



CS SECURE
Protection Information System

ARE YOU CONTROLLING INFORMATION DISCLOSURE?

Preventing information theft

When it comes to security issues, companies have traditionally focused their efforts on protecting their data from hackers, viruses and theft. Vast amounts of money are spent on firewalls, intrusion detection, anti-virus and anti-spam software.

Organisations now need to wake up to the risk of information loss from inside their organisation. The latest statistics and reports show the greatest threat to confidential information comes from inside companies, not outside.

As businesses hold increasing amounts of confidential information in digital formats it is essential for them to protect it from their employees' intentional and unintentional disclosure. Failure to do so can result in lasting damage to company's financial well-being as well as its reputation and customer base.

The challenge is to find the technology. Information must be fully protected from attack without compromising company network's efficiency and agility.

"70% of security breaches that involve losses over \$100,000 are perpetrated from inside the enterprise."

Vista Research

The inside threat

The greatest difficulty in dealing with the inside threat is the internal user's behaviour. Most of today's information leakage is unintentional, caused by users who do not realise the data they are sending could be putting the company at risk.

Are your employees releasing confidential information by mistake? Even the most reliable and committed employee can accidentally send confidential information; increasingly amounts intellectual property, market information, clients' personal information are held in digital format. It is all too easy for the wrong file to be attached and sent to an external email address. Organisations need to prevent this from happening.

The number of different communication channels we have today is adding to the threat. Email, IMS and portable devices that can be connected to the client's personal computer all contribute to the danger of unintentional leakage.

Large corporations have been forced to abandon projects or have lost large investments because one of their employees has sent important information to the wrong address.



The multilevel approach

Traditionally, companies have relied on solutions such as information security policies and discretionary access control systems. These are no longer capable of dealing with the inside threat: a multilevel approach is now necessary.

The defence community, where unauthorised disclosure can lead to loss of life, has been using a multilevel approach for some time. People and information are classified at different levels, according to trust and sensitivity. This controls the access to and circulation of information. A person is given a security clearance to allow them access to classified information to a specific level. Their security clearance is based on a vetting procedure.

Critical Software's solution is to enhance an organisation's commercial off-the-shelf (COTS) applications with a multilevel approach to security. This will allow them to enforce their access and communications policies through their current systems.

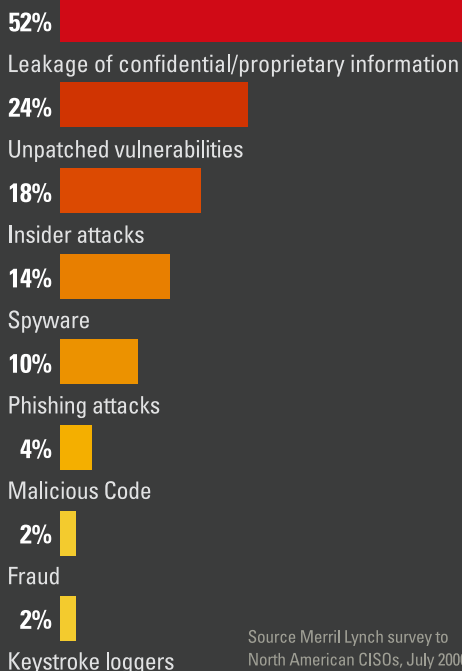
Deutsche Bank loses Hertz IPO Role because of e-mails

Bloomberg.net

"80 to 90% of leaks are either unintentional or accidental"

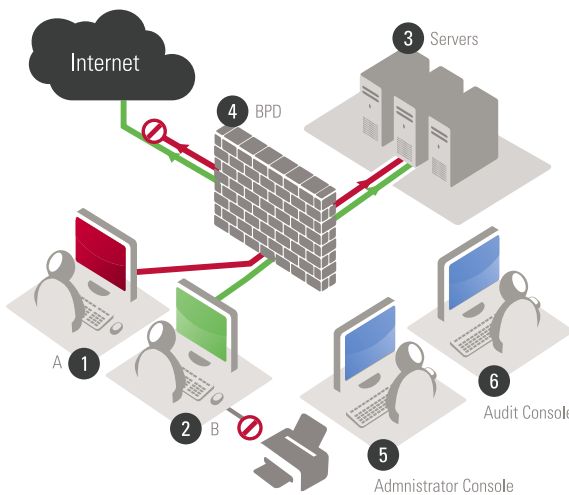
Gartner Report

Organizations Threats



Source Merrill Lynch survey to North American CISOs, July 2006

Policy enforcement in all systems managed centrally.



Workstations:

1 – Users A and B login to the system. Authentication and authorization are performed, and the information access policy is enforced on the workstation.
2 – User B is able to access the document marked but he does not have the printing privilege.

Servers

3 – User B uploads a document to a content manager server and the document is marked according to the level of confidentiality. Information on the servers is encrypted.

Network Edge

4 – User B tries to send a marked, attached document in a marked e-mail message outside of the organization but the border protection device (BPD) filters and blocks it. Solutions for other communication services such as IMS and http are also available.

Central Management

5 – The administrator has access to the administration console to configure the security policies as well as the overall system.
6 – The auditor has access to the audit console to configure the events he wants to monitor and to define the alarm triggers. An audit survey is also performed to determine the non-compliances and the non-compliant users.

Information Security requires security on every part of the infrastructure.

A chain is only as strong as its weakest link. To effectively protect information the solution needs to be applied to each link.

We supply enhancements for the workstations' COTS applications, allowing authorised users to give any file or email created or accessed a security classification. The authorisation is based on the security clearance given to the user. Our system also manages security clearances, which may already exist in a standard directory such as Active Directory.

We define a set of user applications controlling what the user can do – edit, print, copy, paste – based on the information's security classification and the user's security clearance. Each information container (files, email messages etc) is classified and encrypted.

A border protection device (BPD) is used to control the flow of information to the outside world using communications such as email and instant messaging. This is based on COTS communications and proxy servers.

We supply consoles, tailored to meet an organisation's requirements, for configuration and auditing. These can be based on a client server approach or through web systems.

This approach strengthens each link in the chain by enhancing any existing COTS network, providing security at all levels and effectively protecting confidential information.