cross pollination [and] fertilization of ideas from different groups. At one level we operated [a] fairly open internet where a lot of people have access to quite sensitive information and the decision was always [that] the upside in doing that outweighs the risk associated with it." [LD]

Nevertheless, all the people we interviewed also confirmed that there is information which they do not share or share only on a need-to-know basis. Most restrictions involve shared information from partner organizations or customers. In particular, information shared by public bodies is tightly controlled.[9] Ongoing business activities with large clients rely on trust in security and data-handling procedures. Leakages of information have a real two-fold impact. First, there are often built-in penalties for the exposure of sensitive information (including criminal liability in certain cases). Second, and arguably most importantly, is the potential loss of future business, both from the client whose information was exposed and from other prospective customers. Since the size of contracts is frequently very large, such a loss can be a significant percentage of total turnover.

It is felt that competitors might be interested in information on HP business strategy that could be inferred from the research lines undertaken at HP Labs. Hence, information related to ongoing commercial projects and strategy is protected even within HP Labs. However, basic research output from HP Labs is, in the main, freely disclosed internally and in certain circumstances published in the public domain. In practice, such information may only be of use to similar research organizations which share similar norms

[9] For instance, the LD noted that: "If we have information from our business units that is sensitive then it is not widely circulated across the organization. That is more controlled. Similarly, if we have information from partners this is tightly controlled. If we are working with this type of information, which is intranet based we will be working in quite a guarded even in the immediate organization. [...] The only places where we would be really tight, is our stuff related to the government. This would not make it onto the intranet. We would keep that sort of material of the intranet, keep it separately on machines that are air gapped. But this is a very small amount of material and the philosophy is that you would destroy it as quickly as you can. This avoids having copies that could be embarrassing to anyone at any stage. We try and keep it open, but if we have an intern we try and share enough that they know what is going on and can be a part of HP." [LD]

of ethical practice with HP Labs and are unlikely to use this information to gain undue advantage in the research arena.[10]

Information provided by HP Labs to other business units within HP is not routinely restricted. To the extent that such information is controlled, it is often because of a concern that new innovations may be revealed prematurely. Disclosing capabilities or products that are still under development at HP Labs runs the risk of creating inappropriate expectations on the part of other HP divisions or customers. Hence, some restriction on information transmission within HP may benefit to all parties.

4.3 Knowledge protection methods

Our interviews highlighted a number of methods that HP Labs staff use to protect sensitive or valuable information. These methods are discussed below.

Internalized codes of behavior. Decisions concerning the sharing of information are often left to the individual. Hence, it is important that employees have a clear understanding of what is expected of them from a security standpoint.

The LD emphasized that lab employees are loyal to the company and have good to excellent knowledge of how to deal with sensitive information. The research staff are top field experts who are aware of security concerns and want to protect intellectual property in an appropriate manner. HP assists the efforts of HP staff members by providing a structured way to deal with sensitive information. For example, the EL made the following observation:

> "Within HP there is a standard of business conduct which is very clear on what information should be shared and again that comes back down to the data classification: whether it is HP private, HP confidential, or information that can be made public." [EL]

Standards of business conduct and cultural norms are transmitted explicitly via training sessions that provide a set of structured principles regarding knowledge protection. These principles are also built into employee contracts and reinforced through continuous mentoring of more junior staff. Lab employees tended to emphasize (a) discretion and (b) the use of experience within the research group, in deciding on

[10] It is also important to note that most of the research conducted at HPL would require substantial technical infrastructure to make it economically viable. This infrastructure is found in only a few businesses, and a secondary market for illicitly obtained information does not exist.

how information should be distributed amongst researchers. Every person whom we interviewed stressed that cultural norms and internalized codes of behavior are the primary means for ensuring good security practice.

Auditing. The LD also pointed out that legal liability is always needed as a "back-stop" remedy when informal measures for securing cooperation in knowledge protection are not sufficient. Auditing is an important element of such a strategy. HP Labs uses both passive and active auditing procedures. An open sharing of information is viewed as good as long as there is an audit trail to verify who has looked at the information.

The SRM discussed an example of software development that provides an illustration of the importance that HP Labs places on auditing. Software development involves the writing and testing of source code, which is the underlying code used to generate the software. The software is typically distributed to end users only as binary files ready for running on a computer. Unlike the binary files, someone who possesses the source code can potentially understand the program and reproduce or modify the software. Hence, the source code represents particularly sensitive information in the context of a software development project.

To permit development and testing of the software, the source code must be shared among individuals working on the project. As part of the security for the project discussed by the SRM, identifying tags were placed directly into the copies of the source code provided to these individuals. Hence, any version of the source code found to have been leaked could be traced back to the small number of copies that were originally distributed. This procedure allowed for the construction of an audit trail that (a) incentivized good security handling of important information and (b) provided a means to monitor the dissemination of critically sensitive information.

In the experience of several of the individuals with whom we spoke, this method of controlling information was found to be effective. However, it was not without cost. The tagging procedure delayed the distribution of the source code and increased the time it took for the project to be completed. Thus, as discussed in our model, there was a trade-off between security and operational performance. Interestingly, however, the cost of heightened security was not so much in terms of lack of coordination, but rather in

terms of longer delays.

Auditing and geographical separation. The impact of auditing on the ability to transmit information across geographical areas was addressed by many of the researchers we interviewed. For example, the EL argued that:

> "Auditing implies that certain bits of information are not transmitted. Here physical separation matters a bit. If you are not on premise, you cannot rely on informal communication, which is hard to monitor. Working off-premise create[s] coordination problems." [EL]

One role for informal communication appears to be that of facilitating access to legitimate communication channels. One researcher who is restricted from obtaining certain information can nevertheless informally request the information from a second researcher. The second researcher can then outline a properly audited mechanism for sharing this information. Thus "off the record comms are valuable" (EL quote) because they permit researchers to efficiently obtain information.

Geographical distance also matters because organizations working in different countries may have different security protocols and communications sent outside an organization may be subject to additional restrictions. The coordination problems that arose as a result of a collaboration with researchers working in a developing country were discussed by RE1 and RE2. Some of the problems occurred because of rules in the developing country which required electronic messages to be encrypted. On the other hand, because of internal auditing rules, the norm at HP Labs is to send and receive electronic messages as clear text. These differences in procedures caused delays and additional work for HP Labs employees.

Other methods. The individuals we interviewed stressed the importance of cultural norms, training, and auditing as means by which HP Labs engages in knowledge protection. However, other methods also play a role. For instance, there are special formal procedures which must be followed to obtain access to certain business sensitive documents. Non-disclosure clauses are also included in contracts and are considered to be a credible threat to be used in the unusual case of a severe or persistent breach of trust. For example, the SRM notes:

> "I am always typically guarded with any information I share and I always ensure that there is a binding contract between the parties ... So I know when I'm in a meeting that there is a contract in place to protect the information I share." [SRM]

The well-being of staff was also mentioned as being very much in line with security goals. The possible loss of an attractive job can serve as a powerful deterrent. Moreover, several people noted that an individual responsible for a serious breach of security could put at risk not only his or her job at HP Labs but also the ability to get a job in other similar companies.

