

Risk of Insider Threats in Information Technology Outsourcing: *Can deceptive techniques be applied?*

P. Gaonjur[†], C. Bokhoree[†]

[†] School of Business Informatics and Software Engineering (SOBISE)
University of Technology, Mauritius
La Tour Koeing, Pointes aux Sables, MAURITIUS
Tel : (+230) 234-7624 Fax : (+230) 234-1747
Email : pgaonjur@utm.intnet.mu, c.bokhoree@utm.intnet.mu

Abstract

The risks involved in Information Technology Outsourcing has since long been known to affect business decisions of whether to outsource or not. This has lead to numerous research on topics such as: Understanding and Managing Outsourcing Risks, Methodologies to measure Outsourcing Risks, Risk Factors in Information Technology Outsourcing, Assessing the Risk of IT Outsourcing to name a few. But very little research has been conducted on the security aspect of Information Technology Outsourcing. This paper tries to bring the light on security risks in IT Outsourcing, more specifically risk of insider threats. It also tries to bring attention on the fact that security risks can be a lot more damaging and harmful than any other non security threats combined together. After giving a description of different type of security risks, the paper then elaborates on different deceptive and non-deceptive techniques that might be used to mitigate security threats in IT Outsourcing. Finally it is shown that if insider threats are not taken seriously, its consequences can be very damaging. Two recent cases of insider threats in IT Outsourcing have been stated to prove the latter.

Keywords

Information Technology Outsourcing, Risk, IT Security, IDS, Honeypots

1. Introduction

Information Technology Outsourcing (ITO) is defined as a “significant contribution by external vendors in the physical and/or human resources associated with the entire or specific components of the IT infrastructure in the user organization” [1].

ITO has become a widespread organizational practice and has been growing steadily during the past decade. It has been predicted that ITO will reach an estimated \$23 billion by 2007 [2]. Nowadays companies prefer to outsource their IT needs to external suppliers in the expectation to reduce cost and focus more on their core activities. While ITO may bring cost-saving benefits, better quality of service and increased efficiency [3], it is also to be noted that ITO is not without risk.

During the past decades, a lot of research has been done to study the risks involved in ITO [4,5,6,7,8]. Table 1 lists the factors associated with ITO risks, as suggested by transaction costs theory [4,5,6].

SOURCE OF RISK	RISK FACTORS
Transaction	<ul style="list-style-type: none"> • Asset Specificity • Small Number of Suppliers • Uncertainty • Relatedness • Measurement Problems
Client	<ul style="list-style-type: none"> • Expertise with IT operation • Expertise with Outsourcing
Supplier	<ul style="list-style-type: none"> • Expertise with IT operation • Expertise with Outsourcing

Table 1: Risk Factors in Outsourcing IT Operations

However, little research has been done so far on the security risk factors associated with ITO. The main purpose of this study is to point out that insider threats in ITO cannot be taken for granted. A survey conducted jointly by the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI) reported that the average insider attack can cost a company up to \$2.7 million [9].

2. General Security Issues in Information Systems

In this Information age, as we have become increasingly dependent upon complex information systems, there has been a focus on the vulnerability of these systems to computer crimes and security attacks. Because of the high-tech nature of these systems and the technological expertise required to develop and maintain them, it is not surprising that overwhelming attention has been devoted by experts to technological vulnerabilities and solutions. The following are the most recurrent vulnerabilities to Information Systems:

a. Viruses/Worms

A big problem faced by all computer users is viruses. With the advent of the Internet, there has been an increased significance of the problem since the dissemination of software along with the viruses has never been easier. The patterns in the spread of viruses have also changed. For e.g. there are viruses that are creating havoc in some regions of the world but at the same time are virtually unknown in the rest of the world. This locality property will no longer be true as Internet becomes widely available around the world.

A worm, on the other hand, is far more powerful. After gaining access to a computer (usually by breaking into it over the internet) a worm scans for other internet locations and exploits those computers having known vulnerabilities. A worm is also autonomous i.e. at no time it needs user assistance for its operations. Moreover, since worms reside on the internet, all machines are at risk of attack. These computers only defense is to apply patches for known vulnerabilities to their operating systems. Secondly, worms have the capabilities to replicate without any assistance as opposed to viruses. An online worm infected computer can be the cause of thousands of infections by itself. This is due to the fact that worms scan for vulnerable computers in the neighborhood or random IP addresses thus causing a chain reaction difficult to stop.

