# Insider Threats

## Risk to Organization

Atul Rana, Upasana Nigam,
Dr. Deepak Jain

International Research Journal
ISSN 1839-6518
Vol. 2, No. 1, 2012
82800201201204

# Insider Threats: Risk to Organization

Atul Rana, Upasana Nigam,
Dr. Deepak Jain

International Research Journal
ISSN 1839-6518
Vol. 2, No. 1, 2012
82800201201204

# Insider Threats: Risk to Organization

## *ABSTRACT*

*Information security is an essential component and assets for any organization, whether it is commercial government or proprietary business. Report after report keeps pointing to the "insider threat" as one of the greatest information security risks within the modern organization. But what exactly is the insider threat and how we can help reduce this risk? This paper analyzes the importance of information security, benefits of it and how the information can be protected by the various threats which are inside the organization, and may leads to information loss. The aim of this paper is to allow businesses, administrators, developers and designers to produce and provide with some methods or techniques to secure such information so that the risk associated with the information loss can be minimized. In this paper we will break down the various attributes of the insider threat, and suggest some methods have been suggested which can help an organization to secure the sensitive and crucial information.*

***Index Terms —*** *Information Security, Data Security Threats, Information Security Risks*

## Introduction

As information plays a vital and crucial role in each and every organization, so it is the prime responsibility of an organization to protect the information against various threats. These threats that lead to loss of information are categorized as internal threats i.e. the threat from internal sources and the other are external threat i.e. the threats from external sources. In this paper the emphasis is on the internal threat also termed as insider threat.

So, before we proceed we must understand the meaning, impact and causes of different threats that are being faced by an organization. So let's first discuss about the meaning and impact of the word "INTERNAL THREATS".

In general, the term "insider threat" refers to employees or contractors that, due to their access to sensitive data, are in a position to aid or create a security incident. While some insider threat models only look at employees with malicious intent, to truly address this risk we must look at both accidental and malicious insiders

**Insider:** The word "insider" itself defines the people working within the organization at different positions and having different rights and authority to the access the organization information.

**Threats:** A "threat" is a potential occurrence that can have an undesirable effect on the system's assets or resources, and is a danger that may have undesirable consequences such as data privacy or threat to data.

The definition of "insider threats" is a broadening concept on daily basis. It is no longer about the disgruntled and dissatisfied employee within the company who misuses confidential information. It's also where users are accessing systems and data. It is fairly easy to create a small piece of software that will attack the internal network once it is planted on any computer system within the corporate network. Distributing the program can be done by anyone without any special computer skills. The insider threat is often characterized as an employee performing malicious behavior through sabotage, stealing data or physical devices, or purposely leaking of confidential information

Security threats arising from within the organizations are increasing the operational risks of the businesses, due to which:

- There may be a loss of reputation in the esteem of customers, partners or investors associated with an organization if there is an unauthorized access to information that leads to disclosure, modification or destruction of information which belongs to customers, partners.
- There may also be a risk of business interruption and violation of legal and regulatory requirements to protect sensitive customer information because of unauthorized users, i.e. individuals who have not been granted the right to access the system.

The company may sometime loose more of its money, information due to an internal threat than that of natural disaster or external environment as it loses due to the internal environment. The internal environment not only make company lose its personal information even make the company answerable to many clients, other organizations etc. Insider threats are the highest-ranking IT security concern. Insider misuse and unauthorized access by insiders are considered the top two IT security threats by many survey respondents.

According to the market research, the following results were found [1] [2]:

1. 33% of IT professionals are most concerned about data being lost or stolen through storage devices such as USBs.
2. 39% of IT professionals worldwide are most concerned about the threat from their employees than the threat from outsider hackers.
3. Theft of trade secrets has increased by 100% annually for the last two years.

4. 80% of all Cyber Crime is perpetrated from within the victim company.
5. Only 4% of Cyber Attacks and Incidents are reported to Senior Management.
6. 78% of Trojans and Worms since 2003 are designed to steal personal and company information.
7. Publicly traded companies that have suffered cyber crime loose 5% of their stock value within the first 60 days after the public announcement.
8. 70% of all laptops stolen are stolen for their information value, not their physical value.
9. 68% of wireless networks are unprotected.
10. Identity Theft only accounts for less than 20% of all Cyber Crime.
11. 80% of companies polled by FBI reported significant financial losses due to security breaches.
12. Only 7% of Cyber Crime was prosecuted in 2004.

