International Journal of Arts and Humanities

ISSN: 2581-3102

Volume:02, Issue:08 "August 2018"

WHY THE ZEBRA'S STRIPES ARE IMPORTANT: PROTECTING ORGANIZATION INTELLECTUAL ASSETS

Abigail Opoku Mensah (Ph.D)

Department of Management, School of Business,
University of Cape Coast Ghana, Cape Coast, Ghana

ABSTRACT

This article discusses a framework to protect proprietary information drawing upon the Zebra as a metaphor to protect the information that matters to a business. The discourse to shield proprietary information in successful enterprises is divided in four parts in this paper. The first part deliberates about the nature and description of knowhow and how it can be protected from intrusion. Knowhow can be safe by limiting the number of personnel with access to proprietary data within an organization. The second portion debates about recruitment and selection of potential candidates to work in know-intensive value creation system. Background checks can be supported with personality assessments to limit the appointment of those who are not qualified. The third segment examines the importance of historical data which can be analyzed and interpreted in loss control efforts. The fourth section discusses the know-how and how it is ubiquitous in most value creation systems. All practices procedures and tooling should be patented and only selected key personnel should be allowed into the company's data bases to protect the company's competitive advantage all the time.

Keywords: Cryptography software, Encryption, Historical data, Industrial espionage, Intellectual property, Ubiquitous

INTRODUCTION

The Zebra's stripes and hoofs are drawn as a metaphor to denote the importance of proprietary information, patents, and copyrights. The stripes mesmerize predators and the hoofs can deliver a fatal kick to a hungry lion or hyena. Those are some of the tactics the Zebra applies to survive successfully in an environment where there are numerous predators.

Knowledge in organizations can be created, transferred, and diffused to all distributed cognitive areas where it can be utilized to create products and services appreciated by consumers. In this process, it has different labels such as practices and procedures or technology which needs to be protected from leakage. During the Cold War, corporate spying or corporate espionage was a

form of espionage conducted for commercial purposes instead of purely national security. Companies from both the West and East could have spied on each other's proprietary information. The Federal government responded by passing the Espionage Act 1917 soon after the US joined the First World War. The Espionage Law has since been amended many times to protect the interests of corporations (Rogerson, 1969).

Companies invest large sums of money to create new technology, tools, and equipment's to make the creation of new products a reality. However, the loss of knowledge in the form of trade secrets or confidential information to their competitors can lead to the demise of a business. The Espionage Act (1917) as amended, make it a criminal offense for those found guilty of theft of proprietary information. Knowledge leakage is therefore a concern for many organizations engaged in all type of enterprises including knowledge-intensive operations such as management accounting, software engineering, or management information system corporations. This paper focuses on how risk can be minimized by protecting knowledge from leakage in the value creation system. Technology in this paper is seen to be ubiquitous in most organizations. Job specifications and product formulations are pervasive with procedures and practices requiring defined expertise to produce the services and products demanded by customers.

BACKGROUND INFORMATION

The nature and description of proprietary information

Trade secrets misappropriation in pharmaceutical, biotechnology or consumer packaged goods and software industries worth billions can easily be misappropriated by those who know the value of such investment. According to Techtarget (2018), proprietary information can be misappropriated by an industrial spy who could be an insider or outsider. An insider spy is an individual who has gained employment with the company with the purpose of spying to misappropriate trade secrets of the employer and sell them for a profit. A disgruntled employee who trades information for personal gain or revenge is another insider threat. Spies may also infiltrate through social engineering tactics, for example, by tricking an employee into divulging privileged information.

Outsider spies are those who spy on corporations and will sell the information to their competitors. Techtarget suggested that spies can physically breach the target organization and investigate the premises. In that case, a spy might search waste baskets or copy files or hard drives of unattended computers. Increasingly, the intrusion is through the corporate network. Typically, a targeted attack is conducted to gain initial network access and then an advanced persistent threat is carried out for continued data theft. The capacity of cell phones to record and transmit can also be exploited by leaving a phone in a boardroom, for example, and monitoring a

ISSN: 2581-3102

Volume:02, Issue:08 "August 2018"

meeting remotely. Recording devices are also secreted in a variety of items including eyeglasses, pens, watches, necklaces and dress buttons etc.