4.4 Knowledge sharing across organizational boundaries

The starting point of our analysis was the presumption that firms possess capabilities that allow them to handle information more efficiently and more securely than markets (Kogut and Zander, 1992; Grant,1996; Liebeskind, 1996). So far, our discussion has focused mainly on how such capabilities manifest themselves within HP Labs. However, some questions in our interviews were also directed at understanding whether there are differences in how information is handled internally (inside HP Labs, or between HP Labs and other HP units) as opposed to across organizational boundaries (between HP Labs and external organizations).

Consistent with theoretical accounts, our interviews suggest that information flows much more openly inside HP Labs (and HP more generally) than between HP Labs and external organizations. An important reason appears to be the availability inside HP of informal communication channels, which are sustained by relationships of trust. For instance, the RE2 noted that:

> "I don't have that problem so much within HP because within HP you are always able to go to another individual and say 'I am going to tell you something that you absolutely need to know otherwise you are going to make that mistake and you cannot pass the information on or spread it around'. I would always do that if I thought that the company was going to do something really bad and I was in a position to prevent that happening then I would always do that. I would go to the person and say 'I am telling you something I really shouldn't tell you, I am only telling you in order to prevent something bad happening'. On the other hand, when you are dealing with people outside there is information which you can never reveal no matter how badly that will impact on that person." [RE2]

RE2 further explained that:

> "you have to develop this relationship of trust, whereby if something is going wrong you tell your manager because ultimately that is the line which you cannot cross. [...] If something is going wrong you have to tell the guy. It is only when things are going right that you can hide the information." [RE2]

The interview with the external liaison officer was particularly useful to highlight differences in communication patterns between HP Labs and other business units within HP. The EL was affiliated with HP Labs prior to being deployed to a business unit referred to as 'services'. Services originated from a research project in HP Labs, and EL acted there as an expert and as a liaison to coordinate between the unit and HP Labs on related research projects still in development. He noted that:

> "When I was in Labs it was very much an open environment where people freely shared information and it was assumed you were part of a community. [...] But in services most people work from home and there is a real breakdown in communication where typically everything happens over a phone. So it is somewhat blurred regarding how sparse the information flows are between people. And, the managers will hold the information centrally and feed it out as appropriate." [EL]

This quote supports the point made above that distance contributes to compartmentalizing information. In addition, EL suggests that managers often engage in a gatekeeping role, for they tend to relay information on a need-to-know basis only. More generally, however, EL stressed that all employees in contact with customers typically play a gatekeeping role. This is because firms that are clients of HP often do not want their data to be used in the creation of new products. So the consultants undertaking IT servicing contracts have to gate-keep in how they feed information back to the research unit. In addition, HP staff may be unwilling to prematurely reveal capabilities or products that are not fully developed. Thus, interestingly, restrictions on informational flows are often imposed in both directions:

> "As a consultant and working with clients they have requested that, that information does not get fed back into HP and equally HP running a research project were requesting that the research information was not fed to the client." [EL]

5 Discussion and concluding remarks

The goal of this paper is to examine how organizations internally protect their knowledge. The analysis emphasizes a basic trade-off between letting employees communicate freely with each other, which improves decision-making but increases the risk of information leakage, and restricting communication flows, which worsen decision-making but mitigates security risk. We argue that this trade-off is mediated by several factors, such as the sensitivity of information, employee trustworthiness and investments in legal protection mechanisms.

Our case study of HP Labs provides suggestive evidence in support of the proposed framework. The framework postulates that tasks are heterogeneous in terms of security risk and their importance for decision-making. Hence, even within the same organization, some tasks or information items may be subject to more stringent security requirements than others. We found that protecting client confidentiality (especially when the client is a government agency) is always perceived to be of the utmost importance, typically much more so than protecting technical information. Thus, there seems to be significant variation across knowledge items in security costs.

Prima facie, our findings appear to contradict Demski et al.'s (1999) result that market forces alone are typically insufficient to induce firms to protect customer information. However, their result is premised on the absence of effective contractual and reputational solutions to the problem of information leakage. By contrast, the individuals we interviewed pointed out that there are often significant built-in penalties for the exposure of sensitive information (including criminal liability in certain cases). But more important than legal remedies is arguably the risk of losing future business, both from the client whose information was exposed and from other prospective customers. Thus, our evidence suggests that, in some situations at least, market forces can go a long way towards mitigating the problem of customer information leakage.

Our framework highlights two factors that tend to reduce the likelihood and cost of information leakage: employee trustworthiness and investments in legal protection mechanisms. Both factors were noted in our interviews. Concerning legal remedies, non-disclosure clauses were generally perceived as effective deterrents. Such clauses are typically included into contracts, such as those with employees, external consultants, and clients. By contrast, and quite surprisingly to us, hardly any mention was made of patents. We conjecture that this may be related to the nature of research at HP Labs, which tends to be quite close to the basic-research end of the spectrum and focuses on computing. For this type of knowledge, patent protection may not be the most effective protection mechanism (Cohen et al., 2000; Arundel, 2001; Thomä and Bizer, 2013).

The issue of trust featured very prominently in all our interviews. The Lab Director himself noted that HP Labs' culture is not so much about formal rules or "the letter of the law", as about "the spirit of the place and treating staff with respect" (LD quotes). HP Labs trusts its employees to do the right thing on balance, thus pushing decision-making authority quite low down the hierarchy. The individuals

we interviewed consistently emphasized discretion and the use of experience as key factors in deciding on how information should be disseminated. Training and mentoring were also perceived as important tools for establishing the appropriate norms and standards of behavior regarding security. This evidence is supportive of a vast literature highlighting the role of trust in facilitating information exchange (Uzzi, 1996, 1997; Dirks and Ferrin, 2001; Dyer and Chu, 2003; Levin and Cross, 2004), delegation of authority (Arrow, 1974; Bloom, Sadun and Van Reenen, 2012), and the management of complexity (Poppo and Zenger, 2002; Young-Ybarra and Wiersema, 1999; Gulati and Nickerson 2008). In particular, mutual trust is believed to be a critical precondition for the sharing and development of knowledge in innovative organizations (Nahapiet and Ghoshal, 1998; Adler, 2001). However, Bantel and Jackson (1989) and Molina-Morales and Martínez-Fernández (2009) caution that excessively close interpersonal and interorganizational relationships can have a adverse effect on risk-taking, innovation and value creation.

Our interviews also reveal that the well-being of staff is regarded as being very much in line with security goals, since the loss of an attractive job can serve as a powerful deterrent. Our interpretation of this piece of evidence is that the employment relationship in HP Labs contains elements of what is sometimes termed a 'relational contract' (Baker et al., 2002; Gibbons and Henderson, 2012; Baldwin and Henkel, 2015). In economics, relational contracts are non-binding commitments sustained through reputational concerns. A typical example is an employer's offer of continuity of employment, discretionary wage increases and good working conditions in exchange for appropriate behavior. One could view HP's efforts to create a positive working relationship within the company and HP Labs in particular as an attempt to incentivize good security practices.

