ANALYSIS OF THE "HUMAN FACTOR" AS AN INFORMATION THREATH TO TRADE SECRETS AND COUNTERACTIONS – SPYING IS IN!

Tamara Jovanov, *MSc*
Faculty of Economics, "Goce Delcev" University — Stip,
(Republic of Macedonia)

"Economic espionage and trade secret theft threaten our nation's national security and economic well being."[1]
Since the 1970s brought the explosion of the Information Revolution and the rise of personal computers, we've become even more interested in the brain and how it works. We shouldn't be aware of Artificial Intelligence and the smart machines of the 21st Century, but of the people in our surroundings and their ability to be corrupted from our competitors. How can we know who is really working for us and who is on the other side from inside!? The changing business environment is putting a huge pressure on the everyday activities of the corporations and has pushed them into a corner, where they do not choose the means of their survival. People - spies - companies, and even countries are after your company's property…

The flying heads of once well established managers and corporate directors are a consequence of poorly protected corporate secrets and installed moles among the loyal company workers. Virtually no company is immune to the risk of economic espionage. If you think economic espionage happens only to the Fortune 500 giants who have huge secrets to steal and operate on a global basis, think again! While all companies are at risk, the biggest victims of economic espionage are typically smaller businesses. And why? Because these companies have the largest number of competitors, which translates into the largest number of possible spies. Globalization as well has raised their profile significantly. This may make them a target of someone's espionage scope. If the company has confidential "secret" information, legally referred to as a trade secret (it doesn't matter whether it is chemical formula, patent application, marketing plan, business expansion plan, customer list, pricing information, new product launch information, new technology drawing, etc.), which is one type of intellectual property, that has independent economic value, which you have made a reasonable effort to keep secret, and someone illegally gets a copy of it, you have been a victim of economic espio-

[1] President Bill Clinton, Upon signing the Economic Espionage Act, October 11, 1996

nage. Companies are under attack and at enormous risk every day from the global threat of economic espionage, but that risk can and should be lowered and managed. If we don't take for granted the fact that the companies are constituted by people, we can admit that the most common factor of information leaking is the human factor. But why do they do it? It is luxury question to ask if noted that the answers can be various and very individual. Many of the espionage spies do it for money, for greed, for revenge, for their native countries, for opportunity or just because of their huge egos. So it is therefore possible to assume that the anatomy of the spy can be well put in a several counts: young, well educated individual, male or female, with high intellectual potential, ambitious, with money issues, neglected from the company, with troubled childhood, loyal to higher goals. Thanks to the modern age they also have the gadgets to do the job: micro stick - an mini compact audio and video recorder; wrist watches which can record even an rustling conversations with it's hidden voice recorder; dime-size "contact bugs," which anyone could stick to the outside of a conference room window and matchbox-size "SIM bugs"; listen-only cellphones that don't ring or light up, that can be activated by a phone call an hour, a week or a month later; innocuous-looking ballpoint pen with a voice-activated audio recorder; Keyghost; etc. Proprietary and trade secret information are the lifeblood of every company in every industry group. Given how valuable trade secrets are, you would think that companies would bend over backwards to protect them, but that is not the case. If the Pareto rule should be applied, than we could say that 80 percent of the risk comes from inside the company, and only 20 percent from outside the company. Opposite of what it is, the focus on reducing risk of trade secret theft should be on education and ethics, not physical security, but the majority of money spent on protecting a company's assets is spent on protecting the physical assets, and it is spent largely to protect the company from only 20 percent of the risk—from outsiders. Think how tough it sometimes is just to get into some buildings as a visitor. You often have to sign in and be issued a badge. At some locations, visitors have to be escorted in certain sensitive areas. You need to know and then punch in on a keypad special door combinations or have card keys to open doors or have elevators stop at specific floors. Security guards greet and watch you when you arrive in the lobby or walk around or enter or leave the parking lot. Closed circuit TV cameras are mounted in ceilings or some other inconspicuous locations keeping an eye on you. In most cases, what is actually being protected is physical property from outsiders, not trade secrets from insiders. Typical security people in

office buildings are concerned with guarding against thieves walking off with a computer; they wouldn't know a trade secret if their lives depended on it. Given that some 80 percent of trade secret theft is perpetrated by employees or other insiders, most companies simply do not properly address the issue of protecting trade secrets. This lapse only increases a company's risk that an employee, ex-employee, or some other insider will walk off with a valuable trade secret, whether intentionally or not. A trade secret that gets out into the marketplace accidentally can cause every bit as much harm as those that are breached by true spies. The question is: Can anything be done to stop economic espionage and secure the informations? - It is impossible to stop it, but it can be reduced! Information protection should be based on eight major elements:[2]

1. Information protection should support the business objectives or mission of the enterprise – the position of the ISSO (Information Systems Security Officer) has been created to support the enterprise, not the other way around;
2. Information protection is an integral element of due care – the senior management is required to protect the assets of the enterprise and make informed business decisions (an effective information protection program will assist in meeting these duties);
3. Information protection must be cost effective (implementing controls based on pre identified significant risk existence);
4. Information protection responsibilities and accountabilities should be made explicit (it is necessary to publish an information protection policy statement where the roles and responsibilities of all employees would be identified);
5. System owners have information protection responsibilities outside their own organization (monitoring the usage of the information to insure that it complies with the level of authorization granted to the user);
6. Information protection requires a comprehensive and integrated approach (information protection issues should be a part of the system development life cycle and during the initial or analysis phase, information protection should receive as its deliverables a risk analysis, a business impact analysis and an information classification document. Additionally, because information is resident in all departments throughout the enterprise, each business unit

[2] Thomas R. Peltier, Justin Peltier, John Blackley, "Information Security - Fundamentals", CRC Press LLC, USA, 2005, p.1-2

should establish an individual responsible for implementing an information protection program to meet the specific business needs of the department);

7. Information protection should be periodically reassessed (due to the dynamic of the process it must be reassessed at least every 18 months);
8. Information protection is constrained by the culture of the organization (the ISSO must give each business unit the latitude to make modifications to meet specific needs).

The conducting of a "walk – about" for a measurement of the current attitude toward information protection should be focused on five basic control activities:[3]

1. Offices secured;
2. Desk and cabinets secured;
3. Workstations secured;
4. Information secured;
5. Diskettes secured.

The typical office environment will have a 90 to 95 percent noncompliance rate with at least one of these basic control mechanisms.[4] In business, having an effective information protection program is usually secondary to the need to make a profit, and the main reason we don't hear so much about its weaknesses and trade secrets theft in public is because the principals do not want the stockholders or the press getting a hold of the fact that company secrets were leaked because of what that would do to the company's stock price.

References

1. Hedieh Nasheri , "Economic Espionage and Industrial Spying", Cambridge University Press, USA, NY, 2005;
2. John Aycock, "Computer Viruses and Malware", Springer Science+Business Media, LLC, 2006, Canada;
3. Khaled Khan & Yan Zhang, "Managing Corporate Information Systems Evolution and Maintenance", Idea Group Inc., USA, 2005;
4. Mark Osborne, "How to Cheat at Managing Information Security", Syngress Publishing, Inc., Canada, 2006;
5. Mark Stamp, "Information Security – Principles and Practice", John Wiley & Sons, Inc., New Jersey, 2006;
6. Steven R. Barth, "Corporate Ethics – The Business Code of Conduct for Ethical Employees", Aspatore Books, Inc., USA, 2003;
7. Thomas R. Peltier, Justin Peltier, John Blackley, "Information Security - Fundamentals", CRC Press LLC, USA, 2005;

[3] Ibid., p.3

[4] Ibid.