Presented to the Interdisciplinary Studies Program:

UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Applied Information Management
and the Graduate School of the
University of Oregon
in partial fulfillment of the
requirement for the degree of
Master of Science

Intellectual property policy: Risk identification and protection in the global market

CAPSTONE REPORT

TracieLyn Rydzewski
Information Manager
Intel Corporation

University of Oregon
Applied Information
Management
Program

July 2010

Continuing Education
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-2714

Approved by

_____

Dr. Linda F. Ettinger
Senior Academic Director, AIM Program

Title: Intellectual property policy: Risk identification and protection in the global market

TracieLyn Rydzewski

Intel Corporation

Abstract

Organizations that conduct business in the global market expose themselves to potential information risks, including intellectual property (IP) theft, exposure, and breach of laws and regulations (Corbin, 2002). Key elements of this study examine IP risk management and identification practices, IP protection, and the value of building a security awareness IP culture. The creation of an IP policy should evolve to accommodate the shifting economic environment, and the organization's business goals, culture, and operating environments.

Keywords: global market, intellectual property, IP culture, IP policy, IP protection, risk identification, risk management

Table of Contents

List of Tables

List of Figures

Introduction to the Literature Review

Purpose

The purpose of this study is to examine key elements of an intellectual property (IP) policy within an organization, as it relates to risk identification and protection in the global market. A predetermined set of key elements is used to frame the study: (a) IP risk management practices (Hampton, 2009), (b) IP protection (Wheeler, 2008), and (c) a security awareness IP culture (Dobrusin & Krasnow, 2008). For the purposes of this study, IP is defined by the World Intellectual Property Organization (WIPO, n.d.) as creations of the mind: (a) inventions, (b) literary and artistic works, (c) symbols, (d) names, (e) images, and (f) design.

When organizations conduct business in the global market, they expose themselves to the potential information risks, including IP theft, exposure, and breach of laws and regulations (Corbin, 2002). In order to protect against these risks, information security requires not only technology, but also policy that reflects a clear understanding of potential risks, decision-making, cultural behaviors, metrics for evaluating related business, and security policy options for the global market (Johnson, Goetz & Pfleeger, 2009). This means that organizations conducting business in the global market should initiate an IP risk assessment process (Alberts, 2003). A critical prerequisite to this risk assessment process, according to Martinez, De Andino, Tate, and Maddry (2004, p.1), is to determine the potential risk to the organization's IP; organizations should "classify data to ensure that what is being protected is also what is most important to protect" to develop the IP policies (Johnson et al., 2009, p.48).

Specific policies are a necessity for the protection of IP within the organization and are seen as critical activities for capturing the essentials of information security, as it is applicable to the organization (Kadam, 2007). Intellectual property protection policy communicates clear

procedural activities for the organization to follow, so that strict protection enforcement is applied to prevent theft and exposure as well as to create compliance with legal statutes (Lemieux, 2004).

Legal protection for IP varies greatly around the world and the annual losses that companies face from IP violations are substantial (Hanel, 2006). These losses can be reduced through the development of an organization-wide IP policy. Additionally, organizations should continuously monitor risks for industry and environmental conditions that include the changes to complex laws, regulations, and enforcement in foreign countries which are evolving in the global market ("Understanding the WTO: Agreements: Intellectual Property," n.d., para. 22).

The main exploratory questions addressed in this study are:

- What are the key elements of an intellectual property (IP) policy, within an organization that conducts business in the global market?
- What are the relevant risk management concepts and practices to protect organizations from IP theft, exposure, and non-compliance?
- How can organizations create an organization-wide security awareness IP culture for today's global market?

Problem Area

The problem to be examined is how to ensure IP is protected when information is shared or transferred to security risk countries. The number, types, and modalities of potential IP security risks are growing. For example, there is the danger that organizations can lose valuable IP and proprietary business information when organizations experience employee loss through reduction in force, resignation, outsourcing or collaborating with other organizations (Sutin & Goldberg, 1999).

Furthermore, Sutin and Goldberg (1999) state if an organization does business in the global market, there are other risks to consider, such as hiring locally, which may be useful for the success of the business ventures, but which also has the potential to expose intellectual property and to provide access to valuable technologies and new innovations. According to Hanel (2006), if intellectual property related to a new product line falls into the hands of a competitor, such a breach of security could lead to lost business, lawsuits, and in the end could result in significant financial losses for an organization.

Choate's (2005) research contains a number of important insights on various IP international cases. He examines organizations that lack the full understanding and interpretation of intellectual property competition, risk identification, and protection, which can result in significant financial impact, and the loss of competitive advantage in the global market. One example is the case of Geely, one of China's largest automakers, who used Toyota's logo on its Meiri sedan; Toyota subsequently went to court, and the court ruling found that Toyota's brand wasn't recognized in China as a "distinctive brand" (Choate, 2005, p.180).

Significance

Kish (2004) states that according to the International Anti-Counterfeiting Coalition, US companies lost $200 billion in revenue due to worldwide copyright, trademark, and trade-secret infringements, and U.S. companies suffered an additional $9 billion in trade losses due to international copyright piracy. IP policy and protection practices have a purpose within the organization (Dobrusin & Krasnow, 2008). According to the study on insider IP theft of 35 cases by Moore, Cappelli, Caron, Shaw, and Trzeciak (n.d.), 74 % of employees stole information in their area of job responsibility and the study found 41 % of employees had partially developed the information and/or product stolen. The results from this research are significant for IP risk managers, because they codify the literature defining risk management policies for organizations. A clear risk management policy ensures that organizations are more competitive in the global market.

Audience

The target audience for this study is managers who work in organizations engaged in business in the global market and who wish to secure their intellectual property, with the goal to maintain their competitive edge. This study is most useful for managers who work in organizations that have already identified their intellectual property value and next wish to address intellectual property risks within the organization as part of an organization-wide intellectual property (IP) policy. According to Hampton (2009), risk management policies and practices are designed and written especially for the organization after an IP risk assessment is concluded. These policies and risk identification practices are then communicated to the employees to achieve alignment and acceptance at various levels within the organization.

Specifically, the audience is a set of information technology (IT) security managers, IP risk committee members, information risk managers, program managers, information managers, and project managers who are directly responsible for identifying information risk and intellectual property protection within their organizations. The relevant and related roles of IT security managers, IP risk committees, information risk managers, program managers, information managers, and project managers are as follows:

- The risk manager is responsible for the information risk program for the organization (Hampton, 2009).
- The IP risk committee is responsible for providing guidance and suggestions about exposures, initiate research, request the risk owners to investigate risks, monitor trends, technology, and risk transfer (Hampton, 2009).
- The IT security manager is responsible for the security of information within the technology infrastructure and network for the organization (Wheeler, 2008).
- The program manager is responsible to lead a team of project managers and understands how project managers mitigate IP risks within the organization (Interpretive Guidance, 2003).
- The information manager is responsible to understand the organizations security policy and applies control mechanisms to the information flow within the operations of project (Information Manager, (n.d.), *The Princeton Review*).
- The project manager is responsible for documenting the information risks that may likely to occur on a project, defines the protection methods, and manages the risk mitigation (Interpretive Guidance, 2003).

Outcome

The primary outcome of this study is a matrix that defines the key elements that should be part of an IP risk management policy within organizations that conduct business in the global market. These key elements are organized in relation to two larger content categories: (a) IP risk management practices to protect organizations from IP theft, exposure, and non-compliance (Hampton, 2009), and (b) creation of a security awareness IP culture (Dobrusin & Krasnow, 2008).

The purpose of the risk matrix (see Appendix C) is to increase the awareness and knowledge of established IP policies for managers within organizations doing business in the global market. These are managers who are exposed to IP risks because they work within organizations that are: (a) involved in business in security risk countries, technology transfer, use of trademarks, contract development, and marketing; and (b) outsourcing and collaborating with other organizations. Additionally, the matrix is designed to increase recognition of a need to develop and maintain a high level of security culture and awareness to risk to IP within the organization. These managers need to apply risk management practices to protect IP theft, exposure, and in non-compliance with the organizations IP policies.

Delimitations

Topic. As a topic, IP policy and protection falls within the larger information management arena in relation to information security (Johnson et al., 2008). Mashelkar (2002) states IP protection in the twenty first century is critical in regard to innovation. This innovation is the key for production and process of knowledge in the global market. He also claims that nations that wish to gain power to be more competitive to change knowledge into wealth

(Mashelkar, 2002). As a result, this increases the critical importance to protect IP while engaged in business in the global market.

Corbin (2002) states there are key reasons why it is important for organizations to worry about protecting their IP. These reasons (such as exposure vulnerability, patent application, trademark, and copyright preventing usage by others) extend beyond an examination of IP protection within a global context, as framed in this study.

Focus. The topic of IP policy protection is broad. Literature selected for use in this review focuses on four predetermined elements: (a) intellectual property risk management concepts and practices (Hampton, 2009), (b) risk identification (Johnson et al., 2009), (c) security culture (Dobrusin & Krasnow, 2008), and (d) IP protection (Wheeler, 2008) as these are described in a global business context.

Time Frame. The literature collected for this study with a few exceptions has publication dates between 1999 and 2010. This is to ensure the relevance of the collected material in relation to the many specific challenges associated with International IP policies and protection. Risks for industry are rapidly changing due to the implementation of complex laws, regulations, and enforcement in security risk countries ("Understanding the WTO: Agreements: Intellectual Property," n.d., para. 22). Additionally, the time frame of this study is limited by the evolution of technology advancements of e-business transaction and electronic technology (Studt, 2004). Studt (2004) adds that since organizations are challenged by the speed of change, the organizations' strategies of risk management practices and methods of identifying information risks are consistently being revised.

Selection Criteria. The literature selection criteria strategy within this study uses the research fundamentals, guidelines, and review of literature suggested by Leedy and Ormrod

(2005). The discussion of IP within this literature review is limited to establishing the relationship of the key elements of an IP policy and practice within the organization. The objective of this literature review is to study the conceptual understandings of the four topic areas (Figure 1), within the context of organizations engaged in business in the global market.

Literature selection mapping (Creswell, 2009) is utilized to determine the nature and identify a category for the collected related resource material in the study. The literature is divided, sorted, and mapped (see Figure 1). The association between IP, information management, information risk, security policy, and IP protection searches demonstrate the relevance to the study of IP policy risk identification and protection. The selection criteria also include literature that addresses organizations' business ventures and IP protection in the global market. The selection of law literature focuses on international laws around IP protection and the varying degrees of nations who accept the WTO trade agreements and organizations recognizing these variations within their IP policies. As often as possible, literature is selected when written by authors who pose a question or hypothesis, collect data, and answer a question (Creswell, 2009).

The books selected from UO library WorldCat for this study provide a comprehensive overview of risk management (Hampton, 2009), security culture (Dobrusin & Krasnow, 2008), and IP protection (Choate, 2005) which assist in revealing common findings and factors on IP risk identification and protection.

Additional resources selected for this study provide a research context, by defining the global environment and risks to organizations. The research conducted accessing Sciencedirect and IEEE xplore using keywords of information risk (Sumner, 200) and IP security (Johnson et al., 2009) resulted in a collection of scholarly works by the following authors: Thomson, von

Solms, Rossouw, and Louw (2006) and resources (Braunfeld & Wells, 2001) which provide a foundation for the examination of IP information risk identification and protection.

Figure 1. Reference Selection Mapping Strategy (from Creswell, 2009)

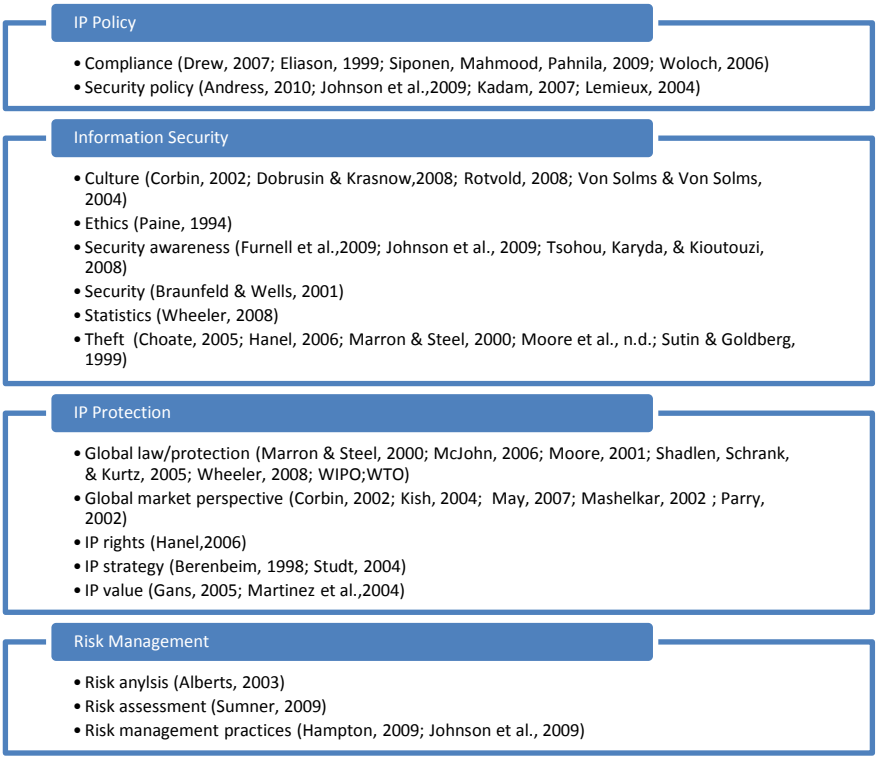

Figure 1: The literature selection mapping (Creswell, 2009) is utilized to determine the nature and identify a category for the collected related resource material in the study.