Our framework posits that open and unrestricted communication is important to improve decision-making and foster innovation. We found evidence that for HP Labs it is critical to provide high-quality and reliable products, as captured for instance by the concern that revealing HP Labs' capabilities or new products too early may run the risk of creating inappropriate expectations on the part of customers or other HP units. However, our subjects more often tended to emphasize the costs of delay that security requirements sometimes impose. For instance, some noted that while tagging procedures are effective at controlling information, they also tend to delay the distribution of source codes, thus increasing the time it takes for the project to be completed. These observations suggest that our framework is incomplete, and

the analysis should be augmented with a discussion of delay costs, as in information-processing models (e.g., Radner, 1993; Patacconi, 2009).

These findings have implications for innovation management. The innovation literature finds that secrecy and lead-time advantage are two of the most important ways in which firms can profit from their R&D activities (Cohen et al., 2000; Arundel, 2001; Thomä and Bizer, 2013). Our evidence suggests that there may be a conflict between these two appropriability mechanisms: security protocols may help mitigate the risk of information leakage, but may also create delays and compromise lead-time advantage.

The need to quickly acquire capabilities and reduce delays in new product development may also help explain changes in publication practices at Apple. Apple has traditionally been a one of the most secretive companies among the U.S. tech giants. But competition to develop more powerful AI is changing that. Apple, Google, Facebook and Microsoft are now all involved in a race to use AI for a myriad of applications including search, face recognition, self-driving cars and medical diagnosis. With competition intensifying, the cost of delay is arguably rising. This may explain why, "when Apple hired computer scientist Russ Salakhutdinov from Carnegie Mellon last year as its new head of AI, he was immediately allowed to break Apple's code of secrecy by blogging and giving talks. At a major machine-learning science conference late last year in Barcelona, Salakhutdinov made the point of announcing that Apple would start publishing, too. He showed a slide: "Can we publish? Yes."" (Regalado, 2017). Thus, consistent with our arguments, it seems that secrecy must sometimes be sacrificed when competition is fierce and time is of the essence.

Finally, research suggests that firms possess capabilities that allow them to handle information more efficiently and more securely than markets (Kogut and Zander, 1992; Grant,1996; Liebeskind, 1996). We found that information tends to flow much more openly inside HP Labs and HP more generally than between HP Labs and external organizations. This appears to be related to the availability inside HP of informal communication channels, which are sustained by relationships of trust. Socialization mechanisms that engender trust among co-workers and allow them to internalize social norms may therefore be powerful factors facilitating information sharing.

Our study is subject to many limitations. The number of interviews is very small. We investigated security practices within a single lab located in one particular country, so we cannot determine to what extent our findings (such as the perceived effectiveness of legal instruments and built-in penalties) are

contingent on the specific institutional environment. The research conducted in the lab also mainly focuses on specific areas of engineering and computer science. Extending the sample to multiple locations and labs performing different types of research would be an interesting avenue for future work. We also believe that it would be worth developing some of the themes featured in our interviews further. Under what circumstances are internalized codes of behavior likely to be effective? What is the role of relational contracts in promoting good security practices? Thus, in the spirit of Eisenhardt (1989), the case study evidence suggests ways to create better theory.

References

Adler, P. S., 2001, "Market, hierarchy, and trust: The knowledge economy and the future of capitalism". *Organization Science,* **12**: 215-234.

Arora, A., S. Belenzon and A. Patacconi, 2017, "Knowledge sharing in alliances and alliance portfolios". Working Paper.

Arora, A., S. Belenzon and A. Patacconi, 2018, "The decline of science in corporate R&D". *Strategic Management Journal*, **39**: 3-32.

Arrow, K., 1974, *The Limits of Organization.* New York, NY: Norton.

Arundel, A., 2001, "The relative effectiveness of patents and secrecy for appropriation". *Research Policy*, **30**: 611-624.

Baker, G., R. Gibbons and K. J. Murphy, 2002, "Relational contracts and the theory of the firm". *Quarterly Journal of Economics,* **117**: 39-84.

Baldwin, C. Y. and J. Henkel, 2015, "Modularity and intellectual property protection". *Strategic Management Journal,* **36**: 1637-1655.

Bantel, K. A. and S. E. Jackson, 1989, "Top management and innovations in banking: does the composition of the top team make a difference?" *Strategic Management Journal,* **10**: 107–124.

Belenzon, S. and A. Patacconi, 2014, "How does firm size moderate firms' ability to benefit from invention? Evidence from patents and scientific publications". *European Management Review,* **11**: 21-45.

Bhaskarabhatla, A. and D. Hegde, 2014, "An organizational perspective on patenting and open innovation". *Organization Science,* **25**: 1744-1763.

Bhide A., 2000, *The Origin and Evolution of New Businesses.* New York, NY: Oxford University Press.

Bloom, N, R. Sadun and J. Van Reenen, 2012, "The organization of firms across countries". *Quarterly Journal of Economics,* **127**: 1663-1705.

Bowles, S., 1998, "Endogenous preferences: The cultural consequences of markets and other economic institutions". *Journal of Economic Literature,* **36**: 75-111.

Brown, J. S. and P. Duguid, 1991, "Organizational learning and communities-of-practice: Toward a unified view of working, learning, and innovation". *Organization Science,* 2: 40-57.

Bryman, A., 2004, *Encyclopedia of Social Science Research Methods.* pp. 1143-1144.

Burton, M. D., J. B. Sorensen and C. M. Beckman, 2002, "Coming from good stock: Career histories and new venture formation". *Research in the Sociology of Organizations,* **19**, 229-262.

Charmaz, K., 2014, *Constructing grounded theory (2nd ed.).* Thousand Oaks, CA: Sage.

Chesbrough, H., 2002, "Graceful exits and missed opportunities: Xerox's management of its technology spin-off organizations". *Business History Review,* **76**: 803-837.

Cohen, W. M., R. R. Nelson and J. P. Walsh, 2000, "Protecting their intellectual assets: Appropriability conditions and why US manufacturing firms patent (or not)". NBER Working Paper 7552.

Corbin J. and A. L., 2014, Strauss, *Basics of Qualitative Research.* Sage.

de Faria P. and W. Sofka, 2010, "Knowledge protection strategies of multinational firms—A cross-country comparison". *Research Policy,* **39**: 956-968.

Demski, J. S., T. R. Lewis, D. Yao and H. Yildirim, 1999, "Practices for managing information flows within organizations". *Journal of Law, Economics, and Organization,* **15**: 107-131.

Denis, J. L., L. Lamothe and A. Langley, 2001, "The dynamics of collective leadership and strategic change in pluralistic organizations". *Academy of Management Journal,* **44**: 809-837.