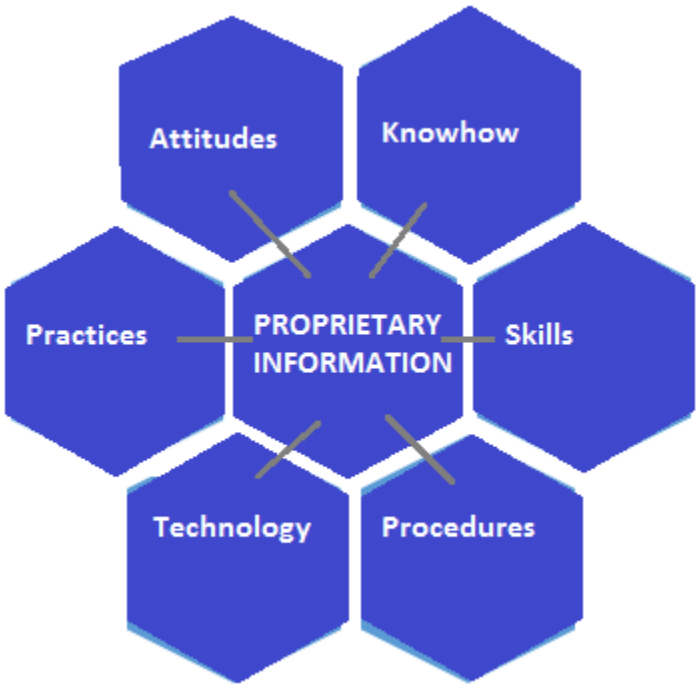

Figure 1: A socially constructed practice (Mupepi & Opoku Mensah, 2018)

Knowhow/Expetise

Knowhow is the practical knowledge and techniques commonly referred to as expertise which is applied in a value creation system to produce goods and services demanded by customers. Expertise can also be gained by experience (see figure 1). Mupepi, Esilla, Opoku Mensah and Mupepi (2018) built upon Thomas Berger and Peter Luckmann to progress the argument that organization's habits can become practices and procedures when the people doing the job gain experience in doing the same tasks over many years. Problems arise when they decide to move on to greener pastures to earn more money or for some other reasons. When they move, they go with their knowledge and skills. Ethically the company cannot stop ex-employees from making a living. A company can develop its own unique practices which can be protected by patent and copyright laws. New recruits can sign contracts of employment or for services which include a section on disclosure agreement.

Practices and procedures

ISSN: 2581-3102

Volume:02, Issue:08 "August 2018"

Knowledge and skills relevant in an industry can be described as practices. What constitute a practice includes trade secrets, product formulations or job specifications. For example, certain knowledge, technology and skills are required to produce a beverage such as coffee or orange soda. The organization can take practical and legal steps to prevent current or former employees from using their confidential information (see figure 1).

Procedures are a way of conducting a business referred to as the modus operandi in Latin. They are part of the practices and can be patented as a bundle. The risk posed by former employees taking confidential information can destroy a business. Trade secrets are the source of what gives life to a business, when they are lost, a business can close down (see figure 1).

Skills

The skill is the expertise put into practice. A skill can be perfected by practice and continuous learning and improvement. However, talent and ability can also be described as exceptional skill to produce something that has value or perform some acts with tact or dexterity. Skill combined with the brashness to do the job and use of appropriate technology can produce products or services appreciated by consumers. When this technique is lost to the competition, a company may fold operations (see figure 1)

Technology

Technology can be referred to as practical knowledge useful in the art and design of tools, equipment, or software useful in making the job easier. A company can have all the technology available but its people make the difference. People doing the job can be empowered and trusted to look after the interests of their employer. Palmer and Shenoi (2009) suggest that advances in information technology over the years, have changed business processes within and between business enterprises. In the 1960s, operating systems had limited functionality, and any workflow management systems that were in use were tailor-made for the specific organization. Improved management information systems education and training have since seen the development of data-driven approaches in organizations, for example data storage and retrieval technologies have improved. This make it possible for software engineers to data-model and build a reliable information system. This notwithstanding, Palmer and Shenoi assert that the business processes had to adapt to information technology because process modeling was neglected. The shift towards process-oriented management occurred in the 1990s. Enterprise resource planning software with workflow management components such as SAP, Baan, PeopleSoft, Oracle and JD Edwards emerged, as did business process management systems (BPMS) much later. Technology has now been at the forefront of business decision making. Encryption technology has also been a tool to protect knowledge from leakage in organizations.