Audience. The audience for this study is managers who work in organizations that have already identified their intellectual property value and next wish to address intellectual property risks within the organization as part of an organization-wide intellectual property (IP) policy and IP culture awareness. There are a number of factors that impact managers that work in organizations doing business in the global market. These factors should be addressed when considering an appropriate audience for this study. An important consideration is addressing the

managers' relationship to their function within the organization (von Solms & von Solms, 2004). von Solms and von Solms (2004) add that IP is created and used differently by departments in the organizations since departments may have different purposes as they conduct business in the global market.

Another factor to consider for the audience selection is organizations that establish business ventures in security risk countries, technology transfer, use of trademarks, contract development, and marketing dramatically increases the organizations exposure and risk of having products counterfeited (Choate, 2005). As a result, the managers should develop their business processes and controls based on those risks. Additional factors of exposure to risk to consider include managers within organizations that hire, outsource or collaborate with other organizations while doing business in the global market (Hanel, 2006).

Exclusions. This literature review is not a study on the following:

- A review of information security technology solutions.
- A review of legal global law jurisdiction and prosecution procedures.
- A review of WTO IP global trade agreements.
- A review of global ethics and cultural differences.

The concept of key elements. The concept of key elements (Dictionary.com, n.d.) within this study refers to the set of predetermined aspects within the larger topic of IP policy risk identification and protection, to be examined by a conceptual analysis of selected literature.

Data Analysis Plan Preview

Data analysis is structured as an examination of key elements (see Figure 2) of IP policy within an organization, as these relate to risk identification and protection in the global market.

A predetermined set of key elements is established, with which to begin the process of conceptual analysis (Busch, De Maret, Flynn, Kellum, Le, & Meyers, 2005). These elements are: (a) IP risk management practices (Hampton, 2009), (b) IP protection (Choate, 2005), and (c) security culture (Dobrusin & Krasnow, 2008). This researcher anticipates the emergence of other key elements.

Literature selected for analysis is obtained by using key words and phrases that meet the evaluation criteria as a way to determine its merit with regard to creditability, reliability, and validity (Busch et al., 2005). Additionally, the conceptual analysis process is designed to provide an appropriate strategy and approach to answering the research questions of this study. The results collected from the conceptual analysis are reported in a matrix presented in Appendix B.

Figure 2. Preliminary Set of Key Elements Used to Guide Conceptual Analysis

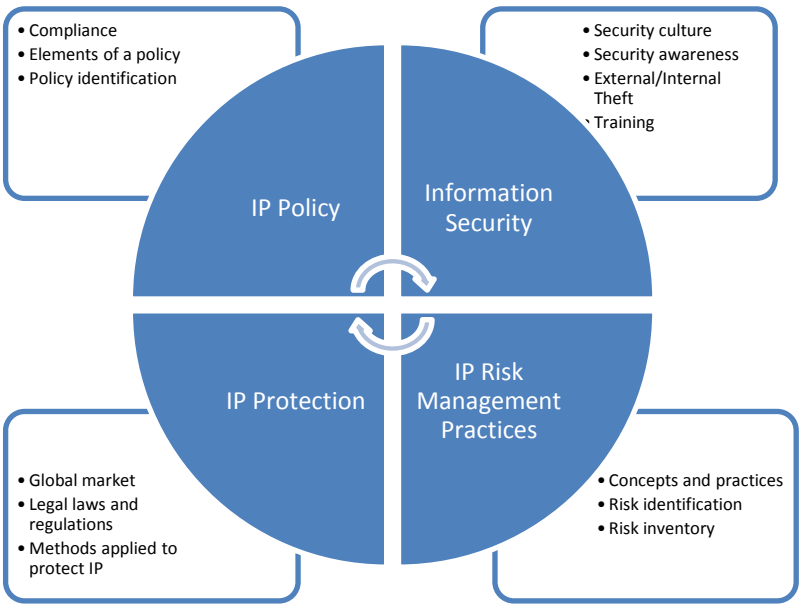

Figure 2: A predetermined set of key elements is used to frame the study: (a) IP risk management practices (Hampton, 2009), (b) risk identification (Johnson et al., 2009), (c) IP protection (Choate, 2005), and (d) a security awareness IP culture (Dobrusin & Krasnow, 2008)

Writing Plan Preview

During the process of conceptual analysis, selected references are coded in order to identify a set of the key elements concerning established IP policy in organizations that are doing business in the global market. Results of the coding process are presented in a matrix (see Appendix B). The matrix is organized in a thematic pattern (Literature Review, 2007) of organization. Themes are defined in relation to each of the four predetermined key elements (see Figure 2) identified to guide the coding process and any additional themes that emerge. The risk matrix (see Appendix C) is designed for risk managers in organizations who are conducting business in the global market and need to have in place a policy to protect IP. Anticipated sections of the literature review include (a) IP risk management practices to protect organizations from IP theft, exposure, and non-compliance (Hampton, 2009); and (b) creation of a security awareness IP culture (Dobrusin & Krasnow, 2008).

Definitions

The terms defined in this section of the literature review come from within the collected resources. These definitions include terminology that is distinctive to the intellectual property protection, risk management, and security fields. The phrases are derived from legal, business, and academic phrases that describe key elements in the literature review. Definitions are provided to make certain that the specific significance is clear.

- Communication – the exchange of thoughts, opinions, messages or information by the organization (Dobrusin & Krasnow, 2008).
- Compliance – policies created within an organization that are enforced and must be followed to the letter by employees (Andress, 2001).
- Compliance strategy – an approach for employee code of conduct adhering to policies that are effectively distributed, understood, and utilized throughout the organization (Eliason, 1999).
- Exposure – a measure of how likely it is that some event will occur (Hampton, 2009).
- Information security risk - is a situation or occurrence that could cause an undesirable outcome, resulting in a negative impact or consequence to critical information within an organization (Alberts, 2003).
- Global market – refers to an integrated world economy with restricted or unrestricted and free movement of goods, services, and labor (Berenbeim, 1998).
- Innovation – is described as IP within an organization that creates market value, which must be secured through patents to protect it from potential competitors (Gans, 2005).
- Intellectual property – is a legal concept that includes trademarks, copyrights, patents, and other related rights ("WIPO Intellectual Property Handbook", WIPO, n.d.).

- Intellectual property policy – is a set of international commerce trade ground-rules which are essentially contracts and agreements which bind governments to keep their trade policies within agreed limits ("Understanding the WTO: Basics", WTO website, n.d., para. 4).
- Intellectual property protection – is to exclude the unauthorized use by contracted employees or third parties of protected information (Mashelkar, 2001). Methods in which an organization protects data leakage and breaches that can negatively affect an organization financial loss (Johnson et al., 2009).
- Intellectual property rights – is the ownership rights generated by individual or corporate invention (Berenbeim, 1998).
- Intellectual property risk – is a potential negative result that brings hardship to the current owner or the rights and interest of the owner of the intellectual property (Choate, 2005).
- Information security policy – is a set of documents that clearly states the intentions of the organization regarding information security that address the multitude of information risk vulnerabilities within the organization (Kadam, 2007).
- Matrix – a collection of theme elements that are associated and presented in rows and columns (Answer.com, n.d.).
- Non-compliance – employees fail to cooperate or comply with policy requirements (Chandra, 2008).
- Policy – a required action or procedure followed by employees within an organization (von Solms & von Solms, 2004).

- Policy compliance guidelines – a method to validate the policy principles that are applied within an organization to ensure that employees are adhering to those policies (Siponen, Pahnila & Mahmood, 2010)
- Risk assessment – is an inventory process that determines information protection strategy and priorities (Hampton, 2009).
- Risk lifecycle – refers to an organization's failure to control exposures or take hold of opportunities during different phases of business activities in the global market (Hampton, 2009).
- Risk management – is the organized process to identify, assess, control, and communicate risks across the organization (Hampton, 2009).
- Risk mitigation – is a systematic approach to apply control methodology to assist with the reduction of information risks in the event of exposure to a risk and the likelihood of its occurrence (Hampton, 2009).
- Security culture – is a collective set of values, norms, and knowledge that is written in the form of rules, regulations, guidelines, and procedures (von Solms & von Solms, 2004).
- Security risk countries – are countries that have not fully accepted to agree to apply the WTO intellectual property protection trade agreements within their country (Berenbeim, 1989).
- Technology – the application of science brought to an organization, industry or country to be used for practical use (Martinsons, 1998).
- Technology transfer – is considered the intellectual property of an organization that is accessed by business investments in security risk countries (Matinsons, 1998).

- Theft – stealing of IP for business advantage as crimes in which current or former employees, contractors, or business partners intentionally exceeded or misused an authorized level of access to networks, systems, or data to steal confidential or proprietary information from the organization. This information is used to get another job, help a new employer, or promote their own side business (Moore et al., n.d.).
- Training – the education or instruction of training employees on IP policy, IP risk identification and protection, which may be comprised of a series of courses and/or communications (Dobrusin & Krasnow, 2008).

Research Parameters

This study uses a literature review as its primary research method (Leedy & Ormrod, 2005). This section of the paper describes the search strategy, including a number of search engines, databases, as well as the approach taken to data analysis and presentation. In addition, this section details how data is documented and evaluated.

The main exploratory questions addressed in this study are:

- What are the key elements of an intellectual property (IP) policy, within an organization that conducts business in the global market?
- What are the relevant risk management concepts and practices to protect organizations from IP theft, exposure, and non-compliance?
- How can organizations create an organization-wide security awareness IP culture for today's global market?

Search Report

This study is an examination of literature related to intellectual property protection within a global context, selected from four core areas. These topic areas are: (a) risk management concepts and practices (Hampton, 2009), (b) risk identification (Johnson et al., 2009), (c) security culture (von Solms & von Solms, 2004), and (d) IP protection (Berenbeim, 1989).

The goal of the search is to utilize key words to find quality resources to effectively address the purpose of this study. The objective is to develop definitions and conceptual understandings of the four topic areas, within the context of organizations engaged in business in the global market.

Search Engines. Using the Google, and UO library search tools with broad key words including *intellectual property, TRIPS, IP strategy, risk mitigation, information risk assessment,*

corporate theft, *information security*, and *security culture* resulted in a number of resources about international laws ("Understanding the WTO: Agreements: Intellectual Property," n.d.), and protection (Shadlen, Schrank, & Kurtz, 2005).

Literature Resources/Online Indexes. Additional searches using academia search premier index, worldcat, EBSCO host research, business and company resources, Sciencedirect and IEEE xplore resulted in a number of articles and academic research papers on intellectual property focusing on information risk assessment (Woloch, 2006), security (Johnson et al., 2009, and international case studies (Marron & Steel, 2000).

A preliminary review reveals that the collected data provide insight to four key elements that should be developed as part of an IP risk management policy, designed for organizations operating in the global market.

The selection of books provides a comprehensive overview of risk management (Hampton, 2009) and IP rights (Moore, 2001) which assist in revealing common findings and factors on IP risk identification and protection.

Additional resources provide a framework for this study, by defining the global environment and risks to organizations. The research conducted using Sciencedirect and IEEE xplore with keywords of *information risk* and *IP security* resulted in academic materials by Thomson, von Solms, Rossouw, and Louw (2006) and articles resources (Rotvold, 2008) which provide a foundation for the examination of IP information risk identification and protection.

Keywords

The key words that follow (see Table 1) are derived from extensive searches, which help to build, shape, and narrow the topic. The majority of the key words are derived from Google search results, by identifying commonly used words within information risk and security articles.

