

## Introduction

Critical infrastructure and businesses with significant financial resources are experiencing a high severe attack rate.

This is seen from the innumerable attacks posed on the network by the outsiders and insiders.

The organization's business processes along with its assets are prone to multiple points of attack from people with malicious mindsets.

## Need

The day to day operations of a company involves huge communication and also lot of transactions which results in an increased risks in security and network availability requirements.

*"Installing IDS, Firewalls and antivirus doesn't make your network secure enough as there are ample ways to breach your security barriers".*

*"Even with the strongest technology safeguards in place, in many cases, IT administrators still only have a limited amount of time and control over what their users do over the Internet".*

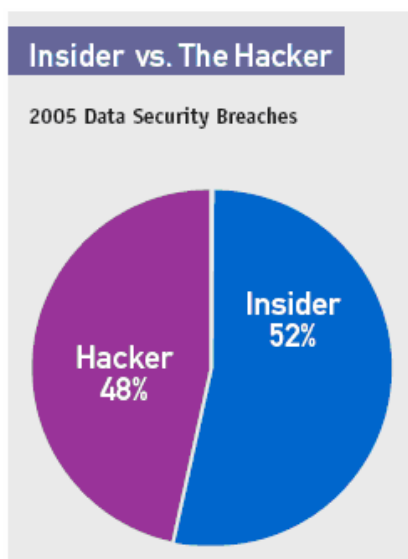
*"The most likely threat to information security is not the typical hacker, virus, or worm, but rather the malicious or careless corporate insider"*

## Risks:

Following are many such reasons on "Why you should do it?"

- Ensuring Confidence and Trust
- Increasingly Sophisticated Attacks
- Trojan Attacks.
- Loss of your Internal Information through remote accessing
- Virus and Worm Attacks
- Unwanted Usage of Bandwidth
- Losses due to loss of confidential information
- Expenditure due to recovery from data loss.

The increased business risks and the effect on network performance are mainly due to improperly configured network and security devices. Lack of stringent security policies also serves to multiply the risk involved in network security. Peer-to-peer file sharing, unnecessary network services and remote-access applications can be those reasons which can introduce significant vulnerabilities inside your network.



## Our Service

We at COE Security expands beyond simple external assessments to offer a comprehensive assessment that may include complete packet analysis in the network, network traffic, band width usage, infected systems in the customer environment. "Network Packet assessment" is the process of capturing network traffic and inspecting it closely to determine what is happening on the network. The assessment delivers the analysis of the audit with recommendations.

### Key Benefits:

- Identification of areas of risk with respect to single points of failure that covers both physical and network.
- Identification of existing scalability limitations
- Identification of network vulnerabilities
- Identification of anomalies in the network
- Improve network performance and availability.
- Increase network resiliency
- Increase end-users productivity and satisfaction
- Increase empowerment over the network.
- Reduce unwanted broadcasting of the infected systems.
- Reduce costly errors in network configuration
- Reduce cost of unwanted bandwidth Usage.

## Attacks to be assessed:

Type Of Attack	Description	Economic Implication
Hackers	Intruders, or skilled programmers who find challenge in breaking into other people's network, were traditionally the greatest threat to organizations' computer security. While they still pose a threat, widespread deployment of countermeasures such as firewalls has caused other forms of more sophisticated malicious attacks to emerge	After breaking into a system an Intruder may steal, delete or alter valuable and confidential data, programs or identities.
Malware	Malware (viruses, worms, etc.) are pieces of hidden code that are typically designed to cause an undesirable event, such as altering existing files or making the computer inoperable. They can be transmitted by disk, email or other communication media. Because email usage is so important in a corporate and traditional security system remain vulnerable to viruses, viruses are now one of the major security concerns for Corporates. 86% of all infections stem from email attachments.	Malware is one of the major concerns to a corporate. The cost of lost productivity, restoring damaged files and cleaning up viruses was a staggering \$13.2 billion worldwide in 2001.
Spam	Unsolicited commercial or personal email messages (spam) are not created with the same malicious intent as threats like viruses, but are now having a negative economic impact on the same order of magnitude.	Spam clogs networks, hogs disk space, and wastes countless hours of users' time reading and dealing with the messages. Estimated cost to U.S. and European businesses in 2002 was \$8.9 and \$2.5 billion respectively.
Denial of Service (DoS)	A DoS attack is one in which the perpetrator deprives an organization of the use of a network resource (such as the email system or web site) by sending network traffic that exploits a weakness in the receiving system. The more sophisticated Distributed DoS attack utilizes a common exploit to first penetrate numerous widely dispersed systems, and then launch the attack from those systems, making it harder to detect and block.	Organizations depend upon these services to conduct business, so the impact on revenues and productivity can be quite substantial and high.
Inappropriate Web Usage	Because Internet usage is difficult to be casually monitored, some individuals use it to access inappropriate material (pornography, hate material, copyrighted audio files) and conduct inappropriate activities (excessive personal business, etc.).	As the Corporates allow large number of employees with Internet access, clearly there are potential productivity issues associated with unrestricted usage. A growing concern is associated legal issues. Allowing the downloading of inappropriate material without controls can result in expensive lawsuits for a hostile workplace environment and copyright violations, for example.
Insider Attacks	Even most of the attacks originate from outside the organization, internal attacks are not infrequent, especially those related to theft or destruction of proprietary information. Roughly more than half such attacks originate internally. Disgruntled employees, as well as those seeking personal financial gain have used their insider status to access, and sell or destroy valuable company information.	Insider attacks can be more harmful than attacks by External attackers due to the knowledge the attacker has about the location and use of valuable data.

For further details Contact us at [www.coesecurity.com](http://www.coesecurity.com)  
Email: [sales@coesecurity.com](mailto:sales@coesecurity.com)