A Framework for Mitigating Leakage of Competitively Sensitive Knowledge in Start-ups

Research-in-Progress

Sam Pitruzzello
School of Computing & Information Systems
University of Melbourne, Parkville, Victoria
Email: spitruzzello@student.unimelb.edu.au

Atif Ahmad
School of Computing & Information Systems
University of Melbourne, Parkville, Victoria
Email: atif@unimelb.edu.au

Sean B. Maynard
School of Computing & Information Systems
University of Melbourne, Parkville, Victoria
Email: sean.maynard@unimelb.edu.au

Abstract

Knowledge leakage is a key risk for start-ups particularly when that knowledge relates to the firm's innovation and is therefore competitively sensitive. Leakage of competitively sensitive knowledge can lead to financial losses and erosion of competitive advantage. Start-ups are particularly vulnerable to knowledge leakage compared to mature enterprises since they have limited resources to devote to protective measures and information systems, rely on relatively fewer product lines to sustain business success, and experience greater organisational change making it difficult to control the complex and evolving security risk landscape. Current research on (knowledge) leakage mitigation methods do not adequately address the needs of start-ups. This paper sets out to address the gaps in current research relating to leakage mitigation particularly focusing on knowledge protection in start-ups. We propose a new knowledge-leakage mitigation framework, the Risk Window, as a precursor to a process model designed to assist start-ups to secure their competitively sensitive knowledge.

Keywords: information security, information systems, innovation, knowledge leakage, start-ups

1 Introduction

Knowledge leakage is a key risk for start-ups particularly when knowledge is competitively sensitive (Ahmad et al. 2014; Olander et al. 2011). Knowledge leakage is the gradual outflow and loss of sensitive organisational knowledge to unauthorised parties as a result of deliberate or intentional actions (Ahmad et al. 2014). While knowledge management systems are a class of information systems (Alavi & Leidner (2001), challenges persist in protecting the tacit knowledge held in people's minds when they leave the organisation (Olander et al. 2011). Since competitively sensitive knowledge is closely linked to firm performance, leakage can lead to financial losses and competitive erosion (Desouza 2006). Therefore, mitigating knowledge leakage is a critical management practice, however it is expensive and requires significant resources (Ahmad et al. 2015; Manhart and Thalmann 2015; Shedden et al. 2010).

Unfortunately, many start-ups do not have adequate resources to protect knowledge so they are particularly vulnerable to leakage (Olander et al. 2011). The challenges faced by start-ups are not limited to lack of resources and they differ from an organisational structure compared to large companies. First, they normally have a small number of product lines exposing them to business risks if competitors beat them to the market with similar offerings (Gans and Stern 2003; Olander et al. 2011). Second, start-ups are young and experience rapid change over short time frames (Blank 2013; Ries 2011). Third, they are or have the potential to be, high growth businesses and normally require external sources of capital to fund growth (Blank 2013; Freeman and Engel 2007). Fourth, failure rates for start-ups are considerably higher than mature enterprises (Shane 2009). Finally, start-ups play an important role in advanced knowledge-based economies, are a source of innovation and contribute to employment (Aspelund et al. 2005; Blank 2013). Research estimates that the economic impact in the USA as a result of cyber-espionage and trade secret theft is in the order of hundreds of billions of dollars (Blair et al. 2017). Since start-ups have poor information systems and knowledge security practices (Gupta and Hammond 2005), they face the same serious threats. In fact, many innovative firms of all sizes are direct targets of international espionage activities (Blair et al. 2013). Therefore, more research is needed to address the gaps and issues confronting start-ups relating to knowledge leakage. This research-in-progress paper asks the question: *How can start-ups mitigate leakage of competitively sensitive knowledge?*

In addition to this research question, determining what information start-ups require to make the right decisions on protecting their knowledge and how IS can support decision making is important. To answer these questions, a risk lens is applied to knowledge protection in start-ups. This paper is a scoping study for a research project that aims to develop a knowledge leakage mitigation process and contribute to knowledge leakage theories. This paper is structured as follows. The next section outlines the research methodology used in this paper followed by a literature review. The literature review provides the basis for developing a leakage mitigation framework (LMF) covered in the discussion section. Finally, an overview of this research project is presented followed by concluding remarks.

