

Organizations are besieged today with the growing list of security risks. The sheer volume of risks in the business environment ensures that discovering them becomes an overwhelming task.

2008 was, without a doubt, a year in which the problems of information protection came sharply into focus. Be it government agencies in the UK losing private citizen information or Indian BPO's battling malicious employees. Expressions such as "identity theft", "computer fraud" and "planted insiders", which were once, limited to information security specialists, have become more and more familiar.

MIEL has always been on the forefront of information security risk management. This document stems from MIEL's own experience in risk management from the last 12 months. The research is based on a sample size of over 30 organizations and is our attempt to create a common awareness platform across our client base. This document addresses the risks "popularly" seen across multiple organizations. Whilst addressing the document, we have also presented some quick pointers towards mitigation of these risks.

Read on, and decide for yourself, if your organization has taken care of the key risks of 2008. You can use this document as a quick-fix approach to mitigate risks within your organization. However, this is by no means a complete list of risks affecting the information in your organization.

TOP 10 INFORMATION SECURITY RISKS IN 2008

FIRE

RANK : 10

THIS IS A SURPRISE ENTRANT! SEVERAL COMPANIES ARE RATING THIS AS A CRITICAL RISK

We did not expect this to be here; it is not the lack of equipment but the lack of procedures that brings this risk to the top 10.

- Heat-generating equipments such as copiers, work processors, coffee makers and hot plates should be kept away from anything that might catch fire.
- Combustible materials such as paper should be stored properly. They should not be stacked up.
- Sprinklers and fire/smoke detectors should be installed in storage areas.
- Storage areas should be located away from heat sources.
- Electricity outlets should not be overloaded. The best way is to assure a sufficient number of outlets.



UNAUTHORIZED PHYSICAL ACCESS

RANK : 9

THE PERENNIAL ENTRY!

Physical devices like laptops, desktops, etc can be accessed by unauthorized people if perimeter barriers and other physical security safeguards are absent. Although organizations take care of their Datacentre, this particular aspect brings it into the top 10.



- Prevent unauthorized entries into the premises and other sensitive areas.
- Identification methods together with authorization and access control such as badge systems, card readers or biometric controls should be implemented.
- Visitor control procedures should be employed to restrict the freedom by which a visitor can access the premises.

MISUSE OF USER RIGHTS**RANK : 8**

KEEPS SNEAKING INTO THE TOP TEN, DESPITE THE ROBUST ACCESS CONTROL FEATURES PROVIDED BY TODAY'S APPLICATIONS

Widespread administrator level access to users, non-removal of access on role-change and privilege escalation has brought this risk in the top 10.

- Principle of least privilege should be followed.
- Every program and every user of the system should operate using the least set of privileges necessary to complete his job.
- If a person does not need an access right, he should not have the right.
- A unique ID and password should be given to each user. Users should be given read only access to the applications present.

**DENIAL OF SERVICE****RANK : 7**

THE GROWTH IN ONLINE BUSINESS HAS SEEN THIS MOVE UP THE RANKS. WE PREDICT THAT IT WILL CONTINUE TO DO SO

Many corporate websites have suffered from illegal denial of service attacks lately. The major contributing factor to this has been a slack in timely hardening and patching of systems.



- An organization should maintain audit trails which describe what has changed in the network and why.
- Anti-virus should be installed and updated regularly.
- Firewalls should be installed and configured to restrict traffic coming into and leaving the computer.
- Email filters should be installed as they help in restricting traffic.

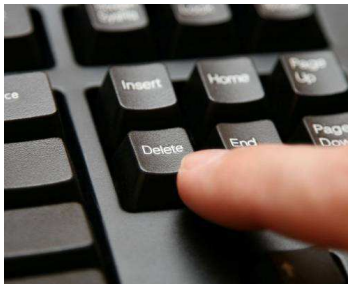
SOFTWARE CORRUPTION / FAILURE**RANK : 6****SOFTWARE CORRUPTION ACCOUNTS FOR 14% OF ALL DATA LOSSES**

Piracy is not the only reason for this to feature in the top 10. Misconfiguration and incorrect software usage have created several issues this year. It happens due to corruption by virulent software, configuration complexity, or improper backups.

- Backups should be taken on a regular basis, so that even if the data gets corrupted due to some reason, the organization is still safe and so is its customer database.
- Pirated copies of software should not be bought even though these copies can be purchased at a lesser price.
- A program should be used only for its intended purpose else it might become corrupt and stop functioning.

