Perceptions of employee knowledge-risks in multinational, multilevel R&D organizations – Managing knowledge leaking and leaving

Olander Heidi, Hurmelinna-Laukkanen Pia

DOI: 10.1142/S136391961540006X

Perceptions of employee knowledge risks in multinational, multilevel organizations – Managing knowledge leaking and leaving

Heidi Olander*

Lappeenranta University of Technology, School of Business
P.O. Box 20, FIN-53851 Lappeenranta, Finland
E-mail: heidi.olander@lut.fi

Pia Hurmelinna-Laukkanen

Oulu Business School, University of Oulu
P.O. Box 4600, FIN-90014 Oulu, Finland
E-mail: pia.hurmelinna-laukkanen@oulu.fi

Abstract: Maintaining innovation potential means that ideas, and the people generating those ideas, should be at the firm's disposal. Furthermore, the firm should be able to capture value from people's ideas. Losing these people therefore poses risks. Managing these risks is challenging, especially without intra-firm consensus on their role. This study examines how and why perceptions of severity and management of risks related to knowledge leaving and knowledge leaking differ across organizational levels and different firm locations. Depending on what types of differences are present, and why similarities and differences emerge, managers can direct their attention to different control or commitment-enhancing practices to address the risk of harmful knowledge loss and imitation. They should do this in a manner that enables them to maintain the prerequisites for future innovation and a creative work environment, while at the same time allowing global coordination and local adaptation.

Keywords: Knowledge protection; employee mobility; knowledge leaking; knowledge leaving; knowledge leakage; informal protection; formal protection; value creation; value capture; appropriability

* Corresponding author

1 Introduction

Prior research has established that structures can support creativity (Brattström et al., 2012), and this definitely applies to human resource management (HRM). One manifestation of this is the potential held by hybrid forms of control and commitment approaches, where both enforcing employee conduct and compliance and providing incentives for desirable behavior are combined to support creativity, innovation, and appropriation of innovation (Arthur, 1994; Su and Wright, 2012). However, there are some areas where control and empowerment come into conflict. One concrete example relates to protecting firm-specific knowledge assets: forcing information security rules on employees may generate distrust (Hannah, 2005), which may challenge commitment-based HRM practices. Yet, at best, both control and commitment allow firms to protect the

prerequisites of innovation. Quite surprisingly, this issue is largely unheeded in research on the role of HRM in knowledge management. While there has been an array of research on enhancing knowledge sharing in R&D through different means and the role of human resources in this process (e.g., Camelo-Ordaz et al., 2011; Hislop, 2003; Minbaeva, 2005), the point of view of human resources as the protectors of firm knowledge has often been disregarded with the exception of a few studies (Hannah, 2005; Hurmelinna-Laukkanen & Puumalainen, 2007; Liebeskind, 1996; Bulgurcu et al., 2010; Hannah and Robertson, 2014). Yet, considering the relevance of innovation appropriability (e.g., Ahuja et al., 2013) and securing future creativity, these issues deserve attention. Considering that employees are recognized both as essential for the firm's innovativeness and as the weakest links with regard to confidential knowledge (Bulgurcu et al., 2010; Hannah and Robertson, 2014), surprisingly little is known about the employee-related knowledge risks. It is not clear how these risks are perceived or in which forms they exist at different organizational levels. Likewise, it is not completely clear what role national differences and cultural aspects play for the turnout of employee-related risks even if such aspects may become highly relevant in multinational companies (Di Minin and Bianchi, 2011).

So far, previous literature has identified two main channels through which a company's knowledge can be lost when human resources are considered: knowledge leaving, which refers to knowledge moving outside the firm's boundaries with a key employee (e.g., Arrow's [1962] early idea regarding employee mobility and R&D spillovers; Hofer-Alfeis, 2008), and knowledge leaking that occurs when current employees (unintentionally or intentionally) disclose information that they are not supposed to disclose (Ritala et al., 2015; Liebeskind, 1997). Similarly, other lines of research have brought up differences existing with regard to the self-efficacy (skills and knowledge) to comply with information security policies that would address such risks, and with regard to the attitudes toward such rules. Such attitudes are, in turn, the sum of a variety of factors, including the potential inconvenience caused by complying, fear of sanctions related to not complying, and understanding the vulnerability of knowledge assets and intrinsic incentives to comply (Bulgurcu et al., 2010; Fuller et al., 2000; Hannah and Robertson, 2014). Furthermore, previous literature has suggested that HRM systems are inherently different in different contexts, such as within different countries. As the determinants of culture, shared values, norms, and beliefs shape the cognition and motivation of people within a collective group, such as a country (Chiu and Hong, 2006; Chua et al., 2014). For example, Su and Wright (2012, p. 2067) have noted that "Chinese cultural traits […] undermine the use and efficacy of high-involvement or high-performance work systems" that "advocate work empowerment and employees' participation." Furthermore, the (strength or weakness of) legal regimes and characteristics of job markets (e.g., mobility and uncertainty) may affect the need to control firm-specific assets (e.g., O'Donoghue and Croasdell, 2009). This means that control-based guidance may be quite necessary in China and in similar countries also considering knowledge (risk) management. Similar notions can be found in Yaula's (2011) study, which states that "The nature of multinational companies (MNCs) adds a layer of complexity to enforcing security policies because MNCs need to consider the effects of different cultural and organizational settings and integrate these in their corporate security policies."

Combining these insights, we assume that there could be differences in how company employees at different levels of the organization and in different countries perceive the risks of knowledge leaving (causing disruption to current projects, impeding creativity, and increasing potential for harmful imitation) and leaking (causing possible problems in chances of value capture and generative innovation). Furthermore, we assume that there could be different emphases regarding the relative criticality of the risks; existence of a

risk may be more or less unnoticed depending on whom (and on which operational level) is evaluating it.

Accordingly, our goal is to identify *what kinds of differences can be detected regarding the perceived relevance of knowledge leaving and knowledge leaking risks across (1) organizational levels and (2) different geographical firm locations*. Addressing this question will help bring much needed attention to knowledge protection by reminding managers that their expectations regarding how employees behave might not always be completely accurate. Furthermore, by revealing the undercurrents behind differing approaches, clear answers to this question will help in addressing these issues, finding appropriate knowledge protection mechanisms, and developing these mechanisms in the right direction. In other words, we suggest that like in many other areas, with regard to managing employee-related knowledge risks and confidential knowledge, it is important to acknowledge that perceptions and expectations differ within different parts of a multinational firm, and what (and why) should be done should differ accordingly.

In the following chapters we will first present the literature review on innovation, knowledge, and human resource management-related literature that was used to form the theoretical framework. Following this, we introduce a qualitative multiple case study research conducted within two large companies' R&D units operating in Finland, the US, and China. Employing a qualitative research design, we are able to examine the differences residing at different organizational levels and in different cultural contexts.

