National Security and threat awareness

F. Ghioni
Telecom Italia Group, Italy

Abstract

Today's ubiquitous technology environment has brought about a change in the threats posed to National Security. As we continue to move from a hierarchical, industrial-based society to a networked, information-based and technology-dependent society, our political, economic, social and technical bases continue to evolve. This has led to a change in both the vulnerabilities of Nations and their infrastructures and in the threats that they may suffer. The emergence of a new crime context has, obviously, opened the way to a new kind of criminal activity: info-terrorism. The most effective tactic that info-terrorists have is to focus the use of Weapons of Mass Destruction not on physical destruction but on area denial or economic damage. Information denial, distortion or theft can be much more destructive than waging a traditional mechanical war. Unfortunately, the proliferation of the Internet and other means of data retrieval, as well as the pervasiveness of information technology have not only facilitated the work of Intelligence experts in both the corporate and the State environments but have also aided the epidemic of cyber-crime.

Such a complex scenario has switched the focus from Information Security to Information Process Security (IPS).

In order to guarantee the integrity of IPS, it is paramount that employee threat awareness is promoted at all levels. This new challenge offers the opportunity to re-think Security Awareness Programs through the management, measurement and the benchmarking of the processes and techniques.

The globalization of information retrieval and transfer bring about the need to create a solid front against these threats. This front should be made up of a network of Government and private sector agencies and should be oriented towards the research, development and implementation of measures that will counter the hazard of Information warfare.

Keywords: intelligence, information process security, threat awareness, national security, critical infrastructure.

1 Introduction

Niccolò Machiavelli said "it is important to reign in accordance to the change in times". Over the last decade there has been a revolutionary change in technology. We live in a ubiquitous technology environment. This has brought about a change in the type of war that countries wage against each other and the types of threats posed to Nations. We are in an era where war is asymmetric, peace is asymmetric and the most deadly weapon is Information manipulation or denial (Information Warfare). Therefore, Defense has to be as polymorphic as the attackers.

On a business level, information systems have become so pervasive within companies, that we often forget that they are there and just how complex the network linking all the various systems has become. This complexity can lead to security flaws in the system. If even a small portion of the network is overlooked or forgotten by security experts, it can mean a feast day for any perpetrator that intends to unlawfully access the mentioned network. For this reason it is essential that any security system put in place is multi-layered and contemplates any and every process that is encompassed in the company's information system network.

2 Information warfare

As Sir Francis Bacon said "Knowledge is power — *Nam et ipsa scientia potestas est*". Knowledge is the elaboration of information using logical inference. Knowledge can thus be defined as processed information.

A great amount of information in National Agencies and companies is stored and exchanged electronically. Today any medium used for information transmission or any location in which it is discussed is vulnerable to infiltration. This new form of information exchange has given life to two new types of perpetrators, cyber criminals and info-terrorists.

Cyber criminals are individuals that attempt to gain unauthorized access to computer systems (government or corporate) their intentions are usually ego-oriented (prove to their peers how good they are) or simply malicious like normal criminals. Info terrorists are those individuals that use electronic means to implement their terrorist intents such as stealing or distorting information via illegal or unethical means (their motivations, like with the classic terrorists, are usually political). The spread of information and networking technology to virtually all corners of the globe is spawning new opportunities for criminals and info-terrorists to wreak havoc through the Internet. The perpetrators can steal or manipulate information from outside an office, they can create new electronic files, erase or corrupt the existing ones, or block access to information to the authorized users without leaving a trace of entry behind them. The victim may not even notice that their system has been violated. In this paper we will not discuss the risks of WiFi networks but this is another path through which the criminals can gain illegal access to information.

The evolution in technology is making the leakage of information through corporate spying and theft of intellectual capital both easier and cheaper. The primary medium through which information passes has changed from paper to computers. Today's competitive environment requires businesses to compete on a global basis, sharing sensitive information with international partners while protecting information from competitors. The spread in computing and the need to share information have exponentially increased the probability of information falling into the wrong hands since more people are handling the information than ever before. The basic technology behind operating systems was never intended to be secure. When this technology is combined with the Internet, which was developed with the intent to provide open information, an ideal environment for stealing secrets is created [1].

According to a recent survey in the next ten years there will be at least one devastating attack on networked information infrastructure or on the US's power grid [2]. An analysis of the malicious software (viruses, worms, etc.) that circulate on the networks at present is a clear indication of the capacity and motivation of hackers and cyber-criminals to disrupt Nation and corporate infrastructures. An interruption or theft of information can be devastating for a Nation just as much as for a company. The terrorists' strategic objective is to attack the minds of the decision makers and not focus on physical destruction but rather on area denial or economic damage.

