CORPORATE ESPIONAGE MASQUERADING AS BUSINESS INTELLIGENCE IN LOCAL BANKS: A DESCRIPTIVE CROSS-SECTIONAL RESEARCH

*Sivave Mashingaidze**

Abstract

Information can make the difference between success and failure or profit and loss in the business world. If a trade secret is stolen, then the competitive playing field is leveled or worse, tipped in favor of the competitor. To complicate the problem even more, trade secrets are not only being sought after by a company's competitors, but from foreign nations as well. They are hoping to use stolen corporate information to increase that nation's competitive edge in the global marketplace. This article looked at corporate espionage, how it's done, how it masquerades as business intelligence. Some solutions to reduce the risk of espionage were given. The methodology used was a descriptive cross-sectional research approach. The results found were that many banks and companies disguise corporate espionage as business intelligence and hack or steal other companies' information.

Keywords: Corporate Espionage, Business Intelligence

* *Post-Doctoral Research Fellow, College of Economic and Management Sciences, Department of Business Management, University of South Africa*

1 Introduction

Rabbi Ron Wolfson (2006) stated that the first question is this: "At the hour you enter [heaven] for judgment, they will ask you, 'Did you deal honestly with people in your business practices?' Here honestly means, doing business intelligently not espionage but Sun Tzu's "The Art of War", states that it will not do for a corporation to act without knowing the competition's strategy, and to know the competition's strategy is impossible without espionage (Tzu, 2012). Sun Tzu created his strategy and philosophy over 2000 years ago and the Japanese still apply it today for business and politics. It is very important to understand the classifications of espionage and how a business can protect its physical and intellectual assets from competitors.

In a perfectly elastic market environment, with changing client demands and preferences, local banks are facing fierce competition. The only panacea or antidote is the adoption of business intelligence where better management and better decision-making process make headway for competitiveness in the local banks. Business intelligence solutions for banks provide the decision makers from all business segments of a bank with the ability to manage and exploit information resources, in order to have a competitive age. Business intelligence systems in banks should be comprehensive and yet simple for the end users. Business intelligence covers many areas of the bank, and among the most important are: Customer Relationship Management (CRM), Performance Management (PM), Risk Management (RM), Asset and Liability Management (ALM), and Compliance. Data warehouse and online analytical processes (OLAP) form the informational basis for the application of business intelligence. Data mining and knowledge retrieval are also important segments of business intelligence and deal with complex statistical analysis, discovering "hidden'' relationships between data and forecasting the behavior trends of business systems. Business Intelligence covers the ability of a company to keep information from its competitors so that they may not gain a competitive advantage from their espionage activities. Theft can take the form of Industrial Espionage (IE), corporate espionage, business espionage as defined by the Economic Espionage Act of 1996 (EEA), where trade secrets are stolen by a foreign governments or agents against, or domestic businesses (Hippenmeyer, Morgan, & Ouellette 2004). Business Espionage, on the other hand, is defined by the Central Intelligence Agency (CIA) as involving the theft of trade secrets by competitors, either foreign or domestic. This may include cases where former workers for a company take the protected trade secrets with them when they take on a new and competitive job elsewhere and use them against a previous employer (Smith, 2005). Corporate espionage is a threat to any business whose livelihood depends on information. The information sought after could be client lists, supplier agreements, personnel records, and research documents, prototype plans for a new product or service. Any of this information could be of great financial benefit to a scrupulous individual or competitor, while having a devastating financial effect on a company. Just about any information gathered from a company could be used to commit scams, credit card fraud, blackmail, extortion or just plain malice2 against the company or the people who work there. A customer lists, for example, could be sold to a competitor or used by a sales person to start his own company; thereby effecting the profitability of the victim company (Rusch, 1999)

Holt & Schell, (2010) posited that corporations are implementing technology faster than they can defend against ways it can be used against them. As corporate infrastructures become more open and complex to handle more sophisticated applications, remote customers and users, remote offices and telecommuters, corporations will become more susceptible to intrusions and information theft. Despite the potential risks, security is usually an afterthought to most companies. Few companies spend the money needed to train personnel or to purchase hardware and software needed to monitor and protect their computers and networks. The reasoning behind businesses not spending money on security is because they do not like to spend money on a problem that they do not think they have.