2 Employees' role in knowledge creation – Origins of knowledge leaving and leaking risks

Employees of a firm form a major source of information in innovative activities. The knowhow that is possessed by creative and innovative R&D employees enables the creation of new inventions. Therefore, new incoming employees may be a valuable source of innovative ideas (McEvily and Chacravarthy, 2002). Employees often create new knowledge in collaboration with others, sharing knowledge with collaboration partners from the same organization or from other organizations. Naturally, a sufficient amount of knowledge sharing is needed in order for innovation-related collaboration to succeed (e.g., Minbaeva, 2005).

However, not everything should be shared, and employees with access to knowledge that is valuable to the organization have certain responsibilities toward that knowledge. They constantly need to make decisions regarding whether or not to reveal specific knowledge. However, that responsibility is not always clear to the employees that may share too much. Likewise, while incoming employees may bring in new insights, these types of knowledge flows are not one-directional. Knowledge risks may be associated with both existing employees and new incoming employees.

2.1 Knowledge leaks and limited value capture possibilities

There are multiple reasons why R&D employees may want to share more knowledge than they should. For example, they may not know what should and should not be shared (Bulgurcu et al., 2010). Therefore, from the firm's point of view, one of the key issues (in addition to determining when to provide access to knowledge in the first place) related to appropriate knowledge sharing is the level of awareness of all employees regarding the confidentiality of knowledge and the handling of such knowledge. In case employees are not aware of their responsibilities in terms of confidential knowledge, unwanted knowledge spillovers to outsiders may occur, which may possibly weaken the firm's chance of value

capture. In addition to unawareness, other reasons for such knowledge leaks (spillovers) could be insufficient caution when aiming to solve a problem together (which may also be referred to as over-enthusiasm), mistakes (such as leaving documents lying on desks or forwarding e-mails containing classified knowledge), or frustration with one's own organization's practices or one's own work (Herath and Rao, 2009). Likewise, there might be misjudgements regarding the confidentiality of knowledge, or the security rules might be broken in the attempt to fulfil work requirements efficiently (Bulgurcu et al., 2010; Hannah and Robertson, 2014). In addition, knowledge leaks could happen in totally different situations outside the actual workplace that do not involve actual collaboration partners; for example, such leaks could occur as the result of careless communication at industry fairs, in online communities, or even in everyday situations, such as careless use of a laptop or smartphone in public places (see Workman et al., 2008). The company can try to prevent these types of risks by educating employees and aiming to increase understanding regarding what is confidential knowledge, how one should deal with it, and what the consequences may be for the company in case such knowledge leaks out. Adequate sanctions may also contribute to induction of such education (Bulgurgu et al., 2010; Hannah and Robertson, 2014).

Problems generated by knowledge leaks are quite obvious, as they may induce unwanted imitation (when knowledge is utilized by others in their innovative activities). Such leaks may also give rise to challenges to innovation appropriation in the sense that such knowledge (that could otherwise have been capitalized on) may be given out for free; the element of surprise may also be lost (even if others would not copy the knowledge as such). Furthermore, knowledge leaks may increase the need to apply for (sometimes quite costly) intellectual property rights or start other activities to ensure that the knowledge that has passed the firm's boundaries will not be abused.

In sum, organizations need to simultaneously encourage employees to share knowledge, but on the other hand, they must also instruct them to keep (certain) knowledge confidential. Balancing between these contradictory messages inherently means that one of these may be diluted at the expense of the other (Bulgurgu et al., 2010). This, in turn, can create both a knowledge leaking and a knowledge leaving risk due to some employees possibly thinking that it is impossible to stay in a contradictory knowledge environment.

2.2 Knowledge leaving and lost sources of future innovation

In his research, Arrow (1962) discussed the link between labor mobility and knowledge spillovers. His work described how difficult it is to protect something as intangible as knowledge and information by legal means. Since then, there has been a vast amount of research examining the R&D spillovers and knowledge transfer between different organizations (Moen, 2005). Among these studies, McEvily and Chacravarthy (2002) have noted that it is possible that competitors may try to utilize this mobility by hiring away important employees, thereby accessing relevant knowledge (see also Geroski, 1995). However, imitation is not the only problem, and may not even be the most pressing one. Instead, the disruptions to development caused by expertise leaving the firm may be quite pronounced when leaving employees bring their skills and competences with them.

There are various situations when an employee might leave the company, such as taking a position with another firm, starting up his own business, moving to another part of the company, or retiring (Hofer-Alfeis, 2008). In this study, by knowledge leaving we mean the leaving related to changing jobs (moving to another company in a related field or even to a company that is a competitor) or starting up one's own company in the same

field, as these are the situations that carry the most knowledge risks that can hurt the original employing company. Furthermore, retiring or other personal reasons related to health, for example, are not something that the company can actively try to prevent apart from trying to sustain the knowledge through documentation. The mechanisms for limiting knowledge leaving are, in fact, for the most part quite soft in nature, meaning that coercion has a limited effect and increasing commitment is more important. Surely, non-competition contracts may be utilized, like long-term employment contracts with sanctions related to early termination, but they typically create only temporary obstacles to knowledge leaving.

3 Risk as a perception causing differences

Considering that the human element is present, it may be that there are different views on the existence of the knowledge leaving risk, the reasons behind this risk, and the appropriate means through which the risk can be managed. The same applies to knowledge leaking risks. For example, self-efficacy (i.e., skills and competencies; Bulgurcu et al., 2010) to follow rules and guidelines that limit knowledge leaking may depend on the employee's awareness of the different risks and education received regarding these aspects. Likewise, social norms regarding conduct at work and allegiance toward the employer, co-workers, and collaborators (Husted and Michailova, 2010; Husted et al., 2013) may play different roles in different cultures, thereby also affecting knowledge leaving and leaking risks differently. Such issues are of relevance when strategies to manage the risks are formulated.

3.1 Differences within organizations – approaches at different levels

Prior research has identified numerous distinguishing factors between different managerial levels (Floyd and Lane, 2000). Regarding differing perceptions, Corley (2004) found that they were largely based on differences in the day-to-day roles enacted at different levels. Whereas top management handles strategic aspects related to the organization's survival, growth, vision, and mission, middle management operationalizes the vision and strategy while operational employees implement them and finalize daily business operations (Corley, 2004). As managers and employees at different levels of the organization need to worry about different things, perceptions of creativity, innovation, and knowledge risks are likely to be different as well.

Depending on the level in the company and a person's task, the assessment of the relevance of confidentiality issues and awareness of these issues will likely vary. Subsequently, the resulting behavior may be different. Managers see the business as a whole and need to consider strategic issues and a competitive environment, etc., which means that the long-term preservation of prerequisites for innovation and issues related to imitation are likely to emerge frequently. On the other hand, operative employees in their everyday work solve different types of problems, and it may be that knowledge protection practices cause impediments to efficient work (Bulgurcu et al, 2010). Therefore, balancing between knowledge sharing and protection also occurs differently at different levels of the company: there is a more clear-cut line at the managerial level about confidential and non-confidential information, whereas something deemed confidential may not seem as such at the operational level. R&D employees may consider a piece of information to be common knowledge, and sales personnel may see confidential knowledge as a crucial selling argument when managers consider it to be part of their core knowledge and competitive advantage. Problems may arise when there is a mismatch of perceptions within the firm.