**DELETION****RANK : 5****JUSTIFY YOUR DATA BACKUP INVESTMENT THROUGH THIS RISK!**

Organizations are still quite lackadaisical towards data-backup. Several companies lacking well-conceived data recovery strategies had to bear both financial as well as legal losses they could ill-afford.



- Backup of data should be taken at regular intervals.
- Restoration capabilities should also be provided such that the backed up data can be restored as and when required.
- Data recovery tools should be present with the administrator such that data can be recovered if it is accidentally deleted.

INTERNET CONNECTIVITY FAILURE**RANK : 4****CRITICAL YET UNPREDICTABLE – THIS RISK SURFACED BECAUSE OF GLOBAL CONNECTIVITY FAILURES**

Global cabling problems aside, several companies are still struggling to make their infrastructure robust for internet access (network and bandwidth management). Service provider selection criteria leave a lot of room for improvement.



- Service provider should be selected depending on the need of the organization.
- A backup service provider should be selected such that if the previous provider is unable to provide optimum services the backup provider could provide them.
- The temperature of the server room should be maintained in order to avoid excessive heating of the devices.

DATA CORRUPTION

RANK : 3

COMBINED WITH SOFTWARE CORRUPTION (#6) - 'CORRUPTION' PROBABLY POSES THE SINGLE LARGEST RISK

Growth in internet usage has also seen the growth in malware infections which significantly contribute to data corruption.



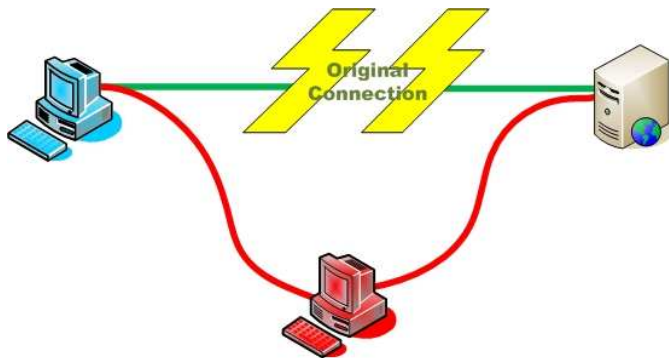
- A computer should not be switched off without proper shutdown procedure.
- Malware infections also lead to data corruption. Thus, one should be very careful while downloading files from the internet.
- Files should always be downloaded from reliable sources.
- Poorly written software if downloaded can also lead to data corruption.

MODIFICATION OF DATA

RANK : 2

DELIBERATE OR INADVERTENT, THIS CONTINUES TO POSE A SIGNIFICANT THREAT

Data integrity is the key to the success of any organization. However due to the limited attention being paid to it, this risk has risen significantly.



- All confidential information should be sent in the form of an attachment.
- Attachment should be encrypted using strong cryptographic controls.
- Digital signatures should be used in order to avoid non-repudiation by sender.

UNAUTHORIZED LOGICAL ACCESS

RANK : 1

AS EXPECTED. WEAKEST LINK IN ALL SECURITY INITIATIVES ARE THE PEOPLE



Lack of password policy awareness was quite rampant this year. Given that the IT infrastructure is only going to get complex from here on, much more needs to be done to ensure that this risk is marginalised.

- Simple passwords should be replaced by stronger, multi-factor authentication passwords.
- Strong identity authentication should be done which includes the use of two or three factors such as something one has (a physical item or token in your possession), something one knows (information only you know) and something one is (a unique physical quality or behaviour that differentiates one person from another).

Conclusion

Internal IT threats, in particular data theft and employee carelessness, remained the greatest danger for organizations in 2008. Despite a slight reduction in the overall index of information security concerns, these threats have remained at the same level and have outstripped all the other threats in terms of importance.

At the same time, the interest in virus epidemics and hacker attacks is gradually decreasing and those problems are being viewed more and more as media sensationalism.

From the point of view of security measures to prevent leaks of confidential data, organizations can be described as moving in the right direction, but not quickly enough. The foundations are already in place to implement complex projects and the problem has been acknowledged, however other external factors have kept the words from turning into deeds.

2009 will bring along fresh challenges. “Effective”, “Efficient” and “Measurability” will become buzz words. On the whole, the changes in the organizations from the point of view of confidential data protection can be described as positive, though the overall situation is far from ideal.

For more information visit: www.mielesecurity.com

Headquarters: C-611/612, Floral Deck Plaza, MIDC Central Road, Andheri (E), Mumbai-93, INDIA

Phone: +91 22 30096969 | Fax: +91 22 28215838 | Email: feelsecure@mielesecurity.com