The consequences of viruses and worms on the internet community has been a turning point allowing different solutions to creep up from Firewalls, Anti-viruses, spyware killers, Intrusion Detection Systems and lately Honeypots. These solutions have temporarily reduced the consequence of viruses and worms on the internet community but new generation worms known as hybrids still goes undetected. The latest solution is to have inbuilt security measures in the kernel of the operating system itself. Microsoft has started this with its Widows Vista edition having inbuilt firewall, spyware killers and spam filtering security measures. Now it's up for end-users to learn how to use these technologies to secure not only themselves but the whole internet community.

b. Hackers

Depending on whom you ask, hackers are harmless pranksters, curious techies, noble freedom fighters or dangerously unpredictable cyberterrorists. As the world goes online, hackers' potential influence and menace grows.

With the global boom in the Internet and ever-cheaper personal computers, hacking is spreading like online kudzu. Hacking is getting more sophisticated and in many cases, a lot nastier. And it is chipping away at the ability of the government, the military and the business community to protect proprietary information and preserve individual privacy.

Many hackers are harmless -- just intensely curious how software or computer networks work. Some hackers seem threatening but are little more than pranksters spreading online graffiti on Web sites. But a growing number are hacking for personal profit, political cause or simply to inflict damage to information systems. Many hackers, trying to distance themselves, call these online abusers "crackers."

So far, individuals using their home PCs are rarely the target of hackers. But that is not the case with businesses and their employees. A study released in June 1998 by the Computer Security Institute and the FBI's International Crime Squad found that nearly two-thirds of more than 500 organizations reported a computer security breach within the past 12 months, up from 48 percent a year ago and 22 percent the year before that [9].

On a broader scale, the federal government is starting to take the threat of online chaos to heart. "Cyberterrorism," "information warfare" and "economic espionage" -- terms that did not exist until recently -- are cropping up often in national security debates.

"If we aren't vigilant, cybercrime will turn the Internet into the Wild West of the 21st century," said U.S. Attorney General Janet Reno.

c. Insider Threats (Most harmful)

While attacks on computers by outsiders (crackers) are more publicized [10,11], attacks perpetrated by insiders are very common and often more damaging. As mentioned above, a survey conducted in 1998 reported that the average cost of an outsider penetration at \$56,000, while the average insider attack cost a company \$2.7 million [12].

Even with the strongest technology safeguard in place, information systems still suffer a lot of damage. The main reason for this is that the security measures such as antivirus softwares, firewalls and Intrusion Detection Systems (IDS) cater only for external threats and none can be used to catch the most dangerous threat, the trusted insider. Little research has been done to counteract the advance insider, the trusted individual who knows your networks and internal organization. Often, these individuals are not after computers, but specific information. This is a risk that has proven far more dangerous, and far more difficult to mitigate [13,14,15,16].

Risk management of the insider threat problems involve a complex combination of behavioural, technical, and organizational issues. Organizations can concentrate on physical and technical security measures such as authentication mechanisms, firewalls, and intrusion detection systems to defend against external cyber threats. However, insiders may be authorized to bypass all of those measures in order to perform their daily duties. Former employees are familiar with internal policies and procedures, which can also be exploited to facilitate attacks. Although insider threats as defined above utilize technology to carry out their attack, a combination of technical, behavioural, and organizational issues must be considered in order to detect and prevent insider threats.

Because insiders are legitimate users of their organization's networks and systems, sophisticated technical capability is not necessarily required to carry out an insider attack. On the other hand, technically capable insiders are able and have carried out more sophisticated attacks that can have more immediate widespread impact on organizations [17]. These technical insiders also sometimes have the capability to "cover their tracks" so that identification of the perpetrator is more difficult.

3. Risks of Insider Threats in Information Technology Outsourcing

Risk is inherent to almost any business decision. ITO can be classified as an example of a risky business endeavor. While ITO can lead to lower costs, economies of scale and access to specialized resources, outsourcing can have unwanted outcomes such as escalating costs, diminishing service levels and loss of expertise, to name a few [18].