Also, it is likely that the company's top management is not able to completely perceive its own knowledge gaps at all times and may thus fall prey to overconfidence (Levitt & March, 1988) in their perceptions related to knowledge protection issues.

3.2 Knowledge protection needs for HRM-related means in different geographical firm locations

In addition to different roles within an organization, differences related to knowledge risks may originate from different cultural and social norms (Ajzen, 1991), as well as the economic situation and legal structures in different regions (O'Donoghue and Croasdell, 2009), which is an important insight in multinational companies. Gelfand et al. (2006) have defined cultural tightness as the strength of social norms and the degree of sanctioning within a given society. Cultural tightness is reflected in a society's practices that affect individual-level cognition, motivation, and behaviors (Chua et al., 2014). Tight cultures promote highly developed systems of constraining and monitoring behaviors (Arnett, 1995), and deviation from such behavior is typically identified and sanctioned, which could indicate that employees in tight cultures would carry out knowledge sharing practices within socially accepted norms and groups. This could mean that people within these cultures could use more guidance related to what is expected from them in terms of knowledge sharing and protection in order to be able to follow these rules.

As an example of the structural and institutional aspects, firm locations differ in terms of the demand-supply ratio of labor markets in technology- and knowledge-based workers, which can be of relevance to knowledge leaving (Kirschenbaum and Mano-Negrin, 1999). The demand for knowledge workers in technology could, for instance, be higher in the new markets with lower production costs than in the traditional industrialized countries with higher labor costs and declining markets. Surely, individual- and organization-level issues play a role when knowledge risks are considered, but since HRM systems are highly affected by institutional elements (Hamill, 1983), certain trends can be observed.

Fenton-O'Creevy et al. (2008, p. 155) distinguish between the national business systems in "the "liberal market economies" (LMEs) of the US, the UK, Ireland, and Australia and the "coordinated market economies" (CMEs) of much of Continental Europe", including many Nordic countries, such as Finland (see Hall and Gingerich, 2004). They further state that firms "operating in the latter context are regarded as significantly more institutionally constrained than those in the former, in the sense that they operate within contexts whose legal frameworks and systems of industrial relations constrain managers' autonomy in applying market driven or technologically contingent management practices." The differences in HRM practices between firms operating in LMEs and CMEs include, for example, reimbursement policies, job security, and employee training (Hall and Soskice, 2001). This means that knowledge risk-related aspects are affected as well. We turn our attention to Finland, the US, and China in the empirical section of this study, and therefore these countries are briefly discussed below.

Finland, as a part of the European Union, follows the principle of free mobility of employees, and has similar rules with regard to norms related to employment legislation like most other EU countries. While differences surely exist within the EU (see, e.g., Ronen and Shenkar, 1985, on country clusters based on work-related attitudes; for example, the Nordic, Germanic, Anglo, and Latin European clusters, with Greece in the near Eastern cluster) (Brewster, 2004), some commonalities can be found. In Finland, as in other Nordic countries, there is a relatively strong and pronounced legislative framework, which means that labor unions play a role with regard to a variety of HRM issues (see also Bévort et al., 1995; Fenton-O'Creevy et al., 2008). Managers can mainly improve the employees'

situation with HRM practices, as legislation sets the framework for such practices. In fact, the mix of social, political, and employers' interests in the collective bargaining system is typical of the Finnish employment environment (Vanhala, 1995), and the situation is relatively similar across firms.

The *US*, as suggested above, belongs to a different setting. Brewster (2004, p. 368) notes that in the US, "the employing organization has considerable latitude in regard to the management of personnel, including inter alia, freedom to operate contingent pay policies; an absence of or at least a minimal influence from trade unions; and an assumption that the organization has sole responsibility for training and development." In line with this, individualism is highlighted in the US (Brewster, 2004). For example, in California, enforcing non-competition contracts restricting movement of employees could become problematic; however, in the US, firms' litigiousness has been shown to significantly reduce "spillovers otherwise anticipated from departures of employee inventors, particularly when the hiring organizations are entrepreneurial ventures" (Agarwal et al., 2009, p. 1349). In fact, litigiousness can be seen as more typical in the US than in China, where relationships and negotiation are relied on (McConnaughay, 2000), or in Finland, where reliance on legislation and negotiations (rather than on case law) reduces litigation to some extent.

In *China*, notable changes have been carried out during recent decades. The so-called "iron rice bowl" employment system characterized by egalitarianism and workforce stability was criticized as being incompatible with the changes in the business environment in China (Ngo et al., 2008). Subsequently, fixed-term employment contracts, performance-based rewards, and a new labor law that regulates employment relations were introduced; there was a change in welfare provision responsibility; and employment policies and practices were decentralized to the enterprise level so that recruitment and firing practices are more under managers' control. However, there still is a certain mix of traditional and market-oriented practices, and differences still exist between state-owned and private enterprises (Ngo et al., 2008), which causes some challenges (Su and Wright, 2012). Gelfand et al. (2011) found that China scored high in cultural tightness measures. However, at the same time, in terms of retaining employees, it has become increasingly easy to change jobs in China, which poses a challenge. O'Donoghue and Croasdell (2009) observed this in their empirical study, where employees' compensation guided their mobility more than loyalty toward the organization. Likewise, the intellectual property rights have not been considered particularly strong in China, adding knowledge-risk challenges.

Already this brief overview suggests that differences may emerge in the HRM practices and their suitability for decreasing risks related to knowledge leaking and leaving, and therefore we conducted an empirical study on these aspects.

4 Methods

For the empirical research on the issues under study we used qualitative interview data gathered in 2011–2012 from fifty employees of two globally operating technology companies' R&D units. The companies were chosen based on a combination of theoretical and purposive sampling, and they were used as instrumental case studies describing the phenomenon in certain contexts rather than merely intrinsically examining these cases (Silverman, 2005, p. 127–131). Both firms have their headquarters in Finland. One of the companies is in the information and communication technology (ICT) industry, and the other is in the high-tech engineering industry.

In order to identify possible cultural differences between different firm locations, we gathered data by conducting semi-structured theme interviews in three countries where the companies had R&D units: in Finland, the US, and China. As we were interested in finding out whether the perceptions of risks and their origins differ by the level within the organization as Corley's (2004) research suggests, we conducted interviews on the following four levels: operative R&D employees, team leaders, managers (HR, R&D), and strategy. We selected informants that were involved in R&D collaboration and confidential knowledge. Each of the interviews lasted between 90 to 120 minutes, and the recordings were later transcribed with the permission of the interviewees.