ISSN: 2581-3102

Volume:02, Issue:08 "August 2018"

Explicit and Tacit knowledge

Soliman (2014) described knowledge as a fluid mix of framed experience, values, contextual information, and expert insight that provides a framework for evaluating and incorporating new experience and information. Knowledge is classified into tacit and explicit, where explicit knowledge refers to knowledge that is easy to communicate and can be written in job specifications and job descriptions etc. Soliman describes tacit knowledge as the knowledge which is only known by an individual and is difficulty to communicate with the rest of the workforce. Nonaka, Tayoma and Konno (2000) add that tacit knowledge is deeply rooted in an individual's actions and experiences, as well as in the ideals, values, and emotions he/she embraces. It has two dimensions where the first is the technical breadth, which encompasses the kind of informal personal skills or crafts often referred to as know-how. The second is the cognitive dimension which consists of beliefs ideas values schemata and mental models which are deeply ingrained in us which are often taken for granted. While difficult to articulate, this cognitive dimension of tacit knowledge shapes the way we perceive the world. Tacit knowledge is difficult to capture since it is embedded in a company's practices and the people doing the job. Tacit knowledge can leak when employee leave for greener pastures.

Encryption software

Encryption is a sophisticated technology to barricade information stop and unauthorized entry into databases containing intellectual property such as a manuscript or a design, to which one has rights and for which one may apply for a patent, copyright, and trademarks. Thakur (2018) posited that encryption software was a technology that applied cryptography to prevent unauthorized access to digital information. This is achieved through password and sign-ins at every level of operations and responsibilities. Organizations deploy cryptography software to protect the digital information on their computers as well as the digital information that is sent to other computers over the Internet. Thakur asserted that software that was implemented to secure cryptography was complex to develop and difficult to get right. Most computer users now make use of the encryption software that already exists rather than writing their own.

Risk assessment and analytical hierarchy process

According to Mupepi, Modak ,Motwani and Mupepi (2017), leakage of knowledge is contested to occur in value creation networks embedded in knowledge-intensive firms. A collaborative approach can be utilized to minimize risk and increase sustainability. For knowledge to be preserved from unintentional outflow, its confidential nature and description must be understood at all levels. They suggested that loss of knowledge can occur at any point; whether it is through the process of consultation or when employees do their work. Forfeiture of information can be unintended or a planned effort. To prevent such unintended leakage, it is important to develop a

ISSN: 2581-3102

Volume:02, Issue:08 "August 2018"

shared mindset among employees to minimize the risk. The socio-technical system design is a philosophical framework that enables companies to simultaneously consider both ethical and technical systems to best match the technology and the people involved. History has shown through many situations that firms that failed to comprehend new opportunities were often limited by stakeholders' thoughts and actions. Knowledge leakage from an organization, for example, may come about when an experienced employee leaves for another job. Knowledge leakage is pervasive throughout an organization but is seldom noticed until the consequence is felt. This intellectual capital risk has to be systematically and effectively identified, assessed and controlled in the whole value chain of an organization. An AHP (Analytic Hierarchy Process) based multi-dimensional decision making and assessment model is developed to determine knowledge leakage risk in an organization.

Risk management involves identifying, prioritizing, responding to, assessing, monitoring and reporting risks. Tsang, Wing and Tsui (2016) propose a risk assessment model to minimize knowledge leakage. The risks may include physical risks like fire and earthquake and financial risks like interest rate instability and payment default. However, there is also an important category of risks not specifically addressed by these common frameworks but related to intellectual capital (IC) of organizations which must be effectively managed to ensure competitiveness and sustainability. These risks, arising from IC not properly managed, are called IC risks. Examples are: knowledge leakage, intellectual property (IP) loss and employee turnover. This paper focuses on risk assessment component of a framework as applied to one of the most important IC risks - knowledge leakage. As for risk assessment, it refers to activities carried out in establishing assessment criteria and scope, determining likelihood and impact of risks, and prioritizing them (Mupepi, Modak, Motwani, and Mupepi 2017).