Table 1 gives a list of risks associated with ITO that have been studied a lot in the past. If these risks are not managed properly, at worst the company will face losses amounting to the cost of the outsourced project but if the risks of insider threats in ITO is neglected, the damage done can cost the company not only in terms of money but the reputation of the company itself might be tarnished. This is due to the fact that most insiders are after the clients' proprietary and confidential information assets or intellectual property of the company, which might be much more costly than losses in terms of money.

The following incident taken from "Averting Security Missteps in Outsourcing" [17] shows the extent of damage that can be done by insiders.

An outsourcing nightmare

On 30 January 2003, Katherine Bardswick, president and CEO of the Co-operators Group, a Canadian insurance company, apologized for a breach of her company's highly valued data security even though her company was not at fault [19]. The media extensively covered the apology because of the number of people involved and the extent to which they might have been affected [20]. The security breach and apology resulted from a security incident involving the loss of personal data at an outsourcing service provider.

On 23 January 2003, Information Systems Management (ISM), a subsidiary of IBM Canada and a large Canadian provider of outsourced information system services, notified Co-operators Life Insurance - one of the Co-operators' companies - that a computer hard drive containing sensitive client information was missing from a secure area at ISM's premises in Regina, Saskatchewan. The disk contained data on more than 1 million people. In addition to Co-operators' customer data (life insurance and pension fund information, as well as social security and health card numbers), it held account information for more than 43,000 businesses in Manitoba and telephone and electrical consumers in Saskatchewan. Co-operators feared the worst would follow: massive identity theft and misuse of accounts and credit.

In response, it performed exemplary damage control to protect its customers and, consequently, protected itself. The company identified affected clients, mailed a letter to each that explained the facts (to avoid misinformation), established a toll-free call center to handle inquiries, and posted updates on its Web site. Co-operators also worked with credit reporting agencies to assist clients placing potential fraud alerts in their credit files. One such agency even set up dedicated telephone lines to serve affected Cooperators clients. This outsourcing nightmare had a happy ending because no one accessed the data—the Regina city police arrested a suspect and recovered the stolen hard drive. It turned out that the suspect was more interested in the hardware than the data it contained.

The above cases are proof of the risks that ITO is facing in terms of insider threats. The threats are real and serious and something must be done to cater for it. People are said to be the weakest link in IT security but insiders are the worst.

This paper therefore proposes possible solutions that might be implemented to counter the risk of Insider Threats in ITO. The following section analyses the possibility to use deceptive techniques against insider threats.

4. Mitigating Insider Threat risks using the following Deceptive/Non-Deceptive Techniques:

a. Intrusion Detection System (IDS) – Non Deceptive

Intrusion detection has been an active field of research for about two decades, starting in the early 1980's with the publication of John Anderson's *Computer Security Threat Monitoring and Surveillance* [21]. This report consisted in improving computer security auditing and surveillance capability of computer systems. Dorothy Denning's seminal paper, "An Intrusion Detection Model," published in 1987, provided a methodological framework that inspired many researchers and laid the groundwork for many commercial products [11]. This paper describes a model for a real-time intrusion-detection expert system that aims to detect a wide range of security violations ranging from attempted break-ins by outsiders to system penetrations and abuses by insiders

Intrusion detection is the process of monitoring computers or networks for unauthorized entrance or activity. IDS can also be used to monitor network traffic, thereby detecting if a system is being targeted by a network attack. There are two basic types of intrusion detection: host-based (HIDS) and network-based (NIDS). Each has a distinct approach to monitoring and securing data, and each has distinct advantages and disadvantages.

Host-based intrusion detection systems analyze data captured on a single information system. They might monitor users or software processes, for example. The data captured can be user data, such as keystrokes, login/logout times, operational profiles, or programs run during a session. Alternatively, the data can be program behavior data such as system calls or internal program states of monitored programs.

Network-based IDSs monitor networks of computers and other devices (i.e., routers and gateways) that are normally subject to attacks. Subsequently, rather than monitoring user activities or software processes just like

HIDS, network-based IDSs primarily use data from network traffic in detecting intrusions. The most popular program used to capture network traffic is tcpdump, which can display or store every field belonging to a TCP packet [22]. Different implementations of network-based IDSs may serve different functions. For instance, some network-based systems may monitor only the traffic activity of a single host, while distributed tools may analyze the aggregate traffic information from a range of devices on the same network.