So, can these insiders who work for the betterment of the organization make the organization face losses? Can they make the organization lose their clients?

If the answers to the above questions are "NO" then why and how company get attacked by the insiders?

These internal threats can either be accidental or deliberate in nature. So the purpose of this paper is to provoke discussion regarding the potential threats in the hope that more Organizations will take the initiative of investigating the realistic threats facing IT infrastructure and information.

Stealing company secrets, passwords and sensitive data is easier than ever. That's why 80 percent of cyber attacks on businesses originate on the inside of a company's computer firewall. When a company hires an information technology (IT) professional, it is essentially giving this person every bit of information they could ever need to destroy the company, steal the confidential data, or help someone else do it. It is like handing over a skeleton key that opens all the doors, drawers, all the mail, and all important filing cabinets.

## Accidental versus Malicious Threats:

When protecting against insiders, one of the first important distinctions to make is between accidental and malicious user activity. Data breach studies often do not make a distinction between these two very different scenarios. But from a control perspective, they may require different protective measures. Each case presents its own challenges. While the malicious insider is far less common, their access to information and determination make it much more likely that they will succeed in their attack.

**Table 1: Human Threats**

| Deliberate Human Threats | Accidental Human Threats |
|---|---|
| Stealing Information | Errors and omissions |
| System Hacking | File deletion |
| Malicious Code (Virus) | Laptop may get lost |
| Information Modification | Storage medium may get lost (CD, floppy, pen-drive, |
| Stealing of information | Password may be shared or there may be a common |
| Misuse of the authority or rights given to access | System may get unlocked |
| Unauthorized access to other system | System may get crash down or get hang without the |
| Using of some other IP address | System may get affected by some virus |

While any employees is generally less likely to have an accident, the sheer number of them and the complexity of the modern IT environment make it likely that some type of accident will eventually occur. The wildcard will be the impact of the accident. In the case of the malicious insider, they are almost always trying to create damage or steal valuable information. In the case of the employee accident, it depends on a variety of factors, including their level of access to sensitive information and the magnitude of the breach as to whether the incident causes real damage. In either case, the potential risk to the organization may be similar.

## Information Security Threats:

All organizations would like to have a secure IT environment but very often this need comes into conflict with other priorities. Organizations often find the task of keeping the business functions aligned with the security process highly challenging. However the reality is that, in such situations, security should be a primary issue. The likelihood of threats affecting your business will probably increase and the impact can be more detrimental if it tarnishes organizations reputation.

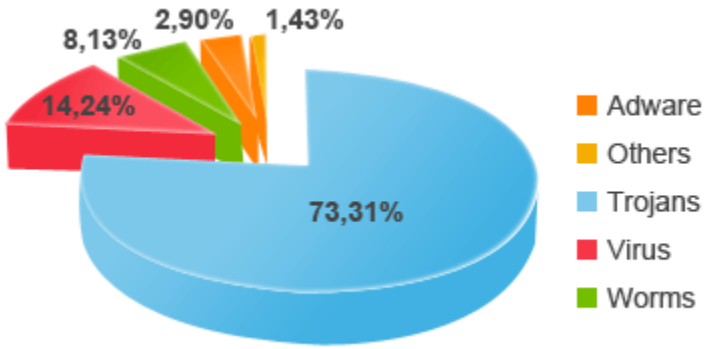


**Figure 1: Malware Infection by type**

As for the number of infections caused by each malware category, it is worth remembering that Trojans cannot replicate automatically, so they are less capable of triggering massive infections than viruses or worms, which can infect a large number of PCs by themselves. The graph below shows the distribution of malware infections this year. The volume of malware that can hit organizations today is enormous and the attack vectors are multiple.

Viruses may spread through email, websites, USB sticks, and instant messenger programs to name but a few. If an organization does not have an anti-virus installed, the safety of the desktop computers will be at the mercy of the end user – and relying on the end user is not advisable or worth the risk.