2 Research Methodology

The literature search initially focused on the search term 'start-ups AND knowledge leakage'. Since knowledge leakage is particular to research intersecting the fields of knowledge management and information security and used in only a few papers (Ahmad et al. 2014; Olander et al. 2011), the search criteria was expanded to include broader search terms. A variety of databases including ACM Digital Library, Compendex and Scopus were searched using the following terms – 'start-ups AND knowledge management', 'start-ups AND innovation', 'start-ups AND IP protection' and 'start-ups AND knowledge leakage' and 'start-ups AND information security'. These searches resulted in over one thousand papers. To reduce the number of articles, two filters were applied. First, papers were limited to those published since the year 2000. Secondly, papers were sorted on citation count from highest to lowest. This resulted in a short-list of 67 papers. A summary of the search results is provided in Table 1 below.

Search Term	**Total Papers**	**No. of papers after filters applied**
Start-ups AND innovation	760	32
Start-ups AND knowledge management	376	24
Start-ups AND information security	15	5
Start-ups AND IP protection	10	4
Start-ups AND knowledge leakage	5	2

TOTAL	**1,166**	**67**

Table 1 – Summary of Search Results

These short-listed papers were then further analysed with a focus on knowledge leakage theories and knowledge protection from an organisational process perspective. This analysis aligns with the main aim of this paper - to develop a leakage mitigation framework (LMF). The final result is the inclusion of 34 research papers in the literature review.

3 Literature Review

The review begins with a theoretical background on knowledge leakage followed by innovation in start-ups. The topics of knowledge leakage and knowledge protection in start-ups are then covered. Table 2 below summarises the key themes from the 34 research articles included in this paper.

Research Article	Key Themes
Acs et al. (2009), Alavi & Leidner (2001), Clarysse et al. (2011), Gompers et al. (2005), Nonaka (1994)	Theories on knowledge management and leakage including knowledge spill-over theory, knowledge transfer through mobility and knowledge management processes
Baum & Silverman (2004), Blank (2013), Bosma et al. (2004), Cohen & Levinthal (1990), Denning & Dunham (2006), Freeman & Engel (2007), Hsu (2006), Park (2005), Rehm et al. (2016), Ries (2011), Van de Ven (2005)	Start-up innovation processes in practice and success factors such as initial resources, funding and inherent qualities.
Christensen (1997), Rogers (1962), Tushman & Anderson (1986)	Seminal works on innovation process and its disruptive impacts
Ahmad et al. (2014), Amara et al. (2008), Bidault & Castello (2010), Cornish (2004), Desouza (2006), Desouza & Vanapalli (2005), Gupta & Hammond (2005), Hannah (2005), Hertzfeld et al. (2006), Lee et al. (2007), Manhart & Thalmann (2015), Molok at al. (2010), Olander et al. (2011), Shih & Wang (2013), Synder & Crescenzi (2009)	Knowledge leakage and knowledge protection in practice

Table 2 – Summary of Literature Review

3.1 Theoretical Background

The review revealed a body of literature covering theories that discuss knowledge leakage. This includes entrepreneurial spawning that investigates the origins of entrepreneurs, the knowledge spill-over theory of entrepreneurship and knowledge transfer through knowledge worker mobility (Acs et al. 2009; Clarysse et al. 2011; Gompers et al. 2005). While this research argues that experience and cumulative knowledge of entrepreneurs largely dictate a start-ups potential for success, they discuss employee mobility between firms and how this activity causes knowledge leakage, loss and gain. This research is largely silent on the application of IS in managing knowledge leakage since they are business focused studies. However, IS features prominently in knowledge management research and it provides insights into knowledge leakage. Knowledge management research is vast with seminal works by Alavi and Leidner (2001) and (Nonaka 1994). Alavi and Leidner's literature review investigated knowledge management from an organisational process view, which consists of four main components – knowledge creation, knowledge storage/retrieval, knowledge transfer, and knowledge application. While not specifically focusing on knowledge protection or leakage, the negative impacts companies have experienced as the result of losing key employees are highlighted (Alavi and Leidner 2001, p. 113).

