Managerial mindset often the biggest threat to IT security

When it comes to a secure IT environment, managerial mindset often poses the biggest threat, explains Marthinus Engelbrecht, CEO of NEWORDER Industries, a local technology company that provides specialised enterprise risk management and pen-testing services to companies in Africa and abroad.

"It would seem logical that management in any business would understand that building a secure organisation is important to business continuity, long-term success and sustainability. Unfortunately, in many organisations, IT security is still seen as an IT issue and not a business one," he says.

Damage to reputation

The impact of security and confidentiality breaches can make or break an organisation. "It's not just the finances at stake. Aside from the costs associated with resolving a security incident, especially if it leads to litigation, and the financial burden of fraud, other factors can severely damage an organisation's ability to operate or damage its reputation beyond recovery."

There's also the common mindset is that if there are firewalls, intrusion detection systems and antivirus programmes in place, IT security is taken care of. "This is a naive approach that leaves a company, its systems and data as vulnerable as if there were no interventions in place," Engelbrecht warns.

Complying with legislation

The biggest challenge for local companies in 2013 will be to implement measures that comply with local legislation - such as the Protection of Personal Information Bill - and conform to governance standards. However, failing to conduct adequate testing or implementing required safeguards will result in companies being more vulnerable to the following attack vectors in the coming year:

- Targeted attacks - corporate entities will be increasingly targeted and face three main attack vectors: data theft, espionage and sabotage.
- Data theft and loss - data equals money in the wrong hands. Corporate entities will be targeted for confidential and client information.
- Malware - malware is getting much more sophisticated and used for financial and destructive gain.
- Hacktivism - online activists will join forces with physical demonstrators to target public figures, industry leaders, and corporate entities, and launching information theft attacks - just to 'make a point'.
- Smartphone attacks - attackers will improve their craft with a focus on mobile banking attacks. For example, consumers may eventually see SpyEye and Zeus, two Trojan banking attacks, migrate from the computer to the smartphone.

"With IT-related theft and fraud on the rise, a bare minimum approach isn't good enough and IT security needs to be elevated to a higher business priority," he concludes.