Regarding analyzing the data, we employed qualitative content analysis to identify key themes (Franzosi, 2006). The identified themes indicated 1) the interviewees' perceived existence of the two types of knowledge risks (leaking and leaving) and 2) the relative severity and origins of these two types of risks. Therefore, we looked for issues related to the interviewees' perceptions of dependency on key employees as indicators of the criticality of the leaving risk, as well as awareness and acknowledgement of knowledge protection-related responsibilities as indicators of the criticality of knowledge leaking risk.

We conducted the analysis within different levels in the organizations and within the three countries. Following Yin's (2003) case study logic, only the repeated findings were further examined. In order to simplify the complexity of the levels and make the findings more manageable, we combined the operative employees and team leaders as the "team level," while the HR and R&D managers together with the strategy-level managers were combined as the "management level." We used this division between the levels to sum up the repeated findings from both companies and the two levels, and these findings were gathered in a matrix (Table 1) in order to visualize the findings.

5 Analysis

Our findings on the perceived knowledge risks are summarized in Table 1 below, which is then followed by more detailed discussion.

Location	*FINLAND*		*THE US*		*CHINA*	
Org. levels	***Leaking***	***Leaving***	***Leaking***	***Leaving***	***Leaking***	***Leaving***
TEAM	LOW	MODERATE-HIGH	LOW-MODERATE	MODERATE-HIGH	MODERATE-HIGH	MODERATE
MANAGER	LOW	MODERATE- HIGH	MODERATE-HIGH	MODERATE-HIGH	MODERATE-HIGH	MODERATE-HIGH

Table 1. Empirical observations on the perceived knowledge risk levels

5.1 Perceptions of leaking- and leaving -related knowledge risks in Finland

For the case firms, Finland as a market area seems to be rather stable in terms of employees staying with the same employer for long periods of time. This could be due to the case of companies having a long history and being reputed and appreciated employers, but it also could be an outcome of Finland's legislative framework and relatively strong power of labor unions referred to above. The HR managers in both case companies note that the company cultures includes a rather open and direct form of discussion and that there is a mutual respect between employees and employers, which can be seen in fair employment contracts and a collaborative spirit in carrying out tasks according to company standards. Nevertheless, the downsides of the relatively long careers and low turnover are also acknowledged; they could cause stagnation, and an HR manager in the other Finish unit notes that with increasing international competitive pressure and the subsequent changes in the field, people should adopt a new type of company culture where additional action is needed beyond "the old model" of coming to work from nine to five and then leaving the office. Creativity is called for. On the other hand, the competitive market situation also challenges the company to be good at retaining the best talent for future innovation. Knowledge leaving would therefore be quite a critical issue.

Team-level perceptions

The *knowledge leaving risk* is perceived as being great among the team-level employees in both industries. The ICT company's employees fear that key employees leaving could cause delays, efficiency problems, and even termination of projects. The interviewees agree that knowledge is very tightly attached to the R&D personnel (that is, relatively tacit), and that the few key people in the collaboration interface are critical.

> Employees are everything in sustaining the competitiveness of the company. The people have the knowhow. You can buy knowhow, but if you need to create it, then it is the people who create it in the company; it does not just emerge (ICT company employee).

> Our knowhow is 100 % in the people (ICT company employee).

In the engineering company, some of the practices in use could enable retaining knowledge within teams. However, even with practices such as codifying and spreading the knowledge within teams, collaborating closely, and creating common knowledge, it is recognized that losing key employees (however infrequent) would still cause a delay in collaboration projects.

> Of course it always causes a downfall [if a key employee leaves] (Engineering company employee).

In terms of *knowledge leaking risks*, the team-level employees in both industries consider the risks to be low. They seem to be well aware of the risks and acknowledge the importance of confidentiality. They are able to give some examples and describe the confidentiality levels for knowledge and information expressed by the management. Even with non-disclosure agreements (NDAs) in place with suppliers and other partners, employees note that they should only give out the knowledge needed.

> Practically everything that is not on the Internet is confidential. [For example information on] forthcoming products. If we give out some of this knowledge, someone else can take it and manufacture based on that (Engineering company employee).

The role of confidentiality seems to be rather critical. The engineering industry involves a lot of knowledge that could be expropriated if revealed. This is acknowledged well by the team-level employees. However, this acknowledgement and awareness is likely not so much the result of specific training, especially in the case of the ICT company, but "comes from within." Furthermore, it is expected to come from within or through informal education provided by superiors, which includes checking with them whenever uncertain:

> It is an expert organization. Superiors are not watching your every move in terms of confidentiality, but they expect you to know these things (ICT company employee).

As a result, there resides a potential problem: one comment suggests that openness is seen as a virtue. If this is not a sign of sensible openness, which would be quite desirable, but rather reflects lack of caution or misjudgement in relation to handling confidential information, problems might emerge.

> We used to be more careful, but nowadays, as we've seen what good it can bring, we are more open (ICT company employee).

Management-level perceptions

Even though the management-level interviewees in the engineering company agree that the employee turnover in the unit has been quite small, they are much more concerned about the risk of key employees *leaving* than about the risk of knowledge *leaking*. Likewise, ICT managers acknowledge the role of employees as resources of innovative ideas, replacement problems that emerge when they leave, and the impossibility of codifying all of the human-related tacit knowledge into explicit form.

> A key person leaving would be a big loss for the company that has used a lot of resources on them. It is not always easy to hire a replacement because of tight resources that we have (Engineering company manager).

> In R&D, the knowledge related to what is coming next is always produced, self-invented, and self-developed by these R&D engineers. I can tell you, on a general level, the input from each and every one of them is significant (ICT company manager).

> In terms of research or technology areas, the people are the essential thing in sustaining the knowledge. Certainly not enough of it is documented to that level, that someone could be inducted through that [such documentation] (ICT company manager).

The management-level interviewees in both industries seem to take *knowledge leaking* and confidentiality issues relatively seriously, which is in line with the acknowledgement of the issue on the team level. Interestingly, whereas the dependency on key people seems to decrease over time, managers agree that the importance of confidentiality issues increases as launches become closer and products materialize and become more explicit. Nevertheless, the management-level interviewees seem to think that the importance of

confidentiality is well acknowledged throughout the firm, indicating a relatively low perceived risk of knowledge leaks.

> People are well aware of what is and is not ok to talk about. In their own area they know very well what is ok to talk about. And then they don't like to talk about anything except their own area, so they would not make any mistakes about this (ICT company manager).

> Especially the launches of new products are critical (Engineering company manager).

However, a comment by an HR manager indicates that there is no absolute certainty that perceiving the risk as low is warranted; there is not much training or follow-up information on how well the trainings guide employee conduct. This indicates that the perceived low risk of knowledge leaks could be based on the managers' trust in their employees' level of awareness, and not on a process of continuous education, for example.