3.2 Innovation Processes in Start-ups

Research on innovation is vast and there are many seminal works on its diffusion and disruptive impact (Christensen 1997; Rogers 1962; Tushman and Anderson 1986). The literature on start-ups covers a variety of themes the most common being venture capital and initial resources (Baum and Silverman 2004; Hsu 2006). This research discusses the endowments inherent or bestowed on the entrepreneur and their start-up venture. In addition, research on start-ups centres on innovation and their entrepreneurs who have unique qualities and the ability to exploit new knowledge (Cohen and Levinthal 1990; Denning and Dunham 2006; Park 2005). While research on innovation and entrepreneurship has become intertwined (Denning and Dunham 2006; Park 2005; Shane and

Venkataraman 2000) it is important to differentiate between each concept. Innovation can be defined as "the combination of technology with market need to create a profitable opportunity" (Park 2005, p. 744, p. 744) and is knowledge intensive, reliant on networks and becoming less of an individual pursuit in creativity (Denning 2004; Van de Ven 2005). Entrepreneurship is the "how, by whom, and with what effects opportunities to create future goods and services are discovered, evaluated, and exploited" (Shane and Venkataraman 2000). There are many models claiming to be the right way to innovate including the highly regarded lean start-up approach (Blank 2013; Park 2005; Ries 2011). Prior to commercialisation, there are three main innovation phases – opportunity recognition (Bosma et al. 2004; Park 2005), innovation building (Blank 2013; Hsu 2006) and networking (Rehm et al. 2016; Van de Ven 2005). Information systems have been identified as valuable assets in innovation and building networks since they allow efficient management of information in a knowledge-intensive environment (Rehm et al. 2016; Van de Ven 2005).

Opportunity recognition involves exploiting trends in technology and markets (Bosma et al. 2004; Park 2005). Entrepreneurs typically apply their knowledge, experience and skills to identify and evaluate the commercial potential of an idea. While opportunity recognition involves the entrepreneurial mind, it does not cover how to develop products or build a business. This is covered in the second phase, innovation building, and involves building technology teams, sourcing funds and creating prototypes or minimal viable products (MVP). MVPs are early stage products offered to customers to obtain feedback for further improvements and development (Blank 2013; Ries 2011). Getting an innovation to the MVP stage requires resources, the most important being money. Attracting venture capital (VC) during the early stages of a start-up's life is difficult since VC's tend to fund mature start-ups or entrepreneurs with a history of success (Freeman and Engel 2007; Hsu 2006). Therefore many entrepreneurs turn to friends, family and angel investors to seed their start-up (Hsu 2006). Once funds have been raised and MVPs built, the next phase is networking which requires collaborative partnerships (Rehm et al. 2016; Van de Ven 2005). Unfortunately, sharing knowledge with external parties increases knowledge leakage risks (Bidault and Castello 2010; Shih and Wang 2013).

3.3 Knowledge Leakage in Start-ups

While knowledge leakage is detrimental to organisations impacting on profitability and competitiveness (Ahmad et al. 2014; Olander et al. 2011), there is scant literature on its effects on start-ups. The loss of competitively sensitive knowledge to rivals provides them with an opportunity to steal market share and imitate products and services (Snyder and Crescenzi 2009). Knowledge can leak in many ways including employees inadvertently or intentionally divulging knowledge to outsiders, staff turn-over particularly when key employees join a competitor and external collaboration (Desouza and Vanapalli 2005; Molok et al. 2010; Olander et al. 2011). Intentional and targeted efforts such as industrial espionage pose the greatest challenges since the perpetrators are highly motivated for financial and economic reasons (Amara et al. 2008; Snyder and Crescenzi 2009). Information systems are commonly targeted by cyber-criminals and the proliferation of mobile devices, social media and cloud computing exacerbates the problem of knowledge leakage (Ahmad et al. 2014; Snyder and Crescenzi 2009).

Start-ups do not have adequate resources to put in place adequate knowledge protection measures making them vulnerable to knowledge leakage (Gupta and Hammond 2005; Olander et al. 2011). However, the challenges faced by start-ups in mitigating leakage are not limited to lack of resources. Start-ups normally have only one product line (Gans and Stern 2003) so if competitors beat them to the market with similar or improved offerings, loss of revenue and profits can be disastrous. In addition, the attitudes around IS and IS security suggest that complacency may play a role due to perceived low chances of being targeted by cyber-criminals or malicious employees and greater concerns over viruses and malware (Gupta and Hammond 2005). Mitigating knowledge leakage is time consuming, expensive and can be seen as a distraction from a start-ups' core activities (Cornish 2004; Olander et al. 2011). Compounding the issues faced by start-ups is the small number of employees that hold valuable knowledge. Losing these employees can have a greater impact on a start-up compared to a large enterprise where knowledge is dispersed throughout the organisation (Olander et al. 2011).