Common frameworks such as those developed by the Committee of Sponsoring Organizations (COSO) (Curtis & Carey, 2012) and CAS (Casualty Actuarial Society, 2013) have similar risk assessment methodology. The determination of the level of risk is important in risk management, including IC risk management. According to Zhi (1995) and Williams (1993), risk is expressed mathematically as: R P = ×I where R is the level of risk, P is the probability for the risk to occur and I is the impact of the risk. In the usual risk management of an organization, the management process consists of many sequential steps: identification, prioritization, aversion, mitigation, assessment, monitoring, reporting and review (Hallikas, Karvonen, Pulkkinen, Virolainen, & Tuominen, 2004). In this study, the focus is on the assessment step which is roughly at the middle of the process. In this step, the performance of the preceding steps is measured. The assessment results then become input to the following steps which depend on such inputs and other information to achieve for example the objectives of monitoring and review. Therefore, a study of risk assessment will yield a high ROI (Return on Investment) and improve the whole

ISSN: 2581-3102

Volume:02, Issue:08 "August 2018"

risk management process significantly. However, the assessment of IC risks has been mainly qualitative and done on individual risks often in isolation from each other. What is lacking is a unified empirical assessment not only at individual risk level but also at functional and organizational levels to obtain better overall management.

Predictive simulation

In Investopedia (2018), the Monte Carlo simulations which is also referred to as probability simulation can be applied to model the probability of different outcomes in a process that cannot easily be predicted due to the intervention of random variables. It is a technique used to understand the impact of risk and uncertainty in prediction and forecasting models. The Monte Carlo simulation can be used to tackle a range of problems in virtually every field such as finance, engineering, supply chain, and science.

A Value Creation System: A divided labor

The article draws from the Adam Smith Pin-production Factory to visualize a value creation process.

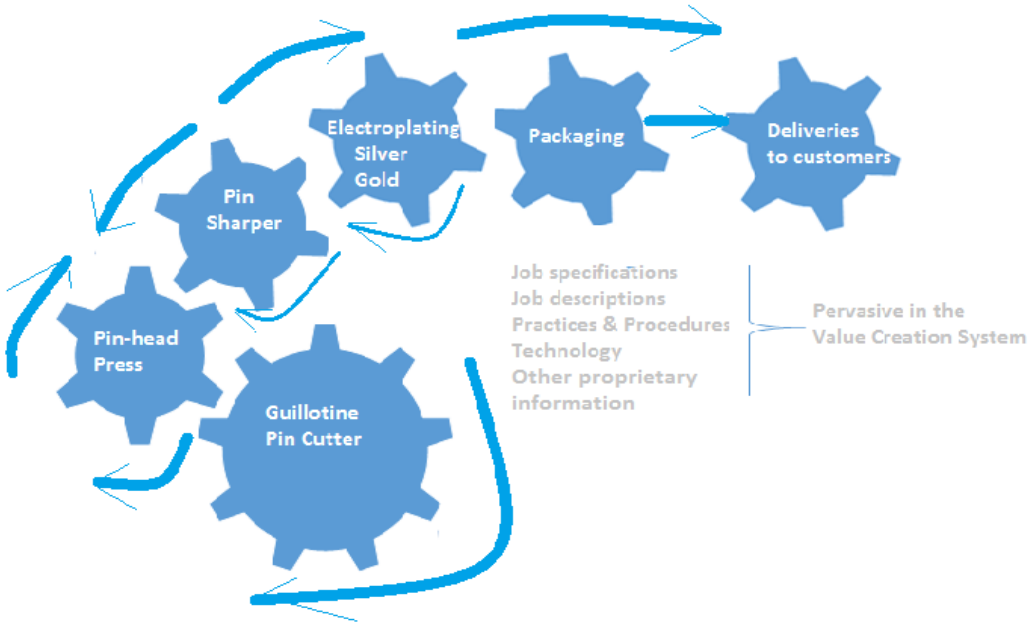

Figure 2: A typical Value Creation System: The Adam Smith Pin Production Factory

According to Mupepi (2014), the divided labor is illustrated with each man doing a specific job such as sourcing the aluminum wire. Another drawing the wire using a guillotine cutter to cut the length of the pin say one inch as specified by the customer. The one-inch pieces of wire are moved to the pin-head press where the operator will be making the "pin-heads" all day. He will