Dirks, K. T. and D. L. Ferrin, 2001, "The role of trust in organizational settings". *Organization Science,* **12**: 450-467.

Dyer, J. H. and W. Chu, 2003, "The role of trustworthiness in reducing transaction costs and improving performance: Empirical evidence from the United States, Japan, and Korea". *Organization Science,* **14**: 57-68.

Eisenhardt, K.M., 1989, "Building theories from case study research". *Academy of Management Review,* **14**: 532-550.

Fosfuri, A. and T. Rønde, 2004, "High-tech clusters, technology spillovers, and trade secret laws". *International Journal of Industrial Organization,* **22**: 45-65.

Gallié, E. P. and D. Legros, 2012, "French firms' strategies for protecting their intellectual property". *Research Policy,* **41**: 780-794.

Gambardella, A., 1995, *Science and Innovation: The US Pharmaceutical Industry during the 1980s.* Boston, MA: Cambridge University Press.

Gertner, J., 2012, *The Idea Factory: Bell Labs and the Great Age of American Innovation.* New York, NY: Penguin.

Gibbons, R. and R. Henderson, 2012, "Relational contracts and organizational capabilities". *Organization Science,* **23**: 1350-1364.

Gioia, D. A., K. G. Corley and A. L. Hamilton, 2013, "Seeking qualitative rigor in inductive research: Notes on the Gioia methodology". *Organizational Research Methods,* **16**: 15-31.

Gompers, P., J. Lerner and D. Scharfstein, 2005, "Entrepreneurial spawning: Public corporations and the genesis of new ventures, 1986 to 1999". *Journal of Finance,* **60**: 577-614.

Grant, R. M., 1996, "Toward a knowledge-based theory of the firm". *Strategic Management Journal,* **17**: 109-122.

Gulati, R. and J. A. Nickerson, 2008, "Interorganizational trust, governance choice, and exchange performance". *Organization Science,* **19**: 688-708.

Hamel, G., 1991, "Competition for competence and interpartner learning within international strategic alliances". *Strategic Management Journal,* **12**: 83-103.

Hannah, D.R., 2005, "Should I keep a secret? The effects of trade secret protection procedures on employees' obligations to protect trade secrets". *Organization Science,* **16**: 71-84.

Hodder, I., 2003, The Interpretation of Documents and Material Culture. In Denzin, N. K and Y. S. Lincoln (eds.), *Collecting and Interpreting Qualitative Materials.* Thousand Oaks, CA: Sage, pp. 155-75.

House, C. H. and R. L. Price, 2009, *The HP Phenomenon.* Stanford, CA: Stanford University Press.

Katz, R. and M. Tushman, 1981, "An investigation into the managerial roles and career paths of gatekeepers and project supervisors in a major R&D facility". *R&D Management,* **11**: 103-110.

Khanna, T., R. Gulati and N. Nohria, 1998, "The dynamics of learning alliances: Competition, cooperation, and relative scope". *Strategic Management Journal,* **19**: 193-210.

Kogut, B. and U. Zander, 1992, "Knowledge of the firm, combinative capabilities, and the replication of technology". *Organization Science,* **3**: 383-397.

Lashinsky, A., 2012, *Inside Apple: How America's Most Admired—and Secretive—Company Really Works.* New York, NY: Business Plus.

Laursen, K. and A. J. Salter, 2014, "The paradox of openness: Appropriability, external search and collaboration". *Research Policy,* **43**: 867-878.

Levin, D. Z. and R. Cross, 2004, "The strength of weak ties you can trust: The mediating role of trust in effective knowledge transfer". *Management Science,* **50**: 1477-1490.

Li, D., L. Eden, M. A. Hitt and R. D. Ireland, 2008, "Friends, acquaintances, or strangers? Partner selection in R&D alliances". *Academy of management journal,* **51**: 315-334.

Liebeskind, J. P., 1996, "Knowledge, strategy, and the theory of the firm". *Strategic Management Journal,* **17**: 93-107.

Liebeskind, J. P., 1997, "Keeping organizational secrets: Protective institutional mechanisms and their costs". *Industrial and Corporate Change,* **6**: 623-663.

Molina-Morales, F. X. and M. T. Martínez-Fernández, 2009, "Too much love in the neighborhood can hurt: How an excess of intensity and trust in relationships may produce negative effects on firms". *Strategic Management Journal,* **30**: 1013-1023.

Nahapiet. J. and S. Ghoshal, 1998, "Social capital, intellectual capital, and the organizational advantage". *Academy of Management Review,* **23**: 242-266.

Newhouse, J., 2007, *Boeing Versus Airbus.* New York, NY: Alfred A. Knopf.

Ouchi, W. G., 1980, "Markets, bureaucracies, and clans". *Administrative Science Quarterly,* **25**: 129-141.

Patacconi, A., 2009, "Coordination and delay in hierarchies". *RAND Journal of Economics,* **40**: 190-208.

Pisano, G. P., 2006, *Science Business: The Promise, the Reality, and the Future of Biotech.* Boston, MA: Harvard Business Press.

Png, I. P., 2017a, "Law and innovation: Evidence from state trade secrets laws". *Review of Economics and Statistics*, **99**: 167-179.

Png, I. P., 2017b, "Secrecy and patents: Theory and evidence from the Uniform Trade Secrets Act". *Strategy Science*, **2**: 176-193.

Poppo, L. and T. Zenger, 2002, "Do formal contracts and relational governance function as substitutes or complements?" *Strategic Management Journal,* **23**: 707-725.

Quan, X. and H. Chesbrough, 2010, "Hierarchical segmentation of R&D process and intellectual property protection: Evidence from multinational R&D laboratories in China". *IEEE Transactions on Engineering Management,* **57**: 9-21.

Radner, R., 1993, "The organization of decentralized information processing". *Econometrica,* **61**: 1109-1146.

Rajan, R. G. and L. Zingales, 2001, "The firm as a dedicated hierarchy: A theory of the origins and growth of firms". *Quarterly Journal of Economics,* **116**: 805-851.

Ramalingam, A. and M. T. Rauh, 2010, "The firm as a socialization device". *Management Science,* **56**: 2191-2206.

Regalado, A., 2017, "Google's AI Explosion in One Chart". *MIT Technology Review.* Available from https://www. technologyreview.com/search/?s=%22Google%E2%80%99s%20AI%20Explosion%20in%20One%20Cha

Ritala, P., H. Olander, S. Michailova and K. Husted, 2015, "Knowledge sharing, knowledge leaking and relative innovation performance: An empirical study". *Technovation,* **35**: 22-31.

Ritala, P., K. Husted, H. Olander and S. Michailova, 2018, "External knowledge sharing and radical innovation: The downsides of uncontrolled openness". *Journal of Knowledge Management*, **22**: 1104-1123

Rønde, T., 2001, "Trade secrets and information sharing". *Journal of Economics & Management Strategy,* **10**: 391-417.