Intrusion detection techniques are generally classified into two categories: anomaly detection and penetration identification (often referred to as misuse detection)

Misuse detection systems try to identify behavior patterns characteristic of intrusions, but this can be difficult if an attack does not follow one of the patterns already known beforehand to characterize an attack. On the other hand, anomaly detectors try to characterize the normal behavior of a system, so that any deviation from that behavior can be labeled as a possible intrusion. After a “signature” is defined that identifies a manifestation of an attack, the attack can be discovered in either monitored network traffic or host-based audit trails. Penetration identification systems typically yield fewer false alarms; however, they require continuous updates, as their signature databases may become outdated fairly quickly [23].

Anomaly detection assumes that misuses or intrusions are correlated to abnormal behavior exhibited by either a user or the system. Anomaly detection approaches must first determine the normal behavior of the object being monitored, and then use deviations from this baseline to detect possible intrusions. Anomaly detection method attempts to differentiate “anomalous” activity from the established normal operating behavior of a computer system, application, or user. Thus, in general, the IDS must first train on data representing normal behavior before it can be deployed in an operative detection mode. The principle advantage of an anomaly detection system is that it can detect previously unknown attacks [24].

Inside attacks are difficult to detect without an IDS. Therefore, connections between the servers and other internal computers must be supervised. If an IDS could provide finer control over internal traffic, it would greatly reduce overall security risk. In this line, IDS was introduced as a complement for firewalls, because Local Area Networks (LANs) are vulnerable to inside attack, once an attacker penetrates the firewall and compromises a single computer, the entire LAN is at risk.

An IDS, therefore, being part of an internal network can be used to track insider threats based on a set of predefined acceptable behaviours of the internal users.

For e.g. users working with confidential data on an outsourced project will not be expected to copy confidential information on an external device for personal use.

An IDS can easily capture the above mentioned anomaly and warn the system administrator before much damage is done.

b. Honeypots - Deceptive

As mentioned earlier, many organizations today use firewalls and IDS as part of their network security defenses. Apart from these two technologies, a honeypot has received much attention in recent years. A honeypot can be thought of as a decoy computer system that uses deception to lure intruders so that we can learn their behaviors. The honeypot is usually a system that is deliberately made vulnerable with fake services to make it look and act like a real system. Intruders who discover the honeypot may choose to compromise it since it is a relatively easy task. As a result, system administrators can investigate the traces left by intruders to learn about their tools and techniques in detail.

Honeypots are a highly flexible tool that comes in many forms and contribute to the overall security of a given network. Figure 1 shows a simple honeypot configuration. They can be used for anything from detecting new attack methods to capturing the latest techniques and tools of attackers. This flexibility, while giving the honeypots their true power, leads to a big confusion and misunderstanding about what honeypots really are.

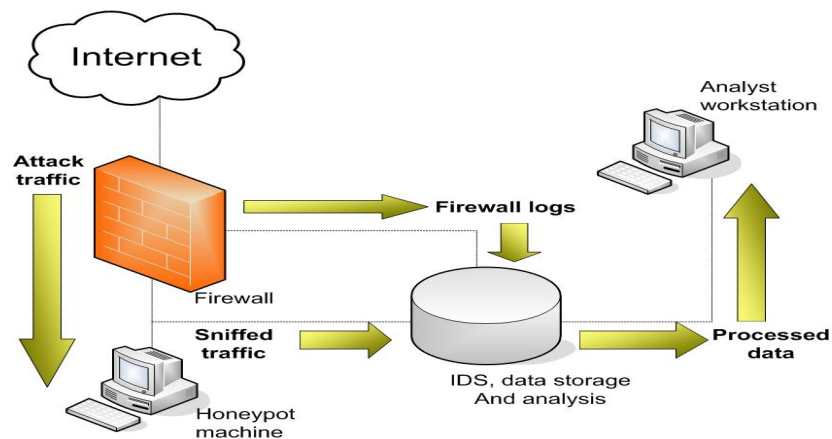


Figure 1: A simple honeypot configuration.