ISSN: 2581-3102

Volume:02, Issue:08 "August 2018"

pass on the finished pin-heads to the pin-sharpener. The next stage is taking the rudiment pins to the pin-polisher who can deploy the electroplating equipment to give the pins a golden, silver, or bronze stain. At each stage, the process adds value to work-in-progress. Various technologies are employed to make the pin-production process efficient and effective. Some of the technologies include software, electroplating gear, injection molding and much more.

Output could be increased

Adam Smith recognized how output could be increased with labor division. In those days, production was dominated by handcrafted goods; one man performed all the activities required during the production process, while Smith described how the work was divided into a set of simple tasks, which could be performed by specialized workers. According to Mupepi (2014), Adam Smith propounded that the division of labor led to the making of the specialists resulting in increased productivity by 24,000 percent. For instance, it was a win-win situation for the pin producer and his pin-makers where the same number of workers made 240 times as many pins as they had been producing before the introduction of labor division.

Knowledge leaking among the specialists

Many good things for the business happened in the divided labor as each man thought about his role and what tools he needed to make his job easier. For example, tools such as the guillotine cutter, electroplating gear, injection molding or software to run production spreadsheets could have been invented by the divided labor. Obviously, those who created special tools were able to make more money through the volume of the pins they could produce. The employer patented the tools or equipment because it was created during the employer's time with resources from the job. The tools and software becomes the employer's confidential information. If this information leaks to their competitors, the employer could go out of business (Giaglis & Paul, 2012).

Employers in this case can take practical and legal steps to prevent current or former employees from using their confidential information. The risk posed to businesses by their former workers has never been greater. But what obligations do employees owe to their former and current employers? And more importantly what steps can employers take to minimize the risks of losing profitability when proprietary information is leaked to the competition?

Sperling (2015) suggested that:

- Contracts of employment should include express and implied obligations owed as part of their contract of employment
- Fiduciary duties to act in their employers' best interests and in their own interests at the expense of their employer which include a duty of not to misuse their employer's confidential or proprietary information

ISSN: 2581-3102

Volume:02, Issue:08 "August 2018"

- Corresponding obligations under Company Act, Statutory law and Common law
- The equitable obligation of confidence

Employees leaving with what they know

Despite the various sources of obligation, knowledge can be compromised in various situations. In Gentile (1996), Ann Hopkins versus Pricewaterhouse is a case brought to the Supreme Court about sex discrimination. Hopkins was denied promotion to become a partner in the accounting firm because of sex discrimination. Hopkins knew how to do her job very well and when she quit in order to start her own accounting practice, some of her clients at Pricewaterhouse went with her. Hopkins later sued Pricewaterhouse for sex discrimination and won her case. After many years of contestations, Pricewaterhouse wanted an injunction to stop Hopkins from practice arguing that she had taken trade secrets with her to her new firm. The judge ruled that the plaintiff had a right to make a living as an accountant and that the clients who followed her to the new practice did so on their own accord because Hopkins was an excellent management accountant. Pricewaterhouse did not win the case. Instead, the judge ruled sex discrimination and ordered that Hopkins be reinstated with back pay for two years and a partnership at Pricewaterhouse.

Access-controlled Databases

Mupepi, Essila, Opoku Mensah and Mupepi (2018) demonstrate how proprietary information can be collected and stored in appropriate databases. These databases can be accessed by authorized personnel only. In the fields of physical security and information security, Access Control (AC) is the selective restriction of access to a place or other resource. Deller (2017) propounds that a commonly accepted framework for the development of policies and supporting regulations that address cyber security vulnerabilities and threats seems to be missing both domestically in the USA and in terms of international collaboration amongst multinational corporation stakeholders. Deller suggested that research aimed at establishing the actions that would allow commonly accepted and established cyber security policies and regulations in industries and the critical infrastructure connected to it could assist organizations to protect intellectual assets.