Schmidt, E. and J. Rosenberg, 2015, *How Google Works.* London, UK: John Murray.

Sofka, W., E. Shehu and P. de Faria, 2014, "Multinational subsidiary knowledge protection—Do mandates and clusters matter?" *Research Policy,* **43**: 1320-1333.

Strauss, A., 1987, *Qualitative analysis for social scientists.* Cambridge, UK: Cambridge University Press.

Thomä, J. and K. Bizer, 2013, "To protect or not to protect? Modes of appropriability in the small enterprise sector". *Research Policy,* **42**: 35-49.

Tushman, M.L. and R. Katz, 1980, "External communication and project performance: An investigation into the role of gatekeepers". *Management Science,* **26**: 1071-1085.

Uzzi, B., 1996, "The sources and consequences of embeddedness for the economic performance of organizations: the network effect". *American Sociological Review,* **61**: 674–698.

Uzzi, B., 1997, "Social structure and competition in interfirm networks: the paradox of embeddedness". *Administrative Science Quarterly,* **42**: 35–68.

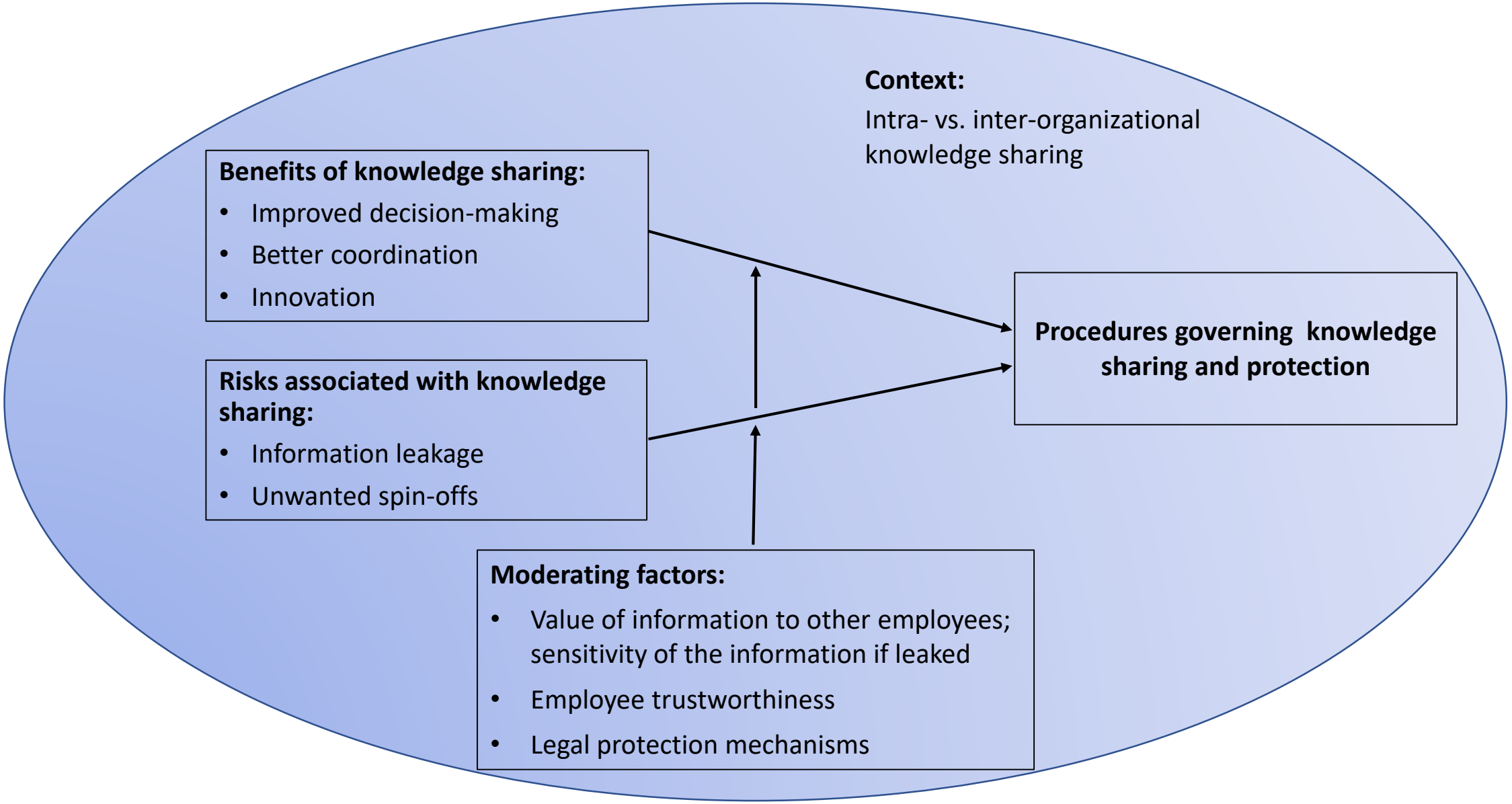
Von Zedtwitz, M., 2004, "Managing foreign R&D laboratories in China". *R&D Management,* **34**: 439-452.

Yin, R. K., 2011, *Applications of Case Study Research.* Sage Publications.

Young-Ybarra, C. and M. Wiersema, 1999, "Strategic flexibility in information technology alliances: The influence of transaction cost economics and social exchange theory". *Organization Science,* **10**: 439-459.

Zhao, M., 2006, "Conducting R&D in countries with weak intellectual property rights protection". *Management Science,* **52**: 1185-1199.

Figure 1: Factors affecting procedures for knowledge sharing and protection



Appendix 1: Designation and role of interviewees

Abbr.	Title	Brief description of role
LD	Lab director	The most senior member on the site and a VP of the firm.
SRM	Senior research Manager	One of several senior specialists managing large projects. The teams working for the SRM are not normally fixed, as these projects frequently require differing skills.
RE1	Research engineer	One of the specialist engineers who undertakes tasks within the research projects commissioned at HP Labs.
RE2	Research engineer	A second specialist engineer, with specific expertise in information security.
EL	External liaison officer	A specialist that is not part of HP Labs, but works closely with them to deliver information to the researchers and ensure that specific business requirements are met. Is a former HP Labs research engineer deployed specifically to the business side.

Appendix 2: Interview Script

1. What is your position with respect to HP Labs?

2. Could you tell us about the methods used to protect sensitive information within HP Labs and in HP Labs relationships with other HP business units and with external partners?

3. Some follow-up questions and/or suggestions for organizing answers:

    a. To what extent do the methods for protecting information rely on formal procedures such as contract clauses or internal company regulations?

    b. To what extend does the protection of information depend on informal methods?

    c. To what extend does the protection of information depend on organizational methods such as restricting communication among employees or finely subdividing jobs so that only senior managers can see the full picture?

    d. To what extend do managers perform a role as information gatekeepers?

    e. Is there any specific instance where the need to protect information has conflicted with other HP goals?

