GUIDE TO SRMBOK

INTELLECTUAL ASSETS

The Security Risk Management Body of Knowledge (SRMBOK) was developed as an initiative of the Risk Management Institution of Australasia Limited (RMIA) in conjunction with Jakeman Business Solutions Pty Ltd (JBS), which provided the lead authors and financially underwrote its publication.

SRMBOK was written to contribute to the identification and documentation of agreed better practice in Security Risk Management. Copies of SRMBOK can be purchased from www.amazon.com

SRMBOK is also supported by many *Guides to SRMBOK* written by independent security professionals that provide more detailed guidance and examples of how the SRMBOK framework can be applied in practice. Whilst each of these Guides is peer reviewed prior to publication, any opinions and views expressed are those of the authors and do not necessarily reflect the opinion of RMIA or JBS.

Security Risk Management

Body of Knowledge

Authors

Paul Curwell — **TOWER Australia**

Paul is a fraud and security specialist with Booz Allen Hamilton's Strategic Security Practice. Specialising in the management of Economic Crime risks with a focus on Financial Crime, Intellectual Property, Proprietary Information and Identity Crime matters, Paul applies his specialist background and knowledge to improve enterprise resilience by reducing corporate loss and managing risk exposure whilst ensuring that competitive advantage is maintained.

Paul has assisted numerous government agencies and private sector companies with specialist advice concerning Fraud and Security from the perspective of strategic risk and planning activities. Paul has previously undertaken related appointments in the Biotechnology, R&D Strategy, Government, Aerospace, Banking, and Finance sectors.

Dr. Damian Hine — THE UNIVERSITY OF QUEENSLAND

In his academic role at the UQ Business School, University of Queensland, Damian has published extensively on entrepreneurship and innovation, as well as intellectual capital issues. He writes on firm based perspectives in international journals and is on the editorial board of a number of international entrepreneurship journals. Damian has recently co-authored a book entitled Innovation and Entrepreneurship in Biotechnology. He is also co-editor of Innovative Methodologies in Enterprise Research.

Damian can be contacted via email at d.hine@uq.edu.au.

Contents

1. INTRODUCTION

1.1. Background

Intellectual assets (IAs) can exist in a variety of forms, though they are all based upon the generation, capture and protection of valuable knowledge. Their foundation is fragile, as it is dependent upon the transition from tacit knowledge possessed by an individual, into the organisation with which they are associated. The organisation must then convert that knowledge into valuing creating processes, products or practices. While intellectual property (IP) is not the only form of IA, it is the most obvious and the most tangible.

A diverse range of criminal and commercial activities threaten the viability of knowledge dependent companies and organisations. At least three separate surveys, all conducted by experienced consulting bodies around the world, serve to highlight the threats to IA's[1].

The scale of the current impact of these threats on business is considerable and growing - one in five respondents to the Kroll Corporate IP Abuse survey indicated losses exceeding US$1million, including one suffering a loss of over US$200million from IP infringements alone[2]. The American Society for Industrial Security (ASIS) 2002 "Trends in Proprietary Information Loss Report" estimates total losses in IP revenue from companies participating in the survey at between US$53 and US$59billion in the year 2001[3]. This worrying situation is further exacerbated by reports from the Kroll survey that "43 percent of patent owners characterised the calculation of their companies IP valuation as 'just a guess" illustrating the difficulties experienced by managers in defining and valuing intellectual assets under current accounting standards[4].

The inability to identify and quantify more valuable assets within the firm is likely to have repercussions in terms of ensuring key information assets receive adequate protection. Unfortunately, if contemporary fraud theory is any example, the greatest threat to IAs is internal with the vast majority of fraud being perpetrated by employees of the company[5]. Thus, the very individuals who are trusted with knowledge most crucial to the knowledge dependent company's very existence are the very same individuals most likely to betray that trust. There

1 Kroll (2003). "Catch them if you can – are you doing enough to safeguard your intellectual property? The Kroll Global Survey on Corporate Response to IP Abuse", www.krollworldwide.com [accessed 12JUN04]. ASIS (2002). "Trends in Proprietary Information Loss Survey Report", American Society for Industrial Security, Pricewaterhouse Coopers, and US Chamber of Commerce and Industry, www.asisonline.org [accessed 07MAR03]. Ernst & Young (2003). "Fraud: The Unmanaged Risk", 8th Global Survey, Global Investigations and Dispute Advisory Services, Ernst and Young, South Africa.

2 Kroll (2003). "Catch them if you can – are you doing enough to safeguard your intellectual property? The Kroll Global Survey on Corporate Response to IP Abuse", www.krollworldwide.com [accessed 12JUN04].

3 ASIS (2002). "Trends in Proprietary Information Loss Survey Report", American Society for Industrial Security, Pricewaterhouse Coopers, and US Chamber of Commerce and Industry, www.asisonline.org [accessed 07MAR03].

4 Kroll (2003). "Catch them if you can – are you doing enough to safeguard your intellectual property? The Kroll Global Survey on Corporate Response to IP Abuse", www.krollworldwide.com [accessed 12JUN04].

5 Pickett, Pickett (2002). "Financial Crime Investigation and Control", John Wiley and Sons, USA.

are many reasons for this; some are accidental such as the scientist discussing his research at a conference prior to patent submission. Others more deliberate. Knowledge sharing is important and valuable, however it can be a two edged sword. The eighth Global Fraud Survey conducted by Ernst and Young indicated that some 85% of the worst frauds were perpetrated by insiders, whilst also showing a worrying trend that the incidence of fraud is increasing[6].

The management of intellectual property and proprietary information is a multidisciplinary activity involving skills in law, finance, human resources, marketing, R&D and sales and distribution. Today, many organisations generate proprietary information as part of their regular business activities. Some companies may extend these activities and convert a proportion of their proprietary information into intellectual property. Intellectual Property Rights (IPRs) confer legal ownership within a jurisdiction and are designed to prevent unauthorised use by third parties for commercial gain. The prevention of unauthorised use precludes competitors from imitating the subject of the IPR, which can be a product or a service.

The extent to which IPRs form part of an organisations competitive strategy is generally dependent upon the organisation, industry and geographical area in which that organisation operates. Some industries considered knowledge intensive, such as biotechnology, ICT and banking and finance, have a heightened awareness of the value of their IAs and place a greater emphasis on their protection as part of an overall IP strategy. The following figure illustrates the nature of these concepts, demonstrating how intellectual inputs transition through to an output or a final product[7].

6 Ernst & Young (2003). "Fraud: The Unmanaged Risk", 8th Global Survey, Global Investigations and Dispute Advisory Services, Ernst and Young, South Africa.

7 Hine, D. and Kapeleris, J, (2006) Innovation and Entrepreneurship in Biotechnology: An International Perspective: Concepts, Theories and Cases. Cheltenham, UK, Edward Elgar Publishing.

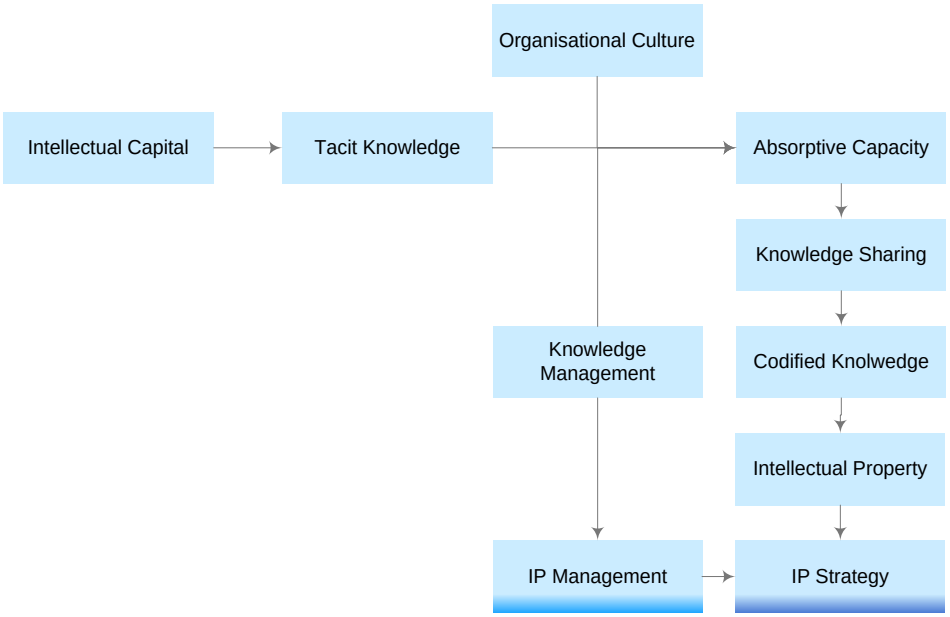


Figure 1: From Intellectual Inputs to Intellectual Outputs

Managing security activities involving Intellectual Assets in this environment requires a solid understanding of security, fraud and risk management concepts as well as a background in Business and Intellectual Property Law. For security practitioners working in a research environment it is also critical to possess a deep level of understanding around how R&D activities are performed and in particular, the softer issues, such as organizational culture, which underpins the interaction of research teams. Security practitioners working in, or with, knowledge-creating organisations will experience a distinctly different organisational culture and method of operation when compared to organisations that are not focused on the generation of knowledge. Without these understandings, it is likely that any security program aimed at protecting intellectual assets will be either poorly conceived, or poorly received and therefore inadequately implemented. This is often overlooked by practitioners within the security domain, as the roles of knowledge generation, knowledge capture and knowledge protection are not easily integrated.

1.2. Scope

This chapter is intended to provide a background to the concepts underpinning Intangible Assets, R&D activities, threats, perpetrators, vulnerabilities and protective mechanisms. However, we do not seek to provide a reference on Intellectual Property Law, Commercialisation or Intellectual Property Management. Where some of these concepts are fundamental to the design of an effective security policy, they have been highlighted. It is recommended that security practitioners who work in an IP-focused organisation such as a

university, research institute, or knowledge-based company read and apply this reference in conjunction with other texts relating to Intellectual Property[8].

This reference is structured firstly to provide the reader with an understanding of why knowledge and intangible assets are important and how they are used in business today. Secondly, the reference provides the reader with an understanding of intellectual assets and how (and why) proprietary information becomes intellectual property. With this understanding, it will become apparent why some traditional security practices simply are not appropriate for the knowledge-based organisation. With an understanding of the context in which a knowledge-creating organisation operates, we move to review the security specific material including vulnerabilities, threats and perpetrators before concluding with a model to protect intangible assets in the R&D environment.

1.3. Security threats and their place in the IA Value Chain

Both internal and external threats need to be managed differently if the firm is to successfully minimise the risk to IAs. Two key factors in managing IA threats are:

- The extent to which the firm controls the use of its knowledge in the public and private domain; and,
- The extent to which it is aware of the IAs its possession[9].

By failing to recognise IA's an organisation firstly fails to properly manage its knowledge resources, and secondly exposing itself to unnecessary losses. The figure below[10] depicts the IA Value Chain by illustrating how knowledge assets relate to IP.

8 McGuinness, P. (2003). "Intellectual Property Commercialisation: A Business Managers Companion", LexisNexis Butterworths, Australia.

9 Medd, K, Konski, A. (2003). "Workplace programs to protect Trade Secrets", Nature Biotechnology, 21, pp.201-203.

10 Curwell, P. (2004). "Intellectual Asset Fraud: Preventative Strategies in Knowledge-dependent Companies", unpublished thesis, The University of Queensland Business School, Brisbane, Australia.

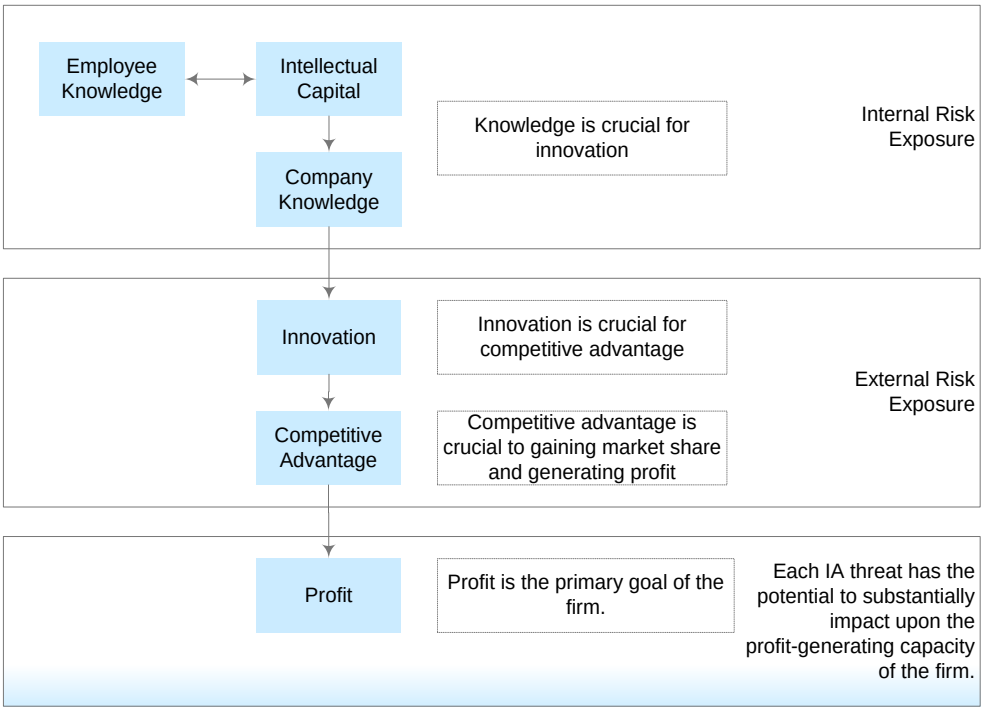


Figure 2: Intellectual Asset Value Chain in relation to Security Risk

Exploring the interrelationships between concepts, the preceding figure identifies 'choke points' in the value chain where both internal and external security risks provide opportunities for the loss of those Intellectual Assets reside[11].

11 Curwell, P. (2004). "Intellectual Asset Fraud: Preventative Strategies in Knowledge-dependent Companies", unpublished thesis, The University of Queensland Business School, Brisbane, Australia.

2. CONTEXT

2.1. Role of Knowledge in Competitive Strategy

The adage 'knowledge is power' has long proven true in many applications, and this is no different within firms today. Intellectual Assets (IAs), a term used herein to refer to knowledge, Intellectual Capital (IC), and Intellectual Property (IP) now comprises a substantial component of a company's value[12]. Like all assets, IAs are extremely valuable as they represent a core capability of firms engaged in developing and applying knowledge to enable their successful competition in what is typically a dynamic and highly evolving marketplace[13]. To operate effectively in the contemporary market organisations have had to adopt flatter operating structures as opposed to the more traditional, hierarchical companies of last century.

Characteristic of these flatter structures is that much of the knowledge, and hence decision making power, is contained at lower levels of the organization when compared to companies operating in the industrial age. A result of the "knowledge revolution", firms have evolved from highly structured organizations where knowledge and power was consolidated at top levels of management into flatter and less hierarchical structures[14]. Flatter organisational structures present new security problems, particularly in respect to proprietary information. In some instances, alteration of the balance of power within the firm has translated into opportunities for internal fraud and theft of IAs. Increased access to valuable information across the organisation also increases its availability and hence provides opportunities for unintentional disclosure.