The act of accessing

The act of accessing may mean consuming, entering, or using. Permission to access a resource is called authorization. Locks and login credentials are two analogous mechanisms of access control. Geographical access control may be enforced by personnel (e.g., border guard, bouncer, ticket checker etc), or with a device such as a turnstile. There may be fences to avoid circumventing this access control (Deller, 2017). Physical access control is a matter of who,

ISSN: 2581-3102

Volume:02, Issue:08 "August 2018"

where, and when. An access control system determines who can enter or exit, where they can exit or enter, and when they can enter or exit.

Evaluating investment in security

Fagade, Konstantinos and Theo (2018) propound that organizations must invest in technical and procedural capabilities to ensure the confidentiality, integrity and availability of information assets and sustain business continuity always. However, given growing productive assets and limited protective security budgets in Ghana, there is a need for deliberate evaluation of information security investment. Optimal resource allocation to security was often affected by intrinsically uncertain variables, leading to disparities in resource allocation decisions. Fagade et al examined how Monte Carlo predictive simulation model could be applied within the context of information technology to reduce these disparities. Using a conceptual enterprise as a case study and verifiable historical cost of security breaches as parametric values, the model shows why using conventional risk assessment approach as budgeting process can result in significant over/under allocation of resources for cyber capabilities. Organizations invest in technical and procedural capabilities to ensure the confidentiality, integrity and availability of information assets and sustain business continuity always. Their model could serve as a benchmark for policy and decision support to aid stakeholders in optimizing resource allocation for cyber security investments.

Electronic access control

Electronic access control uses computers to solve the limitations of mechanical locks and keys. A wide range of credentials can be used to replace mechanical keys. The electronic access control system grants access based on the credential presented. When access is granted, the door is unlocked for a predetermined time and the transaction is recorded. When access is refused, the door remains locked and the attempted access is recorded. The system will also monitor the door and alarm if the door is forced open or held open too long after being unlocked (Fagade, Maraslis, & Tryfonas, 2018)

Assessment and Recruitment Tools

Mupepi, Essila, Opoku Mensah and Mupepi (2018) argued that data collection can be enhanced with survey instruments, including questionnaires. Management can collect data about knowledge and technology usage to pinpoint at individuals who can be held accountable if intellectual assets were misappropriated. Pinpointing at the prevailing organizational cultural conditions as an antecedent to the introduction and management of the amendment is required in a useful company. The data collected can be analyzed and interpreted to develop the metrics required to boost performance. Understanding workers' knowledge and their resourcefulness in

ISSN: 2581-3102

Volume:02, Issue:08 "August 2018"

producing the goods and services demanded by customers is critical in the design and implementation of renovations to progress a business.

There are numerous assessment and recruitment tools available on-line and in hard copies. The MBTL assessment is administered either online or with paper and pencil, most often through a certified individual who has met certain professional requirements for interpreting the results of the instrument. Several options are also available for those who want to take the MBTI instrument:

Personal Feedback:

One can take the MBTI with personal feedback, provided by the Center for Applications of Psychological Type, the non-profit organization cofounded by Isabel Briggs Myers (Seeley, 1986). This service begins with online administration of the MBTI instrument, and includes a highly experienced, certified professional who assists with the interpretation of the results via an hour-long personalized phone consultation.

What to expect when one takes the MBTI instrument:

The person needing the assessment will fill out a multiple-choice questionnaire either in paper form or online. There are no right or wrong answers. The person completing the instrument will select the answers that best fits him or her. Results are most often given in person or by phone through an interactive feedback discussion with a certified practitioner. An interactive feedback discussion with a certified MBTI practitioner allows for personal interpretation that enhances the understanding of MBTI results (Seeley, 1986).