Table 1

Keywords

- Information Protection
- Information Risk Assessment
- Information Security Awareness
- Information Security Risk
- Intellectual Property
- Intellectual Property Strategy
- Organization Policy Management
- Policy and Procedures
- Risk Management

A summary of the search results (see Appendix A) illustrates specific searches conducted using the key words described in Table 1 to capture, evaluate, and summarize the literature (Creswell, 2009). The summary table is organized by the indexes searched and key words to establish relevant resources on the proposed topic. This documented process is used to: (a) determine of the proposed topic is researchable, (b) refine the search strategy as resources are obtained, (c) provide preliminary review of resources, and (d) narrow the key words for relevance so that additional resource materials are located to answer the proposed question within the study (Leedy & Ormrod, 2005). The summary table includes a key that describes the quality, quantity, and relevance resource materials available to support the proposed study. The goal of the search for literature is to find resources that are easy to locate and relevant to the topic (Leedy & Ormrod, 2005).

Search Results

Literature selected for this study is searched in four predetermined areas including: (a) risk management concepts and practices (Hampton, 2009), (b) risk identification (Johnson et al.,

2009), (c) security culture (Furnell et al., 2009), and (d) IP protection (Sutin & Goldberg, 1999). The research on protecting Intellectual Property examines domestic and international laws as well as information risk principles and concepts. Source types include articles in science direct and academic scholarly peer reviewed journals found in academic search premier. In addition, a number of books and article resources are located on *risk assessment concepts* (Alberts, 2003), *information protection* (Maguire, 2009), and *security culture* (Dobrusin & Krasnow, 2008).

Documentation Approach

In this literature review, the first step in the reference selection process is designed to identify a set of predetermined key elements to guide the process of conceptual analysis (Busch et al., 2005). The documentation methods for this study consists of: (a) collect (Leedy & Ormrod, 2005), (b) scan and read (Obenzinger, 2005), (c) resource mapping (Creswell, 2009), and (d) coding process (Busch et al., 2005) of the relevant resource materials.

- Collect – The resource materials are accumulated within a matrix, that tracks the: (a) index location, (b) author(s), (c) year of publication, (d) general topic description (e) date retrieved, and (f) abstract (Leedy & Ormrod, 2005).
- Scan – The resource materials are examined for purpose and relevance to be used for specific written parts of the literature review. Written notes are documented on key elements of risk identification and security awareness culture that tie into the overall themes of the study to be easily identified for future use (Obenzinger, 2005).
- Read – The resource materials are read, then organized in order of importance for the key elements of the study (Obenzinger, 2005).

- Mapping – Is utilized to determine the nature of resources collected as it relates to the relationship to the key elements of the topic and identify categories for the collected related resource material in the study (Creswell, 2009).
- Code – The coding process is the systematic approach of identifying key words and phrases within the collected resource materials (Busch et al., 2005). This process provides detailed information to amplify each of the four predetermined key elements pertaining to the concepts and practices of risk identification and security awareness culture.

Evaluation Criteria

The search for relevant literature utilizes key words in order to find quality resources effectively address the purpose of this study. The evaluation criteria to ensure the selection of high quality information for this study are illustrated by "Criteria Evaluation" on the University of Oregon Library website. These evaluation criteria's are: (a) authority, (b) accuracy, (c) objectivity, (d) quality, and (e) currency.

- Authority – is based in this study on the author's ability to establish the importance of the materials they have written. The author credentials are based on their affiliation with subject matter, organizations, reputation in business, and educational systems ("Criteria Evaluation", UO Library, 2009).
- Objectivity – is based in this study on the clarity of the authors work to inform, explain, and educate the reader on the written literature ("Criteria Evaluation", UO Library, 2009). Materials published by authors on this subject that are found to sell products or services, are to be discarded from the collected materials ("Criteria Evaluation", UO Library, 2009).

- Quality – is based in this study on the authors' ability to describe a methodology and avoids assumptions within their written materials. The material is organized in a logical structure to the literature work and clearly communicates the main points on the subject matter ("Criteria Evaluation", UO Library, 2009).
- Currency – is based in this study on literature collected that, with a few exceptions, has publication dates between 1999 and 2010 ("Criteria Evaluation", UO Library, 2009). This is to ensure that collected materials have relevance to organizations that are challenged by the speed of change, the organizations' strategies of risk management practices and methods of identifying information risks are consistently being revised (Studt, 2004).

Data Analysis Plan

Since this literature review uses a collection of text-based resources as a data source, the qualitative analysis method described by Creswell (2009) is appropriate and applied in this study. Creswell (2009) argues that the data analysis technique provides a basis for identifying and coding implicit terms within the literature. The data analysis begins with mapping (Creswell, 2009) of all the selected resource materials for the literature review. The process continues to the next phase where data is reviewed to obtain a general understanding of IP risk identification and security awareness culture (Creswell, 2009). The data analysis process is used to sort out and understand the relevancy of the resources collected on: (a) risk management concept and practices (Hampton, 2009), (b) risk identification (Johnson et al., 2009), (c) security culture (von Solms & von Solms, 2004), and (d) IP protection (Berenbeim, 1989).

The specific procedure for the analysis includes an eight-step coding process described Busch et al. (2005) on the Colorado University website, designed to identify key elements within the resources of this study.

Each step requires the researcher to consider relevance and application of collected resources within this study using the following rules:

- Step 1: Decide the level of analysis to be coded (i.e., single words or phrases). In this process, single words and phrases are coded:
    - Communication
    - Compliance
    - Exposure
    - Information risk
    - Information security
    - Information security awareness
    - Intellectual property culture
    - Risk identification
    - Risk management practices
    - Theft
- Step 2: Decide how many concepts are to be coded. This process begins with four predetermined coding concepts: (a) risk management concept and practices (Hampton, 2009), and (b) risk identification (Johnson et al., 2009), (c) security culture (von Solms & von Solms, 2004), and (d) IP protection (Berenbeim, 1989). Although coding begins with four predetermined concepts, the researcher remains open to identification of additional key concepts as they may emerge during the coding process.

- Step 3: Decide whether to code for existence or frequency. In this process, the researcher codes for existence of a predetermined concept that appears in the resource materials.
- Step 4: Decide on the level of generalization; locate all text associated with specific codes and interrelated codes that creates a relationship among the code. Selected texts are read with careful consideration to context, so that coding can best identify the initial four predetermined concepts: (a) information security and risk identification, (b) intellectual property protection and information security, (c) information security and security awareness, (d) global market and risk identification, and (e) IP awareness and information security.
- Step 5: Coding rules; apply a translation rule to keep a level of consistency and coherence within the literature review. This is to ensure key elements of the resources to be grouped together (see Figure 2) to make it easier for the audience to follow and comprehend the study. For example, the concepts of *IP Policy* and *Information Security Policy* are defined within this study as the same.
- Step 6: Decide what to do with resource materials that contain irrelevant information. Irrelevant information is not considered, for example as noted in Delimitations, global WIPO agreement laws and regulations.
- Step 7: Decide how to best to apply a systematic approach to code the resource materials. A table (see Appendix B) is designed to document the coding process, comprised of the following header titles: (a) resource number, (b) resource title, (c) author, (d) publication year, (e) relevant predetermined key concept or emergent concept, and (f) specific coding results.

- Step 8: Analyze the results. The results of the coding process are extracted from the coding report table and presented in a matrix (See Appendix B), organized into themes. The plan for organizing and presenting this material is discussed in the writing plan in the following section.

Writing Plan

The results of the coding process are presented in a matrix format (see Appendix B), as noted above in Data Analysis. Coding results are then organized thematically (Literature Review, 2007) in order to address the main research question: How to best frame and disseminate the key elements of an IP Policy within an organization as it relates to risk identification and protection in the global market. Themes align closely with the initial two larger concepts that guide data analysis: (a) IP risk management practices to protect organizations from IP theft, exposure, and non-compliance (Hampton, 2009); and (b) creation of a security awareness IP culture (Dobrusin & Krasnow, 2008). The thematic presentation format follows:

Thematic Outline

I. Key elements of an IP risk management policy, designed to protect organizations doing business in the global market from IP theft, exposure, and non-compliance.
    a. Define risk management.
    b. Risk management key elements within IP policy.
        i. Risk management practices.
            1. Transferring IP information to risk countries.
        ii. Risk identification.
            1. Skills necessary for risk identification.
            2. Training.
    c. Success as a result of risk management practices.
    d. Environmental conditions that lead to increased IP risk in foreign countries.

II. Creation of a security aware IP culture.
    a. Define a security aware IP culture.
    b. Developing a risk free culture.
        i. Training.
        ii. Compliance.
        iii. Communication.
        iv. Practices to protect the organization when there is employee resignation or a reduction of the workforce.

Annotated Bibliography

The annotated bibliography is a collection of the key references used to develop this study. The references provide descriptions of the key elements for two larger content categories: (a) IP risk management practices to protect organizations from IP theft, exposure, and non-compliance (Hampton, 2009); and (b) creation of a security awareness IP culture (Dobrusin & Krasnow, 2008).

Each annotation includes the formal bibliographic citation, an abstract, and comments that explain how the reference is used in support of this study and how the credibility of the reference is determined. These references comprise the data set selected for coding during the data analysis process.

Andress, M. (2001). Effective security starts with policies. *InfoWorld, 23* (47), 56. Retrieved April 24, 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=aph&AN=5558680&loginpage=login.asp&site=ehost-live&scope=site

Abstract. Presents tips for the effectiveness of computer network security policies among companies in the United States. Steps in creating security policies; (a) need to communicate the policies to the employees and (b) ways to enforce security policies.

Comments. Andress is the founder and President of ArcSec Technologies and is a published author on the topic of security. The content within this article is utilized to support the discussion of the key elements of an IP risk management policy, designed to protect organizations doing business in the global market from IP theft, exposure, and non-compliance.

Braunfeld, R., & Wells, T.O. (2001). Protecting your most valuable asset: intellectual property. *IT Professional, 3* (2), 11-17. Retrieved April 12, 2010, from http://dx.doi.org/10.1109/6294.918214

Abstract. As a company grows, protecting its intellectual property could be key to its valuation. We present some basics about trademarks, patents, copyrights, and contracts. Building an organization, managing and motivating people, and finding customers and investors are all difficult and important. The most important thing you could do for your new-economy company is to protect your intellectual property. Without hard assets, protected intellectual property could ultimately determine your company's valuation and even prevent a competitor from entering the same market. Companies create intellectual property daily, and the ability to protect it directly affects its value. There are four main types of intellectual property to consider protecting: trademarks and service marks; copyrights; patents; and trade secrets. We also discuss contractual protections that apply to employing IT staffers, consultants, and subcontractors.

Comments. Braunfeld and Wells are IT security professionals. The content within this study is utilized to support the discussion of key elements of an IP risk management policy, designed to protect organizations doing business in the global market from IP theft, exposure, and non-compliance.

Chandra, I. (2008). The five C's of IT policy. *Internal Auditor, 65* (6), 23-24. Retrieved April 28, 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=35654517&loginpage=Login.asp&site=ehost-live&scope=site

Abstract. The article discusses the importance of reviewing the effectiveness of information security policies, which is a key part of information technology (IT) audit plans. Respondents to Ernst & Young's 2008 Global Information Security Survey say that a security incident would significantly affect their organization's brand or reputation. According to the American Institute of Certified Public Accountants' IT Initiative Survey, the IT initiative has the greatest impact on organizations. It explains the five characteristics of an IT policy.

Comments. Chandra is an experienced compliance auditor at Ernst & Young. The content within this study is utilized to support the discussion of key elements of an IP risk management policy, designed to protect organizations doing business in the global market from IP theft, exposure, and non-compliance.

Choate, P. (2005). *Hot property: The stealing of ideas in an age of globalization*. New York: Knopf. Retrieved April 24, 2010, from http://uolibraries.worldcat.org/title/hot-property-the-stealing-of-ideas-in-an-age-of-globalization/oclc/56809538

Review. Choate surveys the history of intellectual property laws in the U.S. as rooted in our Constitution, reflecting the original commitment to protect inventors for the good of our nation's growth. From this early insight, the U.S. reaped benefits as the nation grew from an agricultural economy to the world's largest industrial and technological economy. The U.S., along with other nations, has undercut protection of intellectual property rights with lax enforcement. Choate points to the growth of the U.S. textile industry, aided by industrial espionage and theft, and the fact that today Japan, Germany, and China are using similar tactics to compete against the U.S. The U.S. is suffering huge economic losses as a result of illegal copying of everything from American films to

music to books. Choate argues that while our nation's disinterest in enforcing our intellectual protective laws is often rooted in geopolitical considerations, we pay a hefty price in our economy and job security.

Comments. Choate possesses a PhD in Economics and has various published works. This book provides insight into today's global commerce involving the importance of intellectual property rights and a description of risk identification in the global market, as presented in this study.

