

**CONTROLLING THE BEAST**

Talking IT management with Al Batha Group CIO Saji Oommen

**INVALUABLE INTELLIGENCE**

How to avoid failure when rolling out a BI system at your company

**LOCKING OUT INTRUDERS**

Saudi Arabia's KACST bolsters its defences with new IT system

**ACN**

# Arabian Computer News

An ITP Technology Publication | Licensed by Dubai Media City

BAHRAIN BDI.5 | EGYPT LEI5 | JORDAN JD2  
KSA SR15 | KUWAIT KDI.5 | OMAN ORI.5  
QATAR ORI.5 | UAE DHS15 | UK £5 | USA \$8

SEPTEMBER 2010 | VOL.23 ISSUE 9

Aligning business and IT strategies for the Middle East

## NEW DAWN

How Cisco is banking on a fresh wave of investment to drive its business in the Gulf

Wayne Hull, General Manager, Cisco UAE





Abhijit Pendse

# Who said IT wasn't a risky business?

It pays to have a policy in place when your systems go down

**O**ver the years, risk management has become paramount across all functions of a company and IT is no exception. Different regulations, standards, frameworks and overlapping concepts have evolved in this area.

The traditional approach has been piecemeal, reactive and driven by specific events or contingencies. However, the time has now come to take a holistic view and develop a robust IT risk management framework to mitigate the known and unknown. Such a framework should encompass all technology assets and resources — applications, infrastructure and operations.

The importance of IT among the support functions of an organisation has been on the rise since its birth. What started as a MIS function with some finance guys crunching data to get reports, has today become the nervous system of most businesses.

With the growing criticality, the cost of IT failure has also proportionately increased. Today, a lot of business functions would literally come to a standstill in case of technology failures. It is no surprise that IT risk management is becoming a critical activity.

Traditionally, risks in IT have always been looked upon as system access risks. The simplistic and most common of the control

mechanisms has been access validation control by use of a password. However, with the passage of time, the realisation has dawned that IT risk management is not just password management and has to be looked at holistically, both from an internal and external threats perspective.

People — employees and external — are regarded as the biggest threat to technology and applications. Common issues include one employee using another employee's credentials to access classified information or employees sharing confidential data with outside sources.

The technical resources in an organisation are also potential threats. Database administrators making unauthorised changes to data, or system administrators making changes to the system configurations that resulted in system behaviour change, have been common issues over the years.

With the proliferation of internet and multiple external touch points, external threats and cyber attacks have grabbed much of the attention in the last decade. Cross site scripting and SQL injections are the two most common techniques used by hackers. People also tend to share a lot of confidential information inadvertently on social networking sites and blogs.

There have been cases where these forums have been methodically used to extract information under the guise of friendships or interviews, or against financial favours.

Inadequate IT infrastructure also poses serious risks from another very significant perspective. Organisations without any backup strategy, disaster recovery sites or contingency plans face the risk of coming to a standstill if any of their production infrastructure stops functioning.

Overloaded infrastructures, carelessness in maintenance of production systems, and hardware beyond the warranty period or without annual maintenance contracts are all common cases of vulnerabilities.

Risk management programmes are ongoing and evolving. The success of such programmes in the industry today depends on the commitment of senior management, the effectiveness of the assessment and monitoring processes, and the periodic enhancement of the framework.

While the success of such programmes goes unnoticed, the failures are disastrous. As a result, however unglamorous they are, they have to be successfully adopted. **ACN**

---

*Abhijit Pendse is Senior Engagement Manager at Cedar Management Consulting International*