Constructed interview

Usually a panel of interviewers' construct questions which will be asked to the interviewee. The questions will be drawn from various aspects of the job and each question can be weighted or awarded points. After the interview, the panel will tally the points awarded to each candidate. The best candidates usually two can be invited to the final interview. Each member of the panel will be given an opportunity to rationalize their scoring about each of the candidates interviewed.

Historical data

Data analytics are useful to appreciate how data was applied in the value creation system. Manufacturing trading and profit and loss accounts are historical aspects of business organization. The data should be understood in cost control and pricing. Analyzing invoices and delivery notes can denote customers and their purchases. This information can be used to create exploitable databases. Outsourced contracts must be analyzed to comprehend performance in varied environments. Therefore, historical data is important in developing the future.

ISSN: 2581-3102

Volume:02, Issue:08 "August 2018"

SUMMARY

The main points presented in this paper are that knowledge can be identified as know-how, technology and explicit practices in the value creation system. Knowledge can leak in the value creation system through disgruntled employees or through industrial espionage. Employers need to include disclosure clauses in contracts of employment and to limit the numbers of employees who can access proprietary information. Assessment and recruitment tools are available online or in hard copies that can enable employers to augment reference and background checks in hiring people possessing the skills, knowledge, and disposition to effectively do the job. Historical data can include facturing trading and profit and loss accounts or outsourcing accounts while Information for analysis can also include invoices or delivery notes. Data analytics help to understand how knowledge and technology were applied in the value creation system. Data analytics are therefore useful to appreciate how data was applied in the value creation system. Out sourced information must be analyzed to comprehend behavior and costs in varied environments

WAY FORWARD

Human resource practices and procedures which include stencils for contracts of employment at all levels should be in place. Line managers should work together with human resources and corporate council to draft contracts of employment and contracts for services. In all agreements, there should be clauses to protect the interests of the employer. There are numerous recruitment and assessment tools available and a company can select what can be beneficial to its business. Greater collaboration among stakeholders is required to protect the interest of the organization.

Differences between explicit practices and tacit knowledge

	Explicit Knowledge	Tacit Knowledge	How can it leak?
Nature	Easily identifiable	Within person knowledge	Misappropriation
Typical examples	Information	Intuition and insights	Employee leaving job
	Know-that	Practical intelligence skills	Employee leaving job
Mechanism for sharing	Codification	Practice, knowledge teams	Employee leaving job

The core concept behind knowledge protection is that the Value Creation System (VCS) is a source of the competitive advantage innovation and organization performance. The key performance areas in the VCS include explicit practices made out from the experience of the people doing the job who, in addition, possess the brashness to progress the job. In the VCS

ISSN: 2581-3102

Volume:02, Issue:08 "August 2018"

explicit practices in the form of proprietary information can be misappropriated by disgruntled employees as well as those seeking pastures elsewhere.

Implications for Human resources practices and procedures

The organization must put into place human resources practices and procedures and continuous learning and improvement plans to give business the edge. Knowledge could also be barricaded by customizing management information systems and limiting access according to responsibility and authority. Continuous learning and improving is not an option in successful organization however, understanding company policy is critical for individuals to develop schemata to learn and improve their skillfulness. In addition, conditions of service must be articulated by all employees to minimize the resistance to learning and change.

CONCLUSION

Knowledge leakage is a serious flaw in organizations. It can lead to a business's demise or can fold up because of the inability to compete. When proprietary information is lost to the competition it means a company will have nothing new to offer its customers and may lay off people from their jobs. The competitive advantage must be maintained on many fronts such as research and development to create new products, improving upon existing products, and continuous training and improvement of those doing the job.

REFERENCES

Curtis, P., & Carey, M. (2012). Risk Assessment in Practice. Retrieved from http://www.coso.org/documents/COSOAnncsOnlineSurvy2GainInpt4Updt2IntrnlCntrlIntgratdFrmwrk%20-%20for%20merge_files/COSOERM%

Deller, R (2017). Influences from Cyberspace and terrorism on social and cultural perspectives of IT influencers. *European Journal of Cross-cultural Competence and Management, 4* (¾), 294-315.