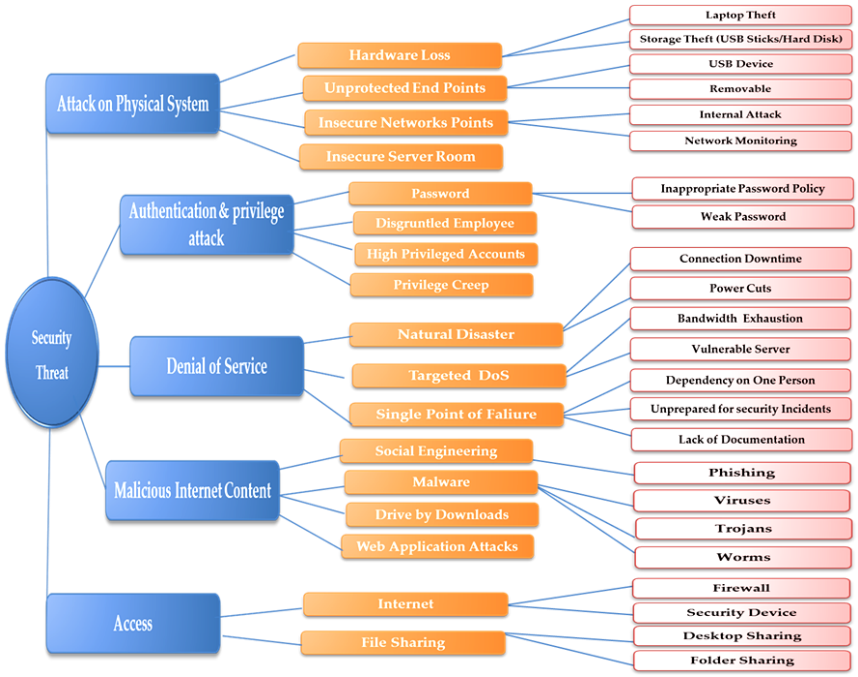


**Figure 2: Security threat map [3]**

## Attacks on physical systems

Internet attacks are not the only security issue that organizations face. Laptops and mobiles are entrusted with the most sensitive of information about the organization. These devices, whether they are company property or personally owned, often contain company documents and are used to log on to the company network. More often than not, these mobile devices are also used during conferences and travel, thus running the risk of physical theft. The number of laptops stolen per year is ever on the increase. Another threat affecting physical security is that of unprotected endpoints. USB ports and DVD drives can both be used to leak data and introduce malware on the network.

One of the possible solutions for the above concerns may be using the "McAfee Endpoint Encryption" for Laptops encryption and "McAfee ePolicy Orchestrator (ePO)" for USB and DVD drives that can keep a check on it.

## Authentication and privilege attacks

Passwords remain the number one vulnerability in many systems. It is not an easy task to have a secure system whereby people are required to choose a unique password that others cannot guess but is still easy for them to remember. Nowadays most people have lots of passwords to remember, and these password used for company business should not be the same one used for personal or webmail accounts, site memberships and so on.

Password policies can go a long way to mitigate the risk, but if the password policy is too strict people will find ways and means to get around it. They will write the password on sticky notes, share them with their colleagues or simply find a keyboard pattern (qwerty@12) that is easy to remember but also easy to guess. Most complex password policies can be easily rendered useless by non-technological means.

In a lot of organization, systems administrators are often found to be doing the work of all domains including server, network and also security domains. Therefore a disgruntled systems administrator will be a major security problem due to the amount of responsibility (and access rights) that he or she holds. With full access privileges, a systems administrator may plan a logic bomb, backdoor accounts or leak sensitive company information that may greatly affect the stability and reputation of the organization.

Additionally, in many cases the systems administrator is the person who sets the passwords for important services or servers. When he or she leaves the organization, these passwords may not be changed (especially if not documented) thus leaving a backdoor for the ex-employee.