4. How does the extent to which HP uses the various methods for managing information that you mentioned vary with the situation?

5. Compared to the procedures for protecting information within HP Labs,

    a. Are there additional and/or different methods in place when staff at HP Lab collaborates with staff in other HP divisions?

    b. Are there additional and/or different methods that you would use in relationships and collaborations with external partners?

6. Can you give some examples of how information is managed differently when collaborations involve external partners? Are there examples of restrictions on exchanging information imposed by external partners (e.g., government agencies)?

7. From the perspective of information security, what are some of the perceived risks and other costs of exchanging information within HP Labs?

    a. Between HP Labs and other HP units?

    b. Between HP Labs and external partners?

    c. Within HP, who is responsible for balancing the benefits versus costs of exchanging information?

8. Additional question to be possibly answered via written material such as an organization chart. Could you give us an overview of HP Labs organizational structure and its links with other business units within HP and with other external business partners?

Appendix 3: Themes, coding and selected interview quotes

Themes and coding	Supporting evidence
Procedures for knowledge sharing and protection	
Procedures for knowledge sharing and protection were documented and tabulated, follow-up discussions were made, with the complete list of procedures mentioned previously made available. Methods for protecting information were classified as follows: (1) formal (e.g., contract clauses, patents, internal company regulations); (2) organizational (e.g., restrictions to communication flows, task fragmentation); (3) informal (e.g., internalized norms, relational contracts); (4) other. Costs incurred to protect information were scored as follows: (1) negligible cost; (2) significant cost. In most cases, cost was measured in terms of time taken to accomplish a task. The integrity of an answer was classified as follows: (1) no response; (2) lack of direct knowledge, but able to provide specific examples; (3) direct knowledge of a case.	“[Communication within HP] works well unless you are using very private material. Clear text emails are fine, this is assumed. If it is HP private information then you have to use a certificate based secure line.” [RE1] "I am always typically guarded with any information I share and I always ensure that there is a binding contract between the parties ... So I know when I'm in a meeting that there is a contract in place to protect the information I share." [SRM] "If we have information from our business units that is sensitive then it is not widely circulated across the organization. That is more controlled. Similarly, if we have information from partners this is tightly controlled. If we are working with this type of information, which is intranet based we will be working in quite a guarded even in the immediate organization. [...] The only places where we would be really tight, is our stuff related to the government. This would not make it onto the intranet. We would keep that sort of material of the intranet, keep it separately on machines that are air gapped. But this is a very small amount of material and the philosophy is that you would destroy it as quickly as you can. " [LD] “Information is typically shared on an ad hoc basis and you have to know the right person to talk to, to be able to get access to the information in the first place. […] You have to know the specific person and you would expect that you could have access to carry out a specific role, but it is about knowing the right person.” [RE2] “Typically because I work with labs in terms of research the tendency is not to share in my business unit because it could land in someone's lap in sales and would feel they could offer something that could differentiate HP to the market place. This would be in order to make a brand new sale and get more customers. Now that would mean delivery of research early into the market and that is not in HP Labs interest. So I am quite straight in what I do in terms of info flow between the two.” [EL]
Intra- vs. inter-organizational knowledge sharing	
Experience within and outside HP Labs was noted. Informal procedures were documented and tabulated; same procedure as above used coding and in the follow-up.	"When I was in Labs it was very much an open environment where people freely shared information and it was assumed you were part of a community. [...] But in services most people work from home and there is a real breakdown in communication where typically everything happens over a phone. So it is somewhat blurred regarding how sparse the information flows are between people. And, the managers will hold the information centrally and feed it out as appropriate." [EL] “[Redacted specific name] there were clear rules about information I could not send out via clear text emails and this limited the way were able to function. We had developments where it was all being centrally managed in a portal. However, they were unable to send out notifications from this portal because that would have violated the clear text rule. This actually impeded the work because I did not know when things were changing. This meant that I had to manually check where if this just had been internally in HP the exchange would have been much easier.” [RE2]

Online Appendix: A simple model of knowledge protection

This appendix develops a simple model of an organization that must carry out a project such as developing new software. The project is composed of several tasks which must be coordinated with each other. The tasks are heterogeneous, both in terms of their security risk and coordination costs. Our goal is to identify how internal and environmental factors affect the choice between open and restricted communication modes.

Consider a project composed of $n+1$ tasks. Each task $i = 1, 2, ..., n+1$ is assigned to a different agent (or group of agents). The agents are also indexed by i, with the understanding that agent i performs task i. Agents possess private information about their tasks. For instance, agent i may have acquired information about a set of clients or task i related technology. Private information is modeled by assuming that each agent i privately observes the realization of a random variable $\tilde{\theta}_i$.[1] The random variables $\tilde{\theta}_i$, $i = 1, 2, ..., n+1$, are normally and independently distributed with mean μ_i and variance ϖ_i^2. This information is common knowledge. The realization of $\tilde{\theta}_i$ is denoted by θ_i.

Tasks must be coordinated for the project to succeed. Following Dessein and Santos (2006), we assume that to coordinate task i with all the other tasks $j \neq i$, the agent in charge of task i must perform a string of n actions $\mathbf{a}_i = \{a_{ij}\}_{j \neq i}$. If $a_{ij} = \theta_j$, then task i is perfectly coordinated with task j. In general, however, coordination will be less than perfect. The expected coordination cost which is incurred when task i is imperfectly coordinated with task j is

$$C_{ij} = c_j \mathbb{E}[\left(a_{ij} - \tilde{\theta}_j\right)^2] \tag{1}$$

where c_j parametrizes the importance of task j on the overall project architecture and $\mathbb{E}[.]$ is the expectations operator.

To tailor the actions a_{ij} to the task specifications θ_j, the agents can communicate. Agent j, in particular, can send a signal s_{ji} to agent i which conveys information about θ_j. Since the random variables $\tilde{\theta}_i$ are independently distributed, the only information which is relevant to i when choosing a_{ij} is s_{ji}. We assume that agents choose their coordinating actions $a_{ij}(s_{ji})$ so as to minimize the coordination

[1] The model can easily be generalized to the case where agent i privately observes the realization of m_i random variables $\tilde{\theta}_{ih}$, $h = 1, ..., m_i$. See Remark 1 below.

cost C_{ij} incurred by the organization. Thus, we abstract from the possibility of agency problems in the choice of a_{ij}. It is a standard result in decision theory that the function $a_{ij}(s_{ji})$ which minimizes the mean squared error in equation (1) is the conditional mean

$$a_{ij}(s_{ji}) = \mathbb{E}\left[\tilde{\theta}_j \mid s_{ji}\right] \tag{2}$$

(see, e.g., De Groot, 1970). We consider two types of communication modes. These communication modes differ along three dimensions: (i) the amount of information that they make available for coordination purposes, (ii) the security risk associated with their use, and (iii) their costs (in particular, the screening costs). The key trade-off we emphasize is between greater security risk when a more open communication mode is selected, and loss of coordination when a more restricted or secure communication mode is selected. Intuitively, as more agents get access to information, coordination improves, but the chance of information leakage also increases.