3.4 Knowledge Protection in Start-ups

There is ample literature on knowledge protection methods and strategies. Knowledge protection methods are implemented to increase barriers to imitation and in partnerships to protect important competitive knowledge (Amara et al. 2008; Hertzfeld et al. 2006; Manhart and Thalmann 2015). Knowledge protection methods can be classified into two main categories - formal and informal.

Formal methods offer legal protections such as patents, trademarks, copyright, trade secrets and design registrations while informal methods lack legislative protections and include design complexity, confidentiality agreements and lead-time advantage (Amara et al. 2008; Hannah 2005; Olander et al. 2011). Counter-intelligence methods can also be employed to minimise knowledge leakage (Desouza and Vanapalli 2005; Olander et al. 2011). As discussed earlier, networking is important for innovation yet it increases the risks of knowledge leakage (Bidault and Castello 2010; Shih and Wang 2013). To maximise the success of networking initiatives, partners should adopt a range of knowledge protection measures and establish common ground with agreements that detail the assets, resources and knowledge that each partner will bring to the alliance (Hertzfeld et al. 2006; Lee et al. 2007). Importantly, there is a lack of research into the role of IS artefacts in knowledge protection (Manhart and Thalmann 2015). It is therefore imperative that this gap is addressed particularly when developing practical solutions and contributing to the body of research on knowledge protection.

Amara et al. (2008) developed a knowledge protection framework from empirical research conducted on knowledge-intensive companies. The researchers made a significant contribution to the problem of determining suitable knowledge protection methods based on different types of knowledge. The framework, while not a comprehensive IS artefact, allows the selection of knowledge protection methods based on the nature of the innovation – that is whether it is tangible or intangible and whether the embedded knowledge is codified or tacit. The knowledge protection framework is relevant to this project since it based on knowledge-intensive businesses with a focus on small to medium companies (SMEs). While the framework makes clear distinctions on the type of protection methods suited to the nature of an innovation, it does not provide guidelines on how or when to apply the measures. Furthermore, it does not consider the people perspective and organisational processes required to secure knowledge. It primarily focuses on the end product/service. Securing organisational knowledge needs to occur at three levels – product, process and people (Desouza 2006; Desouza and Vanapalli 2005). In essence, securing knowledge from leakage is an information systems and knowledge management problem with a strong link to organisational processes and the behaviour of people within and external to the organisation.

3.5 Summary

The literature review yielded assumptions about knowledge leakage in start-ups. The first is that knowledge leakage risks do not change over time (Amara et al. 2008; Hannah 2005; Olander et al. 2011). The second assumption is that people are always involved knowledge leakage (Ahmad et al. 2014; Desouza 2006; Shedden et al. 2009). Third, start-ups do not have resources to adequately minimise knowledge leakage risks (Gupta and Hammond 2005; Olander et al. 2011). Finally, there are two types of knowledge protection methods, formal and informal, and applying them will protect knowledge (Amara et al. 2008; Olander et al. 2011). These assumptions highlight the need for a holistic framework – one that includes product-process-people, provides guidelines on how and when to apply knowledge leakage mitigation methods and is simple to apply in a start-up environment.

4 Discussion

4.1 Role of IS in Protecting Knowledge

The literature review touched on some issues relating to the role of IS in knowledge protection. This section provides further discussion on this topic and covers research that focused on the role of IS in managing and protecting organisational knowledge. To begin with, it was found that research in knowledge protection largely neglects IS as an artefact since he field is firmly planted in strategic management (Manhart and Thalmann 2015). This is an important research gap that needs to be addressed since artefacts provide organisations with tools and guidelines. Extending the idea of artefacts to the application of IS security strategy, Gupta & Hammond (2005) suggest that many SMEs find it challenging to create a comprehensive IS security strategy so there is a tendency for them to cut corners. While taking short cuts is normal in business, the authors argue that it is important to know where and how to cut corners since making the wrong decisions can be costly.

Rehm et al. (2016) provide research into the role of IS in managing and protecting knowledge in innovation networks. The authors suggest that IS can be used in three main ways. First, IS can facilitate the building of trusting and reliable partnerships. Secondly, IS enables the integration of value contributions from each partner, thereby providing a level of protection for individual/organisational ownership of knowledge. Finally, IS allows the coordination of innovation processes. While this point is more of an integrity issue, it is relevant and relates to the management and protection of knowledge.