Despite such risks, knowledge provides employees with the tools they require to undertake a particular function. In today's knowledge intensive world this is likely to involve a component of research and development (R&D), irrespective of whether an organisation creates products or services[15]. Knowledge can be defined as information that is recognised as being important; then, by recombination amongst individuals, learning occurs with existing knowledge being refined and new knowledge being created[16]. For knowledge to be of value to the firm it must be recognised as such and efforts made to actively apply that knowledge to the firms operations. The term "Intellectual Capital" (IC) has been created to refer to valuable knowledge within the firm[17]. The knowledge

12 Stewart, T.A. (2001). "The Wealth of Knowledge: Intellectual Capital and the Twenty-First Century Organisation", Nicholas Brealey Publishing, Great Britain.

13 Germeraad, P. (1999). "Intellectual Property in a time of change", Research Technology Management, 42, 6, pp.34-39.

14 McAdam, R. (2000) "Knowledge Management as a Catalyst for Innovation within Organisations: A Qualitative Study", Knowledge and Process Management, 7, 4, pp.233-241.

15 Powell, W.W. (1998). "Learning from Collaboration: Knowledge and Networks in the Biotechnology and Pharmaceutical Industries", California Management Review, 40, 3, 228-240. Hodgson, J. (2001). "The headache of knowledge management", Nature Bioentrepreneur, 19, pp. BE44.

16 Powell, W.W. (1998). "Learning from Collaboration: Knowledge and Networks in the Biotechnology and Pharmaceutical Industries", California Management Review, 40, 3, 228-240.

17 Ehin, C. (2000). "Unleashing Intellectual Capital", Butterworth Heinemann Publishers, USA.

dependent company must harness its collective IC and convert it into a form which is valuable. In some instances it is applicable to realise this value through legal ownership or title known as 'Intellectual Property Rights' (IPRs). In other instances, it may not be necessary (or even possible) to obtain an IPR for valuable knowledge although this knowledge is in continual use within the organisation. This valuable knowledge is referred to as "Proprietary Information" (PI), and can encompass non-IP IAs and IC.

In contrast to PI, the development of IP provides a mechanism through which the formal ownership of specific knowledge is conferred upon the inventor or assignee (the entity holding legal title to a specific IPR) of that knowledge[18]. As an intangible resource the real value of IC is often overlooked, meaning it is not efficiently captured within the firm, preventing new knowledge integration[19]. According to Porter, the basic goal of every firm is to establish a "profitable and sustainable position against the forces that determine industry competition"[20]. The development of a strong portfolio of IAs can create a multitude of opportunities for firms, including establishment of a 'profitable and sustainable position', otherwise termed 'productive opportunities' by Penrose (1959) to illustrate the potential value of such assets. Start-up companies such as those engaged in research-based activities operate business models and raise capital based on the perceived value of their research, itself a 'productive opportunity' for the firm[21]. For research firms, and particularly those in the start-up phase, security related to their IAs is immensely important. Start-up firms do not recognise their IPRs because of their limited awareness of the importance of their IAs. This is of course dependent upon the firm's strategy, availability of capital and the previous experiences of management. This means that in a start-up, research-based firm the majority of IC is held in as PI.

PI, as will be covered in detail later, is extremely vulnerable to compromise through intentional or unintentional disclosure. Disclosure, whether intentional or unintentional, can have a severe impact upon the ability to obtain an IPR for the research. Patents, which are the primary IPR used by research-based firms, are an example of this as a patent will only be granted for an invention that is novel (new) which contains an 'inventive step'. As previously mentioned the capital raising activities of a research organisation are highly dependent, in part, on the ability to obtain IPRs. Where the ability to obtain an IPR is compromised, such as through disclosure the future viability of the enterprise is severely affected and can result in the organisation being wound up.

18 Hodgson, J. (2001). "The headache of knowledge management", Nature Bioentrepreneur, 19, pp. BE44. Jackson, B.A. (2003). "Innovation and Intellectual Property: The Case of Genomic Patenting", Journal of Policy Analysis and Management, 22, 1, pp.5-25.

19 Zhou, A.Z., Fink, D. (2003). "The intellectual capital web: A systematic linking of intellectual capital and knowledge management", Journal of Intellectual Capital, 4, 1, 34-48. Wensley, A. (1997). "Knowledge Management and Knowledge Creation", Knowledge and Process Management, 4, 3, pp.139-141.

20 Porter, M.E. (1985). "Competitive Advantage: Creating and Sustaining Superior Performance", The Free Press, New York.

21 Zucker, L.G., Darby, M.R., Armstrong, J.S. (2002) "Commercialising Knowledge: University Science, Knowledge Capture, and Firm Performance in Biotechnology", Management Science, 48, 1, pp.138-153.

Today's market forces demand that in addition to simply manufacturing something companies must impart particular attributes into their products or services to distinguish them from other products available on the market. Contemporary companies must innovate to survive[22]. Innovation confers 'competitive advantage' - an attribute capable of providing that firm with an advantage in the market, and technology plays a significant role in providing the firm with such an opportunity[23]. Technology also provides a mechanism through which firms can interact to pool IAs for mutual benefit, providing an excellent platform from which to learn and create new knowledge[24]. In this way technology becomes not only a 'principle driver of competition' but can also confer first-mover advantage on those whose R&D has permitted the application of that technology to the market.

Through efficient use of resources, technology can provide the firm with a competitive advantage derived from a combination of sources, including difficult to imitate product attributes, but also provide access to IC resources 'embedded in dyadic and network relationships"[25]. In this regard the intra and inter-firm learning process confers a type of competitive advantage on participants, especially in knowledge-dependent firms such as high technology industries whereby the generation and exploitation of knowledge demands continual replenishment. However, despite the benefits conferred by access to these networking and inter-firm relationships, they can also expose IAs – the core assets of a knowledge-dependent company – to an unnecessary level of risk through misappropriation. For this reason, theft and fraud against IAs represents a significant threat to the sanctity of the knowledge generation and value-extraction process undertaken by knowledge-dependent firms for their survival in highly competitive environments. As the role of knowledge within the firm becomes increasingly important it is crucial that the dynamics of knowledge creation are understood so that the associated risks can be better appreciated and managed by security practitioners.

2.2. Knowledge as an Intangible Asset

Knowledge-creating organisations generate some IC internally, but the vast majority of valuable knowledge has been demonstrated to arise through external interactions. Obviously, this increases the exposure of the IA to a host of risks including theft and industrial espionage. However, the value gained from this activity cannot be denied. By building alliance-specific assets, knowledge-sharing routines, and effective relational governance mechanisms into external

22 Tidd, J., Bessant, J., Pavitt, K. (2001). "Managing Innovation: Integrating Technological, Market, and Organizational Change", John Wiley and Sons, UK.

23 Porter, M.E. (1985). "Competitive Advantage: Creating and Sustaining Superior Performance", The Free Press, New York.

24 Porter, M.E. (1985). "Competitive Advantage: Creating and Sustaining Superior Performance", The Free Press, New York.. Teece, D.J. (2000). "Strategies for Managing Knowledge Assets: The Role of Firm Structure and Industrial Context", Long Range Planning, 33, pp.33-54.

25 Yli-Renko, H., Autio, E., Sapienza, H.J. (2001). "Social Capital, Knowledge Acquisition, and Knowledge Exploitation in Young Technology-based Firms", Strategic Management Journal, 22, 587-613. Dyer, J.H., Singh, H. (1998). "The relational view: cooperative strategy and sources of interorganizational competitive advantage", Academy of Management Review, 23, 660-679. Lane, P.J., Lubatkin, M. (1998). "Relative absorptive capacity and interorganizational learning" Strategic Management Journal, 19, 5, 461-477.

networks and relationships, firms leverage their relational resources for knowledge acquisition and exploitation[26]. In this manner knowledge can be used as a tool or asset with which to generate wealth for the firm through competitive advantage. However, to maximise the benefit of relational knowledge resources, managers must first have an understanding of the process by which knowledge is created, and how its conversion to IC can be of use to the firm[27]. An understanding of this process is crucial to the security practitioner if they are to accurately assess security risk relating to IAs.

Knowledge is an intangible asset that can be created by harnessing the various forms of intangible capital, including human, social, reputational, relational and intellectual capital available to an organisation, and applying that capital towards a tangible outcome such as a product, process, or service[28]. Knowledge-dependent companies exist because of their ability to harness intangible knowledge assets and create value from them[29]. Knowledge generation is a complex and convoluted process beginning with employees sharing their personal knowledge and concluding with that knowledge being codified and, hopefully, protected by the firm and then applied to the process of innovation[30]. Before an employee can share their knowledge, they must first possess something to share. This is highly likely in knowledge-dependent industries such as Biotechnology where employees are some of the most highly educated of any industry[31].

During the initial stages of scientist or engineer's education most of the learning would have involved sharing the simplest form of knowledge known as 'codified knowledge'[32]. Codification reflects knowledge that is written down as would be encountered during one's schooling or university lectures. Codified knowledge is easily transferred between individuals because concepts have been documented permitting learning to occur easily, such as within a textbook, often with individuals being guided through the learning process simply by absorbing material presented to them[33]. Tacit knowledge, however, is very different.

26 Cyr, D. (1998). "High Tech, High Impact: Creating Canada's competitive advantage through technology alliances", Academy of Management Executive, 13, 2, pp.17-26. Powell, W.W. (1998). "Learning from Collaboration: Knowledge and Networks in the Biotechnology and Pharmaceutical Industries", California Management Review, 40, 3, 228-240.

27 Grant, R.M. (1996). "Toward a knowledge-based theory of the firm", Strategic Management Journal, Winter Special Issue, 17, 109-122. Spender, J.C. (1996). "Making knowledge the basis of a dynamic theory of the firm", Strategic Management Journal, Winter Special Issue, 17, 45-62. Kogut, B., Zander, U. (1992). "Knowledge of the firm, combinative capabilities, and the replication of technology" Organisational Science, 3, 3383-3397.

28 Andersen, B., Struikova, L. (2004). "Intangible Assets and Intellectual Capital: Where Value Resides in the Modern Enterprise", DRUID Summer Conference on Industrial Dynamics, Innovation, and Development, Denmark.

29 Ibid

30 Nonaka, I., Takeuchi, H. (1995). "The Knowledge Creating Company: How Japanese Companies Create the Dynamics of Innovation", New York, Oxford University Press.

31 Norus, J. (2002). "Biotechnology Organisations in Action: Turning Knowledge into Business", Progress in Biotechnology, Volume 20, Elsevier Science B.V., Amsterdam.

32 Soo, C., Devinney, T., Midgley, D., Deering, A. (2002). "Knowledge Management: Philosophy, Processes, and Pitfalls", California Management Review, 44, 4, pp.129-150.

33 Nonaka, I. (1991). "The Knowledge-Creating Company", Harvard Business Review, November-December, pp.96-104.

Tacit knowledge is otherwise known as "experiential knowledge" and refers to the body of knowledge developed by an individual in the course of their life experience[34]. The greater the diversity of exposures an individual has received, the more diverse their tacit knowledge. To examine biotechnology again, as employees accumulate more knowledge and familiarity with the science, the level of their tacit knowledge increases, often cumulating with doctoral or post-doctoral study, and involvement in novel research. Unlike codified knowledge, tacit knowledge is not easily communicated as it is often comprised of technical and abstract concepts that are difficult to articulate[35]. It is as much about a way of thinking as about the actual ideas themselves.

Despite inherent communication difficulties research has shown that tacit knowledge is the form of knowledge more likely to lead to innovative breakthroughs and radical change because the radical concepts conveyed by tacit knowledge are undocumented, in contrast to codified knowledge[36]. The conversion of experiential to codified knowledge forms an integral component of the intellectual asset value chain which depicts the transformation of abstract and creative concepts into knowledge from which concepts of value to the firm then become known as 'IC'[37]. Provided the IC is retained within the firm it can often be found constituting, either wholly or in part, the firm's IP portfolio[38]. Whether the IC forms an entire product, such as a drug molecule capable of treating a specific disease, or is simply the knowledge required to identify candidate molecules during the research process will depend on the type, role, and importance of legally recognised ownership of the knowledge assets themselves. The importance of legal recognition, and ultimate application of the IA are the influencing factors between whether an IA is retained as proprietary or whether it is converted to IP. This concept is illustrated in the figure below[39]:

34 Polanyi, M. 1966 The Tacit Dimension. Garden City, NY. Doubleday.

35 Ibid

36 Nonaka, I. (1991). "The Knowledge-Creating Company", Harvard Business Review, November-December, pp.96-104. Kogut, B., Zander, U. (1992). "Knowledge of the firm, combinative capabilities, and the replication of technology" Organisational Science, 3, 3383-3397.

37 Zhou, A.Z., Fink, D. (2003). "The intellectual capital web: A systematic linking of intellectual capital and knowledge management", Journal of Intellectual Capital, 4, 1, 34-48.

38 Andersen, B., Struikova, L. (2004). "Intangible Assets and Intellectual Capital: Where Value Resides in the Modern Enterprise", DRUID Summer Conference on Industrial Dynamics, Innovation, and Development, Denmark.

39 Hodgson, J. (2001). "The headache of knowledge management", Nature Bioentrepreneur, 19, pp. BE44. Pitkethly, R. (2001). "Intellectual Property strategy in Japanese and UK companies: patent licensing decisions and learning opportunities", Research Policy, 30, 425-442.

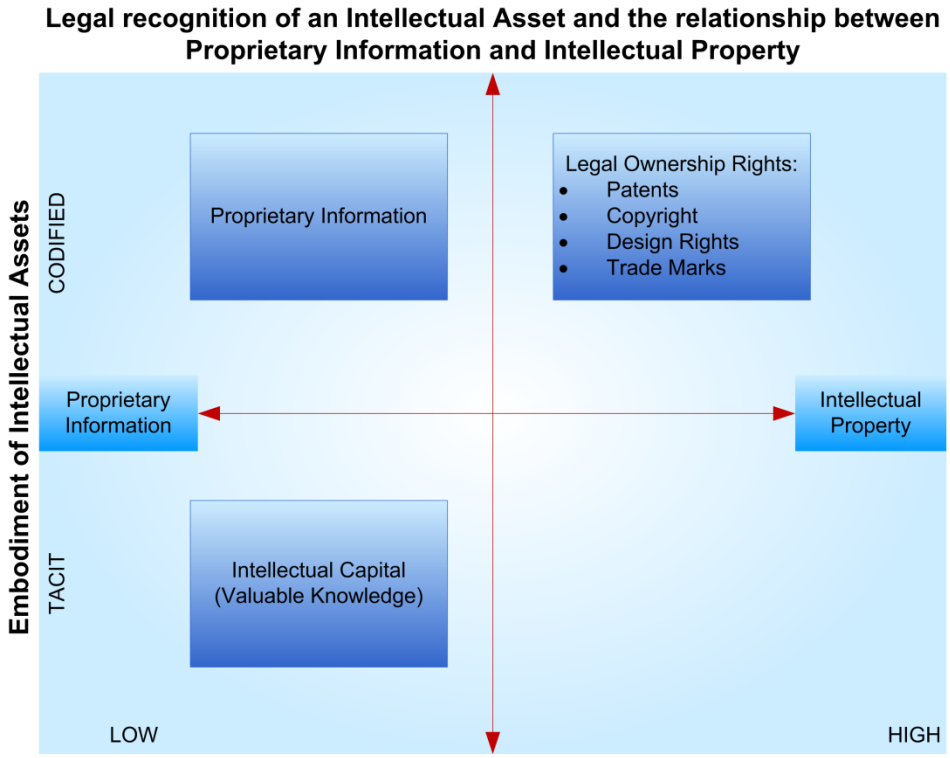


Figure 3: Legal Recognition of Intellectual Asset

Where IC itself is tacit rather than explicit (codified), as illustrated in the figure above, it is impossible to have ownership recognised through IPRs such as patents because every patent application must be lodged in a codified format [40]. For this reason tacit knowledge has a low 'legal appropriability' when compared to codified knowledge[41]. IC is also very transient as an asset, as it is contained within a person's head, a fragile environment at the best of times. Injury, or loss of life, head hunting, retirement or even the refusal to share knowledge are all hazards in converting from tacit to codified knowledge.