Espionage Act (1917). Espionage Act of June 15, 1917, c.30, 40 Stat. 217, 50 U.S.C. § 31. As amended. Washington DC: Supreme Court

Fagade, T., Konstantinos, M. & Theo, T. (2018). Towards effective cybersecurity resource allocation: The Monte Carlo Predictive Modeling Approach. *International Journal of Critical Infrastructures*, *13*(2/3), 152-167.

Gentile, M.C. (1996). *Managerial Excellence through Diversity*. Prospect Heights, Illinois; Wavelength Press

Giaglis, G.M.; Paul, R.J. (2012). *It's Time to Engineer Re-engineering: Investigating the Potential of Simulation Modelling for Business Process Redesign*. In Scholz-Reiter, B.; Stickel, E.(Eds), Business Process. New York: Springer Science & Business Media. pp. 313–329

Hallikas, J., Karvonen, I., Pulkkinen, U.,Virolainen, V. M., & T uominen, M. (2004). Risk management processes in supplier networks. *International Journal of Production Economics, 90(*1), 47–58.

Investopedia (2018). Monte Carlo Simulation Accessed 05/16/18 https://www.investopedia.com/terms/m/montecarlosimulation.asp#ixzz5FeGh0IZ3

Mupepi, M.G. (2014). Can the Division of Labor Be Re-Engineered to Advance Organizational Dynamism? *Sage Open*

Mupepi, M., Modak, A., Motwani, J. & Mupepi, S. (2017). *Shielding the Corporation's Raison d'être: Talent Management in Ubiquitous Value Creation Systems.* In M. Mupepi (Ed.), Effective Talent Management Strategies for Organizational Success (pp. 121-133). Hershey, PA: IGI Global.

Mupepi, G. M., Essila, J., Opoku Mensah, A., & Mupepi, S. C. (2017). Asking questions: Applying survey techniques in building successful enterprise. *International Journal of Systems and service-oriented engineering, 7* (4), 44-55. Hershey, PA: IGI Global.

Nonaka, I., Toyama, R., & Konno, N. (2000). SECI, Ba and leadership: a unified model of dynamic knowledge creation. *Long range planning*, *33*(1), 5-34.

Palmer, C. & Shenoi, S. (2009). Critical Infrastructure Protection III: Third IFIP WG 11.10 International Conference, Hanover, New Hampshire, USA, March 23-25, 2009, Revised Selected in Information and Communication Technology 9th Edition. New York: Springer

Parker, H. (2012). Knowledge acquisition and leakage in inter-firm relationships involving new technology-based firms. *Management Decision*, *50*(9), 1618–1633.

Rogerson, A. (1969). *Millions Now Living Will Never Die*. London, UK; ISBN 0-09-455940-6

Seeley, M. S. (1986). *An evaluation of organizational development studies using the Myers-Briggs Type Indicator in the Arlington County, Virginia Fire Department*. New York: New School for Social Research.

ISSN: 2581-3102

Volume:02, Issue:08 "August 2018"

Soliman, F. (2014). Learning Models for Innovation in Organizations: Examining roles of knowledge Transfer and Human Resources Management. Hershey, PA; IGI Global Premier Reference Source

Sperling, M. (2015). There's a Difference Between: "Confidential and Proprietary Information" and a Trade Secret Accessed 05/13/2018 thttps://www.lexisnexis.com/legalnewsroom/corporate/b/business/archive/2015/07/07/there-39-s-a-difference-between-quot-confidential-and-proprietary-information-quot-and-a-trade-secret.aspx

TechTarget (2018). Industrial Espionage. Accessed 5/15/18 https://whatis.techtarget.com/definition/industrial-espionage

Thakur, D. (2018). Cryptography - What is Cryptography? Accessed 5/13/18 http://ecomputernotes.com/computernetworkingnotes/security/cryptography

Tsang, H. W. C, Wing, B, L. & Tsui, E. (2016). Risk Assessment Model: A Construct-Apply-Control Cycle Approach. *International Journal of Knowledge and Systems Science. 7 (*3), 1-18.

Williams, T. (1993). Risk-management infrastructures. *International Journal of Project Management, 11(*1), 5–10.

Zhi, H. (1995). Risk management for overseas construction projects. *International Journal of Project Management, 13*(4), 231–237.

