

Corporate Espionage

The good old days would be in complete shock if they were to cast a glance at Corporate Espionage today. Less than 50 years ago, you'd have to jump through a number of physical and mental hoops to be able to spy on a competitor in the corporate jigsaw. But thanks to information technology, the spies are back in business!

Amidst the hush-lanes of the corporate world today it has, sadly, become the norm that just about any means to brush aside competition are fair game. Whether the means are ethical or unethical no longer seems to be the question.

Putting Things Into Perspective

Corporate Espionage involves corporate institutions spying over competitor institutions. The methods were more straightforward in the past: picture a cloaked man smoking a cigar discreetly in a corner while eavesdropping on conversations. The scene today is completely different with information technology enabling business to be conducted at the click of a mouse. As a result, many companies may never even find out that they are being spied upon.

Let's consider some statistics. In 2006, U.S. security experts estimated that industrial spying costs global businesses more than \$200 billion a year¹. To put things into perspective, Microsoft's market capitalization stands at \$200.50 billion as of October 24, 2008, the U.S. government's takeover of Fannie Mae and Freddie Mac extended as much as \$200 billion in treasury support to the two companies², and based on figures as of October 8, 2008, \$200 billion would equal to approximately 1 year and 4 months of the Iraq War³.

Modus Operandi

So what exactly are the spies after and how do they do it? The answer to the first part of the question is straightforward. Think about what information is mission critical to your organization. This could include intellectual property, pricing strategies, future plans, research and development data, customer information, patents in progress, source code, and the list can go on. The second part of the question is not as simple. In fact, the answer is changing as we speak.

The computer was first designed to make calculations, processing and other mundane tasks faster and simpler. The computer is also used today by hackers to perpetrate damage. Cell phones, garage door openers, burglar alarms, key fobs, etc. are used to remotely detonate bombs. Advances in science and technology have often proven to be a double-edged sword. While advances in information technology are happening rapidly, keeping pace are the tools and techniques used for corporate espionage. These could be

as simple as walking off with a document lying in a printer or on a desk or advanced techniques such as the use of keyloggers, rogue wireless access points, packet sniffers, bootable operating system CDs/USBs, etc.

Consider some real-life cases –

- An Israeli couple, husband and wife Michael and Ruth Haephrati, developed a Trojan which could infiltrate computers. The initial idea was to spy on Michael's ex-wife but they later started a "software" company that spied on finance and communication companies around the world¹.
- Juju Jiang, a New York resident, installed keyloggers on computer terminals located at Kinko's stores throughout Manhattan to surreptitiously record keystrokes and collect computer usernames and passwords of Kinko's customers⁴.
- A Volterra engineer, Shin-Guo Tsai, stole data sheets containing proprietary product information and sold it to a Taiwan based company called CMSC, Inc⁵.
- Said Farraj, a New York paralegal, tried to sell a confidential Trial Plan to opposing counsel for \$2 million. Farraj obtained unauthorized access to a computer at his firm to get hold of the Trial Plan which exceeded 400 pages and included, among other things, trial strategy, deposition excerpts and summaries, and references to anticipated trial exhibits⁶.
- Daniel J. Baas, from Milford, Ohio, illegally accessed and copied information stored at consumer database giant Acxiom while working for its partner, Cincinnati-based data-mining firm Market Intelligence Group. At the time, Acxiom clients included 14 of the 15 biggest credit card companies, 7 of the top 10 auto manufacturers and 5 of the top 6 retail banks⁷.

Back To The Drawing Board

If you're still wondering if corporate espionage really happens, the answer is a resounding yes. The threat of corporate espionage looms large over organizations today and the advent of information technology makes it a difficult problem to address effectively. While a single solution to the problem is unrealistic, complete eradication is also not possible.

So what really is a feasible way to address corporate espionage? First, go back to the drawing board. Information security is the basic building block of protecting an organization's information assets and implementing it in the correct way is vital.

- **Management Support**

The first, and most important, step to effectively combat corporate espionage is top management's acceptance of its existence. You can only combat something

whose presence you can acknowledge. With this acceptance in place, the steps that follow can be effectively and diligently implemented.

- **Security Culture**

Organizations must imbibe a responsible mentality and attitude towards security and maintain it. If every employee in an organization views security as a personal responsibility, the chances of information leakage are greatly reduced. When the corporate security policy manual becomes more than just a big book gathering dust, espionage and other such security incidents will no longer find space to exist.