4.2 Developing a Leakage Mitigation Framework (LMF)

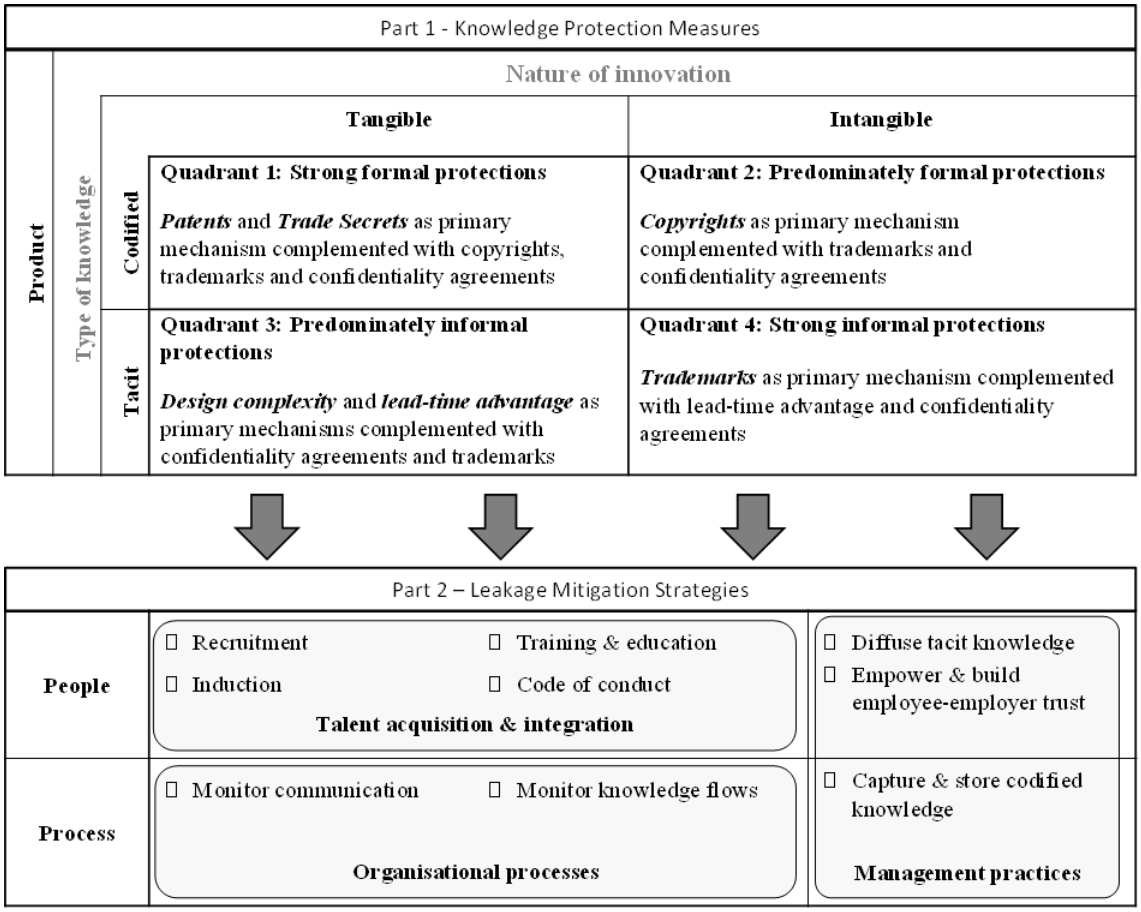

Figure 1: The Leakage Mitigation Framework (Adapted from Amara, et al., 2008)

Start-ups experience dramatic change as they develop innovations, hire employees, turnover staff and collaborate with external organisations (Blank 2013; Freeman and Engel 2007). This suggests that knowledge embedded in a start-up's innovation diffuses to the outside world leading to an important insight – knowledge leakage risks vary over time as innovation progresses through its phases. Therefore, applying a risk lens to knowledge protection requires a holistic framework that can be applied during each innovation phase. To build the LMF (Figure 1), Amara's knowledge protection framework is applied first. The second part of the LMF includes a set of knowledge leakage mitigation strategies. These knowledge leakage mitigation strategies are organisational processes and human resource considerations drawn from the literature review. Strategies include capturing codified knowledge, diffusing tacit knowledge, recruitment, induction programs, information security training and education, monitoring activities and building employer-employee trust (Ahmad et al. 2014; Hannah 2005; Olander et al. 2011). To ensure organisational trust, monitoring activities should include competitive intelligence and surveillance of external parties rather than monitoring internal staff.

