

Malware challenge shows IT still needs a business reality check

By ICTWorld, 5 September 2006 [Print](#) || [Discuss](#) The response of some sections of the IT industry to the growing challenge of malicious software (malware) demonstrates that even leading players in the technology space have a tendency to lag current business realities.

Two realities in particular need to be confronted. Firstly, business today is reluctant to simply throw money at IT. CFOs want to know why, if IT is so smart, it cannot deliver cost-efficient solutions.

The second reality is that successful business is agile business. Speed of response is critical. Information is distributed to the desk-top – and gathered there – to enable a company's frontline to take action and decisions.

An increasingly mobile workforce, powered by cellphone and laptop, provides competitive advantage while optimising human capital uptime in a growth-economy that is increasingly constrained by skill shortages.

Unprotected desktops

In this environment, malware creates a big challenge, as many organisations still do not have an automated and guaranteed way of protecting information assets at the desktop.

The issue was crystallised in an eWeek article, in which a security official for perhaps the world's most pre-eminent IT player suggested that business consider investing in an automated process to wipe hard drives and re-install operating systems. This was presented as a practical way of recovering from malware infestation.

The idea might not square with the realities of cost-sensitive, agile business, but, yes, it is do-able.

A company can design a near-automated process to wipe and rebuild its systems, using some sort of corporate-image CD containing the operating system files, required applications and templates. But what about data created by users?

Is it practical to expect a fast-paced, mobile workforce to comply with preferred IT procedures and place copies of all new business information on the file server?

Cleaned out of data

A global provider of IT market intelligence, such as IDC, believes that up to 60% of an organisation's file data is distributed on user desktops and laptops. A recent study indicates that 75% of this data lies unprotected.

In other words, nearly half of a company's information is exposed to be lost if a business opts to wipe clean and re-install in response to malware infestation.

It is clear that going forward the traditional file server approach is unlikely to suit companies that wish to optimise corporate data ownership.

Data protection and recovery has to be taken to the edge and extended to user desktops and laptops.

This can be a total reversal of current practice. Many IT departments only protect data on servers, completely ignoring desktops and laptops.

Clean out of ideas

Some claim that backing up this data is impractical and expensive; arousing suspicion that the sudden concern about costs and practicalities might be prompted by failure to adopt the right toolset in the first place.

The response that 'it cannot be done' or 'it is not worth it' is a major irritant to CIOs, who see the importance of user information and are concerned by its possible loss.

According to John Clancy, executive vice-president of Iron Mountain Digital, PC data protection is critical to any comprehensive disaster recovery and business continuity plan. As PC storage capacity increases, more and more critical business information is created and saved to the desktop.