However, it must also be recognised that in the case of proprietary information (including Trade Secrets) the firm will not necessarily want that knowledge to be codified as this increases the chances of such knowledge being disclosed to third parties, and reduces the extent to which control over the asset can be exerted.

Failure to have ownership of knowledge conferred legally through IP conventions also means that secrecy is the firm's only real method of protecting such

40 Andersen, B., Struikova, L. (2004). "Intangible Assets and Intellectual Capital: Where Value Resides in the Modern Enterprise", DRUID Summer Conference on Industrial Dynamics, Innovation, and Development, Denmark. Hodgson, J. (2001). "The headache of knowledge management", Nature Bioentrepreneur, 19, pp. BE44.

41 Pitkethly, R. (2001). "Intellectual Property strategy in Japanese and UK companies: patent licensing decisions and learning opportunities", Research Policy, 30, 425-442.

assets[42]. For a firm to be competitive in a knowledge-creating environment, valuable knowledge (IC) must be assimilated and embedded within employees, although this alone is inadequate to guarantee success in a knowledge-creating marketplace[43]. Unfortunately, not only does embedding knowledge statistically increase the chances of public disclosure for PI through sheer weight of numbers, but embedding it within employees also fails to impart the wisdom of how to apply that knowledge in the market[44].

Where knowledge is embedded within a firm, in conjunction with wisdom on how to apply that knowledge, knowledge is converted into an IA and can then be used to generate a competitive advantage[45]. In this manner employees in knowledge-intensive industries leverage their own IC to generate income through employment, providing a division of labour between employee and firm and creating difficulties associated with apportioning ownership, and therefore royalties and recognition, from knowledge assets. To successfully generate income, employees need to feel free to share their ideas and tacit knowledge with others to permit the formation of new knowledge[46].

For a firm to truly profit as a knowledge-creator, new knowledge generated must be codified so that it is available for all employees to apply in the course of their employment. Codification transforms knowledge from an intangible into a tangible form, from which the knowledge identified as IC can then be pursued and harnessed for the benefit of all, not to mention converted to legally recognised IP[47].

The difficulty in protecting IAs arises where tacit resources are withheld by employees (such as a crucial idea or fact being retained in a researcher's head or private notebook) and not disclosed to the firm. Typically, this sort of activity is undertaken either for the employees' personal use (perhaps they are in negotiations with another potential employer) or in an attempt to influence promotional and remuneration prospects within the firm. Although effectively constituting an internal fraud act against the employer this activity is immensely difficult to detect until after the event. Unfortunately, by then it can be too late. This issue represents one of the more difficult challenges for security practitioners responsible for managing operational risk against IAs, as it is as much an organisational culture issue as an IA issue.

42Blattman, A., Irani, S., McCann, J., Bodkin, C. (2001). "Biotechnology IP Management Manual", Spruson & Ferguson and Biotechnology Australia, Canberra, Australia. McGuinness, P. (2003). "Intellectual Property Commercialisation: A Business Managers Companion", LexisNexis Butterworths, Australia. Willman, P. (1996) "Protecting Know-How", London Business School Business Strategy Review, 7, 1, 9-13.

43 Storck, J., Hill, P.A. (2000). "Knowledge Diffusion through 'Strategic Communities'", Sloan Management Review, Winter, pp.63-74. Graham, A., Pizzo, V. (1997). "Competing on Knowledge: Buckmann Laboratories International", Knowledge and Process Management, 4, 1, pp.4-10.

44 Contractor, F. (2000). "Valuing Corporate Knowledge and Intangible Assets: Some General Principles", Knowledge and Process Management, 7, 4, pp.242-255.

45 Graham, A., Pizzo, V. (1997). "Competing on Knowledge: Buckmann Laboratories International", Knowledge and Process Management, 4, 1, pp.4-10.

46 Nonaka, I., Takeuchi, H. (1995). "The Knowledge Creating Company: How Japanese Companies Create the Dynamics of Innovation", New York, Oxford University Press.

47 Andersen, B., Struikova, L. (2004). "Intangible Assets and Intellectual Capital: Where Value Resides in the Modern Enterprise", DRUID Summer Conference on Industrial Dynamics, Innovation, and Development, Denmark.

2.3. Defining Intellectual Assets

Contractor distinguishes three classes of IAs within the firm: IP formally owned by the firm; IAs comprising knowledge and IP; and uncodified human and organisational capital. None of these concepts are independent of the other in a knowledge-dependent company, as represented by Table 1[48]:

Table 1: Defining Intellectual Assets

CATEGORY	DESCRIPTION
Intellectual Property	Legally Registered Intellectual Property: • Patents • Brands • Copyrights • Trade Marks etc
Proprietary Information	Intellectual Assets (unregistered but codified): • Drawings, software, blueprints • Written Trade Secrets • Databases, formulae, recipes
	Intellectual Capital (uncodified human and organisational capital): • Collective Corporate Knowledge • Individual Employee Skills and Knowledge • "Know-how" • Organisational Culture • Customer Satisfaction

As illustrated above, Intellectual Property is represented by the rights (legal title), such as patents, contained at '(I) Intellectual Property' within the figure. The types of Proprietary Information can be almost limitless, but can consist of "Intellectual Assets" and "Intellectual Capital" as outlined at (II) and (III) in the figure above. Crucially, success of the knowledge-dependent firm is intimately tied to both the creation of new, and the protection of existing, IAs from competitors and any other entity wishing to acquire these assets for their own purposes[49].

48 Contractor, F. (2000). "Valuing Corporate Knowledge and Intangible Assets: Some General Principles", Knowledge and Process Management, 7, 4, pp.242-255.

49 Padron, M.S., Uranga, M.G. (2001). "Protection of Biotechnological Innovations: A burden too heavy for the patent system", Journal of Economic Issues, 35, 2, pp.315-322.

Dolan, R. (2001). "Abgenix and the Xenomouse", Harvard Business School Case Study 9-501-061, Boston, USA.
Bellini, F. (1997). "Commercial Perspective on the Drug Discovery Environment for Biopharmaceutical Companies in Canada", Drug Development Research, 42, pp.113-119.

Research shows that not only is a team-orientated approach more effective in terms of generating an innovation, but that it also contributes significantly to the generation of new and even unexpected knowledge[50]. For knowledge creation to occur individuals must be willing to share with, and learn from, each other. Knowledge creation requires a learning-friendly organizational culture accepting of employees expanding their knowledge, part of which is embodied within the firm as "social capital"[51]. Social capital provides an opportunity for the firm to focus on value creation, as opposed to valuation, allowing the firm to borrow the resources of knowledge-sharing entities and thus providing a valuable resource for internal innovative activities. Any security measures developed for knowledge-generating organisations should be mindful of the potential for adverse impact on the sharing and generation of social capital. Obvious, 'in your face' security measures are generally not necessarily conducive to effective knowledge generation, although they have been used effectively in despotic regimes where researchers and their families have been held under duress or threat of actual harm[52].

Unfortunately, the management of knowledge and the processes underlying knowledge creation and organisational learning are complex. According to Styhre "Managing knowledge implies a need to construct substantial social, psychological, and emotional commitments and contracts between organisational employees and management. It is simply not possible to manage knowledge in the same manner as tangible resources because knowledge is…situational, embedded in social practices and worldviews"[53]. It is precisely because of this factor that traditional security practices may not be appropriate in a knowledge-generating environment. If the security practitioner lacks understanding of their environment it is unlikely they will be able to effectively manage the issues present in their organisation. Where the need to manage differently is recognised within the firm, efficient use of intellectual resources will ideally be reflected through positive staff performance. Provided the social, psychological, and emotional commitments identified by Styhre can be obtained from employees and their external networks by managers and harnessed within the firm, innovation is more likely to result.

2.4. The nature of R&D

Organisations whose primary function is knowledge-generation, such as those engaged in scientific and technical domains, typically incorporate some form of R&D function. R&D is a methodical activity incorporating four primary phases of research, development, manufacturing and placement of the product or service in a market. Although there are likely to be many variations all formal R&D activities follow this common theme.

50 Tidd, J., Bessant, J., Pavitt, K. (2001). "Managing Innovation: Integrating Technological, Market, and Organizational Change", John Wiley and Sons, UK.

51 Yli-Renko, H., Autio, E., Sapienza, H.J. (2001). "Social Capital, Knowledge Acquisition, and Knowledge Exploitation in Young Technology-based Firms", Strategic Management Journal, 22, 587-613.

52 Adams, J. (1995). "The New Spies", Pimlico, London.

53 Styhre, A., Ingelgard, A., Roth, J. (2001). "Gendering Knowledge: The practices of Knowledge Management in the Pharmaceutical Industry", Knowledge and Process Management, 8, 2, 65-74.

As R&D activities progress and pass consecutive evaluation phases the ratio of intangible Proprietary Information to tangible Intellectual Property also changes. Typically, IP predominates at the later stages of R&D whilst PI is mostly found early on in the R&D pipeline. The nature of the R&D pipeline and proportion of PI to IP also impacts upon the type of security activities performed. Although present at all stages of the R&D pipeline, internal security activities predominate in the early stages of the R&D as the primary external threat is disclosure of PI. As the product moves towards the market the security focus transitions towards external threats such as counterfeiting, intentional infringement of IPRs and licensing abuse. These concepts are illustrated in the figure below:

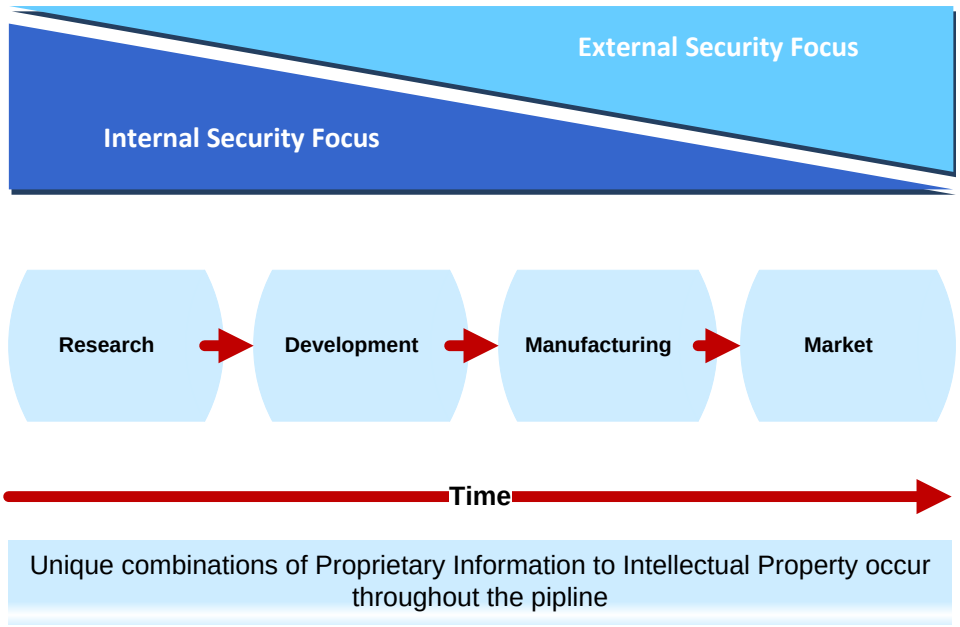


Figure 4: R&D Pipeline in relation to Intellectual Assets

2.5. The function of security and knowledge-intensive organisations

The role of the security practitioner in knowledge-creating firms is broad and should include a focus on internal and external risks. The function of the security practitioner in knowledge-intensive organisations can be summarised as follows:

- Prevent unauthorised release of, and access to, proprietary information from within the organisation.
- Detect, deter and delay external attempts by external parties to obtain proprietary information illegitimately (such as through economic or industrial espionage).
- Conduct security intelligence and counterintelligence activities as required, to maintain the integrity of proprietary information. Information Operations may be employed on a needs basis.

Internal security operations should work to ensure the integrity of the proprietary information, personnel and physical assets (facilities, equipment etc) used to obtain an IPR or competitive advantage. Internal security operations should also encompass 'trusted third parties' such as distributors, suppliers and joint research activities. External security operations should identify and assist with the management of IPR abuse in the market. These activities, referred to as "*market surveillance and enforcement*" within this reference, may encompass investigative and covert surveillance activities such as identifying distribution and storage channels for counterfeit products.

3. PROPRIETARY INFORMATION

3.1. Background

'*Proprietary Information*' is a broad term referring to sensitive or confidential information held within an organisation. This information is sensitive or confidential because it is not widely known within society in general. Proprietary Information typically includes '*Confidential Business Information*' and '*Trade Secrets*':

- '*Confidential Business Information*' is information of significant market value to competitors such as pricing models or marketing strategies. Research data may also be classified as Proprietary. *Confidential Business Information* can also encompass IC.
- '*Trade Secrets*' are generally referred to as Intellectual Property although technically they are not covered under the various Intellectual Property conventions as a category of IP.

A third category of proprietary information exists within many national governments. This is often referred to as '*classified information*' and may be considered proprietary because it is closely held within the respective government. Most nations generally have separate legislation to deal with offences against *classified information*. These offences are generally considered extremely serious and include indictable offences such as treason and espionage.

Research data may be considered proprietary during the early phases of Research and Development. Typically a research organisation will not commit to the significant investment which is a patent until its researchers have firmly established what is known as '*proof of concept*'. '*Proof of Concept*' simply means that the innovation is capable of doing what is claimed. This usually involves some sort of assessment or evaluation to determine whether it is financially beneficial to continue with the investment. Some organisations elect never to protect their inventions under Intellectual Property legislation, instead choosing to protect their inventions as *Trade Secrets.*

3.2. Trade Secrets

While still a legitimate from of IP, contrary to popular belief *Trade Secrets* are not actually a form of Intellectual Property enshrined within World Intellectual Property Organisation (WIPO) conventions. Instead, *Trade Secrets* are covered by legislation within each jurisdiction. For example, in Australia there is no single piece of legislation relating to the protection of *Trade Secrets*. Under Australian law most *Trade Secrets* issues are dealt with under common law[54]. However,

54 McGuinness, P. (2003). "Intellectual Property Commercialisation: A Business Managers Companion", LexisNexis Butterworths, Australia.

some jurisdictions may establish offences under their legislation that relate to abuse of *Trade Secrets*. Where the inventive step between what is common knowledge and what underpins the innovation is not public the inventor of that innovation can potentially protect their innovation whilst concurrently saving on costs by keeping their invention as proprietary.

This may work to help prevent counterfeiting particularly where it is not immediately obvious to a third party how the inventive step was performed. One example of this is where it is not possible to reverse engineer a product to enable a third party to determine how it was constructed. The problem with this approach is that once a third party successfully reverse engineers an invention protected as a Trade Secret the inventor looses all competitive advantages in their market.

As Trade Secrets are not generally enforceable under law, unlike the protection afforded by an IPR, no protection or temporary monopoly in the market exists. However, there may be legal remedies where the trade secret was publicised or successfully engineered with the help of unethical business practices such as some industrial espionage techniques or where a Non-Disclosure (Confidentiality) Agreement has been breached.

3.3. Security and Proprietary Information

Irrespective of the type of proprietary information the measures used to protect it are almost exclusively similar. In general Proprietary Information only remains proprietary, and therefore continues to add value, for as long as its existence is not widely known in the public domain. Once its existence becomes widely known it generally ceases to have value. There are two mechanisms by which PI is publicised:

- The PI may be *independently discovered by third party*, for example, a competitor conducting research into a similar area; or,
- Intentional or unintentional publication or release.