Dobrusin, E.M., & Krasnow, R.A. (2008). *Intellectual property culture*. New York: NY. Retrieved April 24, 2010, from http://uolibraries.worldcat.org/title/intellectual-property-culture-strategies-to-foster-successful-patent-and-trade-secret-practices-in-everyday-business/oclc/166387331

Abstract. The intellectual property culture discusses how to building the culture, and making the culture contagious by: (a) intellectual property within the organization, (b) the role of counsel, (c) earning respect for your intellectual property, (d) giving respect to valid patent rights, (e) constructively sharing and transferring intellectual property, (f) toward a successful intellectual property strategy, (g) trade secrets and other intellectual property, (f) confidential information and effective corporate trade secret programs, and (g) patenting inventions with an International flavor.

Comments. Dobrusin is a founder and shareholder in the law firm of Dobrusin & Thennisch. Krasnow is a Senior Vice President of IP and Chief Patent Counsel at Relypsa, Inc. The content in this book is utilized to explicate the theme of the creation of a security aware IP culture within this study. The content supports the definition of

security awareness IP culture and assists with the concept development of a risk free culture.

Drew, M. (2007). Information risk management and compliance - expect the unexpected. *BT Technology Journal, 25* (1). Retrieved on April 10, 2010, from http://dx.doi.org/10.1007/s10550-007-0004-x

Abstract. This paper sets out to demonstrate how establishing an effective information risk management program is a key element in an enterprise's overall operational risk and governance program. Establishing such a program provides an excellent opportunity to rationalize and align a number of processes and disciplines into an overall effective risk and compliance program. This paper provides the opening steps for establishing such a program to open up the possibility of such an opportunity. The business needs created through legislation and regulation, accounting standards, best practice or contractual commitments for effective governance and appropriate risk management while meeting the need to generate profit and be cost effective. Aspects of financial risk, e.g. credit risk, are supported through mature processes and there is wide commercial experience in many of these finance related areas; however, other aspects of risk may be of such low frequency that little or no experience has been accumulated. For some risks, the processes have not been developed to manage the risk or where a risk management process is present; they are either immature or ineffective.

Comments. Drew is the principle researcher for BT and an experienced engineer. The content within this study is utilized to support the discussion of key elements of an IP risk management policy, designed to protect organizations doing business in the global market from IP theft, exposure, and non-compliance.

Eliason, M.J. (1999) Compliance plus integrity. *Internal auditor, 56* (6), 30. Retrieved April 24, 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=2583464&loginpage=Login.asp&site=ehost-live&scope=site

Abstract. Discusses the balanced approach in the development of corporate values based on compliance and integrity. This article provides details on the two-pronged approach; Assessment of fundamental controls.

Comments. Eliason is a published author and experienced internal auditor at Minnesota Power. The content within this article is utilized to support the discussion of key elements of an IP risk management policy, designed to protect organizations doing business in the global market from IP theft, exposure, and non-compliance.

Furnell, S., Thomson, K., & Thomson, K. (2009). From culture to disobedience: Recognizing the varying user acceptance of IT security. *Computer Fraud & Security, 2009* (2), 5-10. Retrieved March 27, 2010, from http://dx.doi.org/10.1016/S1361-3723(09)70019-3

Abstract. It is often observed that addressing security can be as much about people as it is technology. One of the key aspects here is to establish the correct mindset, and ensuring that people are working for (or at least with) security rather than against it. Unfortunately, people are very often perceived as an obstacle rather than an asset in this regard. Indeed, to quote an Information Security magazine survey from a few years ago, one of the biggest hurdles for organizations to overcome in their attempts to address security is the problem of “unalert, uninterested, lax, ignorant, uncaring end users". One of the most prevalent problems when protecting information assets is the apathetic

attitude, and resulting actions and behavior of employees. Given that the corporate culture of an organization shapes the beliefs and values of those within it, it becomes essential to address the mindsets of employees and ensure that relevant security knowledge and skills are communicated to them. However, organizations cannot assume a uniform starting point; employees have varying degrees of compliance that may evolve to become more compliant or more disobedient depending on the guidance provided by management. This article examines the levels of security acceptance that can exist amongst employees within an organization, and how these levels relate to three recognized levels of corporate culture. It then proceeds to identify several factors that could be relevant to the development of culture, from traditional awareness-raising techniques through to context-aware promotion of security.

Comments. Furnell et al. publish in the area of security and information policy compliance. The content within this article on information security culture supports the theme within this study on security awareness IP culture and assists with the development of the section that describes a risk free culture.

Gans, J. (2005). The dynamic effects of intellectual property practices. *BNet*, Retrieved April 10, 2010, from http://jobfunctions.bnet.com/abstract.aspx?docid=312744

Overview. This paper analyses various intellectual property practices in a dynamic context. Building on a model of Segal and Whinston (2004), the paper considers the rate of innovation when IP (Intellectual Property) licensing is expected versus when it is not. In each case, innovation returns trade off the immediate value from innovation versus the long-term advantages of incumbency. Licensing enhances the former but reduces the

latter relative to no licensing but overall licensing has a positive impact on innovation rates. The paper then turns to consider the impact of other IP practices such as patent breadth, disclosure requirements, experimental use exemptions and protection from expropriation.

Comments. Gans is a Professor of Economics at the Melbourne Business School, University of Melbourne and is a published author on IP practices. The content within this article is utilized to support the discussion of key elements of an IP risk management policy, designed to protect organizations doing business in the global market from IP theft, exposure, and non-compliance.

Grimaila, M.R. (2004). Maximizing business information security's educational value. *Security & Privacy, IEEE , 2* (1), 56- 60. Retrieved May 21, 2010, from http://dx.doi.org/10.1109/MSECP.2004.1264855

Abstract. A business information security course goals and objectives are quite different from most traditional security courses, which focus on designing and developing new security technologies. Business information security primarily concerns the strategic, tactical, and operational management issues surrounding the planning, analysis, design, implementation, and maintenance of an organization's information security program. Core issues include asset valuation, auditing, business continuity planning, disaster recovery planning, ethics, organizational communication, policy development, project planning, risk management, security awareness education and training, and various legal issues such as liability and regulatory compliance. Because businesses cannot afford to mitigate all security risks, students must learn methods to identify and justify the optimal amount of expenditures to ensure that their information assets are sufficiently protected.

Students should also understand the technical components of security so they can appreciate the problems experienced by the people they manage. This paper describes my experiences in the development of an information security course that provides students the knowledge arid experience to succeed in today's competitive information-intensive corporate environment.

Comments. Grimaila is an Assistant Professor of Management of Information Systems at Texas A&M University and is a developer of an information security education program. The article discusses key elements of an organization's information security program. The content within this article on information security culture supports the theme within this study on security awareness IP culture and assists with the development of a risk free culture.

Hanel, P. (2006), Intellectual property rights business management practices: A survey of the literature. *Technovation*, *26* (8), 895-931. Retrieved March 27, 2010 from http://dx.doi.org/10.1016/j.technovation.2005.12.001

Abstract. The survey focuses on the empirical literature regarding the use and management of intellectual property rights (IPRs). It overviews policy changes regarding intellectual property (IP) protection in the US that led, according to some commentators, to patent friendly era in the US. Then it looks at the IPRs use and strategies in the US, Canada, EU, Japan and Australia and at the protection of IP in specific industry groups. Also reviewed is the relationship between the use of IPRs and the size of firm and its ownership (national vs. multinational). Numerous articles show that management of knowledge assets in general and IPRs in particular are increasingly important. The value of firms in knowledge intensive activities is determined by the value of its IP. IP is used

as a financial asset. Firms allocate more human resources to management of IPRs and their training, but there remain important international differences. The recent literature on the impact of IP on the value of the firm, its assessment, valuation, accounting and management of IP are reviewed. The last section of the paper deals with enforcement of IPRs, infringement and dispute resolution. A special attention is given to internet and computer infringement of IP and to insurance as a protection for legal costs.

Comments. Hanel is the author of a number of research papers on technology transfer in the global market and is a Professor of Economics at the University of Sherbrooke. The content within this study is utilized to support the key elements of an IP risk management policy, designed to protect organizations doing business in the global market from IP theft, exposure, and non-compliance.

Herath, T., & Rao, H.R. (2009). Encouraging information security behaviors in organizations: Roles of penalties, pressures, and perceived effectiveness. *Decision Support Systems*, *47* (2), 154-165. Retrieved May 21, 2010, from http://dx.doi.org/10.1016/j.dss.2009.02.005

Abstract. Secure management of information systems is crucially important in information intensive organizations. Although most organizations have long been using security technologies, it is well known that technology tools alone are not sufficient. Thus, the area of end-user security behaviors in organizations has gained an increased attention. In information security, observing end-user security behaviors is challenging. Moreover, recent studies have shown that the end users have divergent security views. The inability to monitor employee IT security behaviors and divergent views regarding security policies, in our view, provide a setting where the principal agent paradigm applies. In this paper, we develop and test a theoretical model of the incentive effects of

penalties, pressures and perceived effectiveness of employee actions that enhances our understanding of employee compliance to information security policies. Based on 312 employee responses from 77 organizations, we empirically validate and test the model. Our findings suggest that both intrinsic and extrinsic motivators can influence security behaviors. Pressures exerted by subjective norms and peer behaviors influence employee information security behaviors. Intrinsic motivation of employee perceived effectiveness of their actions was found to play an important role in security policy compliance intentions. In analyzing the penalties, certainty of detection was found to be significant while surprisingly, severity of punishment was found to have a negative effect on security behavior intentions. We discuss the implications of our findings for theory and practice.

Comments. Herath has a PhD and is an Assistant Professor in the faculty of business at Brock University. Rao has a PhD at the Krannert Graduate School of Management at Purdue University. The article provides a framework for effectiveness of employee actions that play an important role in security policy compliance. The content within this article on information security culture supports the theme within this study on security awareness IP culture and assists with the development of a risk free culture.

Johnson, M.E., Goetz, E., & Pfleeger, S.L. (2009). Security through information risk management. *Security & Privacy, IEEE, 7* (3), 45 – 52. Retrieved April 20, 2010, from http://dx.doi.org/10.1109/MSP.2009.77

Abstract. Managing information risk means building risk analysis into every business decision. Chief information security officers widely agree that action plans must include risk categorization, communication, and measurement.

Comments. Johnson is the Director of Tuck's Glassmeyer/McNamee Center for Digital Strategies and a Professor of Operations Management at the Tuck School of Business at Dartmouth College**,** Goetz was the Associate Director for research at the Institute for Information Infrastructure Protection (I3P) at Dartmouth College, and Pfleeger has a PhD in information technology and engineering from George Mason University. The content within this resource provides a framework for supporting the risk management key elements within IP policy. The goal is to incorporate these elements into every business process within an organization to help the organization move toward security at the source, which means information risk must become everyone's job.

Kadam, A.W. (2007). Information security policy development and implementation. *Information Systems Security*, *16* (5), 246-256. Retrieved April 18, 2010 from http://dx.doi.org/10.1080/10658980701744861

Abstract. Development of the information security policy is a critical activity. Credibility of the entire information security program of an organization depends upon a well-drafted information security policy. Most of the stakeholders do not have time or inclination to wade through a lengthy policy document. This article tries to formulate an approach to the information security policy development that makes the policy document capture the essentials of information security as applicable to a business. The document also conveys the urgency and importance of implementing the policy, not only in letter but also in spirit.

Comments. Kadam has published literature research on information security policy development and is the Chief Knowledge Resource at MIEL e-Security that specializes in information security consulting, training, implementation and audit. The content within

this study supports the discussion of key elements of an IP risk management policy, designed to protect organizations doing business in the global market from IP theft, exposure, and non-compliance.

Martinez de Andino, M., Tate, R.L., & Maddry, T. (2004). Conducting an intellectual property due diligence investigation. *Intellectual Property & Technology Law Journal, 16* (8) 1-3, Retrieved March 28, 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=14149049&loginpage=Login.asp&site=ehost-live&scope=site

Abstract. Discussion on the significance of conducting an intellectual property (IP) due diligence investigation for financing and merger business transactions. Assessment whether the company is being investigated can enhance its market position; Role of the IP attorney in the investigation; Identification of the company's IP assets; Objective of the IP due diligence investigation.

Comments. The authors are experienced lawyers and content experts in intellectual property law. The content within this article is utilized to support the discussion of key elements of IP risk management policy, designed to protect organizations doing business in the global market from IP theft, exposure, and non-compliance.