The main objective of this paper is to explore every distinct feature of corporate espionage masquerading as business intelligence , including internal and external BI. Internal BI refers to the protection and utilization of internal data and external BI refers to the gathering of data and information for competition advantage. It covers some background information on corporate espionage, how the spying is done, a few real life examples, and some guidelines to follow in order to protect a business from becoming a victim.

2 Research Methodology

The article used a descriptive cross-sectional research approach. Descriptive research is a study in which the major emphasis is on determining the frequency with which something (Bless et al., 2013). Salaria (2012), states that descriptive research is devoted to the gathering of information about the prevailing conditions or situations for the purpose of description and interpretation. Literature review of relevant documents was used

3 Internal Business Intelligence and Espionage

Corporate spies, infiltrators or hackers can be classified into two basic categories, Internal and External Espionage. Insiders are usually employees: executives, IT personnel, contractors' programmers, network penetrator or computer auditors), engineers, or janitors who have legitimate reasons to access facilities, data, computers or networks. A frequently quoted statistic states that employees commit 85% of corporate espionage crimes (Huang, Zhou & Zhu, 2012). Internal Business Intelligence covers the ability of a company to keep information from its competitors so that they may not gain a competitive advantage from their espionage activities. Theft can take the form of Industrial Espionage (IE), as defined by the Economic Espionage Act of 1996 (EEA), where trade secrets are stolen by a foreign governments or agents against domestic businesses (Hippenmeyer, Morgan, & Ouellette 2004). Insiders have immediate access to enormous amounts of valuable company information and can misuse their privileges or impersonate someone else with higher privileges to plant a Trojan, copy information, or to taint research data. The basic reasons for insiders to "sell out" to a competition are: lack of loyalty, disgruntled, boredom, mischievousness, blackmail, and most importantly, money. According to Smith (2005) there are three types of Espionage when dealing with trade secrets, businesses intelligence and competitive advantage:

Industrial Espionage – Foreign government vs. Domestic Business

Business Espionage – Foreign or Domestic Business vs. Domestic Business.

Corporate Espionage – Legal and ethical intelligence gathering by domestic businesses, for a competitive advantage.

In 1999, Fortune 1,000 companies lost more than $45 billion from the theft of trade secrets, according to a survey by the American Society for Industrial Security and Price Waterhouse Coopers. Today, theft of trade secrets is estimated to be around $100 billion. Finding accurate statistics on corporate espionage is impossible, because no company wants to admit that it was a victim of trade secret theft. Companies do not usually notify the authorities, because they are frightened that admitting to a security breach will cause its stock prices to plummet or a major deal or negotiation to fall through. Banks are notoriously known for not reporting computer or network security breaches, because they do not want the federal government noseying around their systems or questioning their policies and practices. Small businesses do not report incidents of corporate espionage for fear that their trade partners will not do business with them if they find out that their partner's systems are not secure. (Longmore-Etheridge, 2002).

3.1 Business Espionage on

Section 1832 of the Economic Espionage Act of 1996 describes it as the theft of domestic trade secrets by a foreign or domestic business. In addition, according to the Economic Espionage Act of 1996 the term trade secret means all forms and types of financial business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if

- the owner thereof has taken reasonable measures to keep such information secret; and
- the information derives independent economic value, actual or potential, from not being generally known to and not being readily ascertainable through proper means by, the public.

Besides foreign governments, foreign and domestic companies are responsible for the theft of trade secrets from domestic companies. Some of the case studies that are examples of this type of espionage include:

Retired Kodak employees forming a consulting business passing along Kodak internal information.

Taiwanese Business receiving insider information on creation of labels from an employee of a very Dennison.

A Lockheed Martin employee hired by Boeing bringing along trade secrets.

3.2 Industrial Espionage

According to Harris, (1998), Industrial Espionage is the theft of trade secrets by a foreign instrumentality and/or a foreign agent. The main countries that are actively engaged in Industrial Espionage are:

- France
- China
- Taiwan
- Japan and
- Israel

An example of Industrial Espionage was the French Government, in conjunction with Air France, planting electronic listening devices in the seats in first class. The purpose of these devices was to monitor conversation between first class customers discussing business topics. It is unknown as to the amount of information that was lost during these flights. Based on an ASIS survey of Fortune 1,000 companies 20% of all trade secret thefts are conducted by foreign governments, or agents working for these entities and foreign and domestic competitors.