The security practitioner within knowledge-based organisations must develop appropriate and effective frameworks to manage a diverse array of threats and risks in this environment. A comprehensive risk management framework is presented in Part 7 of this reference.

4. INTELLECTUAL PROPERTY

4.1. Background

The term 'Intellectual Property', commonly known as IP, refers to creations of the mind including inventions, literary and artistic works, symbols, names, images and designs used in commerce and geographical indicators. IP legislation is administered on a number of levels[55]:

- Global Conventions are administered by the WIPO and includes the Paris and Berne Conventions as well as agreements such as TRIPS.
- National Legislation – every signatory country to the WIPO conventions has its own IP legislation, such as Australia's Patent Act. National Legislation is administered by government bodies such as IP Australia, the European Patent Office and the US Patent and Trademarks Organisation (USPTO).

Obtaining IP rights can be a long and convoluted process as IP rights must be obtained in every country where the assignee wishes to utilise the rights to obtain a monopoly. Depending on the type of IP involved, such as a patent, the inventor/assignee must apply for the patent in every country where the assignee wishes to have access to the rights that a patent entails[56]. For example, patent applications will probably be filed in multiple countries which entails multiple patent application filings and annual maintenance fees.

Each type of IP is different and the process of obtaining IP rights varies. However, obtaining IP rights in multiple countries means that IP Management activities must be performed across all of these countries to preserve the owner's IP rights.

4.2. Types of IP

The major types of IP are[57]:

- Patents (inventions);
- Copyright (literary and artistic works);
- Trademarks (symbols, names and images used in commerce);
- Design rights;
- Electrical/Electronic Circuit Layout rights;

55 McGuinness, P. (2003). "Intellectual Property Commercialisation: A Business Managers Companion", LexisNexis Butterworths, Australia.

56 Ibid

57 Ibid

- Plant Breeders Rights; and,
- Geographical Indicators (governs the use of names such as 'champagne').

Other less common categories of IP also exist.

4.3. Managing IP

It is important to remember that IP should simply be viewed as another category of asset. Most people would not leave their cars unlocked in a busy street – they protect them with locks and car alarms. The same concept extends to IP. Being granted IP rights is just like buying a car: Once you have the asset you must look after it. The term "IP Management" collectively refers to all business activities undertaken in the course of managing an organisation's IP portfolio. There are effectively six major elements of an IP Management initiative[58]:

- Maintaining the IP Portfolio – includes ensuring that annual fees to retain patents are made to the various government agencies responsible for managing IP.
- Valuing the IP Portfolio – calculating the value of the IP to your business and in the marketplace.
- Managing licensing agreements – licensing is the practice of authorising a third party to use your IP for profit. This practice includes monitoring royalty payments by licensees and auditing their activities to ensure compliance with any legal agreements.
- Conduct Market Surveillance activities – monitoring the market to ensure that your IP rights are not being abused.
- Undertake Market Enforcement activities – legally enforcing your rights in a market. Litigation is the ultimate market enforcement option available to the inventor or assignee of IP rights.
- Generating Profit – ensuring the IP is used in such a way that it is of financial benefit to the owner.

4.4. Generating Profit from IP

There are three primary ways to profit from IP: Using the IP in house; Selling the IP; and Licensing.

- Using the IP in house: Many organisations undertake R&D activities in areas directly relevant to their business and business plan. Using IP in-house adds value to an organisation by generating a competitive advantage through provision of a temporary legal monopoly (for example,

58 Curwell, P. (2004). "Intellectual Asset Fraud: Preventative Strategies in Knowledge-dependent Companies", unpublished thesis, The University of Queensland Business School, Brisbane, Australia.

patents provide a 20 year temporary monopoly) to the owner. This monopoly prevents competitors from using the owner's IP for their business activities, meaning that all profit generated through the temporary monopoly belongs to the owner or assignee of the IP.

- Selling the IP: This is just like selling a house. Ownership ('title') is legally transferred to another party for profit. Generally, an organisation will choose to sell its IP if it is no longer of use to that organisation (such as where it does not align with their business plan or long-term strategy) or where the costs of maintenance exceed the benefits generated by the IP in the market.
- Licensing IP: Licensing is a three step process involving identifying potential licensees or users of the IP, negotiating terms and formalising the licensing agreement. A licensing agreement does not have to follow a specific structure. In a licensing agreement a Licensor is the owner or assignee of the IP issuing the license and a Licensee is the party receiving the license.

Important considerations for the licensing agreement including royalty calculations and structure, Authorised Use clause, Geography, Audit Clause and Due Diligence.

4.5. IP Due Diligence

IP Due Diligence is essentially a background checking exercise and is more involved than most commercial due diligence activities. IP Due Diligence should assess the strength of an IP portfolio from three perspectives:

- Commercial – is the IP commercially viable?
- Legal – is the quality of the IP, and any associated license agreements, of a high standard and unlikely to be challenged in court?
- Technical – are the scientific or engineering postulations technically sound?

Elements of IP Due Diligence should be undertaken by the licensee and the licensor (or buyer/seller) although the focus will differ. Private security providers who are providing market surveillance or enforcement activities on behalf of another party should undertake appropriate due diligence, or alternately obtain appropriate legal warranties and covenants, to ensure the client is actually entitled to claim ownership in order to avoid potential disputes or future legal action.

5. VULNERABILITIES

5.1. Critical Vulnerabilities

There are two critical vulnerabilities associated with Intellectual Assets:

- Once proprietary information is disclosed the value of that information to the original owner is significantly reduced as disclosure commonly results in the transfer of knowledge to other parties such as competitors over time.
- Protecting IP does not end once IPRs have been awarded. There is a tendency to believe that once legal title or ownership has been obtained, provided any annual renewal fees are maintained, that an intellectual asset is adequately protected. Unfortunately this is far from the case. Assignees must actively defend their IPRs: It is generally not up to the market, or government, to do this on behalf of the assignee.

5.2. Market Surveillance and Enforcement in relation to Intellectual Property

Contemporary IP conventions, such as those administered by the WIPO and national legislation, specifically Patent and Trade Mark protection, introduces a level of risk for those wishing to profit from proprietary information in that it assumes entities will respect the rights of others. Market Surveillance and Enforcement is the defensive process that assignees of IPRs must undertake to manage the critical vulnerability associated with IP to protect their IPRs from infringement and legal challenges.

Market Surveillance should be a continual activity for assignees of IPRs. The activity requires the assignee to remain vigilant for products or services, such as counterfeit designer clothes in retail outlets, which may infringe on either the whole or part of their IPRs. Sales and Marketing staff are generally best-placed to perform this function. If a potential incidence of infringement is identified an investigation should commence.

Where possible, evidence supporting the infringement should be gathered to allow a greater appreciation of the case. Depending on how the organization operates it may be necessary to provide guidance on Evidence Collection and Handling to Sales and Marketing staff if they are involved in obtaining suspect products in the market.

If the investigation supports a case of IPR infringement then *Enforcement* activities can commence. *Enforcement* activities will generally follow normal civil procedure, potentially resulting in litigation, and should be undertaken in conjunction with legal counsel.

5.3. Disclosure of Proprietary Information

The disclosure of proprietary information occurs through two methods: *Information Leakage* and *Information Loss*.

- Information Leakage refers to where information is unintentionally leaked from an organisation, such as where an employee carelessly discloses information to a fellow researcher which subsequently enters the public domain.
- Information Loss occurs where there is some intent on the part of the party perpetrating the unauthorised disclosure. For example, Information Loss occurs where insiders steal information at the request of a third party or where a cyber attack is launched to obtain information.

Increased emphasis on patents and trade secrets, coupled with the extensive patent process, heightens the risk of IP loss by creating a window of opportunity. Short of a firm response from management, there is no remedy capable of preventing employees from publicly disclosing PI without resorting to post-disclosure civil action[59]. As the unauthorised disclosure of an IA is unlikely to be considered a criminal offence, despite such losses amounting to millions in potential revenue, companies lack any real clout in terms of enforcing employee confidentiality. In many instances, management is unaware of a confidentiality breach until after the event, making prevention impossible.

Whilst inadvertent disclosure can be guarded against through awareness training, intentional disclosure to a third party can seriously impact upon the future competitive opportunities available to a firm through IP, just as failing to disclose information created on the firm's time can prohibit a company from realising revenue[60]. In contrast to the risks associated with disclosure of internal IP are those associated with the infringement of IP external to the firm, which can result in anything from lawsuits to civil sanctions enacted by a court, such as an order to cease a particular activity[61]. These risks have created the sub-discipline of 'defensive IP management'.

5.4. Other Vulnerabilities

5.4.1. Networks and Research Partnerships

The use of networks and research partnerships is widespread in knowledge-based industries. Cooperative research and development alliances permit organisations with complimentary experience to partner, sharing resources and

59Medd, K, Konski, A. (2003). "Workplace programs to protect Trade Secrets", Nature Biotechnology, 21, pp.201-203.

60 Ibid.

61 Blattman, A., Irani, S., McCann, J., Bodkin, C. (2001). "Biotechnology IP Management Manual", Spruson & Ferguson and Biotechnology Australia, Canberra, Australia.

knowledge under a common goal[62]. This activity is highly productive in terms of producing positive research outcomes and will almost certainly continue long into the future[63].

Despite the benefits provided through cooperative research and development programmes, social capital and embedded relationships represent clear risks for the firm divulging its IAs in terms of creating opportunities for the misappropriation of those assets. Networks can increase dissemination of proprietary knowledge and isolate the firm's ability to protect their assets by shifting responsibility onto a second party (the alliance partner).

5.4.2. Unapproved Research Activities

Unapproved research activities can potentially extend to instances of internal fraud, particularly where researchers seek to use employer resources, time and facilities to conduct research for personal gain. However, these activities can also expose the employer to excess liabilities if appropriate due diligence has not been conducted to ensure third party IP rights are not being infringed. Infringement of IP rights is very costly, stressful and time consuming for management and typically involves some or all of the steps of civil litigation. Furthermore, where an organisation is found to have intentionally infringed upon another's IPRs the settlement amount awarded by a court may be up to three times as much as that awarded from a judgement of unintentional infringement.

5.4.3. Patent Publications

When a patent is published as part of the process to obtain legal title the details of a specific invention, such as how to create a specific drug molecule, are made available for anyone to view – including competitors. This provides easy opportunities for intentional infringement and counterfeiting, especially in countries where the assignee of the IPR has not applied for such rights, or where these rights are more easily disregarded due to limited regulatory controls.

5.4.4. Pre-Patent Phase

The majority of high value IPRs occur as patents. Patent applications are extremely vulnerable to disclosure during the drafting phase, prior to submission. The content of a draft patent (prior to submission) is actually PI.

5.4.5. Product Diversion and "Grey Markets"

Products which embody IPRs, as with any product, are vulnerable to product diversion and grey markets. These activities, which are typically undertaken by

62 Cyr, D. (1998). "High Tech, High Impact: Creating Canada's competitive advantage through technology alliances", Academy of Management Executive, 13, 2, pp.17-26.

63 Larson, A. (1992). "Network dyads in entrepreneurial settings: a study of the governance of exchange relationships", Administrative Science Quarterly, 37,pp.76-104.

organised criminal networks, prevent the assignee from realising their entitled revenue through lost profits or royalties. More importantly, these activities substantially damage the company's reputation and brand. These activities typically fall under the purview of national Customs agencies who should be contacted if enforcement assistance is required.

5.4.6. Validity of IPRs

The validity of any legally valid IPR can be challenged through the relevant court in a jurisdiction where that IPR is held. Generally, legal challenges are undertaken by rival companies who wish to remove a competitor from a position of influence in the market. With IP the obligation to prove ownership is generally the responsibility of the assignee or inventor, meaning that the assignee or inventor may be liable for any court costs involved in the pursuit of their legal rights64. Legal fees for IP litigation are outrageously expensive - in 1997 the direct costs associated with enforcing a patent were between USD$1m and $3m illustrating the scope of the problem. Other factors involved in settling IP disputes include time lost for normal business, the impact on employees and management, and importantly the prospect of bad publicity and subsequent effects on share price[65].

64 McGuinness, P. (2003). "Intellectual Property Commercialisation: A Business Managers Companion", LexisNexis Butterworths, Australia.

65 McGuinness, P. (2003). "Intellectual Property Commercialisation: A Business Managers Companion", LexisNexis Butterworths, Australia. Somaya, D. (2003). "Strategic Determinants of Decisions not to Settle Patent Litigation", Strategic Management Journal, 24, 17-38.

6. THREATS AND PERPETRATORS

6.1. Internal Perpetrators

Internal perpetrators are those that originate from within an organisation. Typically, internal perpetrators include employees, consultants and contractors who by virtue of their position, or the limited protection of IAs, are provided with privileged information from within an organisation. Prompted by a range of motives, including opportunism, dissatisfaction, malice, revenge, accident, gain or even naivety, internal perpetrators abuse their trusted position to disadvantage the organisation in some way.

Internal perpetrators can also arise from trusted third parties such as joint venture collaborators, suppliers, distributors and financiers to name a few. Although these parties may have different levels of access to IAs they may still pose a threat and should be evaluated in terms of the following:

- Access and exposure to valuable information;
- Legal remedies in place (such as Non-Disclosure or Confidentiality Agreements);
- Internal security practices within each individual entity; and,
- Competitive and market positioning.

6.2. External Perpetrators

As the name suggests external perpetrators are those that originate from outside of an organisation. Examples of external perpetrators in the area of intellectual assets can be categorised similar to those found in other areas of security as illustrated in Table 2 below.

Table 2: Examples of External Perpetrators

SOURCES	EXAMPLES	OVERVIEW	COMMENT
Criminals	Organised Crime, Small time (opportunistic) criminals,	Operating covertly and motivated by financial gain, they are motivated, organised, skilled, and capable. Often well resourced and planned, but with low tolerance for risk to themselves.	Require significant barriers to effectively deter. Activities often go undetected in the case of fraud etc and generally cause little direct damage but significant downstream impacts.
Compromised Persons	Emotionally, psychologically, substance abusers. Employees (extortion, bribery, etc)	Characteristically very committed, with little regard for consequences to themselves.	Uncommon but extremely difficult to anticipate or deter. This group will generally seek to cause maximum damage.
Crusaders	Issue Motivated Groups	Motivated, often well organised, resourced and planned. Intent is to disrupt activities and/or attract media attention.	Usually operate within the law. Consequences can usually be mitigated by sound management practice. This group will generally seek to cause maximum publicity.
Chance Intruders	Hackers, staff, visitors, students, research interns	Breach security out of curiosity. Opportunistic and easily deterred by basic precautions. Causes losses inadvertently (if at all).	Principal risks from this group include the trespass, business interruption, introduction of viruses, data corruption or damage to network systems (Eg. Staff entering server rooms).
Conflict	Politically Motivated Groups, Terrorists or Foreign Intelligence Services	Highly motivated, resourced and trained, this group is motivated by international political activities or ambitions.	Most organisations are unlikely to be capable of deterring this threat without recourse to significant external resource.
Commercial Advantage	Competitors, Suppliers, Business Intelligence Collectors	Seeking commercial advantage from IP or information, this group is highly motivated and resourced.	Determined offenders are difficult to deter however basic precautions are effective against the casual offender. With little appetite for confrontation, this group will normally operate covertly, often leaving no trace of their activities.
Control	Internal or external groups	Introduction of risks due to political circumstances, change of policy, etc	Often difficult to anticipate or control but will benefit from continual monitoring.

The spectrum of perpetrators is specific to each organisation and obviously depends upon the nature of the business that the organisation is engaged in.