Martinsons, M.G. (1998). Hong Kong government policy and information technology innovation: the invisible hand, the helping hand, and the hand-over to China. *Engineering Management, 45* (4), 366-380. Retrieved May 21, 2010, from http://dx.doi.org/10.1109/17.728578

Abstract. Although Hong Kong and Singapore have remarkably similar social, economic, and historical profiles, their policies to promote economic and technological

progress constitute an on-going natural experiment and provide a stark contrast. The well-documented, state-led information technology (IT) effort in Singapore is used here to benchmark the lesser known policies and interventions of the Hong Kong government and to examine their impact on IT innovation. Economic restructuring and political uncertainty in Hong Kong, resulting in the mass emigration of manufacturing operations and the professional elite, have prompted a traditionally noninterventionist state to selectively complement the invisible hand of market forces. The Hong Kong government has supported knowledge building and diffusion and helped to create public goods such as electronic commerce, but it has stopped short of guiding or directly subsidizing IT innovation efforts. Emerging IT issues and policy options are considered as Hong Kong becomes part of the People's Republic of China (PRC) under the principle of “one country, two systems”. Free trade and information flows, efficient telecommunications, property rights protection, and technology management expertise are identified as critical factors if Hong Kong is to remain an attractive conduit for and recipient of technology transfer, and if its businesses are to sustain their fast-follower and focus strategies, synergize technological innovations from China and the West, and capitalize on the vast new domestic market.

Comments. Martinsons is a published researcher and experienced engineer on the subject of technology transfer and IP in the Asia region. This article provides the framework on emerging IP issues and comprehending the impact of global policy within organizations that do business in the global market, as examined in the Literature Review section of this paper. The content is utilized to support the discussion of key elements of an IP risk

management policy, designed to protect organizations doing business in the global market from IP theft, exposure, and non-compliance.

Rotvold, G. (2008). How to create a security culture in your organization. *Information Management Journal*, *42* (6), 32-38. Retrieved April 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=aph&AN=35236220&loginpage=Login.asp&site=ehost-live&scope=site

Abstract. The article discusses the ways that information professionals can create a security culture in their organization. The author examines a study by researchers at the University of North Dakota that reveals the importance of assessment, incident response procedures, and social engineering testing as factors in improving security awareness. Security awareness training advice is included, focusing on the creation of comprehensive policies detailing acceptable use and the assessment of security awareness training programs.

Comments. Rotvold possesses a PhD and is a faculty fellow in the Information Systems and Business Education Department of the University of North Dakota. The content within this article on information security culture supports the theme developed within this study on security awareness IP culture and assists with the development of a risk free culture.

Sumner, M. (2009). Information security threats: A comparative analysis of impact, probability, and preparedness. *Information Systems Management*, *26* (1), 2-12. Retrieved April 7, 2010, from http://dx.doi.org /10.1080/10580530802384639

Abstract. The objectives are: (1) to determine the risk assessment of information security threats, based upon the perceived impact and the perceived probability of occurrence of these threats; (2) to determine the extent of risk mitigation, based upon the perceived level of preparedness for each of these information security threats; and (3) to determine the extent to which the of occurrence and the impact of information security threats relate to the level of preparedness.

Comments. Sumner is a Professor of Computer Management and Information Systems and Associate Dean, School of Business, Southern Illinois University Edwardsville. The content within this article is utilized to support the discussion of key elements of an IP risk management policy, designed to protect organizations doing business in the global market from IP theft, exposure, and non-compliance.

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating information security awareness: Research and practice gaps. *Information Security Journal: A Global Perspective, 17* (5/6), 207-227. Retrieved April 20, 2010, from http://dx.doi.org/10.1080/19393550802492487.

Abstract. The aim of this survey is largely exploratory, namely, to discover patterns and trends in the way that practitioners and academics alike tackle the security awareness issue and to have a better understanding of the reasons why security awareness practice remains an unsolved problem. Open coding analysis was performed on numerous publications (articles, surveys, standards, reports and books). A classification scheme of six categories of concern has emerged from the content analysis (e.g., terminology ambiguity), and the chosen publications were classified based on it. The paper identifies ambiguous aspects of current security awareness approaches and the proposed

classification provides a guide to identify the range of options available to researchers and practitioners when they design their research and practice on information security awareness.

Comments. Kokolakis is an Assistant Professor at the Department of Information and Communication Systems Engineering, Tsohou is currently a Ph.D. student within the Department of Information and Communication Systems Engineering, and Karyda is a Lecturer at the Department of Information and Communication Systems Engineering at the University of the Aegean. Kiountouzis is a Professor Emeritus of Information Systems at the Department of Informatics of the Athens University of Economics and Business, Greece. The content within this reference on information security awareness supports the development of the theme within this study on security awareness IP culture and assists with the development of a risk free culture.

von Solms, R., & von Solms, B. (2004). From policies to culture. *Computers & Security*, *23* (4), 275-279. Retrieved on April 12, 2010, from http://dx.doi.org/10.1016/j.cose.2004.01.013

Abstract. Management normally sets company vision, rules and regulations through policies. These policies should provide guidance to employees and partners as to how they should act and behave to be in line with management's wishes. These policies need to be structured and organized effectively to cater for business and technological dynamics and advances. Having defined a series of company policies does not ensure that all employees necessarily obey these policies. Ideally, these policies must manifest in some company culture to ensure appropriate behavior. This can only be achieved through

a proper education process. This paper addresses exactly the process of integrating policies, education and culture.

Comments. von Solms is a Professor in Information Technology at the Port Elizabeth Technikon in South Africia and von Solms is a Professor in Computer Science at the RAUStandard Bank Academy for Information Technology at the Rand Afrikaans University in South Africa. The content provides an organization cultural model for the collective values and knowledge for employees with information security compliance. This reference provides insight on communications within an organization between management and workers for this study.

Review of Literature

When organizations conduct business in the global market, they expose themselves to potential information risk, including intellectual property (IP) theft, exposure, and breach of laws and regulations (Corbin, 2002). Studt (2004) mentions three actions that an organization should take to protect the organizations IP. These actions by the organization are: (a) determine what defines IP within the organization, (b) understand how much information is known outside and inside the organization, and (c) understand how well the organization is safeguarding the IP.

It is important for organizations to understand the value of their IP, and have a policy in place to protect it, one that includes a clear route to the global market, and an understanding of the global environment as a core aspect of competition (Corbin, 2002). Intellectual property risk identification should be an integral part of the IP policy, and should address the potential risks from (a) sophisticated, organized, malicious groups; (b) employee and supplier theft; and (c) the cultural and political environment (Johnson et al., 2009). Specific policies are a necessity for the protection of IP within the organization and are seen as critical activities for capturing the essentials of information security (Kadam, 2007). Intellectual property (IP) policy should communicate clear procedural activities for the organization to follow, so that strict protection enforcement is applied to prevent theft and exposure as well as to create compliance with legal statutes (Lemieux, 2004).

Legal protection for IP varies greatly around the world and the annual losses that companies face from IP violations are substantial (Hanel, 2006). Hanel (2006) adds these losses can be reduced through the development of an organization-wide IP policy. Additionally, organizations should continuously monitor risks for industry and environmental conditions that include the changes to complex laws, regulations, and enforcement in foreign countries which

are evolving in the global market ("Understanding the WTO: Agreements: Intellectual Property", n.d., para. 22)

Also, organizations are expected to have greater opportunity to collaborate between other organizations and outsourcing within security risk countries that place the organization at risk where employees that lack the knowledge of protection inadvertently exposes information that should be protected ("Guidelines on developing intellectual property policy", WIPO, n.d.).

The Importance of Risk Management

Hampton (2009) states that risk management is the process to identify risks that face an organization, forecast the significance of those risks in the business processes, and address the risks in a systematic and coordinated plan. During the implementation of the risk management plan within the organization, it is important to hold key individuals responsible for managing critical risks within the scope of their responsibilities (Hampton, 2009).

According to Hampton (2009), risk management policies and practices should be designed and written especially for the organization, and only after an IP risk assessment is concluded. These policies and risk identification practices are then communicated to the employees to achieve alignment and acceptance at various levels within the organization.

The desired outcome of the design and implementation of a risk management policy for the risk managers within organizations that conduct business in the global market is to help them apply a systematic approach to identification and mitigation of information risks (Hampton, 2009). Without incorporating risk management practices within an organization, the risk managers may not fully comprehend the global laws and as a result could vastly underestimate the vulnerability of their IP in today's competitive e-business world (Corbin, 2002). In order to protect against these risks, information security requires not only technology, but also policy that

reflects clear understanding of potential risks, decision-making, cultural behaviors, and metrics for evaluating related business and security policy options for the global market (Johnson et al., 2009). Without these IP policies in place to safeguard the organizations interests such as the case of managing collaborative business activities in the global market, the relationship to the ownership of the IP, disclosure, and the distribution of technology transfer should be identified during the risk identification process ("Guidelines on developing intellectual property policy", WIPO, n.d.). Organizations should have in place a process to which there is continuous evaluation of different IP systems in the countries where the acquisition of IP rights is sought so that they are properly evaluated for risk identification and the IP risk is proliferated throughout the organization ("Guidelines on developing intellectual property policy", WIPO, n.d.).

The Role of the Risk Manager

Organizations conducting business in the global market should initiate an IP risk assessment process (Alberts, 2003). A critical prerequisite to this risk assessment process, according to Martinez et al. (2004), is to determine the potential risk to the organization's IP. Organizations should classify data to ensure that what is being protected is also what is most important to protect to develop the IP policies (Johnson et al., 2009).

It is the role of the risk manager to identify exposures, assess the frequency and severity of the exposure, identify alternative approach options, and implement the options (Hampton, 2009). Managing information risk is critical to the organization, and information is essential to business processes and innovation within an organization (Lemieux, 2004). A desired outcome for the organization is the effective utilization of risk management practices and the identification of information risks associated with doing business in the global market. Information Risk Management is a strategy that provides the most effective means of

recognizing, assessing, and mitigating the risk that information is exposed to throughout its lifecycle (Hampton, 2009). Organizations struggle to reach the goal of assisting managers to understand the different IP systems within the global market where the acquisition of IP rights are sought ("Guidelines on developing intellectual property policy", WIPO, n.d.).

IP Policy Key Elements

The development of an IP policy within an organization enables the organization to properly identify, protect, and manage IP in the global market ("Guidelines on developing intellectual property policy", WIPO, n.d.). An IP policy should not be a static document but one that evolves to accommodate changing economic conditions, business plans, corporate cultures, and operating environments (Andress, 2001). Five key elements are described below.

Key element #1: Technical language. Andress (2001) believes that, one of the key elements for consideration for any organization is the *technical language* used within an IP protection policy, such as referring to specific technology types, brands, and functions. The technology and e-business platforms are evolving, and this causes the organization to spend time continuously updating policies that include new technology to address changing risk threats (Woloch, 2006). Andress (2001) states one aspect of this key element within a policy should be a step-by-step process that specifically links the use of certain tools which add to the protection of IP.

Key element #2: The need to create multiple protection policies. Another of the many challenges organizations face is the time consuming efforts in the creation of multiple policies to support all the organizations needs and objectives when doing business in the global market (Andress, 2001). As a result, there is a possibility for an organization to overlook growing risks and not create a policy due to the vast number that is needed to ensure IP is protected. Chandra

(2008) argues that policies should cover all information system elements, including data, programs, computers, networks, facilities, people, and processes; and protection should extend to each of these IP security parameters: (a) confidentiality, (b) integrity, and (c) availability (Chandra, 2008). Organizations should examine whether all mission-critical IP risk identification and protection strategies have been identified and covered in the policies (Chandra, 2008). Some of the policy risk elements for organizations doing business in the global market are:

- Supplier contracts – The language of a contract should include security audits and reviews of the suppliers' infrastructure on how they protect the organizations IP. This language should be in place prior to a supplier within a security risk country contract is signed (Ramer, 2001).
- Patent employment agreements – The agreement should specifically affirm that the employer retains all rights, titles, and interests in ideas that are subject to patent laws and developed during the employees' period of employment (Dobrusin & Krasnow, 2008; Goldberg, 1999).
- Non-competition and non-disclosure contracts – The contract should describe restrictions on competition by employees, suppliers, consultants, independent contractors, and strategic partners (Braunfeld & Wells, 2001; Dobrusin & Krasnow, 2008). Additionally, within the contracts IP is defined so that it can be legally protected (Berenbeim, 1989).
- Computer use agreements – Onsite usage of computer resources by employees, consultants, and independent contractors that defines the usage of host computers, file servers, web servers, workstations, stand-alone computers, laptops, software, data files,

multifunctional copier device, printer/plotters, and communication networks (Dobrusin & Krasnow, 2008; Overly, 1999)

Key element #3: Risk identification. The process of risk identification is to identify risk exposures that take into consideration the organization business goals, threats, and vulnerabilities (Hampton, 2009; Johnson et al., 2009; Ramer, 2001). Within this process Woloch (2006) stresses that it is important that employees have the knowledge of not only the organization business goals, but also the level of understanding of the global market in which it operates, i.e., the legal, social, political, and cultural environments in which the risk exists. A risk identification process can provide a methodical way to ensure that all significant risks are identified within each activity that may cause IP to be exposed. As a result, all associated IP risks related to doing business in the global market should be identified, categorized, and mitigated (Drew, 2007; Ramer, 2001).