3.3 External Business Intelligence and espionage

Outsiders are spies, attackers, or hackers who enter from outside a company. Since the end of the Cold War, a number of countries have been using their intelligence-gathering capabilities to obtain proprietary information from many of America's major corporations too. Outsiders can enter from the Internet, dial-up lines, physical break-ins, or from partner (vendor, customer, or reseller) networks that are linked to another company's network. These are employees who gather the competitor's information as part of their normal employment process. This information can be collected in the following ways:

- Publications
- Conferences
- Internet
- Business Information
- Trade Shows

3.3.1 Publications

Practically every business has some sort of trade publication or periodical that can prove a wealth of information on what a competitor is doing. Information can frequently be found in editorials, articles and even advertisements. Examples of business journals are numerous. In the aviation industry they include such industry standards as "Aviation Week & Space Technology" a 50+ year old weekly that has been also known for years as "Aviation Leak" due to its staff's ability to find and publish otherwise sensitive information in a public forum (Baniak, Baker, Cunningham, & Martin, 1999).

3.3.2 Conferences and Trade Shows

Conferences provide a superb opportunity to see what a competitor is officially advertising as well as to gain intelligence in a less-than-formal atmosphere. Many professional trade organizations organize annual meetings where companies are encouraged to set up booths to show their peers and fellow companies what they have to offer a company's competitors. "Data mining", as it now generally called, can provide more information in a short period of time than was even remotely possible even twenty years ago. Like any other business tool, however, it needs to be used properly to be of any real use.

3.3.3 Use of the Internet for gathering Business Information

The rise of the Internet and the associated Wide World Web (WWW) has opened vast new possibilities as well as areas of concern, in the area of business intelligence. The Internet provides a vast and typically un-moderated avenue of gaining information on. Computers, LANs and the Internet have made the theft of trade secrets very easy. In today's information age, a thief does not always have to break into an office and steal a briefcase full of documents. With the abundant use of technology, a thief can copy digital information onto a floppy or email it across the Internet to an anonymous Hotmail account for retrieval at a later time. As the old saying goes, information is power and power is money, and in the corporate world there is an enormous amount of information. Obviously proprietary information like secret formulas, manufacturing schematics, merger or acquisition plans, and marketing strategies1 all have tremendous value and are targets to cyber thieves (Robinson, 2003).

4 Techniques used to access valuable corporate information

Hacking

Furnell, & Warren, (1999) considered hacking one of the top three methods for obtaining trade secrets, and it is only increasing in popularity. There are two main reasons why hacking is on the rise: (1) the enormous availability of hacking tools. Currently, there are over 100,000 websites that offer free downloadable and customizable hacking tools (Furnell, & Warren, 1999). (2) Hacking is relatively easy to do. There are tools available that require no in depth knowledge of protocols or IP addressing, they are almost as easy to use as point and click. Hacking can be divided into three subcategories: system, remote, and physical. But the most affecting local banks is physical hacking. According to Hafner, & Markoff, (1995), physical hacking requires the attacker to personally enter a facility. Once inside, the intruder can:

- Roam the building searching for a vacant office or unsecured workstation with an employee's login name and password lying around;
- Search for memos or unused letterhead, and then insert the fake documents into the corporate mail system;
- Attempt to gain physical access to a server or telephone room in order to gain more information on the systems in use;
- Look for remote access equipment and note any telephone numbers written on the wall jacks;
- Place a protocol analyzer in a wiring closet to capture data, user names, and passwords;
- Steal targeted information or hardware containing targeted information.

Attach a hardware keystroke logger between the keyboard cable and the keyboard port on a user's workstation. Hardware keystroke loggers do not require drivers, uses no system resources, works on all PC operating systems, installs in seconds, and they do not send alerts to administrators. However, they do record a user's keystrokes character by character until the logger is disabled. When a password is entered, the logger allows access to the recorded keystrokes. Keystroke loggers have recording capabilities ranging in sizes from 8k (8,000 keystrokes) to 64k (more than 65,000 keystrokes).