Open communication. If communication from j to i is open or unrestricted, then j fully reveals his information to i. As a result, i will observe a perfectly informative signal:[2]

$$s_{ji}^{U} = \theta_j. \tag{3}$$

It follows that the coordination cost associated with i's action in support of task j, C_{ij}, is zero, since i can set $a_{ij}(s_{ji}^{U}) = \theta_j$.[3] There are however two additional costs associated with unrestricted communication. First, the risk of information leakage is greater when communication is unrestricted. Let $R_j(k)$ denote the expected security risk to the organization when information about task j is communicated openly to k agents and securely to $n-k$ agents. Let $p\left(\tau,\alpha\right) \in (0,1)$ be the probability that an agent who learns task j information openly will leak this information. Here τ parametrizes the extent to which employees can be trusted with secrets, and α parametrizes the knowledge protection intensity of the firm. For instance, τ could measure the organization's efforts to train and mentor its employees about security, and α may measure its propensity to patent or to impose non-disclosure or non-compete clauses, as well as

[2] The assumption that the signal is perfectly informative is just for simplicity. As will become clear in the following, what matters is that the signals under open communication are more precise than the signals in the restricted communication scenario.

[3] Note that in this model it is not necessarily the case that if j unrestrictedly communicates with i, then i unrestrictedly communicates with j.

environmental factors such as the strength of intellectual property rights in a country. We assume that $p(\tau, \alpha)$ is weakly decreasing in both τ and α. For simplicity, we assume that the probability that an agent who learns task j information securely will leak this information is zero.

For most of the analysis, we posit that the cost of information leakage is borne by the organization only once, when the first leak occurs. We also assume that agents decide independently whether to leak the information. These assumptions are standard in related theoretical work (e.g., Baldwin and Henkel, 2015). However, relaxing them, for instance by assuming that security costs are additive in the number of leaks, would not qualitatively change the results of the paper (see Remark 1 below).

Given our assumptions, the expected security risk to the organization when information about task j is communicated openly to k agents and securely to $n-k$ agents is

$$R_j(k) = r_j(1 - [1 - p(\tau, \alpha)]^k) \tag{4}$$

where r_j denotes the cost to the organization when information about task j is leaked. Hence, $R_j(k)$ is increasing with respect to k, but at a rate that, whilst always positive, is decreasing with respect to k. This is an essentially 'crossing the rubicon' approach, which we will talk about in Section 5 in more detail, it is the initial block of potentially un-secure disclosures that form the majority of the risk, the precise proportion depends upon $p(\tau, \alpha)$.[4]

Security risks may arise because agents may misplace the information, or may leak it to competitors. Also, the organization may fear that if agents have access to valuable information (e.g., a client list), they might decide to leave the organization and set up competing businesses.

The second type of cost associated with open communication is the time and effort that must be spent crafting messages. We assume that for each message s_{ji}^U that it is sent, a communication cost t must be incurred. This communication cost is also eventually borne by the organization because the organization must compensate its employees for their efforts.

Restricted (or secure) communication. Under restricted communication, messages are screened. Screening results in a filtering of sensitive information that mitigates security concerns. Specifically,

[4] This specification assumes that agent j (the agent who is initially endowed with the information) never leaks it. This assumption could easily be relaxed without changing any of the qualitative results of the paper. If agent j could also leak the information, for instance, we would simply have that $R_j(k) = r_j(1 - [1 - p(\tau, \alpha)]^{k+1})$.

we assume that under restricted communication, security risk is zero. The cost of screening is that task coordination may be impaired. To capture this, we posit that, for all i and j, $i \neq j$, restricted communication from j to i results in i receiving a signal

$$s_{ji}^R = \theta_j + \epsilon_{ji} \tag{5}$$

where the variables ϵ_{ji} are random normal variables independently distributed with mean 0 and variance σ^2. σ^2 can be interpreted as an (inverse) measure of the quality of the screening technology. It is clear from inspection of (5) and (3) that restricted communication conveys less (more noisy) information than unrestricted communication.

In practice, communications can be screened in at least two ways. First, communications may be mediated by gatekeepers. For instance, an engineer may communicate data only to his manager, and the manager may then decide to transmit part of this information to other agents. Second, communications may be monitored, which may give rise to self-censorship. Both mediated and monitored communications may result in messages that are less informative but also less risky than the messages sent through open communication channels.

Given (5), the coordination cost C_{ij} associated with restricted communication can easily be computed. Indeed, because θ_j and ϵ_{ji} are normally and independently distributed, the conditional mean and variance of θ_j given the signal s_{ji}^R are given by

$$\mathbb{E}_\theta[\tilde{\theta}_j \mid s_{ji}^R] = \frac{\sigma^2}{\varpi_j^2 + \sigma^2}\mu_j + \frac{\varpi_j^2}{\varpi_j^2 + \sigma^2}s_{ji}^R \tag{6}$$

and

$$\mathbb{E}_\theta[(\tilde{\theta}_j - \mathbb{E}[\tilde{\theta}_j \mid s_{ji}^R])^2 \mid s_{ji}^R] = \frac{\varpi_j^2\sigma^2}{\varpi_j^2 + \sigma^2}$$

(see, e.g., De Groot, 1970). Using the law of iterated expectations, one thus obtains[5]

$$C_{ij} = \lambda_j(\sigma^2)c_j \quad \text{where} \quad \lambda_j(\sigma^2) \equiv \frac{\varpi_j^2\sigma^2}{\varpi_j^2 + \sigma^2}. \tag{7}$$

Lastly, we specify communication costs. Restricted communication is associated with two types of communication costs. First, as in the case of unrestricted communication, the organization incurs a unit cost

[5] In fact the nested expectation is decomposed by $C_{ij} = c_j\mathbb{E}[(a_{ij}(s_{ji}^R) - \theta_j)^2] = c_j\mathbb{E}_{s_{ji}^R}\left[\mathbb{E}_\theta[(\theta_j - \mathbb{E}[\theta_j \mid s_{ji}^R])^2 \mid s_{ji}^R]\right]$.

of t whenever a message s_{ji}^R is created. In addition, there are screening costs s per message. Thus total communication costs for message under restricted communication is $t + s$.

Analysis. We now examine how the organization should design its communication system. The goal of the organization is to minimize the cost of carrying out the project, which is given by the sum of the security, coordination and communication costs.[6] The choice variables are the communication modes for each message s_{ij}. Note that the problem of selecting communication modes for agent i's messages can be analyzed separately from the problem of selecting communication modes for agent j's messages. How message s_{jh} is communicated has in fact no bearing on the costs and benefits associated with the different communication modes for agent i's messages, $j \neq i$. Thanks to the decomposability of the organizational problem, we can thus focus on a representative task i.

Our first result shows that, for each task i, the optimal choice of communication mode (open or restricted/secure) takes a simple form.