Key element #4: Employee skills necessary for risk identification. To ensure the necessary skills are developed with the organization to properly identify risk, employees must understand and follow newly created procedural documents that provide detailed, step-by-step guidance (Andress, 2001). These skills needed by employees are: (a) understand the risk identification process (Andress, 2001); (b) understand the global environment and business context that the risk management process (Johnson et al., 2009); (c) understand how to make use of a risk matrix to identify, prioritize, and manage key risks while doing business within the global market (Drew, 2007; Hampton, 2009); and (d) understand how to define the uncertainty and limitations to quantify risk, including the mitigation of interdependencies between different risk sources (Hampton, 2009).

Key element #5: Risk management training as a cultural value. In many organizations today, the focus on training employees on risk management practices is missing (Woloch, 2006). Woloch (2006) argues that IP protection requires a different holistic approach toward IP risk identification and protection, than the traditional risk management practices and training of employees. Woloch's (2006) approach requires a self-perpetuating, real-time mitigation strategy that requires everyone in the organization to apply risk identification and protection practices to help mitigate their portion of the risk management. This new approach allows the organization to be more agile and adapt quickly to risk changes in the environment (Woloch, 2006). The key to self-perpetuating and real-time mitigation is training employees and organizations is changing the perception that IP protection and security is a necessary evil to the perception that IP protection and security is an added company value (Woloch, 2006).

Benefits of Adopting Risk Management Practices

There are a number of benefits for organizations that adopt risk management practices. Woloch (2006) states that risk management practices should not be about compliance; compliance should be a byproduct of the overall risk management practices within an organization. Hampton (2009) points out that risk management supports the strategic and organization business goals. As a result, the organizations promotes continuous improvement, and face fewer risk shocks and unwelcome surprises, while at the same time gaining an agile grasp of new opportunities to mitigate risks (Hampton, 2009; Johnson et al., 2009; Woloch, 2006). Making risk management a part of the organizations culture allows all levels of the organization to identify and mitigate risk, which allows the organization to methodically address the risks by integrating risk management practices day-to-day employee activities at all levels within an organization (Woloch, 2006).

Some of the benefits of risk management illustrated by Hampton (2009), Johnson et al. (2009), and Woloch (2006) are:

- When integrated into IP security policy and practices, risk management supports creation of a definition of information risk and assigns a risk owner for every category of risk (Hampton, 2009).
- Risk management contributes to the lifecycle of information by controlling exposures during different phases of business activities in the global market with risk managers (Hampton, 2009).
- Risk management provides a decision support system practice that facilitates risk managers to understand the information risks, and is a tool to support in the identification of risk and recognize the scale of each risk exposure (Drew, 2007; Hampton, 2009).
- Risk management provides opportunities to identify additional links between information and business risks (Johnson et al., 2009).
- Risk management provides the ability to reduce operating costs to monitor and protect IP from inside or outside threats (Drew, 2007; Woloch, 2006).
- Risk management contributes to the reduction of IP security events by involving all levels of the organization to watching out for risks (Grimaila, 2004; Woloch, 2006).

IP Protection in Security Risk Countries

Organizations should not assume that employees are able to understand or identify the potentially hundreds of risk exposures in foreign countries (Grimaila, 2004; Johnson et al., 2009). It is a known fact that most of the U.S. manufacturing has moved to the Asia Region for a lower cost to manufacture its products as a way to do business in the global market with lower cost engineers and less restrictive regulatory environments (Kish, 2004; Martinsons, 1998). Kish

(2004) emphasizes doing business in foreign countries also includes the complications of IP protection.

Innovation risks. Mashelkar (2002) states IP protection in the twenty first century is critical in regards to innovation. This innovation is the key for production and process of knowledge in the global market. In relation to innovation, Kish (2004) argues there are two forms of counterfeiting theft that can occur in foreign countries. These counterfeiting forms are (a) cloning, where a competitor copies a design and then reproduces it; and (b) reverse engineering, where the competitor takes the design, applies an analysis process, and reproduces it (Kish, 2004).

Local government policies. In many security risk countries, the political environment that attracts outside foreign businesses into their country is, for the most part based on the effort of the country to further its social and economic development (Berenbeim, 1989; Martinsons, 1998; Parry, 2002). Martinsons (1998) states that within these security risk countries, government policies are in place not to protect companies coming into the country to do business, but to promote economic and technological progress for their country. As a result, this increases the critical importance to protect IP while engaged in business in the global market.

Outsourcing risks. There are a number of growing security risks related to outsourcing in the global market, particularly in software development (Ramer, 2001). Ramer (2001) discusses that it is important for organizations to understand the environment the outsource suppliers have in place, in relation to a security infrastructure. Ramer (2001) argues that it is vital that organizations check source coding for trojans, viruses, or embedded code that performs unspecified or even illicit activities. Software development creates complications of IP protection and with the sophistication of terrorists and hackers today, software development can

infiltrate an organization for many different reasons: (a) to be disruptive, (b) to steal trade secrets, or (c) to steal customer data (Ramer, 2001). Ramer (2001) states the organizations should consider the type of software development performed by suppliers in security risk countries to ensure IP is protected. Ramer's (2001) point is that security measures for security risk countries that have outsourcing projects should fit the risks to the organizations IP. Duran, Conrad, Conrad, Duggan, and Held (2009), and Sumner (2009) emphasize that organizations doing business in the global market through employees, strategic partnering, outsourcing or hiring contracted employees should apply risk management practices to address IP risk through greater levels of risk mitigation.

Transferring IP information to security risk countries. The World Trade Organization (WTO) introduced the WTO Agreement on Trade-Related Aspects of Intellectual, Property Rights (TRIPS) that is a binding international agreement, which sets a universal standard for how countries grant and protect IPRs (May, 2007; Parry, 2002; Shadlen, Schrank & Kurtz, 2005). This agreement plays a significant role in the way organizations protect their IP in the global market. Although TRIPs went into effect in 1995, a number of developing countries were granted transition periods to comply with this agreement (Parry, 2002; Shadlen et al., 2005). Marron and Steel's (2000) research on international IP protection states that developed countries provide greater IP protection then do developing countries. As a result, these developing countries are considered security risk countries since they have deficient practices, laws, lenient customs, and policy procedures to enforce IP protection (Berenbeim, 1989; Marron & Steel, 2000; Martinsons, 1998; Shadlen et al., 2005). Furthermore, organizations should investigate which countries are reluctant to recognize or enforce IP rights and take appropriate action to protect their IP (Berenbeim, 1989). Kish (2004) argues that it is important to file patent

applications in as many countries as possible as early as possible and to monitor and prosecute any products that infringe on those patents. However, Kish (2004) also states those organizations that use this approach to apply for patents may have the challenge to maintain and enforce patent rights which requires significant engineering and legal resources. The patent-application process is time-consuming as it can take up to two to three years to receive a patent and this can be a difficult proposition in a global market in which many product lifecycles are half that long (Kish, 2004). Studt (2004) comments that an organization should be aware that when they apply for a patent, the organization might no longer have a trade secret because the patent becomes available for the entire world to know. In the global market, this is one more example, as noted by Thomson, von Solms, and Louw (2006), that one of the biggest threats to the success of IP protection in an organization is the actions and behavior of employees when making a decision on the treatment of the IP. Furthermore, by encouraging IP risk identification and development of policies that holds every person in the organization accountable to manage their portion of the organization's risk, organizations can begin to mitigate the risks brought by new IP threats (Woloch, 2006).

Conclusions

This study is intended to provide a conceptual understanding of the goals and objectives of risk assessment and risk management related to intellectual property. The study is designed for risk managers of organizations doing business in the global market. There are three questions explored in the literature review: (a) what are the key elements of an intellectual property (IP) policy, within an organization that conducts business in the global market, (b) what are the relevant risk management concepts and practices to protect organizations from IP theft, exposure, and non-compliance, and (c) how can organizations create an organization-wide security awareness IP culture for today's global market.

Risk Identification Practices

It is important for an organization to build the necessary risk management knowledge and skills for employees who are required to identify risks. Johnson et al. (2009), Kadam (2007) note in their research that risk identification practices (see Appendix C) help risk managers understand the impact of IP threats to the organization doing business in the global market. By first performing a risk assessment, organizations are able to identify potential threats to the IP and identify which policies are critical to develop (Chandra, 2008; Kadam, 2007). Chandra (2008) and Kadam (2007) argue that during the risk assessment process, there are critical questions to address. These questions are documented in a risk matrix (see Appendix C) and as such can be monitored by risk managers. For each IP potential threat that is identified by the risk manager, there is a mitigation process to be applied by the organization. This risk assessment process provides an insight into the number of potential threats that may arise and into the types of IP protection that are critical to allow the organization to conduct business in the global market (Chandra, 2008; Kadam, 2007).

Creation of a Security Aware IP Culture

Johnson et al. (2009) notes that establishing a level of IP risk tolerance is an informed choice and with the practice of risk identification, the organization should prioritize the risks that are most critical to mitigate by creation of an IP policy. Creating an IP policy requires the development of a security aware IP culture, a compliance strategy, and the communication plan within the organization.

It is important to create a security aware IP culture because in most organizations' employees have no or limited experience and understanding about how and why it is important to protect IP in the global market (Furnell et al., 2009). In addition, they may possess a mindset of "business as usual", which weakens the ability for the organization to secure information (Furnell et al., 2009). In today's organization, employees may view risk as a cultural phenomena that reflects societal and group values, rather than as a potential threat to be expected when conducting business in a global market (Tierney, 1999). Tierney (1999) believes the organization should understand how social change continually modifies risk and vulnerability.

Organizations want to cultivate attitudes and behaviors that recognize IP, respect IP, and trade upon the value of IP (Herath & Rao, 2009). To cultivate the right attitudes and behaviors, the organization must have management support for the goal to build an IP awareness culture (Duran et al., 2009; Siponen, Pahnila & Mahmood, 2009; Voss, 2001). Without managements' endorsement, financial resources will most likely not be made available to support activities (Voss, 2001). Woloch (2006), Dobrusin and Krasnow (2008) argue that an organization's approach to building an IP awareness culture should be to cultivate the culture within all levels of the organization. Dobrusin and Krasnow (2008) note that all organizations have an IP culture; however, it can be a culture of ignorance, indifference, avoidance or sophistication by the

employees. The organization's objective is to foster a healthy and aware IP culture that can be embraced by all employees (Dobrusin & Krasnow, 2008). Dobrusin and Krasnow (2008) assert that the creation of an IP awareness culture is not only for the research and development group within the organization but for the whole organization. An organization's IP can come from many groups within the organization, including (a) sales, (b) marketing, (c) information technology (IT), (d) supply chain, and (e) engineering.

To gain the outcome of a "healthy IP culture" most likely requires changing the current IP culture within the organization, including the employees' values, norms, and attitudes towards employing risk management practices for the protection of IP (Drew, 2007; Thomson, von Solms, & Louw, 2006). Dobrusin and Krasnow (2008) state that, to establish an IP awareness culture, the organization must possess a framework of building blocks to train employees about IP protection in the global market. These are: (a) establish awareness of the needs and benefits of protecting IP, (b) recruit managers who can lead by example, (c) establish policies and practices intended to protect IP, and (d) build an infrastructure that encourages employees to be sensitive to the value of IP to the organization.

Compliance Strategy

There has been a growing concern of the effectiveness of compliance and non-compliance of IP protection policies within organizations because of the increase in the number of potential IP threats organizations face while doing business in the global market (Drew, 2007). Eliason (1999) reveals that a compliance strategy defines the boundaries that management communicates to employees within policies. Management may communicate a "zero-tolerance" around their IP policies and utilize consequences of violations of the policy (Eliason, 1999; Siponen et al., 2010). Eliason (1999) asserts that an organization should also have an integrity

strategy built into the IP policy, which is viewed by the organization as a necessary element to help employee's comprehend issues and concerns that are not indicated within policies. An organization's failure to prevent or minimize IP protection because of a lack of a zero-tolerance policy or a lack of the combination of compliance and integrity strategies is an indication of a failed IP policy (Furnell & Thomson, 2009). Certainly, it is important for organizations to assess whether employees are aware or ignorant of the need to protect IP, since ignorance may result in erroneous behavior (Furnell & Thomson, 2009). Furnell and Thomson (2009) argue that merely communicating to people about what they need to do to protect IP so that they are no longer ignorant of the issues is not sufficient enough to produce an acceptable level of compliance. Siponen et al. (2009) note employees who are in non-compliance to the IP policy may not understand the vulnerability and severity of the IP risk. Siponen et al. (2009) go on to say if the employees do not believe that the policy will remove the threat, adherence or compliance to IP policy will not happen. Organizations must provide adequate training of the application of these policies and understanding of the value of IP protection for the organization (Siponen, Pahnila & Mahmood, 2010).