Lance Spitzner defines the term Honeypot as follows:

“A Honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource” [14].

Conceptually, all the honeypots work the same. No connection should be expected since they are not supposed to provide any valuable service. That means that any interaction with the Honeypot is most likely unauthorized or anomalous activity.

Many people are not aware of the security risks their computer system faces. Further, they jeopardize their personal or company data. In fact, many people do not even notice that their system has been compromised. An attacker has an interest in concealing his or her activities to be able to keep access to a compromised system. Today’s operating systems are insecure when they come freshly out-of-the-box and need to be patched. This is mainly due to the pace that security vulnerabilities are discovered. If an unprotected system is connected to the Internet simply to download the needed security fixes, it might get comprised in that short period of time—possibly unnoticed by the user of the system.

Honeypots are important tools in protecting computer systems, and they must be deliberately deceptive to be effective.

Honeypots can therefore be used to catch insider threats that will go unnoticed by the IDS. In the event that we have users with appropriate access rights to a resource but using it illicitly, the IDS will fail to detect this anomaly.

For e.g. an employee trying to access confidential information about clients after office hours will be directed to a honeypot and his activities will be logged for forensics. The insider won’t even be aware that his activities are being logged by a honeypot and that he is not actually copying the real confidential information of clients but bogus information (Honeytokens) found on the honeypot. Thus legal action can be taken against the insider along with proof.

c. Honeynets - Deceptive

A Honeynet is an actual network of computers left in their default (and insecure) configuration. This network sits behind a firewall where all inbound and outbound data is contained, captured and controlled. This captured information is then analyzed to learn the tools, tactics, and motives of the hacker community.

The concept of the honeynet first began in 1999 when Mr. Lance Spitzner, founder of the Honeynet Project published the paper “To Build a Honeypot”. In this paper, Mr. Spitzner proposed that instead of developing technology that emulated systems to be attacked, why not deploy real systems behind firewalls waiting to be hacked.

In the most basic sense, a honeynet is a type of honeypot, more specifically, a type of high interaction honeypot. And thus being a high interaction honeypot, nothing is emulated; all services, applications and operating systems are as real as in any production environment. An important characteristic that

separates a high interaction honeypot from a honeynet is that a honeynet contains one or more honeypots. It is a network of multiple systems creating an illusion of a production network. It is through this network, specifically through the network access device, is where hacker activity is monitored, recorded and controlled. Based on all of this, we can construct the basic definition of a honeynet:

A honeynet is a network of high interaction honeypots that simulates a production network and configured such that all activity is monitored, recorded and in a degree, discretely regulated.[13]

A honeynet, just like honeypots, works by creating a highly controlled environment. Honeynets as opposed to honeypots though takes the concept one step further. Instead of just one computer or a number of unconnected computers, a network is set up in such a way that everything in the honeynet appears like a normal network. All applications and services are real though all systems running within the honeynet are considered honeypots. No modifications are done to the system such as placing monitoring tools or creating jailed environments like chroot within the host. This kind of setup makes the honeynet the most interactive and authentic of all honeypots.

In a large LAN or Metropolitan Area Network (MAN), a single honeypot might not be enough to cater for all possible type of attacks, hence Honeynets can be used to identify and capture insiders that are after clients' confidential information in these types of networks.

5. Conclusion

This research paper serves as a reference and purposely highlights the definitions of IDS, Honeypots and Honeynets with the intention enabling the reader to make a choice in securing their networks with these technologies. Many organizations allude to the fact that it may not be necessary to know what your trusted insiders are doing. But if this reasoning is followed, the consequences might be damaging. Hence it is of paramount importance to know the different types of IDS, honeynets and honeypots and to understand the best method to deploy them customized to the respective organizations needs. A properly secured network with appropriate IDS, honeypots and honeynets configuration will help ensure the security and integrity of clients' confidential information. This will in turn reduce the risk associated with ITO and allow companies make decisions whether to outsource or not based on an appropriate risk analysis, with more emphasis on internal security aspects.