> I really don't know. I assume that people know. I don't know how well they are actually being inducted, or if it is knowhow. We have it [rules on confidentiality] explicit on our intranet, emails, and in documents. But I am not sure how well the researchers really acknowledge it [the rules] (ICT company manager).

5.2 Perceptions of leaking- and leaving-related knowledge risks in the US

When asked about the specialties of the US as a firm location, interviewees responded that it is a rather independent environment where the companies operate with less emphasis on regulation of the labor markets and also highlighted the role of freedom of anonymity and personnel privacy. However, the HR department's hands are more tightly bound in terms of labor legislation-based employment contracting with notice of leave. An employee may leave at any time, with the national norm being two weeks' notice. Depending on the particular job, sometimes people will inform their employers well in advance. In the case that an employee informed his employers that he was leaving for a competitor, they would most likely be told to leave immediately. Knowing when an employee may possibly retire (the age of employees) is also not known unless the employee wishes to share such information. This poses challenges for successor planning and talent management, for example. In addition, the US knowledge-intensive workforce is generally perceived as individualist and ambitious, and it is rather easy for them to change jobs. The HR managers interviewed from the two companies think that in the US markets there can be certain short-term behavior. Employees value experiences and achievements, which is seen as a challenge for employers to hold on to this workforce. However, the HR managers note that the turnover in their companies has been relatively lower than within their respective industries in general (this could be because of location issues or may also be related to the opportunities, benefits, and company culture, etc.).

Team-level perceptions

Like in Finland, the team-level employees in the US in both industries acknowledge quite strongly that knowledge is within the people, highlighting knowledge *leaving risk* and problems in capturing (documenting and institutionalizing) tacit knowledge. The employees in the engineering company think that unwanted turnover causes both inconveniences and more serious problems as people in the unit are relatively few and everyone is focused on their own specific field. Similar issues apply to the ICT firm.

> …we don't have the luxury of being able to document things and have back-ups for everybody (Engineering company employee).

> It would definitely be a problem. There are so few of us; the knowledge base is very concentrated. But not so many have left (Engineering company employee).

> People are really important; there is so much tacit knowledge that cannot be in databases. It is the easiest way to know the latest information by asking others (ICT company employee).

In terms of the perceived criticality of *knowledge leaking*, team-level employees in both companies seemed to know what the question was about. Their comments indicate that knowing the limits of knowledge sharing is not an issue, but common sense suffices, and they mainly consider the leaking risk to be rather low. On the other hand, referring to common sense could indicate that limiting knowledge leaking is not based on education, but instead calls for employees' inner understanding and sense of responsibility. In particular, the employees think that such skills are required when competitors are included in the conversations.

> It's well understood that our technical data compiled is proprietary. Everybody knows you don't send drawings out to people who don't need them (Engineering company employee).

> For me it is common sense (Engineering company employee).

> It depends on the case. We can use our consideration in research (ICT company employee).

> That's not really an issue. The guys in the code committees would have to be a little bit more careful, because you're with your competitors and not suppliers there. But what we are doing, if we just send drawings to a supplier after he asked for a certain drawing and they're making this part for us, then its ok (Engineering company employee).

Management-level perceptions

At the management level within the engineering company, the *leaving* of key employees is seen as a great risk causing different types of problems. Like team-level employees, managers think there are not enough back-ups for everyone's expertise. Part of the criticality of knowledge leaving is that knowledge is spread in pieces, and is therefore difficult to retrieve. If key employees were to leave it would cause a serious time lag in terms of restoring the situation. However, even the managers do not seem to consider the risk of imitation (competitors hiring their employees) much; instead, they are mainly concerned with issues related to losing the accumulated knowledge. ICT company managers consider things mostly in the same vein, although they do not consider the risk to be quite as a high as in the engineering company since many employees had not yet left the relatively young organization at the time of the interviews. A manager noted that leaving cannot be completed prevented, and that the company just needs to learn how to deal with it. One space of dealing with it is documenting the knowledge in order to make such knowledge more explicit and restorable.

> If we lost that guy, we don't really have any backups. We have some people, but that knowledge will tend to be scattered around to five or six people who know a little individual piece because

> they have worked in a different design team… Much time is needed [to recover from a key employee leaving] (Engineering company manager).

> The main documents are in SharePoint. I think the bigger problem is that if somebody leaves, nobody is there working on it and it just stays there idle (ICT company manager).

For the management-level interviewees in the engineering company, *knowledge leaks* seem to be a reality, especially unintentional ones. There are even indications of some managers being doubtful about the knowledgeability of employees with regard to knowledge protection. Nevertheless, knowing the confidentiality requirements seems to be considered as belonging to the realm of common sense, and in general, managers believe that knowledge workers know their responsibilities in relation to knowledge protection. The managers recognize that many of the risks related to knowledge leaks are present when working with the suppliers (which was recognized as a risk on the team level as well). A management-level interviewee in the ICT company also acknowledges the challenges in drawing the lines in knowledge sharing. The interviewee seems to emphasize carefulness.

> It is not easy to know what and what not to share. Employees are important, but of course I feel there are leaks, even today… but I would say not on purpose (Engineering company manager).

> I believe for lab personnel there is no doubt regarding what can and what cannot be shared. I think everybody has common sense about what can and cannot be shared (Engineering company manager).

> Generally speaking, I don't think so [that there would be a good level of knowledge about confidentiality]; in R&D, maybe yes (Engineering company manager).

> We employ a need-to-know basis (ICT company manager).

Either the level of acknowledgement of confidentiality among the R&D personnel is not very well known to manager-level interviewees or the opinions vary. Thus, the perceptions of how well confidentiality is acknowledged on the team level are somewhat contradictory, which in fact is in line with the finding that confidentiality is not considered that high of a priority among many of the US team-level interviews.

5.3 Perceptions of leaking- and leaving-related knowledge risks in China

The HR managers in China think that, in general, employees have relatively more interest in career development and wishes related to being promoted and recognized. These internal ambitions match well with the multinational corporations' performance-based salary systems. Therefore, the engineering company prefers not to recruit freshly graduated students, but those who have been working already for a few years: they want not only to make sure that the applicant has the practical experience of working, but also to avoid employees using the company merely to build one's CV in order to advance in one's career.

Team-level perceptions

Regarding the *leaving risk*, the ICT company team-level interviewees acknowledge the dependency on key employees' knowledge, but they do not see it being as vital as in other

locations. There is some inconsistency in the excerpts, as some informants think that leaving causes trouble, whereas others believe that recovering just takes a while. The relatively smaller perceived risk level could also have something to do with the low turnover compared to the industry in general. However, the consensus however is that key employees leaving causes disruption.

> The role of employees is accentuated overall, -- but not many people have left (ICT company employee).

> Most work can be replaced with many documents and coding, it just means that another guy will spend time to get to know everything (ICT company employee).