A keystroke logger can be used to record:
E-mail compositions
E-mail compositions
Instant Messaging
Chat room activity
Web URL's
User names and passwords
Anything else a user types

4.1 Social engineering

Granger, (2001) propounded that Social engineering is another popular method of obtaining valuable corporate information. The basic goals of social engineering are the same as hacking in general: to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network. Social Engineering is the tricking of a person into revealing their password or other valuable corporate information. Even not-so-casual conversations with unsuspecting relatives of company executives have become conventional tools in corporate espionage. A classic social engineering trick is for an attacker/hacker to send email claiming to be a system administrator. The hacker will claim to need user's password for some important system administration work, and ask the user to email it to him/her. A hacker will usually send this email message to all the users on a system, hoping that one or two users will fall for the trick. Another common social engineering trick is "shoulder surfing", someone looking over an employee's shoulder while he or she types in a password. Password guessing is an additional easy social engineering technique. If a person can find out personal things about other people, he can usually use that information to guess a password. For example, the names of children, their birthdays and anniversaries or social security number are all likely candidates for guessing as passwords

4.2 Dumpster diving

Dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network (Long, 2011). . Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes. It is a very successful technique for acquiring trade secrets and other valuable information. No matter how disgusting dumpster diving sounds, it is legal. Once trash is discarded onto a public street or alley, it is considered fair game. It is only private property if there is a 'no trespassing' sign and you had to trespass to get into the dumpster. The LAN Times (Farley, Stearns, & Hsu, 1996) listed the following items as potential security leaks in corporate trash: company phone books, organizational charts, memos, company policy manuals, calendars of meetings, events and vacations, system manuals, printouts of sensitive data or login names and passwords, printouts of source code, disks and tapes, company letterhead and memo forms, and outdated hardware.

Trash can provide a rich source of information for any corporate espionage agent. Phone books can give a hacker names and numbers of people to target and impersonate. Organizational charts contain information about people who are in positions of authority within the organization. Memos provide small amounts of useful information for creating authentic looking fake memos. Policy manuals show hackers how secure and insecure a company really is. Calendars can tell an attacker which employees are out of town at a particular time. System manuals, sensitive data, and other sources of technical information may give an attacker the exact information he needs to access the network. Discarded hardware, particularly computers with hard drives, can be restored to provide all sorts of useful information (Farley, Stearns, & Hsu, 1996)

4.3 Whacking

Kern, (2004) basically, describing whacking is wireless hacking. To eavesdrop (Listen without the speaker's knowledge) on a wireless networks, all an intruder needs is the right kind of radio, and to be within range of a wireless transmission. With the wide usage of 802.11b devices,(Saha, Chaudhuri, Sanghi, & Bhagwat, 2003) it is possible to pick up signals from outside an office building. Once tapped into a wireless network, an intruder can easily access anything on both the wired and wireless networks, because the data sent over networks is usually unencrypted. 10 If a company is not using wireless networking, an attacker can pose as a janitor and insert a rogue wireless access node into a supposedly secure hard-wired network. Once the WAP, wireless access point, is installed, an intruder can safely sit outside an office building with a laptop and a wireless NIC, and leisurely sniff and explore a company’s network looking for weaknesses and information to exploit. If the WAP is discovered, it will most likely be mistaken for a hub or Jet direct box.

4.4 Phone Ease Dropping

Ease dropping on phone transmissions is yet another tool in the game of corporate espionage (Lin, & Tsai, 2007). A person with a digital recording device can monitor a FAX line and record a FAX transmission and reception. By playing the recording back into a modified Group III or Group IV FAX machine, an intruder can reproduce an exact copy of a message without anyone’s knowledge. Even without monitoring a FAX line, a FAX sent to a “communal” FAX machine can easily be read or copied before it picked up from the incoming FAX basket for delivery to the intended recipient. By picking up an extension or by tapping a telephone, it is possible to record the tones that represent someone’s account number and password using a tape recorder. The tape recording could be replayed over the telephone to gain access to someone else’s account.

4.5 Examples of Corporate Espionage

An example of Industrial Espionage was the French Government, in conjunction with Air France, planting electronic listening devices in the seats in first class. The purpose of these devices was to monitor conversation between first class customers discussing business topics. It is unknown as to the amount of information that was lost during these flights. Based on an ASIS survey of Fortune 1,000 companies 20% of all trade secret thefts are conducted by foreign governments, or agents working for these entities and foreign and domestic competitors (Fitzpatrick, & Burke, 2003)

Retired Kodak employees forming a consulting business passing along Kodak internal information.