The knowledge leakage mitigation strategies are grouped into three categories – talent acquisition and integration including induction programs, organisational processes that involve monitoring activities and people-centred knowledge and general management practices. Amara's original knowledge protection framework has been modified to include descriptive categories for each quadrant. The first quadrant, '*Strong formal protections*', applies to tangible innovations with high levels of codified knowledge. The second quadrant, '*Predominate formal protections*', suit innovations that are intangible and mainly consist of codified knowledge. Quadrant 3, '*Predominate informal protections*' relate to tangible innovations with tacit embedded knowledge. Finally, the fourth quadrant, '*Strong informal protections*', applies to innovations that are intangible and mainly consist of tacit knowledge.

4.3 Applying the LMF

Applying the LMF involves two steps. First, it is necessary to determine which quadrant in the knowledge protection framework the innovation fits best – is it tangible or intangible and is the

embedded knowledge codified or tacit? For example, if an innovation is tangible and knowledge codified, protection methods in the first quadrant apply – patents complemented with copyright, trademarks and confidentiality agreements. An innovation can sit in more than one quadrant if there is a mix of tangible and intangible products and knowledge is codified and tacit. The quadrant where the innovation lies normally does not change during the lifecycle of an innovation.

The second step requires deciding on organisational processes and people strategies to minimise leakage. This step is applied at each innovation phase and reviewed during times of change. This contrasts to the first step where the selection of knowledge protections is fixed. For example, during the first phase, opportunity recognition, very few people would be employed therefore managing knowledge flows is simple exercise. However, during the networking phase, the start-up would have hired staff, experienced employee turnover and released early product versions. Therefore, knowledge of the innovation will be in hands and minds of many more people increasing the risk that knowledge has leaked so it is prudent to implement leakage mitigation strategies during the latter innovation phases.

5 Future Research

This research project aims to develop a new knowledge protection process (KPP) for use in start-ups and to contribute to the body of research on knowledge leakage. The KPP will be developed from the LMF presented in this paper. An important output from the research will be an IS artefact therefore a design science approach will be used since it provides a process for creating artefacts for use in practice (March and Smith 1995; Venable and Baskerville 2012). Furthermore, design science will improve the chances of a successful outcome – adoption of the KPP. Two primary research methods for data collection are relevant in this project – action research and case studies. It is anticipated that action research may be onerous and too great an impost for the typical start-up so case studies may be more suitable. Conducting case study research with multiple organisations will provide valuable information and insights to develop the KPP. Between eight and twelve case studies are needed to adequately support the research questions (Neuman 2012; Yin 2013).

Start-ups located in Australia will be focus of this research project. Australia has a vibrant start-up eco-system particularly in the biotechnology and software industries. Start-ups to be targeted for inclusion in this research project will ideally be no older than six years and have been in existence for at least three years. Limiting the study to this group will ensure that participants have made good progress with developing their innovations and are more likely to have clients and conducted initial market tests. Case study participants will be engaged early next year. Before engaging the participants, a set of questionnaires will be designed from research in the fields of innovation, information security, knowledge protection and knowledge management. Furthermore, this research project will contribute to the fields of innovation and knowledge leakage particularly in relation to knowledge-intensive start-ups where there has been limited research to date.

6 Conclusion

Ensuring that innovation is not eroded due to the leakage of sensitive knowledge is a critical concern for start-ups. Unfortunately, there are many ways that knowledge can leak to the outside world and start-ups are particularly vulnerable to knowledge leakage. It is crucial that start-ups have a clear understanding of what valuable knowledge assets are embedded in their innovation and people. While most research assumes that knowledge leakage risks are constant, this paper argues that leakage risks vary during the innovation process. This paper set out to answer the research question – *How can start-ups mitigate leakage of competitively-sensitive knowledge?* This question has been answered by proposing a leakage mitigation framework (LMF). The LMF will be applied during the research project to develop a new knowledge protection process (KPP). The KPP needs to be suitable for start-ups while saving them time and resources leading to better outcomes. Contributions have been made to the body of research on knowledge leakage, how leakage risks vary during innovation processes and the effect leakage has on start-ups.