Confidentiality issues and *knowledge leaking*, on the other hand, are acknowledged by the team-level interviewees as posing a moderate risk in both companies. Sometimes employees do not know if some information is confidential or not. Employees can rely on their superiors in case they are uncertain, but whether or not this happens is not always certain. Employees in the engineering company find the issue of confidentiality a real challenge, as open knowledge sharing is part of the culture. Employees mention using strict means to restrict access to certain files and folders as a necessary and often utilized way of managing leaking-related risk. The leaking risk seems to be perceived by the team-level employees as being slightly higher in China than in the other firm locations.

> Most things are...company confidential, I think most things, I think all of them, if there isn't any signed paper or something else, I couldn't tell it to anyone else (ICT company employee).

> If you don’t care about that then it’ll easily go outside. Because the people are so open, they feel that it is normal to share information (Engineering company employee).

Management-level evaluations

In terms of *leaving risk* and dependency on key people, the Chinese management-level interviewees of both companies very clearly acknowledge knowledge to be within the people and that leaving-related risk has a high impact. This in line with the managers in Finland and the US as well. The different cultural attitudes toward career planning, a small number of employees, and the limited chances to find and attract capable talent increase the vulnerability related to leaving risk, especially in the ICT company. According to the interviewees, loyalty levels toward one’s employer are not perceived to be very high in China in general, and interviewees note that it would be easy for their capable employees to change employers (even joining their competitors) without too much trouble. Thus we find the leaving-related risk to be perceived as being rather high in the Chinese units. The dependency on the tacit knowledge of key employees that is seen in all of the studied countries is even more emphasized in countries where turnover is faster and thus there is not enough time to transfer tacit knowledge, which is apparent in the comments of interviewees from both industries in China.

> If someone leaves, it is very difficult to find a replacement that is capable (Engineering company manager).

> Career planning is a lot more aggressive here (Engineering company manager).

> Attracting talent is challenging (ICT company manager).

> Even though China has a big population, this talent pool [competent employees in the exact field] is very small (Engineering company manager).

The manager-level interviewees of the engineering company in the unit in China are inconclusive about whether the policies related to *knowledge leaking* and confidentiality are clear to employees. They agree, like on the team level, that open knowledge sharing is part of the culture. One manager noted that while some people do not adequately acknowledge confidentiality issues, others with a background in business do understand it. A manager in the ICT company is not aware of any leaks happening, but thinks there is not much they could do about it anyway. This indicates rather high knowledge leaking risk perceptions in the Chinese units (even if such risks had not occurred in a harmful way at the time of the data collection).

> …they don't know what the negative side is when they share something. They are not aware of this. They don't do it on purpose, but they just don't understand the severity (Engineering company manager).

> I emphasize to Chinese colleagues that this is a risk, and it can be very expensive to the company and very negative if something leaks outside. Because here people don't know what is confidential and what is not…The culture is like that. They share everything (Engineering company manager).

6 Findings

Our examination reveals similarities and differences across the different organizational levels and firm locations with regard the perceived importance of HR-related knowledge risks. The empirical evidence indicates that *while leaking risk is mainly considered low or moderate in the Finnish and US units, it is considered higher on all levels in the Chinese organization*. On the other hand, the *leaving risk is considered to be moderate to high in all locations*. As leaving risk is perceived to be moderate to high on all levels and in all market areas as illustrated by the interviewees' highlighted reference to the impossibility of sufficient codification to sustain knowledge, we find that the tacit knowledge has a crucial role in the knowledge protection needs within both industries.

In addition to the country-related differences in the perceived risk of knowledge leaking, we can see some *mismatch between organizational levels*. This occurs especially *in Finland and the US with regard to knowledge leaking, and also occurs in terms of knowledge leaving in China*.

When taking a closer look at the reasons behind interviewees perceived risk levels, yet another set of diverging aspects can be found. Table 2 summarizes the main findings in terms of both where and what kinds of matches and mismatches we found. We discuss the details below.

Market	*FINLAND*		*THE US*		*CHINA*	
Org. levels	***Leaking***	***Leaving***	***Leaking***	***Leaving***	***Leaking***	***Leaving***
TEAM	LOW Well acknowledged (Engineering) Open or just negligent (ICT) *Mismatch*	MODERATE-HIGH *Match*	LOW-MODERATE Higher for code committees, otherwise low worry (Engineering) Taken seriously (ICT) *Mismatch*	MODERATE-HIGH *Match*	MODERATE-HIGH *Match*	MODERATE Worry limited to disruption *Mismatch*
MANAGER	LOW Naïve trust that they know without much education or following up (ICT)	MODERATE-HIGH	LOW-MODERATE-HIGH Not sure how well it is understood (Engineering) Well taken care of (ICT)	MODERATE-HIGH	MODERATE-HIGH	MODERATE-HIGH Loyalty on low levels + difficult to find and attract top talent. Imitation risk present with fierce competition for employees (Both)

Table 2 Matrix of the findings from empirical data examining the levels and countries

In addition to illustrating *what* types of differences are present, we are able to see *why* some differences (or similarities) emerge. There are differences between organizational levels in how the knowledge risks are perceived to occur, and in terms of the main problems related to unwanted knowledge leaving and leaking.

First, regarding the location-related differences, it seems that culture does play a role; that is, there are culture-based *appropriate conduct assumptions* that may explain these differences: informants note that knowledge sharing is considered a common norm in China, and dealing with this issue calls for specific action. Combined with the fact that employees leave easily and utilize all accumulated skills to advance their careers, there is a risk that competitors end up having and expropriating firm-specific knowledge assets. The esteemed role of higher managers in the Chinese culture (Su and Wrigth, 2012) might ease communicating the relevance of confidential knowledge to the employees, but Western managers may sometimes lack experience and readiness to use this approach (either because they approach these issues reactively, as a result of litigiousness being quite normal in their home countries, or because referring to legislation and taking tight control often is interpreted as accusatory rather than instructive). However, it may be that more restrictive mechanisms are needed than in many other locations. It may not suffice to give clear guidance on knowledge protection, and it may be necessary to adopt practices where knowledge is distributed on a need-to-know basis within firm boundaries. The weaker legal regimes and tendencies to avoid litigation also increase the need to draft adequate firm-

specific policies (McConnaghay, 2000; O'Donoghue and Croasdell, 2009). Knowledge leaving risks in the US and Finland seem to relate more to causing disruption than possibly enabling imitation, meaning that there are different *risk outcome assumptions* behind the level of evaluated leaving risk. In this case, it is increasing commitment and motivation (to maintain tacit knowledge in particular) rather than contractual remedies that are needed. However, in this respect, the normative environment is again different as suggested in the theoretical discussion and empirical examination.