Companies engaged in scientific or technical research with national security implications are more likely to be targeted by foreign intelligence services, and terrorist groups. Organisations producing consumer goods (such as computer games, pharmaceuticals or machine parts) are more likely to be targeted by Organised Crime through some sort of counterfeiting operation. All organisations, irrespective of industry, are potential targets for competitors, business intelligence collectors, interns, students and opportunistic criminals.

6.3. Motives

A range of motives which were originally developed for fraud can also be applied to non-fraud threats against IAs[66]. As illustrated below these motives have been categorised on the basis of whether they are internal or external:

Table 3: Motivations of Potential Attackers

Motivations to Commit Internal Fraud	Motivations to Commit External Fraud
• Greed • Revenge • Blind ambition • Ego • Disillusionment • Ownership of research / knowledge • Job insecurity • Personal Debt • Over-work • Poor remuneration (actual / perceived) • Recognition	• Blackmail • Conspiracy • Corruption or financial self-interest • Self-interest (job offer elsewhere; feels competition will 'value' them more) • Sex • Ideology • Compromise • Ego

6.4. Threats

The threats to IAs can be categorised as either commercial or criminal threats depending on their nature. Commercial threats are more likely to involve civil proceedings whilst criminal threats (such as counterfeit pharmaceuticals which subsequently result in the death of a patent) typically involve criminal legislation. Commercial threats can come from:

66 Pickett, Pickett (2002). "Financial Crime Investigation and Control", John Wiley and Sons, USA. Curwell, P. (2004). "Intellectual Asset Fraud: Preventative Strategies in Knowledge-dependent Companies", unpublished thesis, The University of Queensland Business School, Brisbane, Australia.

6.4.1. Joint Ventures and Alliances

Alliances and Joint Ventures bring together distinct companies or organizations, as opposed to the individuals involved in smaller networks or IC webs, to achieve a sizable goal such as bringing a drug to market[67]. All parties allocate resources towards the goal on the basis of agreeing to share the benefits of the end result. Despite the many advantages of participating in an alliance, one major drawback for the knowledge creating company is that a certain level of trust or faith is required on behalf of the disclosing firm to permit the sharing of proprietary information in the hope that by sharing such knowledge there will be reciprocation on the part of other participants[68].

6.4.2. Mergers and Acquisitions

The merger and acquisition (M&A) process involves a high degree of disclosure in terms of information. In the case of research companies, where information is their primary asset, IAs will also be examined. The danger from the M&A process is that an organisation will disclose its PI to what subsequently materialises as an unsuccessful activity. Dangers also arise from a lack of control over who has access and, potentially, where copies of information are sent to. In poorly executed M&A activities the organisation can be exposed to the full spectrum of internal and external perpetrators.

6.4.3. Market Competitors

Market Competitors are entities operating in a similar space in the market to the owner of the patent. Many competitors will not countenance the thought of engaging in unscrupulous business practices. However, some do and the threat from competitors is omnipresent. Two of the most common tactics used by competitors are Industrial Espionage and Infringement of IPRs.

There have also been instances of companies who have obtained a competitor's R&D data so as to duplicate that R&D project in an accelerated fashion. This results in the production of a product earlier than the true inventor. This often precludes the rightful inventor from obtaining IPRs on their product but also removes any competitive advantage they may have. These sorts of activities can result in millions of lost revenue in terms of time, R&D seed funding and opportunity cost. In some instances, particularly with small to medium sized enterprises, a subsequent loss of capital is also incurred from potential investors.

67 Powell, W.W. (1998). "Learning from Collaboration: Knowledge and Networks in the Biotechnology and Pharmaceutical Industries", California Management Review, 40, 3, 228-240.

68 Baughn, C.C., Denekamp, J.G., Stevens, J.H., Osborn, R.N. (1997). "Protecting Intellectual Capital in International Alliances", Journal of World Business, 32, 2, pp.103-117.

6.4.4. Business Intelligence Collectors

Business Intelligence Collectors often frequent trade shows and conferences where they have direct access to individual researchers. Many researchers feel quite passionate about their research and some have a tendency to reveal too much in the belief that they are talking to a fellow researcher (obviously critical information should not be revealed irrespective of whether the person is a legitimate researcher or not without the proper legal agreements being in place). These revelations can jeopardise a company's competitive, and potentially IPR, position.

6.4.5. Financiers

Financiers can include banks, venture capitalists or investment angels. Typically an investment is only made after full disclosure of a company's activities, including a review of IAs. This activity can increase the dissemination of PI, with Trade Secrets being particularly vulnerable to future intentional or unintentional disclosure.

6.4.6. Consumers

The most prominent consumer threat to IAs arises in the area of copyright infringement and/or licensing abuse. These activities are more commonly referred as 'piracy' and typically affect music, film and computer software. Whether consumer piracy activities represent a case of copyright infringement or licensing abuse is product specific. For example, copyright infringement occurs when someone duplicates a copyrighted product without permission. Most copyright legislation permits a certain amount of a copyrighted item to be copied without permission. Where the copy quota is exceeded an infringement occurs.

Licensing abuse is more common with music, movies and computer software. Licensing abuse is reviewed in detail below. The most interesting fact about the consumer threat is that most of the IP at risk by this group is popular consumer goods. Unfortunately, a significant proportion of the consumer threat group are those to whom product marketing and sales are directed, such as young people, but that same target market is also least able to afford these consumer goods. This undoubtedly has some impact on the prevalence of licensing abuse and copyright infringement and creates a whole new set of problems for the security practitioner working in this domain.

6.4.7. Criminal Threats

Criminal threats are predominately external, although the spectre of infiltration-based threats combines an internal and external basis for the threat.

6.4.8. Organised Crime

Organised criminal elements may be involved in any activity from the theft of PI through to counterfeiting of products in the marketplace. Often, the theft of PI is achieved through the use of insiders. The insider threat is discussed in more detail below. Criminal elements who participate in this type of intentional IPR infringement typically copy the complete product, even down to the product's Trade Marks, branding and packaging. The perpetrators of this type of activity are most often Organised Crime elements within a particular community and their activities are referred to as 'counterfeiting' (forgery is a distinctly different concept to counterfeiting although it is often mistakenly used interchangeably)[69].

Organised Crime elements have proven their willingness to counterfeit anything that is capable of generating a profit. Patented products most commonly counterfeited include[70]:

- Machinery components (especially vehicle and aircraft replacement parts);
- Pharmaceuticals and Nutraceuticals; and,
- Consumer electronic goods (computer software, music, movies and other 'pirated' goods).

Importantly, patented goods counterfeited by organised crime do not have to actually work as the legitimate owner intended. All that is really required is to complete the exchange of sale – the criminal has no interest in providing a warranty for their product. Counterfeiting is one IP crime that typically cuts across multiple individual IP rights. For example, a counterfeit machine part complete with packaging might infringe on a patent, design right, trade mark and copyright.

6.4.9. Small time, opportunistic Criminals

Small time criminals are typically opportunistic. They can make attacks directly on the IAs of an organisation, such as breaking and entering to steal a laptop, or may seek to exploit IPRs on a small scale such as by selling pirated software to friends.

6.4.10. Foreign Intelligence Services, Terrorists and Insurgent Groups

Foreign Intelligence Services (FIS), Terrorist and insurgent groups are treated collectively as their modus operandi is very similar. Economic Espionage conducted by FIS has been on the increase since the 1970s, prompting the US

69 SOCA (2006). "The United Kingdom Threat Assessment of Serious Organised Crime", Serious Organised Crime Agency, United Kingdom.

70 Hopkins, D.M., Kontnik, L.T., Turnage, M.T. (2003). "Counterfeiting Exposed: Protecting Your Brand and Customers", John Wiley Publishers, New Jersey, USA.

Government to enact the Economic Espionage Act of 1996[71]. At least twenty countries, including developed and undeveloped nations, have been identified as actively tasking their intelligence communities to the collection of scientific, technical and economic information in the USA. However, there is no reason to assume that the USA is the sole target of these efforts. It is important to remember that there is no such thing as a friendly intelligence agency.

In 2002 the President of the USA has established an Office of the National Counterintelligence Executive (NCIX) to provide advice to Government and Industry[72]. Similar advice is also provided through the US Department of Commerce Bureau of Industry and Security and the US Department of Defense. Unfortunately, no such advisory mechanisms exist in most countries, including Australia, although the Australian Security Intelligence Organisation (ASIO) has recently established a Business Liaison Office which could potentially provide such advice in the future.

This category of threat generally seeks to remain undetected and typically have a defined objective, such as obtaining specific information on a topic. These objectives may be achieved through the use of techniques including cultivating and running agents and sources, technical intelligence collection techniques (telecommunications intercepts and technical surveillance), surreptitious entry, optical surveillance, social engineering and the use of insiders[73]. Insiders can be recruited through a variety of methods including blackmail, extortion and threat of (or actual) violence. In the average company it is very unlikely that FIS activities, at least by any competent service, will be detected without significant effort or outside assistance. Whilst it is hoped that any activity by this threat will, if detected by the intelligence community or law enforcement, be addressed discretely with the organisation concerned such action may not always occur.

Security practitioners should use the threat assessment process to determine whether they may be at risk from this specific threat. Sufficient open source information on the practices of these groups is available to determine whether an organisation may be a target. For example, if an organisation is involved in research relating to a microbiological agent of obvious use to a terrorist group then a potential threat can be considered to exist. The threat assessment process should evaluate the threat, ideally in conjunction with intelligence agencies or law enforcement, and determine appropriate security measures to manage risk.

71 Van Cleave (2005). "Statement for the record: House Judiciary Committee on Immigration, Border Security and Claims hearing on source and methods of foreign nationals engaged in economic and military espionage", National Counterintelligence Executive, 15 September 2005, United States Government, available at www.ncix.gov.

72 National Office of the CounterIntelligence Executive, www.ncix.gov

73 Van Cleave (2005). "Statement for the record: House Judiciary Committee on Immigration, Border Security and Claims hearing on source and methods of foreign nationals engaged in economic and military espionage", National Counterintelligence Executive, 15 September 2005, United States Government, available at www.ncix.gov.

TECHNIQUES REGULARLY EMPLOYED BY FIS TO COLLECT PROPERTY INFORMATION (as identified by the US National Counterintelligence Executive)[74]
• In the majority of cases foreign collectors simply ask for the information or technology.
• Exploitation of visits to businesses or facilities
• Computer network penetration (hacking etc)
• Business travellers abroad (especially laptops and PDAs)
• Use of research interns or work experience students
• Provision, or offers, of services or technology (particularly IT support) from foreign firms to target organisations
• Joint ventures and cooperative research with, or buyouts of, target firms.
• Exploitation of offices (or LAN/WAN/VPN access to), target companies from their offices or subsidiaries overseas.

Table 4: Proprietary Information Collection Techniques

Additional techniques that may also employed by foreign intelligence services to collect Proprietary Information include:

- Corruption, collusion and coercion;
- Infiltration of agents as employees; and,
- Forced or surreptitious entry.

6.5. Specific Threats: IPR Infringement

There are two recognised types of IP *infringement – intentional infringements ('violations')* and *unintentional infringements ('errors')*. In any infringement case it is imperative to determine whether the act was committed wilfully and with intent. Where intentional infringement is found to have occurred by a court the infringer's liability for damages is substantially increased.

Intentional Infringement is where the infringer knows that an object has been protected by an IPR and chooses to wilfully undertake an activity which will infringe that IPR despite legal ownership being assigned to another party[75]. *Intentional Infringers* are typically organised criminal groups / networks, such as counterfeiters, or business competitors.

74 Ibid

75 McGuinness, P. (2003). "Intellectual Property Commercialisation: A Business Managers Companion", LexisNexis Butterworths, Australia.

Point of Law

It is lawful for a third party to reproduce a patented product in a country where the inventor or assignee has not filed for a patent (applications for a patent must be filed in each country where the holder wishes to receive such protection and must also be renewed annually). In these circumstances, third parties can manufacture and sell such products provided they do not attempt to export them to a country where a valid patent is held. This activity is generally in breach of Customs regulations and other legislation for the jurisdiction concerned. These sorts of offences are generally treated as civil rather than criminal matters.

Unintentional Infringement usually results from organizations failing to perform adequate, or any at all, due diligence activities[76]. If an organization produces products or services it is that organizations' responsibility to survey the market to identify whether there are other organizations performing similar tasks. Provided these tasks are not the subject of IPRs, such as a patent, infringement cannot occur[77]. Where due diligence activities have not been performed thoroughly pre-existing IPRs may be overlooked. *Unintentional Infringers* may still be required to pay damages for the infringement although the damages are likely to be less severe than if the infringement is intentional[78].

Point of Law

The burden of proving infringement, and then Intentional versus Unintentional Infringement, rests on the plaintiff who is usually the inventor or assignee for the patent.

Solutions to litigation include mergers, acquisitions, licensing, or sales and IP assignments[79]. Irrespective of the solution undertaken, to defend the company against unintentional infringement and associated sunk costs it is recommended

76 Ibid

77 Ibid

78 Ibid

79 Bednarek, M., Ineichen, M. (2004). "Patent pools as an alternative to patent wars in emergent sectors", Intellectual Property and Technology Law Journal, 16, 7, pp.1-5.

that firm's undertake regular patent screening, due diligence, and competitive intelligence activities at all levels so as to minimise risk exposure[80].

The role for Security in Infringement cases generally relates to the provision of investigative services and the handling of evidence. Depending on the organization, security staff may be involved in proactive approaches including the provision of awareness training and the performance of intelligence functions within the market.

6.6. Specific Threats: Fraud

Fraud is defined as "*obtaining a benefit by deception*", where a benefit can be tangible (such as money or property) or intangible (such as information or an advantageous negotiating position with respect to an employee's remuneration)[81]. External IA fraud involves attempts by competitors to obtain assets belonging to another, whether tangible or intangible, with the goal of profiting from the deception. External fraud primarily consists of two activities:

- Intentional infringement of IPRs through activities such as counterfeiting; and,
- Licensing abuse.

External fraud relating to IAs is much less common in comparison to internal fraud, with only around 15% of all fraud being committed predominately by competitors[82]. One obvious exception to this concerns music, movies, computer software where the volume of external fraud is significant.

In part, the issues arising from external IA fraud are created by the international Intellectual Property system itself. The problem with IP is the assumption that others will respect the rights conferred by the WIPO conventions and not intentionally infringe on those rights. Unfortunately this situation is not always the case, and as highlighted in the eighth annual Ernst and Young Global Fraud Survey[83]. An outline of the external threats to IAs are listed in the table below[84]:

80 Barrett, B. (2002). "Defensive use of publications in an intellectual property strategy", Nature Biotechnology, 20, 191-193.

81 Attorney-General's Department [AG] (2002). "Commonwealth Fraud Control Guidelines", Commonwealth of Australia, Canberra.

82 ASIS (2002). "Trends in Proprietary Information Loss Survey Report", American Society for Industrial Security, Pricewaterhouse Coopers, and US Chamber of Commerce and Industry, www.asisonline.org [accessed 07MAR03].

83 Ernst & Young (2003). "Fraud: The Unmanaged Risk", 8th Global Survey, Global Investigations and Dispute Advisory Services, Ernst and Young, South Africa.

84 Hamilton, P. (1967). "Espionage and Subversion in Society", Hutcheson, London, pp.222-223. Curwell, P. (2004). "Intellectual Asset Fraud: Preventative Strategies in Knowledge-dependent Companies", unpublished thesis, The University of Queensland Business School, Brisbane, Australia.