Taiwanese Business receiving insider information on creation of labels from an employee of a very Dennison.

A Lockheed Martin employee hired by Boeing bringing along trade secrets.

In addition to government entities, many companies in the energy, defense and pharmaceutical sectors are also becoming the targets of espionage and IP theft. According to the UK Cyber Cabinet Office, industrial cyber crime, including firms spying on each other, costs around GBP7.6 billion (US$12.4 billion)(Billand, Bravard, Chakrabarti, & Sarangi, 2009).

5 Rehabilitation/risk reduction measures for espionage

Protection of this espionage should be the most important aspect of domestic banking operations. The question arises that if 20% of all trade secret thefts are conducted by foreign governments or businesses, which makes up the remaining 80%. The same study shows that 30% are employees (e.g., Avery Dennison), 28% are former employees (e.g., Kodak and Lockheed Martin/Boeing), and the remaining 22% are vendors, contract employees, OEM employees, and consultants. These people are outsiders that have insider’s access and privileges. It is easy to see that the majority of the trade secret thefts come from inside the business (Fink, 2003)

5.1 First line of defense against espionage

The basic first line of defense against any form of corporate espionage is a two- bifurcated approach: 1. controlled access and 2. Knowing your employees and customers.

5.1.1 Controlled Access

Protect the most critical data by encrypting it (Schultz, 2005). If it is encrypted and it is stolen it will be useless to anyone. If your network is on the Internet, use a firewall and audit the servers for security holes on a regular basis. Also make sure that the operating system has all of the latest security patches and fixes installed. Schultz, (2005) suggested that sensitive information about your business should never be stored on a networked computer. Instead, it should be kept on a stand-alone computer with no connection to any other computer or telephone line. This computer must be kept in a separate locked office or room at all times. Secure the room by using quality deadbolt locks and steel clad doors, adequate lighting, and install a monitored alarm system in the room. Allow only those who need to know or use the sensitive information to have access to the room. Anti-virus and password security software should be installed on the secured system. This computer should be checked for viruses on a weekly basis and the password used to access sensitive files should be changed just as often. The computer hardware should be locked or bolted down to a very, large piece of furniture or to the floor or wall. It is also advisable to place a disk drive lock over the disk drive bays of the computer to stop anyone from making a copy of files onto a floppy, or worse, inserting a disk or memory stick and placing a virus in the computer. Educate traveling executives who carry company laptops about using precautions to prevent theft and examine communications with overseas facilities with an eye toward installing commercially available encryption that is extremely hard to crack

5.1.2. Cyber police unit

It's a designated web watchdog team that will be responsible for targeting specific networking websites that engage in espionage and incite riots (Hughe, & Love, 2004).

5.1.3 Knowing your personnel staff

Like customer due diligence, talent acquisition due diligence is also very crucial. Knowing employees means verifying the backgrounds of new employee applicants or employees assigned to work on sensitive projects. When hiring new employees in sensitive areas or who will have access to sensitive data, do a thorough background check. Call all of the references the prospective employee provides and then call the human resource departments of his or her last few jobs and ask for additional references. Confirm that they are who they say they are and not an undercover operative looking to photocopy company secrets for profitable sale to your competitor (Srivastava, & Bhatnagar, 2008).

6 Recommendations

In addition to controlling access to sensitive areas and data, and talent acquisition due diligence, the following basic security to do list will help to defend against corporate espionage:

Conduct routine security awareness training for all employee

Lock all doors. Computer passwords alone won't keep determined infiltrators from stealing

Encrypt sensitive computer files.

Secure all dumpsters and post 'NO TRESPASSING' signs.

Do not discuss company secrets in unsecured environments.

Require that all visitors be escorted at all times

Keep wire closets, server rooms, phone closets, and other locations containing sensitive equipment locked at all times

If possible, place locks on computer cases to prevent hardware tampering

Never leave a voice mail message or e-mail broadcast message that gives an exact business itinerary or names and telephone numbers of clients where you can be reached

Institute a security policy for your company network and use it. Train all of the employees on safe computing practices. Teach them how to keep their data and computers safe from unauthorized access.

