New aspects of cyber intelligence

Deloitte in the Western Cape hosted a chief information officers' breakfast in Cape Town late last week, entitled 'Technology Trends of 2011 - The natural convergence of business and IT'. Led by Mark White, principal US consulting chief technology officer, Deloitte Consulting.

White said that despite the growing global requirements for cyber security, protection of data and privacy, most companies are not adequately equipped to identify and deal with breaches.

He went on to deal with trends that will affect and dictate the way businesses approach their information and communication technology. He said that companies must constantly adapt and take a proactive approach to stay ahead of the rapid developments in the sector.

"Chief IT officers today need to be more than just stewards of the business and strategists. They have to be aware of the potentially disruptive capabilities of cloud, social computing and mobility that are changing the world of business and transforming how business is done.

Amongst the major concerns of CIOs should also be the fact that most vulnerabilities facing corporates are assessed and acted upon according to past events. "They are not based on emerging cyber threats or on the actual risk profile of organisations. Protecting vital information assets demands a 'cyber approach' that covers a full spectrum of functional issues. A 'protect the perimeter and respond when attacked' mentality is no longer sufficient.

"Cyber intelligence today represents a vastly more sophisticated and full set of threat management tactics. They take the v step of providing tools to move to a more proactive threat awareness posture that looks beyond existing corporate horizons

Cyber intelligence, for full effectiveness, should be considered over four areas in 2011 and into the future, namely: cyber security, cyber forensics, cyber analytics and cyber logistics.

Cyber security

Here the emphasis must move away from perimeter intrusion and protection, identity and access management solutions, manual technology solutions and the traditional role of the chief information security officer as a technologist with deep domain knowledge, but without a seat in the boardroom.

"Cyber security is now increasingly framed as a combination of architecture, practices and processes, with equal focus demanded on internal and external threats.

"Highly integrated tool sets and investments in cyber analytics have helped identify previously undetectable exposures. Automatic identity management tools are incorporated into day-to-day tasks, including smart cards, biometrics, and fingerprint and handprint scanners. As befits the changing demands of the environment, the role of the CSO has also changed, demanding a blend technology and leadership skills," he says.

Cyber forensics

The challenges of cyber forensics, previously based on the premise that incident investigations would conclude, once root cause analysis were determined and cleaned and self-contained analysis was rarely used to augment existing controls or update policies, has also moved beyond the host to the network layer.

"Cyber forensics is now looking at the network layer and determining the source of malware. This is correlated with other internal and known external threats using cyber analytics in an attempt to inform of future vulnerabilities."

Cyber analytics

Where previous challenges were a reactive approach, based on situational awareness and descriptive analyses and an understanding of the values of business analytics, cyber analytics has moved to a situation where it is now predictive, prescriptive and a part of a closed loop cycle of continuous refinement based on other cyber intelligence activities.

"Cyber analytics in 2011 is an established tradecraft of analytics, reinforced by the realisation that threats and opportuniti are often hidden in plain sight."

Cyber logistics

Prior to 2011, these were typically limited to deal signings and cursory annual audits and typically notable in manufacturin reliance on ever-changing sub-contractors and small hardware providers, each with their own risk profiles, which created potential weaknesses upstream in the supply chain.

Personnel checks occurred only during hiring or contracting processes, with clearance processes mainly handled by larg unknown third parties. "Cyber logistics in 2011 has moved to include extensive analysis to identify, assess and mitigate ris posed by vendors subject to foreign ownership, control or influence or other significant concerns prior to purchases being made or contracts being entered into.

"Continuous auditing of suppliers, including organisation structures, corporate activity and on-going verification of the integrity of goods is at the forefront of concerns. Finally, cyber intelligence strategies are in place that includes provisions for personnel security, and automated reinvestigation of executives and privileged roles," he concludes.