POSSIBLE EXTERNAL THREATS TO INTELLECTUAL ASSETS
• False negotiations, alliances, or partnership propositions • Industrial spies (business intelligence collectors), moles, and people 'planted' within the organization • Hiring former employees with the goal of soliciting information about the former employer • Theft and burglary • Bribery, blackmail or extortion of the organisation itself, employees, suppliers, or distributors, whether for money or information, within the supply chain • Eavesdropping, stealing rubbish ('dumpster diving'), and other similar activities • Information and Communication Technology-based threats including hacking, 'war driving' (the use of Signals Intelligence or Electronic Warfare techniques to exploit wireless communications), and other computer crimes. • Licensing abuse

Table 5: Potential Threats to Intellectual Assets

The previous table illustrates the variety of external threats to IAs. Many of the threats have been in existence for some time and are commonly variations on traditional military or intelligence techniques. However, the threat of licensing abuse specifically IP relates to IAs.

For ease of reference a typology of Intellectual Asset Fraud has been produced. Whilst there are undoubtedly new types of fraud arising this typology provides the security practitioner with a ready reference to the more common frauds affecting knowledge-based organisations[85].

Taxonomy of Intellectual Asset Fraud[86]

The following table presents a typology of the most common internal frauds against IAs:

85 Curwell, P. (2004). "Intellectual Asset Fraud: Preventative Strategies in Knowledge-dependent Companies", unpublished thesis, The University of Queensland Business School, Brisbane, Australia.

86 Ibid.

ISSUE	ACTIVITY	IMPACT
Misappropriation of Intellectual Assets	• Theft of proprietary information • Embezzlement of knowledge generated in the course of working at the firm • Withholding intellectual assets from an employer for the purposes of capitalising upon those assets on termination of employment • Use of proprietary knowledge for unauthorised purposes	• IP and IC • Competitive advantage • Financial viability
Misleading or Deceptive Conduct	• Failure to disclose ideas, data, or concepts which are directly relevant to an employee's position of employment within their firm as required under Australian Employment Law. • Intentionally deceiving the firm of its rightful intellectual assets • Misleading the firm by failing to disclose, or providing an untrue, version of events so as to obtain a benefit which would not have occurred naturally.	• Knowledge Generation • IP outcomes • Competitive Advantage
Conspiring to disadvantage the firm	• Encouraging others to improperly document research outcomes so as to prejudice the firm's ability to obtain credible IP rights	• IP portfolio opportunities
Misrepresentation	• Falsification of research results to benefit a particular outcome or position	• Long-term Competitive Advantage • IP portfolio
Unauthorised disclosure	• Unauthorised disclosure of proprietary information, such as before patenting. •	• IP portfolio • Competitive Advantage
Academic Misconduct	• Failure to properly acknowledge the contribution of others to research outcomes for one's own benefit. • Misappropriation of the ideas or concepts of others with the intention of gaining recognition for those ideas or concepts at the expense of the inventor.	• Knowledge sharing

Table 6: Typology of Internal Intellectual Asset Fraud[87]

Whilst there is some degree of similarity between many internal and external frauds the focus is inherently different. A typology of external frauds against IAs is presented in the table below:

87 Ibid

ISSUE	ACTIVITY	IMPACT
Misappropriation of Intellectual Assets	• Declaring an untrue version of events as they occurred in the course of negotiations and research disclosures for the benefit of another • Theft of Trade Secrets or confidential information for the purposes of improving a competitors market outlook • Industrial Espionage	• IP and IC • Competitive Advantage • Financial Viability
Academic Misconduct	• Failure to properly acknowledge the contribution of others to research outcomes for one's own benefit. • Misappropriation of the ideas or concepts of others with the intention of gaining recognition for those ideas or concepts at the expense of the inventor.	• Knowledge sharing
Conspiring to Disadvantage others	• False negotiations, alliances, or partnerships • Licensing Abuse • Misrepresentation of one's position so as to gain access to otherwise restricted information • Industrial Espionage	• IP position • Protection of IC • Competitive Advantage
Intentional Deprivation of IP Rights	• Failure to nominate inventors on a patent • Patent Infringement • Copyright Infringement • Trademark Infringement • Licensing Abuse	• IP portfolio • Financial position of the firm in question
Falsification of Events	• Declaring an untrue version of events as they occurred in the course of negotiations and research disclosures for the benefit of another • Falsification or misrepresentation of research data in the course of a patent application	• IP portfolio
Obtaining Benefits by Solicitation	• Bribery, corruption, extortion and blackmail so as to solicit proprietary information from former employees • Industrial Espionage	• Security of Intellectual Assets • Competitive Advantage

Table 7: Typology of External Intellectual Asset Fraud[88]

88 Ibid

6.7. Specific Threats: Licensing Abuse

A license is effectively a legal agreement between the owner of the product being licensed (the 'licensee') and the user of that product (the 'licensor'). Licensing provides opportunities for knowledge-creating companies to generate capital at all stages of the R&D pipeline and can also generate new options for market strategies and profits across industries or regions which are not the primary focus of the licensee. Akin to renting a house, licensing also provides the licensor with complete flexibility, allowing them to generate capital ('royalties') for a specified period of time, in a specified geographical region, for specified activities on their terms (assuming they can be agreed upon by the licensee). According to surveys conducted by Kroll, the threat of licensing abuse is growing[89]. In reality though, it has probably always been an issue. It is more likely that poor awareness of the problem, coupled with proprietary sensitivities and the absence of appropriate surveys are responsible for the increased reporting.

Licensing Demystified

In the case of computer software the cost of the product, such as Microsoft Office, is generally the licensing fee. Purchasing a copy of Microsoft Office does not necessarily mean it is owned by the consumer. The consumer has merely purchased a single user licence providing them with accessibility to the software on one computer only. Licensing abuse occurs where a consumer accepts the terms of a license for an item of IP and then breaches the terms of that licence. Referring back to the Microsoft example earlier, with a single user license it is probably perfectly acceptable to install the software on one computer. However, the license may be breached where the software is installed on multiple computers (irrespective of the owner).

Increasingly, companies are either blatantly infringing one another's rightful IP for their own benefit, or they are purchasing some licences and failing to abide by the terms agreed at purchase. Most licenses for IP contain audit clauses whereby the *licensor* is permitted to audit the *licensee* to ensure they are abiding by the terms as required[90]. Commonly, licensees are required to pay royalties

89 Kroll (2003). "Catch them if you can – are you doing enough to safeguard your intellectual property? The Kroll Global Survey on Corporate Response to IP Abuse", www.krollworldwide.com [accessed 12JUN04].

90 McGuinness, P. (2003). "Intellectual Property Commercialisation: A Business Managers Companion", LexisNexis Butterworths, Australia.

on top of lump sum payments for the licence itself, and it is these royalty payments that should be the prime concern of the licensor[91].

What is not common to licensing considerations is how to protect the licensor from license fraud, with the Kroll survey indicating that 44% of licensors have no license audit coverage at all, whilst a further 36% only audit occasionally[92]. The survey work undertaken by Kroll indicates that many licensees are abusing the terms of the licence, either intentionally or otherwise; however, the licensor is often uninterested or unable to audit the licensee and is thus reliant upon honest reporting from the firm[93]. Given that many knowledge-creating companies create IP portfolios with the goal of raising revenue from licensing, it is important to note that these same companies are unlikely to be realising their true profits as a result of licensing fraud – at least from the perspective of an investor.

6.7.1. Specific Threats: Espionage

There are effectively two types of espionage activity that relate to IAs:

- Economic Espionage is generally performed by State actors, such as Foreign Intelligence Services, and typically aims to obtain or influence scientific, technical or economic data94.
- Industrial Espionage is performed by non-State actors, such as competitors or business intelligence collectors95.

The differences between Economic and Industrial Espionage are typically defined by the motivations of the perpetrators, and from a legal perspective by each nation's criminal legislation, although "Economic Espionage" may is a relatively new term and may simply be referred to as "Espionage".

6.8. Specific Threats: Insiders

Insiders become a threat when they are given access to information, products or technology, by virtue of their positions, which would not normally be available. There is a strong chance that many incidents will remain undetected, or if they are detected by fellow workers, go unreported. In this regard the security threat posed by insiders is very similar to that of internal fraud. Indeed, the major delineation between a fraud or security threat is a legal definition hence, it is possible to draw reliable inferences from fraud research and apply them to internal security.

91 Cohen, W.M., Merrill, S.A. (Eds.) (2003). "Effects of Research Tool Patents and Licensing on Biomedical Innovation", in Patents in the Knowledge-Based Economy The National Academies Press, Washington D.C.

92 Kroll (2003). "Catch them if you can – are you doing enough to safeguard your intellectual property? The Kroll Global Survey on Corporate Response to IP Abuse", www.krollworldwide.com [accessed 12JUN04].

93 Ibid

94 Nasheri, H. (2004). "Economic Espionage and Industrial Spying", Cambridge University Press, England.

95 Ibid

Many of the perpetrators of internal crime work alone and apply their ill-gotten gains for personal reward, or they may sell them to a competitor, business intelligence collector or criminal element. At the other end of the spectrum is the organised activity which may involve infiltration of criminal elements into a company under the cover of a legitimate employee, job applicant or the recruitment of source and agents, by criminal elements for the purposes of obtaining information or committing a specific act.

The task of the insider is often simplified by the absence or inadequacy of internal controls and security arrangements. Technology can also be a major vulnerability in terms of the protection of proprietary information. Whilst some insider threats towards information or data are perpetrated by low-technology approaches, such as stealing a paper copy of a document, a considerable volume of data is easily removed by products such as iPods, USB sticks and USB watches. Unfortunately there is no universal solution to the insider threat problem save for a well conceived and implemented, organisation wide, security plan.

6.9. Specific Threats: Computer Crimes

Whilst making IAs readily available computers have also created new threats and vulnerabilities. IPRs can be infringed and licenses abused using computers. However, access to an organisation's PI can also be obtained through techniques such as hacking or by using vectors such as viruses and malware to extract information or obtain login details. Information and Communication Technology (ICT) Security is an entire field in itself and will not be dealt with here, save for mentioning that an adequate level of security is unlikely to be afforded to IP and PI unless the security plan manages the risk exposure incurred through computers and associated networks.

6.10. Outlook

Given the ever increasing reliance on IAs within commercial operations more and more products, in particular, are being protected through IPRs worldwide. This will increase pressures on both sides of the market (owners/assignees versus their competitors) in terms of effectively managing their assets. As these pressures increase the market surveillance and enforcement functions will continue to gain importance within knowledge-based companies more broadly.

Conversely, legitimate (non-criminal) competitors are likely to come under pressure to innovate so as to survive. Competitors who are unable to innovate and produce their own inventions may be tempted to infringe on the IPRs of others to remain viable. In specific markets, such as Biotechnology and Pharmaceuticals, there is also a high volume of patenting within a relatively small research domain. This increases the likelihood of unintentional infringement and legal challenges to granted IPRs. It also provides increased scope for the use of illegitimate tactics by competitors such as Industrial Espionage and 'insider-based' threats.

7. PROTECTING INTANGIBLE ASSETS IN THE R&D ENVIRONMENT

7.1. Effectiveness

It is essential that the security professional within a knowledge-creating company understands the dynamics of how knowledge is created and shared and the steps involved in any research activity. Only when these dynamics are completed appreciated is it possible to develop and implement a tailored security plan specific to the organisation and to begin the organisational change process to empower employees to protect the company's intellectual assets and ultimately their own interests. Employee buy-in and commitment to the company is perhaps the most essential element of any security program within a knowledge-creating company.

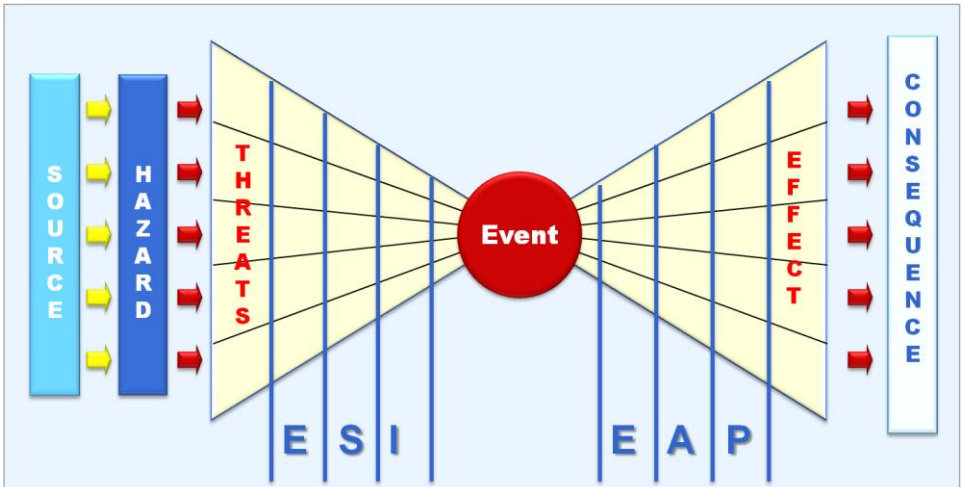
Without employee support at all levels, from senior management to the most junior researcher, proprietary information holdings will not be adequately secured. One example of this is when the employee is away at a conference and engages in detailed technical discussions with their scientific peers who may also be competitors (or employees of competitive intelligence firms). Employee buy-in impacts directly on the security professional's ability to maintain the integrity of PI within an organisation. This buy-in also depends upon awareness and education as to the risks amongst employees and associates of the organisation. This is clearly the responsibility of the organisation.

To be truly effective the security measures employed to protect proprietary information should be seamless and cover the entire operational risk spectrum. The ESIEAP Model is a useful tool to assist managers in planning how to manage PI and IP risk exposure, as illustrated in the following table:

Table 8: Application of ESIEAP to Management of Risk to IA

Risk	[Internal] – Unauthorised disclosure of PI	[External] – Infringement of IP Rights by a third party
Eliminate the risk	Don't disclose PI **This may not be an option, so:**	Don't trade in markets where IPRs are not easily enforced (e.g. against counterfeiting etc)
Substitute the risk	Limit disclosure to a select few	Implement market surveillance and enforcement programmes
Isolate the asset	Employ security in depth principles to shield the asset	Obtain a robust, extensive portfolio of IP rights (especially with patents)
Engineering controls	Introduce ICT and Information Security controls	Conduct compliance monitoring (especially licensees / customers)
Administrative controls	Utilise pre-employment screening; Introduce robust policies and procedures	Conduct due diligence and thoroughly document actual or potential collaborations
Protective equipment	Utilise IP assignments, Non-Disclosure agreements, non-competition agreements etc	Impose limiting sales contracts (i.e. no resale clauses), MOUs and competitor intelligence programs

The ESIEAP model illustrated above can be used independently or in conjunction with other holistic approaches such as the 'Surveiller Cycle' (see 7.3 below) to provide a comprehensive toolset for understanding and responding to IA risk exposure within the knowledge-dependent organisation. It can be envisaged as fitting more holistically into the overall risk management process when viewed in conjunction with the "Risk Bow Tie" model, pictured below:



Note: *The alignment of ESIEAP with Bow Tie is provided as an INDICATIVE MODEL ONLY. ESI not will always align with likelihood management nor will EAP necessarily be associated with consequence management. In some cases however, it may prove useful to consider Bow Tie in alignment with ESIEAP for discussion purposes.*

Figure 5: Bow-Tie and ESIEAP

Whilst there are many different controls and risk management methodologies available to security managers, some or all of which may be applicable depending on the specific situation, it must be appreciated that within knowledge-creating companies the security measures employed must be omnipresent yet unobtrusive. Obtrusive security measures within a knowledge-creating company stifle innovation and effective knowledge exchange. Remember that innovation and effective knowledge exchange are the core business of a knowledge-creating company and that without such activities these companies will cease to exist. Any security professional who proposes obtrusive/intrusive security measures within a knowledge-creating company is likely to face significant opposition from all levels of the organisation. At the very least, if the presence of these security professionals continues to be tolerated their recommendations are unlikely to be accepted.