Lemma A1. *Information on task i is either communicated openly to all agents, or is communicated securely to all agents.*

Proof of Lemma A1. Suppose that task i information is communicated openly to $k = 0, 1, ..., n$ agents and securely to $n - k$ agents. As noted in the body of the paper, the total cost associated with task i (inclusive of security and coordination costs) is

$$Cost_i(k) = r_i(1 - [1 - p(\tau, \alpha)]^k) + (n - k)\lambda_i(\sigma^2)c_i + nt + (n - k)s.$$

The organization must minimize this cost with respect to k (or, equivalently, maximize $-Cost_i(k)$). Ignoring integer constraints, one can differentiate $-Cost_i(k)$ and obtain $-\partial^2 Cost_i/\partial k^2 = r_i[1-p(\tau, \alpha)]^k(\ln(1-p(\tau, \alpha)))^2 \geq 0$. Because $-Cost_i(k)$ is convex in $k \in [0, n]$, the solution of the maximization problem will typically be a corner solution: either all the information is communicated openly ($k = n$) or all the information is communicated securely ($k = 0$). This proves Lemma A1. ■

To see why Lemma A1 is true, consider the general case where agent i communicates openly with $k = 0, 1, ..., n$ agents and securely with $n - k$ agents. The total cost associated with task i (inclusive of

[6] Although revenues are not included in the model, the analysis could easily be generalized to incorporate them. See Patacconi (2009) for an example in a similar context.

security and coordination costs) is

$$r_i(1-[1-p\,(\tau,\alpha)]^k)+(n-k)\,\lambda_i(\sigma^2)c_i+nt+(n-k)\,s. \tag{8}$$

Ignoring integer constraints, one can easily show that these costs are concave in k. The organization must *minimize* these costs with respect to k. Thus, the solution of this problem will typically be a corner solution: either all task i information is communicated openly ($k=n$) or all the information is communicated securely ($k=0$).[7] Intuitively, because security costs are incurred as soon as the first leak occurs, the marginal security benefits to restricting communication are increasing. If it is optimal to restrict some communication channels originating from task i, then it is optimal to restrict all of them.

Lemma A1 is useful because, when selecting the optimal communication modes for task i information, the organization has only to compare the costs associated with fully secure communication, $n[\lambda_i(\sigma^2)c_i+t+s]$, to the costs associated with fully open communication, $r_i(1-[1-p\,(\tau,\alpha)]^n)+nt$. Proposition A1 characterizes the optimal choice of communication modes for all tasks $i=1,2,...,n+1$.

Proposition A1. *Let tasks be indexed so that* $\Psi_i \equiv r_i(1-[1-p\,(\tau,\alpha)]^n)-n\lambda_i(\sigma^2)c_i$ *is weakly increasing in* i. *There exists an integer* $\hat{l}\in[0,n+1]$ *such that, for all tasks* $i\leq\hat{l}$, *open communication is optimal, and for all tasks* $i>\hat{l}$, *restricted communication is optimal, where* $\hat{l}$ *is the largest integer such that:*

$$r_i(1-[1-p\,(\tau,\alpha)]^n)-n\lambda_i(\sigma^2)c_i\leq ns. \tag{9}$$

The number of tasks $\hat{l}$ *for which open communication is optimal is weakly increasing in* $\left(-r_i,c_i,\tau,\alpha,\sigma^2\right)$.

Proof of Proposition A1. The proof of Proposition A1 follows from Lemma A1 and the comparison between $r_i(1-[1-p\,(\tau,\alpha)]^n)+nt$ and $n[\lambda_i(\sigma^2)c_i+t+s]$. Open communication of task i information is optimal when $r_i(1-[1-p\,(\tau,\alpha)]^n)+nt\leq n[\lambda_i(\sigma^2)c_i+t+s]$ or, equivalently, when $r_i(1-[1-p\,(\tau,\alpha)]^n)-n\lambda_i(\sigma^2)c_i\leq ns$. Because $r_i(1-[1-p\,(\tau,\alpha)]^n)-n\lambda_i(\sigma^2)c_i$ is weakly increasing in i, all information regarding tasks with index i less than or equal to some critical threshold $\hat{l}$ is optimally communicated openly. The comparative statics result is obtained by considering parameter changes that make the quantity $r_i(1-[1-p\,(\tau,\alpha)]^n)-n\lambda_i(\sigma^2)c_i$ smaller. ■

[7] In the eventuality that all admissible k are optimal, we assume that the organization also selects a corner solution.

When condition (9) holds, then the information on task i is deemed sensitive and communications are restricted (or secure). Conversely, when (9) does not hold, then the information on task i is not deemed sensitive and communications are open. Intuitively, it is optimal to restrict/screen communications when the cost of information leakage is large (r_i big) and task coordination is unimportant (c_i small). Restricting communication channels is also less likely to be optimal when employees are trustworthy and the organization has invested in legal protection mechanisms (τ and α are high). The greater the noise induced by security restrictions, σ^2, the more likely it is the open communication mode will be selected.

In addition, the model also shows that achieving coordination through communication is only important when ϖ_i^2 is not very small. Intuitively, ϖ_i^2 measures the extent to which task i can deviate from the initial specification μ_i. If ϖ_i^2 is small, then the need for adaptation is limited and, as a result, the need for (ex post) communication is reduced. If ϖ_i^2 is sufficiently small, the best communication mode is arguably no communication at all (restricted or unrestricted). Coordination can perfectly be achieved through initial planning (in the model, by simply setting $a_{ij} = \mu_j$ for all i, j).

Remark 1. The model assumes that the organization bears the full cost of leakage of task j information as soon as the first leak occurs. An alternative polar assumption would be that the cost of information leakage is additive in the number of leaks that occur. Then the expected security risk associated with communicating openly task j information to k agents would be $R_j(k) = kr_j p(\tau, \alpha)$. Lemma A1 would continue to hold and condition (9) would become $r_j p(\tau, \alpha) - \lambda_i(\sigma^2)c_i \leq s$. All the comparative statics results of the paper would remain unchanged.

Remark 2. The coordination costs c_i can be interpreted as a modularity parameter. Consider a setting where a group of agents i must integrate their task with other tasks. If c_i is small, then group i can spend little time tailoring the design of their system's component to the characteristics of the other components (high modularity). However, as c_i grows large, then coordination with other groups becomes more important (lower degree of modularity).

Remark 3. A different interpretation of the network of agents $i = 1, ..., n + 1$ is as a collection of possibly independent contractors. Under this interpretation, both stronger IP protection laws (which would

increase α) or greater societal trust (which would increase τ) would enable the disintegration of the vertically integrated firm, because they reduce the need for centralized monitoring. This information security argument complements existing explanations for the trends toward outsourcing and vertical disintegration based on the codification of previously tacit knowledge and the growth of technology markets.

Supplementary References

Dessein W, Santos T. 2006. Adaptive organizations. *Journal of Political Economy* **114**(5): 956-995.