The company's management team may also have administrative privileges on their personal computers or laptops. The reasons vary but they may want to be able to install new software or

simply to have more control of their machines. The problem with this scenario is that one compromised machine is all that an attacker needs to target an organization. The firm itself does not need to be specifically picked out but may simply become a victim of an attack aimed at a particular vulnerable software package.

Even when user accounts on the network are supposed to have reduced privileges, there may be times where privilege creep occurs. For example, an employee who got migrated to different domain may retain the old privileges for years even after the handover! When his or her account is compromised, the intruder also gains access to the old domain of the employee.

One of the possible solutions for the above concerns may be using the "Change Management Process" documented in the "ITIL" according to which for every access a change should be raised that will keep track on User and its right and will be reviewed on regular interval. All domain server machines password should be regularly changed and documented.

## Denial of Service

In an attempt to minimize costs, or simply through negligence, most small and some medium-sized businesses have various single points of failures. Denial of service is an attack that prevents legitimate users from making use of a service and it can be very hard to prevent. The means to carry out a DoS attack and the motives may vary, but it typically leads to downtime and customers losing confidence in the organization - and it is always not necessarily due to an Internet-borne incident.

Reliability is a major concern for most businesses and their inability to address even one single point of failure can be costly. If an organization is not prepared for a security incident, it will probably not handle the situation appropriately.

If a virus outbreak does occur, who should handle the various steps that need to be taken to get the systems back in shape? If an organization is simply relying on the systems administrator to handle such incidents, then that organization is not acknowledging that such a situation is not simply technical in nature. It is important to be able to identify the entry point, to approach the persons concerned and to have policies in place to prevent future occurrences apart from simply removing the virus from the network. If all these tasks are left to a systems administrator, who might have to do everything ad hoc, then that is a formula for lengthy downtime.

One of the possible solutions for the above concerns may be having top level support from the service provider and highly qualified system administrator having complete knowledge of the product as well as having complete details of escalation matrix of the service provider so in any case of emergency same can be reached without wasting any time and appropriate action to quarantine the problem.

## Malicious Internet Content

Most modern organization requires an Internet connection to operate. This has made email a primary means of communication. Even phone communications are changing shape with Voice over IP becoming a standard in many organizations.

At some point, most organizations have been the victim of a computer virus attack. Many small organizations cannot afford to employ prevention mechanisms such as network segregation. These factors simply make it easier for a worm to spread throughout an organization.

Malware is a term that includes computer viruses, worms, Trojans and any other kinds of malicious software. Employees and end users within an organization may unknowingly introduce malware on the network when they run malicious executable code (EXE files). Sometimes they might receive an email with an attached worm or download spyware when visiting a malicious website. Alternatively, to get work done, employees may decide to install pirated software for which they do not have a license. An organization that operates efficiently usually has established ways to share files and content across the organization. These methods can also be abused by worms to further infect computer systems on the network.

Computer malware does not have to be introduced manually or consciously. Basic software packages installed on desktop computers such as Internet Explorer, Firefox, Adobe Acrobat Reader or Flash have their fair share of security vulnerabilities. These security weaknesses are actively exploited by malware writers to automatically infect victim's computers. Such attacks are known as drive-by downloads because the user does not have knowledge of malicious files being downloaded onto his or her computer. In 2007 Google issued an alert 1 describing 450,000 web pages that can install malware without the user's consent.

Then you get social engineering attacks. This term refers to a set of techniques whereby attackers make the most of weaknesses in human nature rather than flaws within the technology. A phishing attack is a type of social engineering attack that is normally opportunistic and targets a subset of society. A phishing email message will typically look very familiar to the end users – it will make use of genuine logos and other visuals (from a well-known bank, for example) and will, for all intents and purposes, appear to be the genuine thing.

Additionally, the move towards web applications has introduced a large number of new security vulnerabilities that are actively exploited by attackers to gain access to these web applications. If these services are compromised there is a high risk that sensitive information can be leaked and used by cyber-criminals to commit fraud.

One of the possible solutions for the above concerns may be using mail scanning tools like "Cisco Iron Port" for email scanning which will include different policies that can be

implemented on user mail ID according to the requirement and also an antivirus that will scan the mails and block all spam mail. The other steps that must be used is using only licensed software and keeping a track on the CMBD of every system.