Woloch (2006) emphasizes that a compliance-based approach to risk management and IP culture is invariably a focus of attention not on doing what is right but on doing what is wrong. Woloch (2006) continues with a related point that a compliance-based IP policy program cannot promote the essential values of the organization because rules are often perceived as negative, whereas values almost invariably reflect the positive; and an aim is to promote a positive set of values, norms, and principles. Dobrusin and Krasnow (2008) argue that values do inspire and Woloch (2006) points out that rules do not inspire employees to comply with IP policies. The inspiration concept articulated by Woloch (2006), Dobrusin and Krasnow (2008) is the fuel for a

self-motivated IP awareness culture and risk identification approach to protect IP that relies equally on people and technology.

A Communication Plan

In most organizations, a communication plan is implemented between management and workers as a way to establish the understanding of the importance of protecting IP at all levels within the organization (Dobrusin & Krasnow, 2008). Knowing how to best communicate information is difficult, since information may be interpreted differently based on specific organizational context (von Solms & von Solms, 2004). Furnell and Thomson (2009) affirm that merely developing and circulating a policy, or directing employees to an intranet page that details security procedures, is not sufficient to foster a healthy IP culture. Dobrusin and Krasnow (2008) suggest the best way to communicate is by developing a communication plan that addresses the following questions: (a) what is IP, (b) what is competitive advantage, (c) what is the importance of their work in regards to IP, and (d) how to identify IP risks in daily work by showing specific examples. As a result, employees can be empowered to protect the IP of the organization and support IP awareness culture. Dobrusin and Krasnow (2008) note the most common mistake organizations can make with communication to employees is to present the policy in legalese; instead, communications should be framed within the following key parameters: (a) relate to the employees everyday work (Voss, 2001;Yuen-Yan &Wei, 2008); (b) relate IP to the business goals such as the global market and competitors, (c) share security war stories; (d) incorporate a healthy dose of humor when presenting, and (e) use didactic images within the presentation.

References

Alberts, C. (2003). *Managing information security risks: The OCTAVE approach*. Upper Saddle River: NJ. Retrieved April 24, 2010 from http://uolibraries.worldcat.org/title/managing-information-security-risks-the-octave-approach/oclc/49383854

Andress, M. (2001). Effective security starts with policies. *InfoWorld, 23* (47), 56. Retrieved April 24, 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=aph&AN=5558680&loginpage=login.asp&site=ehost-live&scope=site

Bell, C., & Smith, T. (2009). Criteria evaluation of information sources. Retrieved on May 01, 2010, from http://libweb.uoregon.edu/guides/findarticles/credibility.html

Berenbeim, R. (1989). *Safeguarding intellectual property*. New York, N.Y.: Conference Board. Retrieved April 24, 2010, from http://uolibraries.worldcat.org/title/safeguarding-intellectual-property/oclc/19569670

Best practices, (n.d.) Businessdictionary.com. Retrieved April 24, 2010, from http://www.businessdictionary.com/definition/best-practice.html

Braunfeld, R., & Wells, T.O. (2001). Protecting your most valuable asset: Intellectual property. *IT Professional, 3* (2), 11-17. Retrieved April 12, 2010, from http://dx.doi.org/10.1109/6294.918214

Busch, De Maret, Flynn, Kellum, Le, & Meyers. (2005). Colorado state university writing guide: Conceptual analysis. *Colorado State website*. Retrieved April 24, 2010 from http://writing.colostate.edu/guides/research/content/com2b1.cfm

Chandra, I. (2008). The five C's of IT policy. *Internal Auditor, 65* (6), 23-24. Retrieved April 28, 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=35654517&loginpage=Login.asp&site=ehost-live&scope=site

Choate, P. (2005). *Hot property: The stealing of ideas in an age of globalization*. New York: Knopf. Retrieved April 24, 2010, from http://uolibraries.worldcat.org/title/hot-property-the-stealing-of-ideas-in-an-age-of-globalization/oclc/56809538

Conducting IP audits, (n.d.). *Concept Foundation*. Retrieved April 10, 2010, from http://www.iphandbook.org/handbook/

Corbin, R.M. (2002). Managing risk and protecting intellectual property. *Ivey Business Journal***,** Retrieved April 28, 2010, from http://www.iveybusinessjournal.com/view_article.asp?intArticle_ID=344

Creswell, J. W. (2003). *Research design: Qualitative, quantitative, and mixed method approaches*. Thousand Oaks, Calif: Sage Publications. Retrieved May 3, 2010, from http://uolibraries.worldcat.org/title/research-design-qualitative-quantitative-and-mixed-method-approaches/oclc/49558924

Dobrusin, E.M., & Krasnow, R.A. (2008). *Intellectual property culture*. New York: NY. Retrieved April 24, 2010, from http://uolibraries.worldcat.org/title/intellectual-property-culture-strategies-to-foster-successful-patent-and-trade-secret-practices-in-everyday-business/oclc/166387331

Drew, M. (2007). Information risk management and compliance - expect the unexpected. *BT Technology Journal, 25* (1). Retrieved on April 10, 2010, from http://dx.doi.org/10.1007/s10550-007-0004-x

Duran, F., Conrad, S.H., Conrad, G.N., Duggan, D.P., Held, E.B. (2009) Building a system for insider security. *Security & Privacy, 7* (6), 30-38. Retrieved May 21, 2010, from http://dx.doi.org/10.1109/MSP.2009.111

Eliason, M.J. (1999) Compliance plus integrity. *Internal auditor, 56* (6), 30. Retrieved April 24, 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=2583464&loginpage=Login.asp&site=ehost-live&scope=site

Furnell, S., Thomson, K., & Thomson, K. (2009). From culture to disobedience: Recognizing the varying user acceptance of IT security. *Computer Fraud & Security, 2009* (2), 5-10. Retrieved March 27, 2010, from http://dx.doi.org/10.1016/S1361-3723(09)70019-3

Gans, J. (2005). The dynamic effects of intellectual property practices. *BNet*. Retrieved April 10, 2010, from http://www.mbs.edu/home/jgans/papers/IP-Dynamic.pdf

Grimaila, M.R. (2004). Maximizing business information security's educational value. *Security & Privacy, IEEE , 2* (1), 56- 60. Retrieved May 21, 2010, from http://dx.doi.org/10.1109/MSECP.2004.1264855

Guidelines on developing intellectual property policy for universities and R&D organizations, (n.d.). *World Intellectual Property Organization website*. Retrieved April 10, 2010, from http://www.wipo.int/uipc/en/guidelines/pdf/ip_policy.pdf

Hampton, J. (2009). *Fundamentals of enterprise risk management*. AMACOM, New York: NY. Retrieved April 24, 2010, from http://uolibraries.worldcat.org/title/fundamentals-of-enterprise-risk-management-how-top-companies-assess-risk-manage-exposures-and-seize-opportunities/oclc/298188255

Hanel, P. (2006), Intellectual property rights business management practices: A survey of the literature. *Technovation, 26* (8), 895-931. Retrieved March 27, 2010 from http://dx.doi.org/10.1016/j.technovation.2005.12.001

Herath, T., & Rao, H.R. (2009). Encouraging information security behaviors in organizations: Roles of penalties, pressures, and perceived effectiveness. *Decision Support Systems, 47* (2), 154-165. Retrieved May 21, 2010, from http://dx.doi.org/10.1016/j.dss.2009.02.005

Identification, (n.d.). *Dictionary.com*. Retrieved April 27, 2010, from http://dictionary.reference.com/browse/identification

Information manager, (n.d.). *The Princeton Review*. Retrieved April 21, 2010, from http://www.princetonreview.com/Careers.aspx?cid=80&page=1&uidbadge=

Institutional policies and strategies, (n.d.). *Concept Foundation*. Retrieved April 10, 2010, from http://www.iphandbook.org/handbook/

Interpretive guidance for project manager positions, (2003). *U.S. Office of Personnel Management***.** Retrieved April 21, 2010, from http://www.opm.gov/fedclass/cg03-0001.pdf

Johnson, M.E., Goetz, E., & Pfleeger, S.L. (2009). Security through information risk management. *Security & Privacy, IEEE, 7* (3), 45 – 52. Retrieved April 4, 2010, from http://dx.doi.org/10.1109/MSP.2009.77

Kadam, A.W. (2007). Information security policy development and implementation. *Information Systems Security, 16* (5), 246-256. Retrieved April 18, 2010 from http://dx.doi.org/10.1080/10658980701744861

Key elements, (n.d.). *Dictionary.com*. Retrieved April 27, 2010, from http://dictionary.reference.com/browse/elements

Kish, D. (2004). IP security: a challenge for the global community. *EDN*, *49* (25), 118-118. Retrieved April 10, 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=aph&AN=15306111&loginpage=Login.asp&site=ehost-live&scope=site

Leedy, P.D. & Ormrod, J.E. (2005). *Practical research: Planning and design*. Upper Saddle River: NJ. Retrieved April 27, 2010, from http://uolibraries.worldcat.org/title/practical-research-planning-and-design/oclc/44046930

Lemieux, V.L. (2004). Two approaches to managing information risks. *Information Management Journal*, *38* (5), 56-62. Retrieved April 10, 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=aph&AN=14416100&loginpage=login.asp&site=ehost-live&scope=site

Literature review. (2007). *University of North Carolina*. Retrieved April 24, 2010, from: http://www.unc.edu/depts/wcweb/handouts/literature_review.html

Maguire, J. (2009). Protect and survive management IP protection. *Engineering & Technology*, *4* (11), 74-75. Retrieved April 10, 2010, from http://dx.doi.org/10.1049/et.2009.1119

Marron, D.B., & Steel, D.G. (2000). Which countries protect intellectual property? The case of software piracy. *Economic Inquiry*, *28* (2), 159-74. Retrieved April 10, 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=eoh&AN=0531615&loginpage=Login.asp&site=ehost-live&scope=site

Martinez de Andino, M., Tate, R.L., & Maddry, T. (2004). Conducting an intellectual property due diligence investigation. *Intellectual Property & Technology Law*

Journal, *16* (8) 1-3. Retrieved March 28, 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=14149049&loginpage=Login.asp&site=ehost-live&scope=site

Martinsons, M.G. (1998). Hong Kong government policy and information technology innovation: The invisible hand, the helping hand, and the hand-over to China. *Engineering Management, 45* (4), 366-380. Retrieved May 21, 2010, from http://dx.doi.org/10.1109/17.728578

Mashelkar, R.A. (2001). Intellectual property rights and the third world. *Current Science*, *81* (8), 955. Retrieved April 18, 2010, from http://www.ias.ac.in/currsci/oct252001/955.pdf

Matrix, (n.d.). *Answers.com*. Retrieved June 20, 2010, from http://www.answers.com/topic/matrix

May, C. (2007). The WIPO development agenda: The campaign to reform intellectual property policy-making. *Global Governance*, *13* (2), 161-170. Retrieved April 10, 2010, from http://www.atypon-link.com.libproxy.uoregon.edu/LRP/doi/pdf/10.5555/ggov.2007.13.2.161

Moore, A. D. (2001). *Intellectual property & information control: Philosophic foundations and contemporary issues*. New Brunswick, N.J.: Transaction. Retrieved April 24, 2010, from http://uolibraries.worldcat.org/title/intellectual-property-information-control-philosophic-foundations-and-contemporary-issues/oclc/46937493

Moore, A.P., Cappelli, D.M.,Caroni, T.C., Shaw, E., & Trzeciak, R.F. (n.d.). Insider theft of intellectual property for business advantage: A preliminary model. *CERT Software Engineering Institute*. Retrieved April 25, 2010, from http://www.cert.org/insider_threat/docs/Insider_Theft_of_IP_Model_MIST09.pdf

Obenzinger, H. (2005). *What can a literature review do for me? How to research, write, and survive a literature review*. Stanford University. Retrieved May 1, 2010, from http://edtech.wku.edu/~tsuzuki/LTCY519Spring2010/LiteratureReviewHandout.pdf