Companies and national agencies post more and more information on the Web. Internet has thus become an excellent instrument for competitive intelligence research purposes and all that is needed is a quality search engine. The proliferation of corporate Web sites can backfire on a company or agency. If their information security policies are not watertight, their site can become an entry highway to their corporate network to any malicious intruder that has a certain level of intrusion know how and that can easily use the Web portal to enter the network.

3 Threat awareness and the need for information process security

3.1 The private sector

The progressive expansion in the use of personal computers and the subsequent increase in use of the Internet both in the domestic and business spheres, have brought about a dramatic increase in the number of potential cyber crime scenes. The targets being the computers themselves as well as the networks that may connect any number of them and the data stored on these machines. As long as the computers are not connected to the exterior (even if they are networked), the threat of an intrusion remains relatively low, as it will necessarily have to be a physical intrusion, thus significantly increasing the probability of being traced. Portable computer theft is another matter, that will be discussed shortly.

When computers are connected to the outer world, the threat becomes real. Without adequate protection, it is child's play for a hacker to access a domestic computer without being perceived. The same goes for an unprotected business

network. Unfortunately, the average user is unaware of the risks that he faces. Consider the average housewife or pensioner. Until a couple of years ago they probably had rarely (if ever) used a computer. Today the housewife can chat with her friends, find a new recipe for the family dinner or order the shopping online and save time. The pensioner can also order his shopping and have it delivered and avoid carrying heavy bags, play chess online and even chat with relatives that may live far away. All this at the click of a mouse and on a flat rate Internet subscription. What do these people know about viruses, worms and hackers? Probably very little. It is also true that they probably have very little or no interesting material stored on their hard drive, but this would not stop viruses or worms from proliferating on the machines and the latter from being used as a proxy machine to send out malicious software. On the other hand, if they order their groceries online, they will have to give their credit card details and these would be of great interest to any perpetrator.

Now take the case of a small business with a computer network. Let us say that they have a simple firewall that was brought off the shelf and at installation the factory settings were left unchanged. The HR department stores all the personnel records on both the individual hard drives and the main server. Accounting stores the books on the same server and all the other Business Units do the same. E-mails are the standard form of communication and faxes that come in with client orders are stored electronically. The post server is a partition of the main server. Every computer in the company has access to the Internet and several managers have portable computers. If, as we said, the only form of information security is the off-the-shelf firewall, then this company is just as susceptible to information theft as the housewife or the pensioner. The difference is that, in this case, there will be interesting information on the server and if stolen, it can fall into the hands of an unscrupulous competitor and cause the company to lose clients or money.

3.1.1 Information process security

The company may be a little more aware of the surrounding threats and go about installing a more robust information security system. Businesses must realize the threats that they face. There are malicious hackers that have broken into government networks that tend to have a higher security protection; these hackers would have no problem in breaking into a corporate network if this is not sufficiently protected. If the company's information security system is more complex than what is described above, there is some hope that its data is not stolen.

In order to have a well-designed information security system, today it is necessary to consider Information Process Security (IPS).

In IPS, each component of the information process must be analyzed and the criticality of each part evaluated and classified. On the basis of these parameters a security system put in place. For instance, it may be necessary to store the Human Resources data on a separate server from the other company data. Any sensitive data should be stored in encrypted form on a server. The data flow of such data should also be protected. Every incoming/outgoing flow of sensitive information (i.e. e-mails or faxes) should be protected by some form of

encryption key, the higher the data sensitivity the more complex the key. The level of document protection should be determined by a data classification model. Employee document access rights should be classified within the same model. Employee system and data access should also be determined in the same way.

An example of data classification and IPS implementation
Human Resources data can be of various levels of sensitivity. HR employees will have access to generic data and according to their level and function they will have access to more or less reserved data. HR managers will have access to more confidential data, always on the basis of the role they cover. Employees within the company will not have access to the HR records unless there is a specific business reason. Most HR data should not leave the premises.
This kind of security can be achieved by "flagging" all sensitive data according to its discretionary level. This system allows that if the Head of HR sends an e-mail to HR manager A, he may follow the document through its entire path until reception and if, inadvertently or not, manager A forwards the document to manager B (who does not have access rights for the file) an alarm is immediately sent to the document originator, informing him that there has been an attempt to violate security. The same will occur if an attempt is made to send the file outside the company. The security system will also prevent the recipient from receiving the file for which he does not have rights.
Manager A may have sent the file in good faith but it is also known that one of the major causes of information leakage is employees, both involuntarily and intentionally.

Returning to the information security system. Internet connections are one of the major access points to the company. A strict enforcement of major security policies in this part of the network is just as important as the above mentioned. The Internet implies a two way data flow. Outbound towards the Web (the user types the URL of the required site and hits Enter); inbound, the requested page. If the page is clean, there is no risk for the user. If there is a valid security system any "bad" pages will be blocked on entry. The main risk is an apparently clean page that can contain a hidden a Trojan (for instance in a dynamic plug-in such as ActiveX). Ideally the security system should be able to scan the threat before allowing the page to open on the computer. If the Trojan manages to override the first barrier, it must manage to stop it once it has been activated. In a worst-case scenario, the Trojan may lie dormant for some time until it is instructed to open a backdoor for the perpetrators.