## Roles of Information Security:

Information Security is defined as the protection of valuable information which may be in form of digital information or paper information from the breaches such as theft, sabotage or forgery, lost, destroyed either accidently or deliberately. Information security in today's scenario plays a vital role as it protects the information and documents of the organization from various threats. If information of the organization is not protected or safeguarded in an appropriate manner then it can make business face many unavoidable situation and circumstances

It's not always the financial losses that can spoil the goodwill of the company even the information that the organization consists of which belongs to different clients, partners, employees can make the organization lose its goodwill, reputation, contract, shares etc.

The factors associated with information security are [4]:

1. Confidentiality: It means that the information must only be accessed, used, copied, or disclosed by authorized individuals only.

2. Integrity: It means that the data cannot be created, changed or deleted without authorization.

3. Availability: It means that the information and the computing system that are being used to process the information and security controls that are used to protect the information should all be available and correctly functioning when the information is needed.

Just start by taking the following steps, an organization can reduce the chance of your company succumbing to an inside cyber crime:

1. Know New Hires: - An organization must be aware of the complete information about its employee. The person interviewing prospective hires should have at least some expertise in the software the new employee will be using, the Operating Systems used, and an understanding of the computer network.

2. Back Ground Check: - Double, Triple and Quadruple Background Screening. If the company does not regularly perform comprehensive, national-database background checks, it needs to find someone who does it before hiring a new Information Technology professional. Large investigation firms often use clerical workers who do very limited searches and routinely end up missing red flags for

untrustworthiness. If you need to outsource this function, you can hire an officer to dig into your candidates' past. It may cost a little more, but it will significantly lower the company's and the clients' risk of catastrophic loss in the long run.

3. Limit IT Personnel Access: - Chances are that the most of the people hired are not corrupt, malicious people. But sometimes when people find themselves privy to all the company secrets, a phenomenon, we call "creeping criminalization" grabs hold of them. They get hordes of privileged information and start seeing profit or personal gain potential. They may even begin rationalizing seemingly small but costly infractions. An organization can help protect the company from creeping criminalization by actively restricting each employee's access to certain areas of information. Start by assigning particularly sensitive areas of the network to your most trusted employee only and regularly monitor information flow. Next, implement a strong policy that forces periodic changes in passwords and limits easy-to-break alphanumeric combinations. Also, have employees sign an annual agreement outlining:

    a. The employee's obligation to safeguard company information

    b. The company's exclusive information ownership and right to examine all correspondence and information on any of its computers

    c. The company's right to monitor all computer activity.

    d. The company's methods, policies, and procedures regarding the use of company computer resources.

    e. And finally, change all passwords and access codes every time an IT employee leaves the company. That means; financial services, Web sites, routers, wireless access points, computers, servers, company FTP sites, and communications equipment, to name some.

4. Get A Cyber Security Audit: - When most companies get an audit to find out what's wrong with their security system, it's in reaction to a major security breach. But a reputable and experienced security audit firm can also detect a problem well before it grows into disaster. If an organization has even an inkling of concern about your IT security, find a cyber security firm to perform a full audit. If the audit does uncover illegal activity, the organization will need a meticulously-executed investigation with expert preservation of evidentiary material to protect the company and share the Root Cause Analysis (RCA) for the same.

5. Security Incidents: - An organization should encourage Staff Members to Report Computer Security Incidents to Senior Management. A study showed that only four percent of all computer security incidents, such as password collecting, information leaks and file copying are reported to managers. Encourage an honest environment by developing an anonymous informant system, in which employees learn exactly what to expect and can earn rewards for reporting questionable incidents.