Second, the organization-level differences are based on different aspects. Firstly, the leaving risks are seen as critical either because the competitive environment was turbulent, which causes challenges in terms of threat of imitation and replacement problems, or because leaving would make accomplishing the tasks more difficult. Whereas managers are more worried about the first reason, employees assess the criticality of leaving based on the latter reason more often. The *risk outcome assumptions* are therefore different as in the case of location differences. This aspect is most visible in the Chinese unit. Secondly, there are some differences with regard to the perceptions of capabilities to evaluate confidential knowledge correctly. We call the source of these differences *self-efficacy assumptions*. For example, whereas the risk of knowledge leaking is considered rather low in the Finnish units in general, there is some mismatch between the higher levels and the team level with regard to the underlying reasoning: the managers think these issues are already well understood by the employees, whereas at the team level, employees reveal that they share knowledge based on their own evaluations of the confidentiality of the knowledge. Problems might emerge if either managers or employees evaluate the capabilities of employees to assess the limits of confidential knowledge inaccurately. A similar example from the US data is that according to the team-level employees, the risk of knowledge leaking is rather low because they do not consider their work to involve confidential issues, whereas the managerial level is concerned about team-level awareness of the importance of confidential knowledge. Surely, in the US there are also signs of approaching internal knowledge exchange and outbound communication differently, but it is also left to the employees to decide what to disclose.

We think that while regional and cultural differences and organizational roles could explain some of the variation, there could also be more universal problems in the communication of confidentiality-related issues between the different organizational levels – especially in multinational companies (see Su and Wright, 2012; Yaula 2011). While there are some indications that securing confidential knowledge and prerequisites for innovation would be approached differently in different situations, it is not clear that this type of an approach would take into account specific features of each unit. This case-by-case type of misalignment could become costly, and therefore our study has some important contributions.

7 Conclusions

Our study increases the awareness and understanding of human resource management aspects that are often left in the shadows but regularly cause problems with regard to protecting future innovation (Delerue and Hamid, 2014; Bulgucu et al., 2010; Hannah and Robertson, 2014). We argue that it is important for companies to see the human resources as one key issue affecting the appropriability of innovation as it has to do with both sustaining the prerequisites of creativity and value creation (for example, the knowledge within the employees) and value capturing possibilities (e.g., trade secrets that have leaked out are no longer protected).

Our study contributes to existing knowledge by considering the challenges related to employee knowledge risks at different organizational levels and in different firm locations. While there are previous studies suggesting that management practices related to information security can be similar across different parts of multinational organizations (Anakwe et al., 2000; Igbaria, et al. 1995), opposing findings have also been introduced. Yaula (2011), for example, states that "neglecting the cultural and institutional differences may result in loss of resources, high employee turnover, and even increased security breaches." The matrix in table 2 generated in this paper illustrates how perceptions of knowledge leaking and leaving vary. Our study focuses not only on the observable differences, but also looks behind the similarities across organizational levels and locations. The findings indicate that the different perceptions of risk levels among managers and operational-level employees, as well as the differing underlying assumptions, mean that managers need to conduct a "reality check" every now and then. Based on these findings, we suggest that the two types of knowledge risks require different types of remedies in different countries even within the same corporation. This is further reinforced by the finding that even if the risk level is seemingly similar between managers and operational-level employees, the reason for this may not be that there is a consensus on the ways and importance of managing these risks across different organizational levels. Rather, this may be an indication of serious problems: if the reason for considering risk as low is due to negligence rather than confidence in skills in dealing with the risks, managers should be prepared to take action. Problems may escalate unnoticed when managers do not address the confidentiality risks thinking that they do not exist.

While we cannot tell based on our data whether managers or operative employees are right or wrong in having the perceptions they have for the reasons they have, the mismatch between different levels and between countries suggest that certain "strategic disintegration and discrimination," that is, informed variation in and adaptability of knowledge protection policies, is warranted. When managers talk about knowledge risks and managing such risks with employees, different communication and mechanisms are needed compared to discussions carried out among top management. It cannot be taken for granted that confidentiality is understood in the same way. Likewise, whereas strict restrictive mechanisms reducing knowledge leaking may be problematic in countries where empowerment of employees is central (see Hannah, 2005), in countries where authority is expected and appreciated, these may be quite imperative (Su and Wright, 2012). Without such informed disintegration it may be that the mismatches lead either to overprotection (e.g., managers impose too strong protection that inhibits knowledge sharing and therefore causes unnecessary problems for operative-level employees) or under-protection (e.g., managers are right about the knowledge risks, but falsely believe that employees have the same idea and ignore communication on these aspects).

Our study is limited by the fact that it was conducted in only two companies from two different industries. Therefore, further empirical work is needed to verify to what extent the differences are organization- or country-specific. Also, while we have shown that differences exist and suggested that having varying policies across levels and geographical areas of a multinational firm could be the solution to deal with these differences, our empirical study does not reveal the practical ways of implementing such a solution. We only can make assumptions, e.g., on the usability of different mechanisms in different countries. Nevertheless, we believe that we have been able to provide a basis for further studies bridging the gap between innovation, value creation and capture, knowledge sharing and protection, and human resources management, and hopefully we have provided tools for expanding the discussion to inter-firm collaboration (e.g., partners may not behave as expected with regard knowledge protection) and other contexts as well.

References

Ahuja, G., Lampert, C.M. and Novelli, E. (2013). The second face of appropriability: generative appropriability and its determinants, *Academy of Management Review*, 38, 2, 248–269.

Ajzen, I. (1991). The Theory of Planned Behavior, *Organizational Behavior and Human Decision Processes*, 50, 2, 179–211.

Anakwe, U.P., Igbaria, M. and Anandarajan, M. (2000). Management practices across cultures: Role of support in technology usage. *Journal of International Business Studies*, 31, 4, 653–666.

Arnett, J. J. (1995). Broad and narrow socialization: The family in the context of a cultural theory. *Journal of Marriage and the Family*, 57: 617–628.

Arrow, K. J. (1962). Economic welfare and the allocation of resources for invention. In *The Rate and Direction of Inventive Activity: Economic and Social Factors*, vol. 13, ed. R. R. Nelson, 609–25. NBER Special Conference Series. Princeton, NJ: Princeton University Press.

Arthur, J. B. (1994). Effects of human resource systems on manufacturing performance and turnover. *Academy of Management Journal*, 37, 3, 670–687.

Bévort, F., J.S. Pedersen, J.S. and Sundbo, J. (1995). Denmark, in I. Brunstein (ed.) *Human Resource Management in Western Europe, Berlin: Walter de Gruyter*, 31–58.

Brattsröm, A., Löfsten, H. , Richtnér, A. (2012). Creativity, trust and systematic processes in product development. *Research Policy*, 41, 743–755.

Brewster, C. (2004). European perspectives on human resource management. *Human Resource Management Review*, 14, 365–382.

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

Camelo-Ordaz, C., Garcia-Cruz, J., Sousa-Ginel, E. and Valle-Cabrera, R. (2011) The influence of human resource management on knowledge sharing and innovation in Spain: the mediating role of affective commitment, *International Journal of Human Resource Management*, 22, 7, 1442–1463.