Overly, Michael. (1999). *E-policy: how to develop computer, email, and internet guidelines to protect your company and its assets*. New York: AMACOM. Retrieved April 21, 2010, from http://uolibraries.worldcat.org/title/e-policy-how-to-develop-computer-e-mail-and-internet-guidelines-to-protect-your-company-and-its-assets/oclc/39269566

Parry, B. (2002). Cultures of knowledge: Investigating intellectual property rights and relations in the pacific. *Antipode*, *34* (4), 679-706. Retrieved on April 7, 2010, from http://dx.doi.org/10.1111/1467-8330.00265

Reference. (n.d.). *Dictionary.com*. Retrieved April 25, 2010 from http://dictionary.reference.com/browse/requirements

Rotvold, G. (2008). How to create a security culture in your organization. *Information Management Journal*, *42* (6), 32-38. Retrieved April 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=aph&AN=35236220&loginpage=Login.asp&site=ehost-live&scope=site

Shadlen, K., Schrank, A., & Kurtz, M.J. (2005). The political economy of intellectual property protection: The case of software. *International Studies Quarterly*, *49* (1), 45-71. Retrieved April 7, 2010, from http://dx.doi.org/10.1111/j.0020-8833.2005.00334.x

Shaw, R.S., Chen, C.C., Harris, A.L. & Huang, H. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52* (1), 92-100.Retrieved May 21, 2010, from http://dx.doi.org/10.1016/j.compedu.2008.06.011

Siponen, M., Pahnila, S. & Mahmood, M. (2009). Are employees putting your company at risk by not following information security policies? *Communications of the ACM*, *52* (12), 145-147. Retrieved April 24, 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=aph&AN=45580327&loginpage=login.asp&site=ehost-live&scope=site

Siponen, M., Pahnila, S. & Mahmood, M.A. (2010). Compliance with information security policies: An empirical investigation. *Computer*, *43* (2), 64-71. Retrieved April 24, 2010 from http://dx.doi.org/10.1109/MC.2010.35

Studt, T. (2004). Protecting your intellectual property. *R&D Magazine*, *46* (4), 22-24. Retrieved April 10, 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=12939109&loginpage=Login.asp&site=ehost-live&scope=site

Sumner, M. (2009). Information security threats: A comparative analysis of impact, probability, and preparedness. *Information Systems Management*, *26* (1), 2-12. Retrieved April 7, 2010, from http://dx.doi.org/10.1080/10580530802384639

Sutin, A.N. & Goldberg, E. (1999) Protecting intellectual property. *HR Magazine*, *1999* (10). Retrieved April 19, 2010, from http://www.allbusiness.com/legal/intellectual-property/325280-1.html

Thomson, K.L., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, *2006* (10), 7-11. Retrieved April 2010, from http://dx.doi.org/10.1016/S1361-3723(06)70430-4

Tierney, K.J., (1999). Toward a critical sociology of risk. *Sociological Forum, 14* (2) 215-242. Retrieved May 21, 2010, from http://www.jstor.org/stable/684794

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating information security awareness: Research and practice gaps. *Information Security Journal: A Global Perspective, 17 (*5/6), 207-227. Retrieved April 20, 2010, from http://dx.doi.org/10.1080/19393550802492487

Understanding the WTO: Agreements, (n.d.). *World Trade Organization website*. Retrieved April 2, 2010, from http://www.wto.org/english/thewto_e/whatis_e/tif_e/agrm1_e.htm

von Solms, R., & von Solms, B. (2004). From policies to culture. *Computers & Security, 23* (4), 275-279. Retrieved on April 12, 2010, from http://dx.doi.org/10.1016/j.cose.2004.01.013

Voss, B.D. (2001). The ultimate defense of depth: security awareness in your company. SANS Institute. Retrieved on June 2, 2010, from http://www.sans.org/reading_room/whitepapers/awareness/ultimate-defense-depth-security-awareness-company_395

Wheeler, T. (2008). Organization security metrics: Can organizations protect themselves? *Information Security Journal: A Global Perspective, 17* (5/6), 228- 242. Retrieved April 10, 2010, from http://dx.doi.org/10.1080/19393550802541200

WIPO. (2004). IP and business. *WIPO Magazine,* 10-13. Retrieved May 3, 2010 from http://www.wipo.int/freepublications/en/general/121/2004/wipo_pub_121_2004_01-02.pdf.

WIPO Intellectual property handbook: Policy, law and use, (2004). *World Intellectual Property Organization website*. Retrieved April 10, 2010, from http://www.wipo.int/about-ip/en/iprm/

Woloch, B. (2006). New dynamic threats requires new thinking – Moving beyond compliance. *Computer Law & Security Report, 22* (2), 150-156. Retrieved April 12, 2010, from http://dx.doi.org/10.1016/j.clsr.2006.01.008

Yuen-Yan, C. &Wei, V.K. (2008). Teaching for conceptual change in security awareness. *Security & Privacy, 6* (6), 67-69. Retrieved on May 21, 2010, from http://dx.doi.org/10.1109/MSP.2008.157

Appendix A

Search Results Summary

Search Results Key

Good – Credible resources; supporting topic

Fair – Resource of average quality; high effort to find those supporting topic

Poor – Resource of very low quality; not supporting topic

Search Tool	Key Words	Records	Quality Results
Academic Search Premiere	Intellectual Property, Strategy	546	Good
Harvard Business Review	Intellectual property, strategy	252	Fair
Emerald (Information Management Journal)	Information Management security	404	Good
LexisNexis	Intellectual property	998	Fair
	IP Strategy	20	Poor
	Intellectual property, Information Management security	999	Good
	Intellectual property, Risk mitigation	99	Good
	Corporate theft, Intellectual property	201	Good
Business and Company Resources	Intellectual property	8586	Good
	(By Subdivision) Access and Use	3	Good

Search Tool	Key Words	Records	Quality Results
	Crime against	35	Good
	Forecast and Trends	79	Good
	Evaluation	64	Fair
EBSCO host	Intellectual Property, business processes	20	Good
	Intellectual property, Due diligence	61	Fair
	Intellectual property, Culture	220	Fair
	Information, Risk Assessment	20	Fair
FirstSearch/Wildcat	Intellectual Property, business process	15	Fair
	Intellectual property, Ethics	1008	Poor
Google	Information Protection Intellectual property	139,000	Fair
	Intellectual property, corporate culture	1,380,000	Fair
	Intellectual property policy	87,800,000	Fair
	Intellectual property strategy	21,000,000	Fair
Safari Books Online	Intellectual Property, corporate culture	101	Good
ScienceDirect	Security Culture	100	Good
IEEE/Eplore	Information Risk, security	1,086	Good

Appendix B

Coding Report

Resource Number	Resource Title	Author	Publication Year	Relevant Key concept or emergent concept	Coding Results
1	Effective security starts with policies	Andress, M	2001	Compliance	0
				Information Security	0
				Policies	19
				Policy Development	1
				Security	23
2	Protecting your most valuable asset: intellectual property	Braunfeld, R. & Wells, T.O.	2001	Agreements	21
				Exposure	1
				Intellectual Property	19
				Risk	1
				Countries	3
3	The five C's of IT policy	Chandra, I.	2008	Compliance	11
				Communication	4
				Information Security	16
				Policy	32
				Risk Assessment	11
				Training	0
4	Hot property: The stealing of ideas in an age of globalization	Choate, P	2005	Intellectual Property	Chap. 1,2,3
				Exposure	Chap.4, 5,6
				Policy	Chap 7,8,9
				Security Risk Countries	Chap.4, 5,6
				Risk	Chap4,5 ,6
				Theft	Chap. 3
5	Intellectual property culture	Dobrusin, E.M. & Krasnow, R.A.	2008	Awareness	20
				Compliance	11
				Communication	2

Resource Number	Resource Title	Author	Publication Year	Relevant Key concept or emergent concept	Coding Results
				Culture	20 Chap.1, 2, 3
				Information Security	1
				Intellectual Property	Chap 5,6,7,8
				Policy	3
				Risk Management	72
				Technology Transfer	Chap 8
				Training	7
6	Information risk management and compliance - expect the unexpected	Drew, M.	2007	Awareness	1
				Compliance	22
				Communication	2
				Culture	2
				Information Security	1
				Intellectual Property	10
				Policy	3
				Risk Management	2
				Technology Transfer	0
				Training	0
7	Compliance plus integrity	Eliason, M.J.	1999	Awareness	1
				Compliance Strategy	14
				Communication	3
				Culture	3
				Information Security	0
				Policy	0
				Risks	2
				Training	0
				Compliance and controls	2
8	From culture to	Furnell, S.,	2009	Communication	12

Resource Number	Resource Title	Author	Publication Year	Relevant Key concept or emergent concept	Coding Results
	disobedience: Recognizing the varying user acceptance of IT security.	Thomson, K., & Thomson, K.			
				Compliance	12
				Culture	40
				Security	10
				Awareness	22
9	The dynamic effects of intellectual property practices	Gans, J.	2005	Compliance	0
				Information Security	0
				Intellectual Property Protection	11
				Policy	3
				Policy Development	0
				Security	0
10	Maximizing business information security's educational value	Grimaila, M.R.	2004	Awareness	2
				Compliance Strategy	0
				Communication	4
				Culture	0
				Information Security	11
				Policy Development	4
				Risks Management	3
				Training	0
				Compliance and controls	1
11	Intellectual property rights business management practices: A survey of the literature	Hanel, P.	2006	Compliance	0
				Countries	20
				Information Security	0
				Intellectual Property	11

Resource Number	Resource Title	Author	Publication Year	Relevant Key concept or emergent concept	Coding Results
				Intellectual Property Protection	1
				Trade Policy	9
				Trade Policy Enforcement	11
12	Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness	Herath, T & Rao, H.R.	2009	Awareness	2
				Compliance	58
				Communication	2
				Culture	1
				Information Security	2
				Policy	17
				Risks Management	0
				Training	0
13	Security through information risk management	Johnson, M.E., Goetz, E. & Pfleeger, S.L.	2009	Information Security	12
				Policy Process	13
				Risk	32
				Risk Management	11
				Threats	15
14	Information security policy development and implementation	Kadam, A.W.	2007	Awareness	1
				Compliance	3
				Communication	1
				Culture	0
				Information Security	26
				Policy Development	63
				Risks Management	3
				Threat	56
15	Conducting an intellectual property due	Martinez de Andino, M.,	2004	Intellectual Property	10

Resource Number	Resource Title	Author	Publication Year	Relevant Key concept or emergent concept	Coding Results
	diligence investigation	Tate, R.L., & Maddry, T.			
				Risks	2
				Risk Identification	0
16	Hong Kong government policy and information technology innovation: the invisible hand, the helping hand, and the hand-over to China.	Martinsons, M.G.	1998	Countries	7
				Government	61
				Government Policy	16
				Technology	43
				Technology Transfer	7
17	How to create a security culture in your organization	Rotvold, G.	2008	Awareness	45
				Compliance	6
				Communication	0
				Culture	4
				Information Security	13
				Policy	4
18	Information security threats: A comparative analysis of impact, probability, and preparedness	Sumner, M.	2009	Intellectual Property	10
				Risk identification	0
				Risk Mitigation	19
				Risk Management	1
				Security Risks	23
				Threat	40
19	Investigating information security awareness: Research and practice gaps	Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E.	2008	Awareness	45
				Compliance	6
				Communication	0
				Culture	4

Resource Number	Resource Title	Author	Publication Year	Relevant Key concept or emergent concept	Coding Results
				Information Security	13
				Policy	4
20	From policies to culture	von Solms, R., & von Solms, B.	2004	Awareness	35
				Compliance	10
				Communication	3
				Culture	15
				Information Security	13
				Policy	0

Appendix C

Risk Identification Matrix

IP area of IP concern	What are the areas of IP threats impact business in the global market? (Kadam, 2007)	
Observation threat-source	Describe the threat and answer why these threats exist? (Kadam, 2007)	Describe the threat and answer what are the vulnerabilities corresponding to the threats to IP? (Kadam, 2007)
Vulnerability	Document why the vulnerabilities may exist? (Kadam, 2007)	Document how these vulnerabilities will be exploited? (Kadam, 2007)
Existing control	Document where this may happen and what are the current controls? (Kadam, 2007)	Document when the attack may happen and what are the current protection controls? (Kadam, 2007)
Recommended controls	Document how these protection controls will be changed to remove the threats? (Johnson et al., 2009)	Document how these protection controls will be changed to remove the vulnerabilities? (Johnson et al., 2009)
Level of exposure	Document the critical level of exposure for IP threat? (Johnson et al., 2009)	Document the exposures that are the high priority to take action against by the organization. (Johnson et al., 2009)