7 References

Acs, Z. J., Braunerhjelm, P., Audretsch, D. B., and Carlsson, B. 2009. "The Knowledge Spillover Theory of Entrepreneurship," *Small business economics* (32:1), pp. 15-30.

Ahmad, A., Bosua, R., and Scheepers, R. 2014. "Protecting Organizational Competitive Advantage: A Knowledge Leakage Perspective," *Computers & Security* (42), pp. 27-39.

Ahmad, A., Maynard, S. B., and Shanks, G. 2015. "A Case Analysis of Information Systems and Security Incident Responses." Elsevier B.V., p. 717.

Alavi, M., and Leidner, D. E. 2001. "Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues," *MIS quarterly*), pp. 107-136.

Amara, N., Landry, R., and Traore, N. 2008. "Managing the Protection of Innovations in Knowledge-Intensive Business Services," *Research Policy* (37), pp. 1530-1547.

Aspelund, A., Berg-Utby, T., and Skjevdal, R. 2005. "Initial Resources' Influence on New Venture Survival: A Longitudinal Study of New Technology-Based Firms," *Technovation* (25:11), pp. 1337-1347.

Baum, J. A., and Silverman, B. S. 2004. "Picking Winners or Building Them? Alliance, Intellectual, and Human Capital as Selection Criteria in Venture Financing and Performance of Biotechnology Startups," *Journal of business venturing* (19:3), pp. 411-436.

Bidault, F., and Castello, A. 2010. "Why Too Much Trust Is Death to Innovation," *MIT Sloan Management Review* (51:4), p. 33.

Blair, D., Huntsman Jr, J. M., Barrett, C., Gordon, S., Lynn III, W. J., WinceSmith, D., and Young, M. K. 2013. "The Ip Commission Report: The Report of the Commission on the Theft of American Intellectual Property," *The National Bureau of Asian Research*).

Blair, D., Huntsman Jr, J. M., Barrett, C., Gordon, S., Lynn III, W. J., WinceSmith, D., and Young, M. K. 2017. "Update to the Ip Commission Report: The Report of the Commission on the Theft of American Intellectual Property," *The National Bureau of Asian Research*).

Blank, S. 2013. "Why the Lean Start-up Changes Everything," *Harvard Business Review*), pp. 63-72.

Bosma, N., Van Praag, M., Thurik, R., and De Wit, G. 2004. "The Value of Human and Social Capital Investments for the Business Performance of Startups," *Small Business Economics* (23:3), pp. 227-236.

Christensen, C. M. 1997. *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*. Boston: Harvard Business School Press.

Clarysse, B., Wright, M., and Van de Velde, E. 2011. "Entrepreneurial Origin, Technological Knowledge, and the Growth of Spin-Off Companies," *Journal of Management Studies* (48:6), pp. 1420-1442.

Cohen, W. M., and Levinthal, D. A. 1990. "Absorptive Capacity: a New Perspective on Learning and Innovation," *Administrative Science Quarterly* (35:1), pp. 128-152.

Cornish, W. R. 2004. *Intellectual Property: Omnipresent, Distracting, Irrelevant?* Oxford University Press on Demand.

Denning, P. J. 2004. "The Social Life of Innovation," *Communications of the ACM* (47:4), pp. 15-19.

Denning, P. J., and Dunham, R. 2006. "Innovation as Language Action," *Communications of the ACM* (49:5), pp. 47-52.

Desouza, K. C. 2006. "Knowledge Security: An Interesting Research Space," *Journal of Information Science and Technology* (3:1), pp. 1-7.

Desouza, K. C., and Vanapalli, G. K. 2005. "Securing Knowledge in Organizations: Lessons from the Defense and Intelligence Sectors," *International Journal of Information Management* (25:1), pp. 85-98.

Freeman, J., and Engel, J. S. 2007. "Models of Innovation: Start-Ups and Mature Corporations," *California Management Review* (50:1), pp. 94-119.

Gans, J. S., and Stern, S. 2003. "The Product Market and the Market for “Ideas”: Commercialization Strategies for Technology Entrepreneurs," *Research policy* (32:2), pp. 333-350.

Gompers, P., Lerner, J., and Scharfstein, D. 2005. "Entrepreneurial Spawning: Public Corporations and the Genesis of New Ventures, 1986 to 1999," *Journal of Finance* (60:2), pp. 577-614.

Gupta, A., and Hammond, R. 2005. "Information Systems Security Issues and Decisions for Small Businesses," *Information Management & Computer Security* (13:4), pp. 297-310.