- **Policies and Procedures**

A comprehensive set of policies and procedures can go a long way in checking corporate espionage. With care and diligence in developing the right blueprint, implementation falls into place perfectly. Policies provide directions on how to manage, protect and distribute information. Procedures are then designed, based on these policies, to reflect exactly how the policy will be implemented.

- **Penetration Testing**

If you were to view your organization as a house, penetration testing would be akin to hiring a thief and asking him to try and break into your house. This way you learn how vulnerable your house is to theft. While it is a fact that no organization can do business if it poses as a fully locked house, the goal is to only keep the yard open for business while protecting the inside of the house so that a thief doesn't stare at the new chinaware on your dining table with intent. Penetration testing can effectively help achieve this goal and, further, can be instrumental in minimizing the chances of espionage.

- **Wireless Assessments**

The convenience of wireless networks have made them exceedingly popular. However, they bring a host of vulnerabilities that can and will be exploited by the willing. There have been numerous examples where sensitive information has leaked out of an organization through a wireless network hole, including the well-known case at retailer T.J. Maxx⁸. Wireless assessments locate wireless loopholes and enable an organization to proactively fix them before they are exploited. Considering that a "do it yourself" wireless antenna can be made out of a can of Pringles potato chips⁹, wireless assessments should be top priority for organizations wary of the threat of corporate espionage.

- **Social Engineering Assessments**

Social Engineering methods exploit the weakest link in information security: people. Hence, social engineering assessments can give an organization a clear view of exactly what could happen if a corporate spy was to use smooth talk, sympathy drawing, or other such ploys to dupe employees into leaking sensitive information. With advancements in technology, well-known *phishing* attacks have come to the fore and fall into this category as well. These involve bogus websites

that look almost exactly like the original and lure unsuspecting users into divulging personal information. Targeted training programs, based on results of social engineering assessments, educate employees about the threat of social engineering and go a long way in preventing corporate espionage.

- **Security Audits**

Security audits are technical reviews of configurations and installations of operating systems and applications. Default installations of operating systems and applications are seldom secure and can leave a number of security holes for an intruder to exploit. A corporate spy, for instance, could take advantage of lapses in configurations to cause leakage of the information that he/she is looking for. Security audits, done correctly, can play an important role in preventing sensitive information from being compromised.

- **Physical Security Audits**

Too often, physical security is overlooked when securing an organization. In the quest to secure digital information, it is sometimes forgotten that the old-fashioned methods of stealing information still apply. Physical security audits identify shortcomings in security measures applied to those sections of the organization where sensitive information takes a physical form, albeit for a short period of time. These audits often reveal the fact that there is a lot more to physical security beyond video surveillance, document shredding and security guards.

- **Background Checks**

A large number of cases in corporate espionage involve insiders selling information about their parent organization to outsiders. The employees of an organization with required authorization to bypass security measures really do have the keys to the kingdom. Background and reference checks are absolutely essential to ensure that the person being hired is trustworthy. While this is not a panacea, it definitely is the right step forward.

Final Words

Corporate espionage is undoubtedly a growing menace for organizations. An organization at the receiving end could find itself completely losing course on its mission goals. The best, and proven, weapon against corporate espionage is to protect your information assets well. An organization with a responsible attitude towards information security and proactive measures to implement it will find its walls strongly fortified.

Ensure that these walls remain strong at all times and corporate espionage will not disfigure your organization's growth curve. To quote Sun Tzu: *"The ultimate in disposing one's troops is to be without ascertainable shape. Then the most penetrating spies cannot pry in nor can the wise lay plans against you."*

References

1. <http://news.bbc.co.uk/2/hi/technology/5313772.stm>
2. http://money.cnn.com/2008/09/07/news/companies/fannie_freddie/index.htm?pos-tversion=2008090711
3. <http://usliberals.about.com/od/homelandsecurit1/a/IraqNumbers.htm>
4. <http://www.cybercrime.gov/jiangPlea.htm>
5. <http://www.usdoj.gov/criminal/cybercrime/tsaiPlea.htm>
6. <http://www.usdoj.gov/criminal/cybercrime/farrajSentence.htm>
7. http://www.theregister.co.uk/2003/08/11/man_charged_in_axiom_cracking/
8. <http://www.informationweek.com/news/mobility/showArticle.jhtml?articleID=199500385>
9. <http://en.wikipedia.org/wiki/Cantenna>