The problem for knowledge-creating companies is the impact that a more restrictive environment may have on the free flow of knowledge, especially during the early stages of research and development. This also makes the firm more vulnerable because employees in knowledge-dependent firms are often

highly educated and therefore find themselves working in a less structured and monitored environment. This offers more opportunities for crimes such as fraud[96]. As a result of the interrelationships between rigid employment environments and poor creativity, the role of security awareness training and good human resource practices are paramount. The first line of defence against fraud lies with employees themselves, both as possible perpetrators and whistleblowers[97]. In addition to recognizing the value of employees to preventing fraud, it is relevant to consider the reasons why people often commit fraud, and the types of personalities often found within an organization. About fifty percent of individuals will take advantage of a situation and bend or break the rules if the situation is appropriate[98].

7.2. Human Capital Issues

One of the most serious human-capital issues for knowledge dependent companies is that some employees who commit fraud have admitted that the prime motivation for their actions are that they feel they do not receive the recognition they deserve from their employer for particular actions, especially in the domain of research breakthroughs[99]. This adds yet another layer of complexity to the protection of IAs. Typically, morale may not be considered as a control in asset protection as other more reliable alternatives are available. However, when dealing with intangible assets that may lie inside an employee's head, employers may need to do everything possible to gain the commitment of employees towards an endeavour. Creating a positive work environment is one way of helping to manage the problem, as well as other factors such as remuneration and recognition.

This situation has the potential to dramatically affect the culture of the organization in relation to the development and sharing of knowledge, as well as impacting upon the willingness of the employee to impart their knowledge to other staff and with their employer[100]. Failure to acknowledge achievements of employees in an organisational structure where the balance of knowledge power lies with the bulk of employees could easily create a culture where employees cease to care about the progress of their company, and stop providing information as they would normally because they feel it will not be received in the fashion that it deserves. Instances where employees feel maltreated by their

96 Pickett, Pickett (2002). "Financial Crime Investigation and Control", John Wiley and Sons, USA. Huntington, I.K. (1992). "Fraud: Prevention and Detection", Butterworths Publishing, UK.

Isacson, J.P. (2000). "Maximising profits through intelligent planning and implementation", Nature Biotechnology, May, 18, pp.565-566.

97 Medd, K, Konski, A. (2003). "Workplace programs to protect Trade Secrets", Nature Biotechnology, 21, pp.201-203. O'Gara, J. (2004). "Corporate Fraud: Case Studies in Detection and Prevention", John Wiley Publishers, USA. Fenton-Jones, M. (2004). "Culture key to employee fraud", Tuesday 28 September 2004, The Australian Financial Review, p.50.

98 Pickett, Pickett (2002). "Financial Crime Investigation and Control", John Wiley and Sons, USA. Huntington, I.K. (1992). "Fraud: Prevention and Detection", Butterworths Publishing, UK.

99 Medd, K, Konski, A. (2003). "Workplace programs to protect Trade Secrets", Nature Biotechnology, 21, pp.201-203.

100 Peebles, E. (2002). "Inspiring Innovation", Harvard Business Review on The Innovative Enterprise, HBS Press, Boston, USA.

employer have historically resulted in a combination of internal and external fraud[101].

It is essential that staff with access to R&D data, are remunerated adequately. Ideally, remuneration packages for those involved in creating R&D data should be structured to provide share options in the event that a product makes it successfully to market. An options based approach is suitable here as it does not require capital commitments until the product is successful. Providing employee buy-in in this manner also helps to encourage reporting of suspicious activities by co-workers. Surreptitious behaviour in highly technical areas may not be detected without specialist knowledge. Adequate remuneration helps obtain buy-in from all employees. As all employees are likely to suffer a loss at the hands of a few individuals their tendency to report such behaviour is increased.

This can help to minimise loss of any information whilst providing an opportunity to strengthen the bonds of loyalty between employees and the employer. Some companies have mentoring arrangements to further guide and develop employees at all levels of the business, which can also help increase employee loyalty and commitment. Booz Allen Hamilton typically assigns a junior and senior mentor to all employees. This not only assists with the employee's personal and professional development but can also provide a confidential avenue for employees to raise grievances or to question particular business practices in private. Mentoring practices can provide an avenue to gain perspective on why a company undertakes a particular practice and can therefore gain employee acceptance voluntarily rather than force acceptance through stringent controls and management oversight. Providing a mechanism for disgruntled employees to publicly raise grievances with senior management in an anonymous and transparent manner is also critical to minimising these risks.

7.3. The 'Surveiller Cycle' as a Potential Solution

The Surveiller Cycle[102] presents a risk management framework from which managers and security practitioners can logically implement a range of IA security solutions to reduce the risk exposure to their organisation. The Surveiller Cycle framework has been developed to provide logical and interrelated solutions to IA risk exposure across all aspects of the knowledge-dependent organisation from early research through to market activities. Often, the most difficult part of risk management is identifying the range of threats faced by a given entity. Readers should refer to the section entitled "Threats and Perpetrators" for guidance on their potential threat spectrum. The "Surveiller Cycle" is illustrated graphically below:

101 Clarke, M., Wheeler, S. (1990). "Business Crime", Polity Press, Cambridge, United Kingdom. Hagan, F.E., Simon, D.R. (1999). "White Collar Deviance", Allyn and Bacon Publishing, USA.

102 Curwell, P. (2004). "Intellectual Asset Fraud: Preventative Strategies in Knowledge-dependent Companies", unpublished thesis, The University of Queensland Business School, Brisbane, Australia.

Figure 6: The Surveillance Cycle

The following table expands upon each phase of the Surveiller Cycle and presents a list of suggested actions to be undertaken by the organisation concerned. Importantly, some of these actions should/may not be performed by the security section per se but rather by other business units, such as legal.

7.4. Surveiller Cycle

"The Surveiller Cycle" – An Intellectual Asset Fraud Prevention Framework[103]

103 Curwell, P. (2004). "Intellectual Asset Fraud: Preventative Strategies in Knowledge-dependent Companies", unpublished thesis, The University of Queensland Business School, Brisbane, Australia.

Table 9: The Surveiller Cycle

Phase of Surveiller Cycle	Action Undertaken by Firm
1. Initial Employment – During the hiring process and probationary tenure is when an employee is most likely to form habits within the firm	
A. Pre-Employment Screening	Background Checks
	Corroboration of Qualifications and Claims made in Resume
	Psychometric Testing
	Interviews
B. Induction for New Employees	Employment Contract essentials include: IP assignment Confidentiality Clauses Moral Rights Restraint of Trade (if applicable)
	Security and Fraud Awareness Training
	Introduction of 'Ethical Framework' of the firm including codes of conduct and mechanisms for reporting complaints or breaches.
	Provide employees with examples of what is and is not permissible behaviour, especially with regard to disclosing research results in public forums, how much latitude is permissible to share information during networking events, behaviour at conferences and seminars, capturing outside knowledge within the firm through knowledge management practices, and how to go about developing research partnerships within the firm.
	Teach employees about the information security practices used within the firm, especially with regard to the handling of confidential or sensitive information and Trade Secrets. It should be remembered that information is not necessarily a Trade Secret or deemed proprietary in some localities if it is not acknowledged as such by caveats like 'confidential' or 'for internal use only'. Each company should adopt its own system whereby sensitive information is classified as such, with each staff member being instructed on what behaviour is appropriate to safeguard that level of information.
2. Continuing Employment: This is applicable throughout an employees' period of employment within the firm. The support and participation of senior management should be sought	
a. Staff Training and Development	Regular refresher awareness training should be incorporated into staff development practices, and staff should regularly sign off on having read and understood the relevant policies and procedures relating to fraud. In these policies it should be stated explicitly what is and is not permissible, and indicate that if a staff member undertakes activities that breach their obligations to the firm they can be held liable.
b. Marking of Sensitive Information	The firm should routinely mark sensitive information (confidential data, Trade Secrets, or proprietary information) as such and ensure employee compliance.
c. Personal and Professional Development	Develop and implement an employee mentoring program to provide employees with support from more experienced colleagues.
d. Internal communication	Provide employees with anonymous and transparent communication opportunities to discuss grievances and question unpopular management practices.
3. Project Identification and Evaluation Phase: Basic research is underway in this phase and	

Phase of Surveiller Cycle	Action Undertaken by Firm
boundaries are being established within the project.	
a. Selection and Evaluation of Research Projects and Priorities	Collect contact details (such as business cards) and attendance lists from employees to identify who they met during events
	Form a multidisciplinary research or project group and have these individuals identify possible business opportunities for commercialization and research direction
	Conduct background research in preparation for funding applications
	Early IP value chain activity underway
4. Early Research: Projects have been selected and research focused on the project goals has commenced, although the scope of research undertaken within the project goals remains broad.	
a. Due Diligence	Commence Due Diligence process examining IP, markets, competitors, and where applicable possible business partners.
b. Awareness Briefings	As part of Staff Development it is essential that employees be aware of what they can and cannot do with research data, how to protect that data, and specifically just how much information they can share with other members of their Intellectual Capital Webs.
c. Legal Protective Mechanisms	Confidentiality Agreements are required for all staff not employed by the firm. Where possible a tracking mechanism should be developed to document who had access to what research material and when – such a mechanism could even be in the form of minutes from meetings or computer access logs to specific files.
	Legal due diligence on potential partners and even key aspects of the supply chain should be undertaken. The risk assessment should identify key material that could provide competitors with guidance on what research is being carried out by the firm. Key risks should then be mitigated through due diligence, including identifying practices such as employment contracts from suppliers which do not adequately protect confidential information.
d. Knowledge Audit	Managers undertake a Knowledge Audit to identify existing knowledge (including identifying highly valuable 'knowledge nuggets'). The Knowledge Audit also helps identify knowledge gaps n the organization and within the public domain, thus illustrating what new information must be protected if it is successfully generated during the research process.
e. Documentation of Research	Research data should be documented, signed, witnessed, and stored as appropriate under the relevant IP legislation.
	Duplication of Research Data
f. Documentation of Collaborations	Collaborations, networks, and alliances are very important for the creation of knowledge and as a method for sharing skills and competencies to increase the success of a product in the market. However, where the financial return is allocated on the basis of participation in the Research and Development process, documentation of the collaboration (who provided or did what) – acknowledged as true by all parties – can help reduce the incidence of problems later on in the event of civil action.
5. Late-stage Research: Projects have been selected during Phase 3 and 4, with research becoming more focused during Late Stage Research. Knowledge gaps become identified, and product prototypes are designed and/or created. Serious thought is given about the market and how to sell to that market.	
a. Knowledge Audits	Regular Knowledge Audits should be undertaken to 'catalogue'

Phase of Surveiller Cycle	Action Undertaken by Firm
	existing intellectual capital and identify knowledge gaps.
b. Awareness Briefings	Continuation of the regular Awareness Briefings described in 2a help ensure the issues are at the forefront of employees minds, as well as providing an avenue from which to update staff on new 'modus operandi'.
c. Due Diligence continues	Due diligence, especially into IP, collaborators, and supply chains should continue in an effort to remain aware of any important developments.
d. Documentation of Research	Continues as per 4e for the life of the research
e. Documentation of Collaborations	Continues as per 4f for the life of the research
f. Legal Protective Mechanisms	Continues as per 4c for the life of the partnerships or alliances
g. Commencement of Competitor and Market Intelligence Programs	Development and implementation of Competitor and Market Intelligence programs to gain greater awareness of external activities likely to affect the firm.
h. Risk Assessment / Management	Drawing on data collected in earlier phases of this Framework, threats and vulnerabilities should be assessed and a Risk Management Plan devised to mitigate project and market risk.
i. Increased level of control over the research information	Core intellectual capital for a project is restricted to a critical audience until patent applications are filed and experiments completed.
6. Market: A product has been created during the final stages of the Late Research Phase. The challenge now is to successfully launch the product on the market, displacing existing products in the market or raising barriers to entry for new competitors. Sales and marketing is the predominate consideration here.	
a. Change of focus	Veil of secrecy now lifted on aspects of the Research, Development, and Manufacturing process.
b. Market Strategy	Market Strategy now represents key information to the firm and requires protecting
c. Competitor Intelligence Program	Maintain continued awareness of external activities, market and operating environment likely to affect the firm.
d. Compilation of prospective customer database (for niche products)	During earlier marketing and business development activities the firm should have already identified potential customers. These, and new customers, should be entered into a database with the ability to cross-reference this information with the Competitive Intelligence Database
e. External Security Awareness Training	Firm conducts refresher awareness training specifically focusing on external fraud threats including industrial espionage, competitive intelligence professionals, and other competitors. Staff are provided with examples of what could happen using real-life case studies to raise awareness levels. Prevention and detection mechanisms are also outlined, as is the role of External Fraud in the firm's overall business strategy incorporating IP management, Industrial Security, Risk Management, Business Development, and Strategic Planning.
7. Compliance and Enforcement: The last part of the process is about ensuring that revenues which belong to the company are actually realized so that a return on investment can be generated and to provide capital for further research and development programs.	
a. Compliance Monitoring of Licensees or	Establish monitoring program to ensure licence compliance and/or that customers are behaving appropriately (i.e. not replicating your product

Phase of Surveiller Cycle	Action Undertaken by Firm
Customers	in their lab and producing it unlawfully for internal use)
b. Market Surveillance: Identification and Monitoring of Infringers (intentional or unintentional)	Supplementary to 7a above, the identification of infringers is used to highlight entities using the firms IP unlawfully, and those using the firms IP in countries where patent protection was not sought (eg. India or China) and attempting to sell counterfeit or copy goods to countries in which the firms IP is protected (eg. US, EU, etc).
c. Market Enforcement: Pursuing of Enforcement Strategies	The primary goal here should be to either obtain lawful revenue from infringers. When confronted with evidence of infringement companies essentially have three choices: Desist, purchase a licence, or continue infringing and possibly contest the patents validity in court.
d. Generation of Profit	Profit provides shareholders with a on their investment, as well as providing capital for future projects and the concurrent employment of additional personnel.