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), pp. 71-84.

Hertzfeld, H. R., Link, A. N., and Vonortas, N. S. 2006. "Intellectual Property Protection Mechanisms in Research Partnerships," *Research Policy* (35:6), pp. 825-838.

Hsu, D. H. 2006. "Venture Capitalists and Cooperative Start-up Commercialization Strategy," *Management Science* (52:2), pp. 204-219.

Lee, S.-C., Chang, S.-N., Liu, C.-Y., and Yang, J. 2007. "The Effect of Knowledge Protection, Knowledge Ambiguity, and Relational Capital on Alliance Performance," *Knowledge and Process Management* (14:1), pp. 58-69.

Manhart, M., and Thalmann, S. 2015. "Protecting Organizational Knowledge: A Structured Literature Review," *Journal of Knowledge Management* (19:2), pp. 190-211.

March, S. T., and Smith, G. F. 1995. "Design and Natural Science Research on Information Technology," *Decision support systems* (15:4), pp. 251-266.

Molok, N. N. A., Ahmad, A., and Chang, S. 2010. "Understanding the Factors of Information Leakage through Online Social Networking to Safeguard Organizational Information," *Proceedings of the 21st Australasian Conference on Information Systems*.

Neuman, W. L. 2012. "Basics of Social Research: Qualitative and Quantitative Approaches,").

Nonaka, I. 1994. "A Dynamic Theory of Organizational Knowledge Creation," *Organization science* (5:1), pp. 14-37.

Olander, H., Hurmelinna-Laukkanen, P., and Heilmann, P. 2011. "Do Smes Benefit from Hrm-Related Knowledge Protection in Innovation Management?," *International Journal of Innovation Management* (15:3), pp. 593-616.

Park, J. S. 2005. "Opportunity Recognition and Product Innovation in Entrepreneurial Hi-Tech Start-Ups: A New Perspective and Supporting Case Study," *Technovation* (25), pp. 739-752.

Rehm, S.-V., Goel, L., and Junglas, I. 2016. "Information Management for Innovation Networks - an Empirical Study on The "Who, What and How" In Networked Innovation," *International Journal of Information Management* (26), pp. 348-359.

Ries, E. 2011. *The Lean Startup*. New York: Crown Business.

Rogers, E. M. 1962. *Diffusion of Innovations*. New York: Free Press of Glencoe.

Shane, S. 2009. "Why Encouraging More People to Become Entrepreneurs Is Bad Public Policy," *Small business economics* (33:2), pp. 141-149.

Shane, S., and Venkataraman, S. 2000. "The Promise of Entrepreneurship as a Field of Research," *Academy of management review* (25:1), pp. 217-226.

Shedden, P., Ahmad, A., and Ruighaver, A. 2010. "Organisational Learning and Incident Response: Promoting Effective Learning through the Incident Response Process,").

Shedden, P., Smith, W., Scheepers, R., and Ahmad, A. 2009. "Towards a Knowledge Perspective in Information Security Risk Assessments–an Illustrative Case Study," *Proceedings of the 20th Australasian Conference on Information Systems*, pp. 74-84.

Shih, W. C., and Wang, J.-C. 2013. "Will Our Partner Steal Our Ip?," (91), pp. 137-141.

Snyder, H., and Crescenzi, A. 2009. "Intellectual Capital and Economic Espionage: New Crimes and New Protections," *Journal of Financial Crime* (16:3), pp. 245-254.

Tushman, M. L., and Anderson, P. 1986. "Technological Discontinuities and Organizational Environments," *Administrative Science Quarterly* (31:3), pp. 439-465.

Van de Ven, A. H. 2005. "Running in Packs to Develop Knowledge-Intensive Technologies," *MIS Quarterly* (29:2), pp. 365-378.

Venable, J., and Baskerville, R. 2012. "Eating Our Own Cooking: Toward a More Rigorous Design Science of Research Methods," *Electronic Journal of Business Research Methods* (10:2), pp. 141-153.

Yin, R. K. 2013. *Case Study Research: Design and Methods*. Sage publications.

Acknowledgements

To my supervisors Dr Atif Ahmad and Dr Sean Maynard for their contribution. To my colleague and fellow PhD student Abdulaziz Murad for his honest feedback. To my wife Sarina and daughter Siena for their never-ending patience and support.

Copyright