Conclusions

Although business intelligence/information can make the difference between success and failure or profit and loss in the business world, but if a trade secret is stolen (espionage), then the competitive playing field is leveled or worse, tipped in favor of the competitor. This article revealed has shown how internal and external corporate espionage is done and the article also provided some ways to reduce the risk of espionage from the interior to the exterior.

References:

1. Baniak, J., Baker, G., Cunningham, A. M., & Martin, L. (1999). Silent Sentry passive surveillance. Aviation week and space technology, 7, 134-139.
2. Billand, P., Bravard, C., Chakrabarti, S., & Sarangi, S. (2009). Corporate espionage.
3. Farley, M., Stearns, T., & Hsu, J. (1996). LAN times guide to security and data integrity. Osborne McGraw-Hill.
4. Fink, S. (2003). Sticky fingers: Managing the global risk of economic espionage. iUniverse.
5. Fitzpatrick, W. M., & Burke, D. R. (2003). Competitive intelligence, corporate security and the virtual organization. Journal of Competitiveness Studies, 11(1), 20.
6. Furnell, S. M., & Warren, M. J. (1999). Computer hacking and cyber terrorism: the real threats in the new millennium?. Computers & Security, 18(1), 28-34.
7. Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics.Security Focus, December, 18.
8. Hafner, K., & Markoff, J. (1995). Cyberpunk: outlaws and hackers on the computer frontier, revised. Simon and Schuster.
9. Harris, J. R. (1998). Industrial espionage and technology transfer. Aldershot: Ashgate.
10. Hippenmeyer, P., Morgan, R., & Ouellette, D. (2004). Business Intelligence: Overview and Case Reports.
11. Holt, T. J., & Schell, B. H. (Eds.). (2010). Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications. IGI Global.
12. Huang, X., Zhou, H., & Zhu, H. (2012). Assessing the systemic risk of a heterogeneous portfolio of banks during the recent financial crisis. Journal of Financial Stability, 8(3), 193-205.

13. Hughes, V., & Love, P. E. (2004). Toward cyber-centric management of policing: back to the future with information and communication technology.Industrial Management & Data Systems, 104(7), 604-612.
14. Kern, B. D. (2004). Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law. Santa Clara Computer & High Tech. LJ, 21, 101.
15. Lin, Y. B., & Tsai, M. H. (2007). Eavesdropping through mobile phone.Vehicular Technology, IEEE Transactions on, 56(6), 3596-3600.
16. Long, J. (2011). No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing. Syngress.
17. Longmore-Etheridge, A. (2002). LEADERSHIP FOR TODAY AND TOMORROW Steven C. Millwee, CPP, ASIS's new president, discusses past accomplishments and future plans for growing the Society. SECURITY MANAGEMENT, 46(1), 63-69.
18. Pooley, J. H., Lemley, M. A., & Toren, P. J. (1996). Understanding the Economic Espionage Act of 1996. Tex. Intell. Prop. LJ, 5, 177.
19. Robinson, S. W. (2003). ESPIONAGE 101.
20. Rusch, J. J. (1999, June). The “social engineering” of internet fraud. In Internet Society Annual Conference, http://www. isoc. org/isoc/conferences/inet/99/proceedings/3g/3g_2. htm.
21. Saha, S., Chaudhuri, K., Sanghi, D., & Bhagwat, P. (2003, March). Location determination of a mobile device using IEEE 802.11 b access point signals. InWireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE (Vol. 3, pp. 1987-1992). IEEE.
22. Schultz, E. (2005). The human factor in security. Computers & Security, 24(6), 425-426.
23. Smith, R. (2005). OSS: the secret history of America's first central intelligence agency. Rowman & Littlefield.
24. Srivastava, P., & Bhatnagar, J. (2008). Talent acquisition due diligence leading to high employee engagement: case of Motorola India MDB. Industrial and Commercial Training, 40(5), 253-260.
25. Tzu, S. (2012). The art of war. e-artnow.
26. Winkler, I. (1997). Corporate Espionage: what it is, why it is happening in your company, what you must do about it. Prima Lifestyles.
27. Wolfson, R. (2006). The spirituality of welcoming: How to transform your congregation into a sacred community. Jewish Lights Publishing.