The intention of the Surveiller Cycle is that it should complement the existing security in depth measures employed by an organisation, as illustrated below:

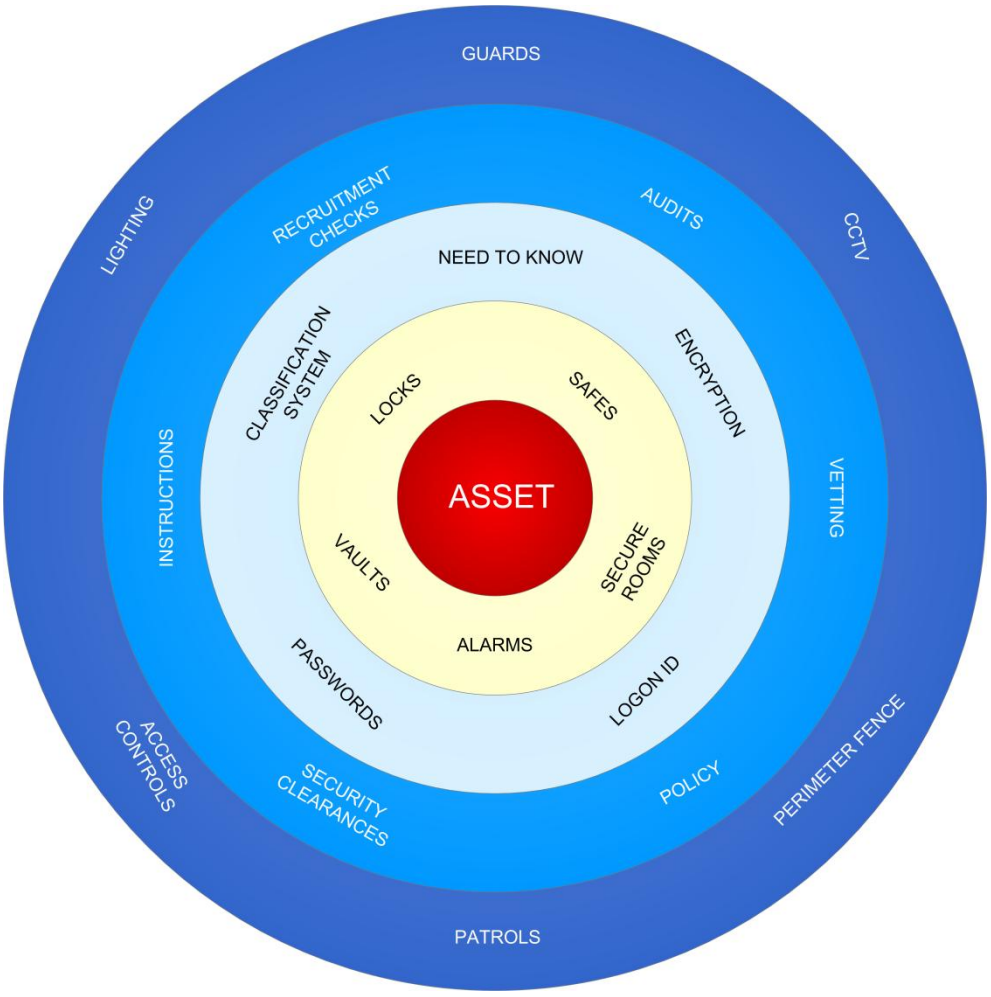


Figure 7: Example of the Security-in-depth approach

7.5. Checklist for the protection of PI and IP

The key to protecting Proprietary Information lies in keeping it secret. For small organisations this may be an easy task, particularly where employee loyalties towards the organisation are strong. For medium and large sized organisations it can be very difficult to protect proprietary information whilst concurrently enabling the knowledge exchange commitment from employees (particularly R&D staff). Protection measures should be developed using a layered approach and might be assessed against the following criteria:

Table 10: Self-Assessment checklist for protection of IP and PI

Practice Area: Physical Security	**Self Assessment Rating**
• Is the premises secured appropriately? • Have the principles of deter, detect, delay and detain been considered? Refer to the SRMBOK Chapter on Physical Security for additional guidance here.	
Practice Area: Personnel Security	**Self Assessment Rating**
• Is a pre-employment screening (vetting) program in place? • You may wish to consider psychological testing as a means of identifying potential employees with undesirable personality traits. Refer to the SRMBOK Chapter on Personnel Security for additional guidance here.	
Practice Area: Information Security	**Self Assessment Rating**
• Have IT systems and networks secured appropriately? • Have audit trails for computers, multifunction devices, photocopiers, fax machines which are robust, and cannot be edited or deleted been implemented? • Do you encrypt sensitive data for transmission and/or storage? • Is it necessary to compartmentalise sensitive stored data? • Have passwords, screen saver locks, anti-virus and firewall software been installed and are they regularly updated? • Have all computers, networks, servers and server rooms been secured appropriate to the organisations risk exposure? • Have all communication channels including internet, email, fax, photocopier, VoIP, messenger, telephone been secured appropriate to the organisations risk exposure? • For highly sensitive information, is it worthwhile using a stand-alone computer which is not connected to any network or internet and is held in a secure room and accessible only to a limited number of people? • Have backups, disaster recovery and business continuity been adequately addressed? • Have you developed and adequately publicised the use of classification markings to clearly identify the owner of the material and that it may be considered confidential? • Does each employee acknowledge their awareness of your organisation's information marking policies, such as obtaining signed, dated and witnessed declaration from each employee that they having been briefed on these practices during their induction? • Is this practice continued on a regular basis (perhaps annually) throughout the employees' tenure?	

• If compartmentalisation and 'need to know' practices are implemented, are indoctrination certificates (such as those similar to those suggested for information marking policies) utilised? • Have you introduced a mobile phone and email policy? Ideally, no employee would be permitted to take a mobile phone (especially one with a camera) or any personal data storage device (such as a USB watch) into an employer's facility. • Do you retain originals of all such records for a reasonable period of time to allow for potential legal action in the future? Refer to the SRMBOK Chapter on Information Security for additional guidance here.	
Practice Area: Security Risk Management	**Self Assessment Rating**
• Have Policies and Procedures been developed, are they updated regularly and are employees aware of them? • Do you conduct regular education and awareness training sessions? • Have robust and effective audit trails been developed? • Are Non-Disclosure and Non-Competition Agreements for employees, suppliers, distributors, contractors, consultants, joint venture participants etc irrespective of role in the company? • Are IP Assignments obtained prior to an employee's commencement of work with the organisation? • Is a robust incident reporting (not just ICT but physical, information and personnel) process in place? • Do you maintain an incident log? • Have you assessed your market – is it highly competitive? Are you likely to be subjected to a higher level of threat? • Do you undertake security risk assessments and perform threat assessments on your organisation and market? • Do you collect and analyse intelligence on competitors? Are they actively seeking information on you? Conversely, are they being attacked by another element in the market such as another competitor? • Are organisations with similar operating models/practices or products experiencing difficulties in their market? Case studies can be useful here to determine how your organisation would deal with such threats. • Do you require a counterintelligence program? If so, has a plan been developed and appropriate steps implemented? • Has a loyal and trustworthy culture been created such as through adequate remuneration and a happy, healthy working environment? • Have strong commitments towards successful outcomes for the company are obtained from employees? Refer to the SRMBOK Chapter on Personnel Security for additional guidance here.	

The previous table provides a quick scoring methodology which can be quickly used to determine the status of an organisation's IP and PI protection and help to identify any gaps. Where further assessments or more detailed information is required, such as on physical security, readers are encouraged to access the appropriate SRMBOK chapter for additional guidance.

Remember:

In addition, depending on the organisation and information to be protected some of these measures may not be practical or cost effective. It is simply not realistic to employ all of these more extreme security measures within the average

company. Some may be illegal or may be considered to be in breach of human rights. Secondly, and perhaps more realistically they will not encourage either the right sort of staff (highly talented, intellectually curious) into the organisation as employees, nor are they likely to result in the knowledge exchanging commitments between employees and the employer in knowledge-creating companies. Without these knowledge exchange commitments it is practically impossible for the knowledge-creating company to survive or to compete in a market.

8. BIBLIOGRAPHY

Adams, J. (1995). "The New Spies", Pimlico, London.

Andersen, B., Struikova, L. (2004). "Intangible Assets and Intellectual Capital: Where Value Resides in the Modern Enterprise", *DRUID Summer Conference on Industrial Dynamics, Innovation, and Development*, Denmark.

ASIS (2002). "Trends in Proprietary Information Loss Survey Report", *American Society for Industrial Security, Pricewaterhouse Coopers, and US Chamber of Commerce and Industry*, www.asisonline.org [accessed 07MAR03].

Attorney-General's Department [AG] (2002). "*Commonwealth Fraud Control Guidelines*", Commonwealth of Australia, Canberra.

Barrett, B. (2002). "Defensive use of publications in an intellectual property strategy", *Nature Biotechnology*, 20, 191-193.

Baughn, C.C., Denekamp, J.G., Stevens, J.H., Osborn, R.N. (1997). "Protecting Intellectual Capital in International Alliances", *Journal of World Business*, 32, 2, pp.103-117.

Bednarek, M., Ineichen, M. (2004). "Patent pools as an alternative to patent wars in emergent sectors", *Intellectual Property and Technology Law Journal*, 16, 7, pp.1-5.

Blattman, A., Irani, S., McCann, J., Bodkin, C. (2001). "*Biotechnology IP Management Manual*", Spruson & Ferguson and Biotechnology Australia, Canberra, Australia.

Clarke, M., Wheeler, S. (1990). "*Business Crime"*, Polity Press, Cambridge, United Kingdom.

Cohen, W.M., Levinthal, D.A. (1990). "Absorptive capacity: a new perspective on learning and innovation", *Administrative Science Quarterly*, 35, 128-152.

Contractor, F. (2000). "Valuing Corporate Knowledge and Intangible Assets: Some General Principles", *Knowledge and Process Management*, 7, 4, pp.242-255.

Curwell, P. (2004). "Intellectual Asset Fraud: Preventative Strategies in Knowledge-dependent Companies", unpublished thesis, The University of Queensland Business School, Brisbane, Australia.

Cyr, D. (1998). "High Tech, High Impact: Creating Canada's competitive advantage through technology alliances", *Academy of Management Executive*, 13, 2, pp.17-26.

Dyer, J.H., Singh, H. (1998). "The relational view: cooperative strategy and sources of interorganizational competitive advantage", *Academy of Management Review*, 23, 660-679.

Ehin, C. (2000). "*Unleashing Intellectual Capital*", Butterworth Heinemann Publishers, USA.

Ernst & Young (2003). "*Fraud: The Unmanaged Risk*", 8th Global Survey, Global Investigations and Dispute Advisory Services, Ernst and Young, South Africa.

Fenton-Jones, M. (2004). "*Culture key to employee fraud*", Tuesday 28 September 2004, The Australian Financial Review, p.50.

Germeraad, P. (1999). "Intellectual Property in a time of change", *Research Technology Management*, 42, 6, pp.34-39.

Graham, A., Pizzo, V. (1997). "Competing on Knowledge: Buckmann Laboratories International", *Knowledge and Process Management*, 4, 1, pp.4-10.

Grant, R.M. (1996). "Toward a knowledge-based theory of the firm", *Strategic Management Journal*, Winter Special Issue, 17, 109-122.

Hamilton, P. (1967). "*Espionage and Subversion in Society*", Hutcheson, London, pp.222-223.

Hine, D. and Kapeleris, J, (2006) Innovation and Entrepreneurship in Biotechnology: An International Perspective: Concepts, Theories and Cases. Cheltenham, UK, Edward Elgar Publishing.

Hodgson, J. (2001). "The headache of knowledge management", *Nature Bioentrepreneur,* 19, pp. BE44.

Hopkins, D.M., Kontnik, L.T., Turnage, M.T. (2003). "*Counterfeiting Exposed: Protecting Your Brand and Customers",* John Wiley Publishers, New Jersey, USA.

Isacson, J.P. (2000). "Maximising profits through intelligent planning and implementation", *Nature Biotechnology*, May, 18, pp.565-566.

Kogut, B., Zander, U. (1992). "Knowledge of the firm, combinative capabilities, and the replication of technology" *Organisational Science*, 3, 3383-3397.

Kroll (2003). "*Catch them if you can – are you doing enough to safeguard your intellectual property? The Kroll Global Survey on Corporate Response to IP Abuse*", www.krollworldwide.com [accessed 12JUN04].

Lane, P.J., Lubatkin, M. (1998). "Relative absorptive capacity and interorganizational learning" *Strategic Management Journal*, 19, 5, 461-477.

Larson, A. (1992). "Network dyads in entrepreneurial settings: a study of the governance of exchange relationships", *Administrative Science Quarterly*, 37,pp.76-104.

McAdam, R. (2000) "Knowledge Management as a Catalyst for Innovation within Organisations: A Qualitative Study", *Knowledge and Process Management*, 7, 4, pp.233-241.

McGuinness, P. (2003). "*Intellectual Property Commercialisation: A Business Managers Companion*", LexisNexis Butterworths, Australia.

Medd, K, Konski, A. (2003). "Workplace programs to protect Trade Secrets", *Nature Biotechnology*, 21, pp.201-203.

Nasheri, H. (2004). "Economic Espionage and Industrial Spying", Cambridge University Press, England.

Nonaka, I. (1991). "The Knowledge-Creating Company", *Harvard Business Review*, November-December, pp.96-104.

Nonaka, I., Takeuchi, H. (1995). "*The Knowledge Creating Company: How Japanese Companies Create the Dynamics of Innovation*", New York, Oxford University Press.

Norus, J. (2002). "Biotechnology Organisations in Action: Turning Knowledge into Business", *Progress in Biotechnology*, Volume 20, Elsevier Science B.V., Amsterdam.

O'Gara, J. (2004). "*Corporate Fraud: Case Studies in Detection and Prevention*", John Wiley Publishers, USA.

Padron, M.S., Uranga, M.G. (2001). "Protection of Biotechnological Innovations: A burden too heavy for the patent system", *Journal of Economic Issues*, 35, 2, pp.315-322.

Peebles, E. (2002). "Inspiring Innovation", *Harvard Business Review on The Innovative Enterprise*, HBS Press, Boston, USA.

Penrose, E. (1959). "*The theory of the growth of the firm*", Blackwell Publishing, Oxford, UK.

Pickett, Pickett (2002). "*Financial Crime Investigation and Control*", John Wiley and Sons, USA.

Pitkethly, R. (2001). "Intellectual Property strategy in Japanese and UK companies: patent licensing decisions and learning opportunities", *Research Policy*, 30, 425-442.

Polanyi, M. 1966 The Tacit Dimension. Garden City, NY. Doubleday.

Porter, M.E. (1985). "*Competitive Advantage: Creating and Sustaining Superior Performance*", The Free Press, New York.

Powell, W.W. (1998). "Learning from Collaboration: Knowledge and Networks in the Biotechnology and Pharmaceutical Industries", *California Management Review*, 40, 3, 228-240.

SOCA (2006). "The United Kingdom Threat Assessment of Serious Organised Crime", Serious Organised Crime Agency, United Kingdom.

Somaya, D. (2003). "Strategic Determinants of Decisions not to Settle Patent Litigation", *Strategic Management Journal*, 24, 17-38.

Soo, C., Devinney, T., Midgley, D., Deering, A. (2002). "Knowledge Management: Philosophy, Processes, and Pitfalls", *California Management Review*, 44, 4, pp.129-150.

Spender, J.C. (1996). "Making knowledge the basis of a dynamic theory of the firm", *Strategic Management Journal*, Winter Special Issue, 17, 45-62.

Stewart, T.A. (2001). "*The Wealth of Knowledge: Intellectual Capital and the Twenty-First Century Organisation"*, Nicholas Brealey Publishing, Great Britain.

Storck, J., Hill, P.A. (2000). "Knowledge Diffusion through 'Strategic Communities'", *Sloan Management Review*, Winter, pp.63-74.

Styhre, A., Ingelgard, A., Roth, J. (2001). "Gendering Knowledge: The practices of Knowledge Management in the Pharmaceutical Industry", *Knowledge and Process Management*, 8, 2, 65-74.

Tidd, J., Bessant, J., Pavitt, K. (2001). "*Managing Innovation: Integrating Technological, Market, and Organizational Change*", John Wiley and Sons, UK.

Van Cleave (2005). "Statement for the record: House Judiciary Committee on Immigration, Border Security and Claims hearing on source and methods of foreign nationals engaged in economic and military espionage", National Counterintelligence Executive, 15 September 2005, United States Government, available at www.ncix.gov.

Willman, P. (1996) "Protecting Know-How", *London Business School Business Strategy Review*, 7, 1, 9-13.

Yli-Renko, H., Autio, E., Sapienza, H.J. (2001). "Social Capital, Knowledge Acquisition, and Knowledge Exploitation in Young Technology-based Firms", *Strategic Management Journal*, 22, 587-613.

Zhou, A.Z., Fink, D. (2003). "The intellectual capital web: A systematic linking of intellectual capital and knowledge management", *Journal of Intellectual Capital*, 4, 1, 34-48.

Zucker, L.G., Darby, M.R., Armstrong, J.S. (2002) "Commercialising Knowledge: University Science, Knowledge Capture, and Firm Performance in Biotechnology", *Management Science*, 48, 1, pp.138-153.