Headline **ICT security action**
Date **27 Jul 2009**
MediaTitle **New Straits Times**
Section **Tech & U**
Journalist **Abdul Rahman Shafi**
Frequency **Daily**
ADValue **2,478**

Language **English**
Page No **14**
Article Size **179 cm²**

Color **Black/white**
PRValue **7,435**


Surprising lack of global clout

# ICT security action

**By Abdul Rahman Shafi**

THE Y2K (Year 2000) bug has raised awareness among firms on the impact of computer system glitches to the business and the country. Not surprisingly, investment in ICT is always going up for firms to continually improve productivity and profitability. Although firms generally need to look at the smooth running of their business, the ICT unit has to address all issues related to downtime and business recovery from computer glitches.

Recovery plans for computer systems, service level agreements and computer recovery centres have been thought to be sufficient to address system failures. And although agencies such as the Securities Commission and Bank Negara have guidelines on how to address issues that keep firms viable, emphasis is usually on financial and technical matters such as generating electricity and manufacturing products.

For better implementation of ICT security, it is important to see this within the context of corporate governance, which covers all aspects of security and viability of the business.

Annual reports now have to highlight the corporate governance initiatives taken. This is where firms must adopt in principle the ISO/IEC 17799 standard within its corporate governance policy. Only by implementing the various policies within the standard can a firm fully address the security issues related to ICT systems.

With the implementation of online payment systems, there are questions on whether conducting financial transactions over the Internet is safe. Theft of financial data is still a concern.

And with Wi-Fi networks and wireless technologies, the gate is even wider for such information to be tapped or some form of sabotage of ICT systems to take place.

For firms that form the economic backbone of the country, it is important that they adopt the ISO/IEC 17799 standard. The respective ICT units need to do an impact analysis of how disruption can take place and what the impact is on their business. A full-time unit tasked to look at protecting systems from security threats needs to be formed.

Continuous monitoring of various disruptions such as downtime, virus attacks and attempts on unauthorised access also is needed so the real impact of any disruption can be addressed effectively.

All these efforts will boost confidence in business transactions with other firms which have adopted similar standards.

To address the issue, a number of initiatives have been taken at the national level as well. For example, CyberSecurity Malaysia has drafted the National Cyber Security Policy which provides the framework for protecting the country's Critical National Information Infrastructure. And Mimos is involved in activities under the Ultimate Digital Fortress.

In short, it is vital that firms keep up-to-date with such developments and incorporate them in their security policies.

The writer is an ICT consultant.