REFERENCES

- [1] L. Loh and N. Venkatraman, "Determinants of Information Technology Outsourcing: A cross-sectional Analysis", *Journal of Management Information Systems* 9(1), 1992
- [2] Wonsock Oh, "Why do some firms outsource IT more aggressively than others? The effects of organizational characteristics on IT Outsourcing decisions", *Proceedings of the 38th Hawaii Conference on system sciences*, 2005
- [3] W. McFarlan and L. Nolan, "How to Manage an IT Outsourcing Alliance", *Sloan Management Review*, 1995
- [4] B. A. Aubert, M. Patry, S. Rivard, "Assessing IT Outsourcing Risk", *Proceedings of the 31st Hawaii International Conference on System Sciences*, Jan 1998
- [5] B. A. Aubert, M. Patry, S. Rivard and S. Dussault, "Managing the Risks of IT Outsourcing Risk", *Proceedings of the 32nd Hawaii International Conference on System Sciences HICSS*, Jan 1999
- [6] B. A. Aubert, M. Patry, S. Rivard and H. Smith, H, "IT Outsourcing Risk Management at British Petroleum", *Proceedings of the 34th Hawaii International Conference on System Sciences HICSS*, Jan 5-8, 2001
- [7] M. J Earl, "The Risks of Outsourcing IT", *Sloan Management Review*, 37, 3, Spring 1996
- [8] L. Willcocks, M. Lacity, T. Kern, "Risk mitigation in IT outsourcing strategy revisited: Longitudinal case research at LISA", *Journal of Strategic Information Systems*, 8, 1999
- [9] R. Power, 2002 CSI/FBI computer crime and security survey. *Computer Security Issues & Trends* 8, 1 (2002)
- [10] B. Mukherjee, L.T. Heberlein, and K.N. Levitt, "Network Intrusion detection", *IEEE Network*, Vol.8, No. 3, 1994.
- [11] D.E. Denning. "An Intrusion Detection Model", *IEEE Transactions on Software Engineering*, 13(2), 1987
- [12] R. Power, 1998 CSI/FBI computer crime and security survey. *Computer Security Issues*.
- [13] L. Spitzner, "The Honeynet Project: Trapping the Hackers," *IEEE Security & Privacy*, March/April 2004
- [14] L. Spitzner, "Honeypots: Catching the Insider Threat" *Proceedings of the 19th Annual Computer Security Applications Conference*, IEEE Computer Society, 2003
- [15] C. E. Irvine, "Cybersecurity Considerations for Information Systems", *Handbook of Public Information Systems*, 2nd. Edition, ed. D. Garson, CRC Press, 2004
- [16] C. Eagle, J. L. Clark, "Capture-the-Flag: Learning Computer Security Under Fire", *Proceedings from the Sixth Workshop on Education in Computer Security*, Monterey, CA, 12-14, July 2004
- [17] Michael Lesk, "Averting Security Missteps in Outsourcing", *IEEE Security and Privacy*, 2005
- [18] A. Benoit Aubert, Sylvie Dussault, Michel Patry, Suzanne Rivard. *Managing the Risk of IT Outsourcing*. *Proceeding of the 32nd Hawaii International Conference on System Sciences*, 1999
- [19] CBC Online News, "Co-operators Life CEO Apologizes for Theft of Sensitive Customer Data," 30 Jan. 2003; www.cbc.ca/stories/2003/01/30/cooperators030130
- [20] A. Mullholland, "Computer File with Vital ID Data Goes Missing," *CTV.ca*, 31 Jan. 2003; www.ctv.ca/servlet/ArticleNews/story/CTVNews/1043943775310_127
- [21] Anderson. "Computer security threat monitoring and surveillance" Technical report, James P. Anderson Co., Fort Washington, PA, April 1980
- [22] V. Jacobson, C. Leres and S. McCanne, "Tcpcdump", Available via anonymous FTP from [ftp.ee.lbl.gov](ftp://ftp.ee.lbl.gov). 1989
- [23] John McHugh, Alan Christie, and Julia Allen, "Defending Yourself: The Role of Intrusion Detection Systems", *IEEE Software*, 2000
- [24] R. A. Kemmerer and G. Vigna, "Intrusion detection: a brief history and overview", *IEEE Security & Privacy*, URL <http://computer.org/computer/sp/articles/kem/>, 2002