Protecting profits through proactive risk management

South African executives are well aware of the importance of risk management in every area of their businesses. Unfortunately, most are of the view that reacting to attacks after the fact is an acceptable form of managing risk.

"Reacting to risk is simply admitting criminals got the better of you," says Hedley Hurwitz, MD of Magix Security. "The only risk mitigation strategies that work are those that identify suspicious events and raise the alarm before any damage is done."

He adds that many companies, while having the latest technologies available, seem to practice risk management in the same manner they did years ago. In today's turbulent world, effective risk management must cover all points of business vulnerability through an integrated 360-degree view.

Operating reactively requires the business to wait until an audit is done before it realises something has happened. By then the harm is done and the perpetrators have vanished.

Hurwitz notes that almost all aspects of business operations today depend on computer systems, whether it's finance, HR, IT, administration and so forth. The most effective way to manage risk proactively is through these systems as they relate to the company's infrastructure, data and people.

Doing a risk assessment on the corporate infrastructure is the first and most important step in managing the threats companies face. Furthermore, protecting your data requires specific tools and knowledge, as well as insight into the processes through which legitimate users access and use the data.

In managing people risk, employers can't simply assume their employees are all honest. Seamlessly monitoring employees as they go about their jobs allows companies to spot anomalies in their operating procedures and highlight suspicious activity without being intrusive and hindering productivity.

When you have real-time data as well as the knowledge of what legitimate activities happen in the course of the day, it's a simple step to monitoring this information and identifying suspicious activities. It's no longer about waiting until someone discovers something has happened, but examining and identifying the context of countless daily business events to identify the few that go against the norm.

Once identified, set processes can then be activated to protect the company from financial or other losses, while the appropriate people investigate and deal with the matter.

"A solution of this nature is not possible when companies react to historic

events, but only to those which have identified areas in which they are at risk and proactively monitor and manage those vulnerabilities," concludes Hurwitz. "With their finger on the pulse of daily operations, businesses can not only improve their productivity, but reduce potential damages and protect their profits."