Chiu, C.-Y., and Hong, Y. (2006). *Social Psychology of Culture*. New York: Psychology Press.

Chua, R.Y.J., Roth. Y. and Lemoine, J-F. (2014). The impact of culture on creativity: How cultural tightness and cultural distance affect global innovation crowdsourcing work. *Administrative Science Quarterly* (in Press).

Cohen, W.M., Nelson, R.R. and Walsh, J.P. (2000). Protecting their intellectual assets: Appropriability conditions and why U.S. manufacturing firms patent (or not). Working Paper 7552, National Bureau of Economic Research, Inc.

Corley, K. G. (2004). Defined by our strategy or our culture? Hierarchical differences in perceptions of organizational identity and change. *Human Relations*, 57, 9, 1145–1177.

Delerue, H., and Hamid, M. (2014). Who are these people? Personality traits and judgments about trade secret misappropriation in post-employment activities. *Business Ethics: A European Review* (in Press), doi: 10.1111/beer.12075.

Di Minin, A. and Bianchi, M. (2011). Safe nests in global nets: Internationalization and appropriability of R&D in wireless telecom. *Journal of International Business Studies*, 42, 910–934.

Duan, M. (2012). The role of formal contracts with weak legal enforcement: A study in the Chinese context. *Strategic Organization*, 10, 2, 158–186.

Fenton-O'Creevy, M. Gooderham, P. and Nordhaug, O. (2008). Human resource management in US subsidiaries in Europe and Australia: Centralisation or autonomy? *Journal of International Business Studies*, 39, 1, 151–166.

Franzosi, R.P. (2006) Content analysis, in *Handbook of Data Analysis*, eds. Hardy, M. and Bryman, A. Sage Publications Inc. Thousand Oaks, California.

Floyd, S. W., and Lane, P. J. (2000). Strategizing throughout the organization: Managing role conflict in strategic renewal. *Academy of Management Review*, 25, 1, 154–177.

Fuller, S. R., Edelman, L. B., and Matusik, S. F. (2000). Legal readings: Employee interpretation and mobilization of law. *Academy of Management Review*, 25, 1, 200–216.

Gelfand, M. J., Nishii, L.H. and Raver J. L. (2006). On the nature and importance of cultural tightness-looseness. *Journal of Applied Psychology*, 91, 1225–1244.

Gelfand, M. J., Raver, J. L. Nishii, L. Leslie, L. M., Lun, J., Lim, B. C., Duan, L. et al. (2011). Differences between tight and loose cultures: A 33-nation study. *Science*, 332: 1100–1104.

Geroski, P. A. (1995). Do spillovers undermine the incentive to innovate? In *Economic Approaches to Innovation*, ed. S. Dowrick, 76–97. Aldershot: Elgar.

Hall, P.A. and Gingerich, D.W. (2004). Varieties of capitalism and institutional complementarities in the macroeconomy, MPIfG Discussion paper 04/5, Berlin: Max Planck Institut für Gesellschaftsforschung.

Hall, P.A. and Soskice, D. (eds.) (2001). *Varieties of Capitalism: The Institutional Foundations of Comparative Advantage*. Oxford: Oxford University Press.

Hamill, J. (1983). The labor relations practices of foreign-owned and indigenous firms. *Employment Relations*, 5, 1, 14–16.

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, 1, 71–84.

Hannah D.R. and Robertson, K. (2014). Why and how do employees break and bend confidential information protection rules? *Journal of Management Studies* (in Press).

Herath, T. and Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness, *Decision Support Systems*, 47, 2, 154–165.

Hislop, D. (2003). Knowledge integration processes and the appropriation of innovations, *European Journal of Innovation Management*, 6, 3, 159-172.

Hofer-Alfeis, J. (2008). Knowledge management solutions for the leaving expert issue. *Journal of Knowledge Management*, 12, 4, 44–54.

Hurmelinna-Laukkanen, P. and Puumalainen, K. (2007). Nature and dynamics of appropriability: Strategies for appropriating returns on innovation, *R&D Management*, 37, 2, 95-110.

Husted, K and S Michailova (2010). Dual allegiance and knowledge sharing in inter-firm R&D collaborations. *Organizational Dynamics*, 39, 1, 37–47.

Husted, K., Michailova, S., & Olander, H. (2013). Dual allegiance, knowledge sharing, and knowledge protection: An empirical examination. *International Journal of Innovation Management*, 17, 6, 1340022-1-1340022-33.

Igbaria, M., Tor, G. and Gordon, B.D. (1995). Testing the determinants of microcomputer usage via a structural equation model. *Journal of Management Information Systems*, 13, 1, 127–143.

Kirschenbaum, A., and Mano-Negrin, R. (1999). Underlying labor market dimensions of "opportunities": The case of employee turnover. *Human Relations*, 52, 10, 1233–1255.

Levitt, B. and March, J.G. (1988) Organizational learning. *Annual Review of Sociology*, 14, 319–340.

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, 3, 623-663.

McConnaughay, P. (2000). Rethinking the role of law and contracts in east-west commercial relationships. *Virginia Journal of International Law*, 41, 2, 427–480.

McEvily, S.K. and Chakravarthy, B. (2002). The persistence of knowledge-based advantage: An empirical test for product performance and technological knowledge. *Strategic Management Journal*, 23, 285–305.

Minbaeva, D. (2005). HRM practices and MNC knowledge transfer, *Personnel Review*, 34, 1, 125-144.

Moen, J. (2005). Is mobility of technical personnel a source of R&D spillovers? *Journal of Labor Economics*, 2005, 23, 1, 81–114.

Ngo, H. Y., Lau, C. M., and Foley, S. (2008). Strategic human resource management, firm performance, and employee relations climate in China. *Human Resource Management*, 47, 1, 73–90.

O'Donoghue, N. and Croasdell, D.T. (2009). Protecting knowledge assets in multinational enterprises: A comparative case approach, VINE, 39, 4, 298–318.

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

Ronen, S. and Shenkar, O. (1985). Clustering countries on attitudinal dimensions: A review and synthesis. *Academy of Management Journal*, 10, 3, 435–454.

Silverman, D. (2005). *Doing Qualitative Research*. Sage Publications, Thousand Oaks, California.

Su, Z. X., and Wright, P. M. (2012). The effective human resource management system in transitional China: A hybrid of commitment and control practices. *The International Journal of Human Resource Management*, 23, 10, 2065–2086.

Vanhala, S. (1995). Human resource management in Finland. *Employee Relations*, 17, 7, 31–56.

Workman, M., Bommer, W. H., and Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24, 6, 2799–2816.

Yaula, A. (2011). Enforcing information security policies through cultural boundaries: A multinational company approach. European Conference on Information Systems, ECIS 2011 Proceedings. Paper 243. http://aisel.aisnet.org/ecis2011/243.

Yin, R.K. (2003) *Case Study Research, Design and Methods*, 3rd edition, Sage Publications, Thousand Oaks.