6. Endpoint security: -A lot of information in an organization is not centralized. Even when there is a central system, information is often shared between different users, different devices and copied numerous times. In contrast with perimeter security, endpoint security is the concept that each device in an organization needs to be secured. It is recommended that sensitive information is encrypted on portable devices such as laptops. Additionally, removable storage such as DVD drives, floppy drives and USB ports may be blocked if they are considered to be a major threat vector for malware infections or data leakage. Securing endpoints on a network may require extensive planning and auditing

7. Backup and Redundant systems: - Although less glamorous than other topics in Information Security, backups remain one of the most reliable solutions. Making use of backups can have a direct business benefit when things go wrong. Disasters do occur and an organization will come across situations when hardware fails or a user (intentionally or otherwise) deletes important data. A well-managed and tested backup system will get the business back up and running in very little time compared to other disaster recovery solutions. It is therefore important that backups are not only automated to avoid human error but also periodically tested. It is useless having a backup system if restoration does not function as advertised. Redundant systems allow a business to continue working even if a disaster occurs. Backup servers and alternative network connections can help to reduce downtime or at least provide a business with limited resources until all systems and data are restored.

Security policies are used to protect the organization's business and client's information within its custody by safeguarding its confidentiality, integrity and availability. It also helps to establish safeguards and policies to protect the organization's information resources from theft, abuse, misuse or any other form of damage and to establish all the responsibilities and accountabilities for information security within the organization. Security Policies are also used to encourage management as well as staff members to maintain an appropriate level of awareness, knowledge, skills so as to allow them and help them in minimizing the occurrence and security of information security incidents.

So the protection of the information must be the prime motivate of any organization. The following are the advantages of information security:

1. Information security takes steps to prevent different types of data leakage and hence increases the reliability of the information.
2. Information security increases the confidentiality of the document.
3. Information security allows the protection of less sensitive material through username and password technique and more sensitive materials though installation of tools like biometrics, firewalls or detection systems.
4. It allows the organization to keep the vital and private information out of wrong hands.
5. Information security protects clients as well as users valuable information both while in use and while it is being stored.

Incidence rates of outside hacking to gain company information are almost miniscule in comparison to the number of crimes initiated from within large and small businesses. Being proactive about your company's cyber security is the only way to protect yourself against cyber "crime without punishment."

## Conclusion

Security in an organization is more than just preventing viruses and blocking spam. Every year, cybercrime is expected to increase as criminals attempt to exploit weaknesses in systems and in people.

Cyber-espionage and social networking attacks will be the predominant threats to safeguard against this year and coming years. The rise of social media, which has increased communication between people all over the world, has its own disadvantages too. Cyber-thieves can infect and steal data from thousands or millions of users in one go. Hacker no longer needs to be a computer whiz to gain control of a system or edit malicious code to generate new malware strains.

The growing number of Internet users means there is no shortage of potential victims. Cyber – criminals are just like pickpockets in a busy city square during the shopping season. The problem is that today the number of cities and squares (platforms, social networking sites, cell phones, tablet computers, etc.) has multiplied and they are busier than ever, leaving you with more chances of exposing your organization and its contents to thieves. There are more potential victims for more pickpockets.

But this rather bleak outlook should not stop you from enjoying the benefits of the Internet: online banking and shopping, instant communication with friends and relatives all around the world, the ability to read books on your phone or tablet. We just need to take a few precautions.

This paper aims to give managers, analysts, administrators and operators in an organization a snapshot of the IT security threats facing their organization. Every organization is different but in many instances the threats are common to all. Security is a cost of doing business but those that prepare themselves well against possible threats will benefit the most in the long term.

## References

1. Annual Report- PandaLabs 2011: DOI – http://pandalabs.pandasecurity.com
2. Cisco Public Information: DOI – https://www.cisco.com/go/offices
3. InfraGard Tampa Bay - The Sylint Group: DOI – http://infragardtampabay.org
4. Julio Cella, “Antivirus at SMTP Gateways Level”:
   DOI – http://www.sans.org/infosecFAQ/malicious/gateway.htm
5. SECURITY THREATS – GFI Software: DOI – http://www.gfi.com
6. Symantec Antivirus Research Center ”Security Updates”:
   DOI – http://www.symantec.com/avcenter/vinfodb.html

# Certificate of Recognition

*This certificate is awarded to*

## *Atul Rana*

*in recognition of his / her contribution*

**"Insider Threats: Risk to Organization"**

*to* Vol. 02, No. 01, 2012 *of*

IARS International Research Journal

*Editor in Chief*

IARS International Research Journal 08 FEB 2012