Probably the best available preventive solution for such malicious acts is a parametric interception system that is able to intercept the attacks in real time, set off alarms in a "control room" and activate defense measures that will block the attack and avoid information loss.

3.1.2 Threat awareness

It is inevitable that if domestic computer users as well as corporate employees are not made aware of the threats that they undergo, they will not be willing to

implement the necessary protective measures. It is also important that the threats be explained in clear terms, so that the real risk may be understood by even the least IT oriented. The use of media, such as newspapers and news programs, to warn people that there are new threats and to explain what has to be done, is probably one of the most effective threat awareness solutions. One security measure that has to be repeated *ad nauseam* to users and then enforced by the latter, is the use of passwords and screen locking.

3.2 The public sector

If we consider some differences, such as the size of the networks involved and the level of secrecy of certain information. All the above-mentioned principles of security should be applied to the Public sector of a Nation. Each national agency can be considered as a company for security process analysis, and then on a greater scale, each Agency can be considered as a node of the national critical infrastructure network. The national critical infrastructure is the network of national agencies, Government and private companies from vital sectors such as telecommunications, health, etc.

When analyzing and implementing information security in the public sector, it must not be forgotten that in addition to all the threats mentioned above, including hackers that want to prove their worth by defacing Internet sites, often for political reasons, they have to contend with political enemies and terrorist organizations such as Al Qaeda or ETA. These "enemies" have the necessary money to invest in intrusion tools that could bring a single or multiple agencies to a complete standstill with a DDoS (Dedicated Denial of Service) or decrypt sophisticated encryption keys used to protect data that could be vital to a country and fateful for the same country if it falls into enemy hands.

Most technology is available to anybody who wants it or has the money to buy it. This is the case also because a great part of the most sophisticated technology available is developed by private companies. National agencies have the means and the manpower to develop the same technology and could probably go beyond but, unfortunately, they are tied down by bureaucracy, which has the bad habit of slowing down anything that has comes its way. An example of this is the recent case of the FBI. In 2001 the Federal Bureau of Intelligence invested $170 million in a computer program designed to allow agents to share information instantly and fix a main problem identified after the Sept. 11 attacks. Alas, the *Virtual File Case* is now ready but it is obsolete and a new system will have to be designed to reflect the present needs of the FBI [3].

This example underlines the need for a tight collaboration between private sector technology companies and the national Critical Infrastructure "components". The above mentioned obsolete intelligence system is such because more performant and efficient systems have been developed in the private sector and have outclassed it. Another case, always related to the FBI, is the Carnivore software package. Carnivore was developed to intercept the e-mail and other online activities of suspected criminals. The software has never been used because agents preferred using more efficient and advanced commercial

solutions to conduct court-ordered Internet surveillance in criminal investigations [4].

In a recent interview, Richard Clarke, former White House adviser on national security and cyber threats, stated, "the world's most advanced military powers are using the Internet to spy on their enemies and prepare digital attacks against rogue targets". This issue proves two things, firstly that the Internet has become so efficient that it is now useful in state espionage; secondly, there is an insufficient protection of classified information if it is so readily available for spies to steal and decrypt it.

3.2.1 Threat awareness

As with private sector employees, public sector and national critical infrastructure component employees need to be aware of the danger they put their country in if they do not protect the information they are in possession of. They must realize that the basic rules such as not talking about classified information in public places or over unprotected telephone lines are not put in place for the sake of complicating their lives but effectively to protect the country from information theft. It is quite common to read on the newspaper that an intelligence civil servant or agent lost or forgot a portable pc with vital information on a train or a taxi.

4 Conclusions

Employees are often given a security induction training on entering a company. Initially the majority abide by the rules and restrictions. As time goes by, routine sets in and these lessons are forgotten or put aside as being cumbersome. This leads to errors in data classification, information leakage, flaws in a network system and other mistakes that can make a company or national agency vulnerable to competitor or enemy attack.

It is therefore paramount that information security is repeated regularly. This allows for employees to be made aware of the changes in the security threats that they face and in the measures that they need to put in place.

References

[1] Nakra, P., Info-Terrorism in the Age of the Internet: Challenges and Initiatives, Journal of Competitive Intelligence and Management, v. 1 n. 2, pp. 1-10, Summer 2003.

[2] PEW, Internet & American Life Project, The Future of the Internet, January 2005.

[3] Reuters, Nations Use Net to Spy, Plot Attacks Ex-Bush Aide, Nov 5, 2004.

[4] Reuters, FBI Retires Controversial E-Mail Surveillance Tool, Jan 18, 2004.