Call for 'cyber warriors' to fight fraud

With a dire lack of skills to counter South Africa's spiralling instances of cyber fraud, it is little surprise that the country ranks third among those most targeted for cyber attacks. So claimed Professor Basie von Solms, director of the University of Johannesburg's (UJ) Centre for Cyber Security, in reaction to the 2012 Norton Cybercrime Report. The report places South Africa hard on the heels of China and Russia as a favourite plundering ground for cyber criminals.

Image: Free Digital Photos

With developments such as extra broadband, a growing number of mobile applications and the establishment of numerous technology hubs, South African cyber space will become increasingly attractive to offenders, unless the threat is substantially diminished.

This alarming situation was highlighted at a talk to alumni of UJ's Academy of Computer Science and Software Engineering last week, delivered by Von Solms. His address follows news of tens of millions of rands worth of losses experienced by South African shops, restaurants and hotels, caused by a new variant of the malware known as Dexter, on payment card systems.

Von Solms noted that cyber risk has escalated so dramatically, it has risen from 12th to third position on the Lloyd's 2013 Risk Index Report of concerns to global business. The report states that the most costly cyber crimes involve malicious code, denial of service and web-based attacks exploiting vulnerabilities.

Holder of multiple awards and author of numerous reports on information security, Von Solms advocates the united efforts of industry, government and academia to tackle the crisis and build desperately needed skills in the field of cyber security.

He has called for the formation of a platform on which all three entities can work to fill critical gaps. "Capacity building is at the core and is urgent," he stated, pointing out that demand for cyber security expertise worldwide is currently 12 times higher than the requirement for IT professionals. Countries that recognise this includes the UK, where 11 centres for cyber skills development, allied to universities, have been established. The Indian government is currently sponsoring the training of 500,000 "cyber warriors" while South Korea is churning out 5,000 cyber specialists a year.

Awareness campaigns crucial

Von Solms said that campaigns to up awareness of cyber security issues are essential. The public, especially new users, are not sufficiently aware of ID theft, phishing schemes, cyber stalking and at a social level, bullying. Governments and industry, he said, are rolling out mobile systems throughout Africa without cautioning customers of fraud dangers. A campaign to be commended is that of the South African Cyber Security Academic Alliance, which educates youngsters, in indigenous languages, on cyber risk. UJ is a founding member of this alliance.

Von Solms called for proactive cyber counter-intelligence in both government and business spheres. "It is clear that traditional, reactive approaches to information security are not enough anymore, and more aggressive methods must be designed to go out there, identify attackers and their motives." He also criticised the government for dragging its feet in effecting legislation.

The National Cyber Security Policy, which has been approved by the government, remains under wraps. The Electronic Communications and Transactions Act of 2002, presently being rewritten, defines the concept of cyber inspectors to ensure national cyber security, but to date has not been fully implemented, mainly a result of the skills shortage problem.

Von Solms also suggested that the establishment of a parliamentary committee on cyber security to review the safety of government and business systems, and provide a platform for ordinary citizens to seek recourse when victimised by cyber crime. "Such a committee should hold oversight hearings at which government and business can be held accountable for the security of the systems they roll out, and where ordinary citizens can testify about their cyber problems, such as identity theft and financial losses," he stated.

Just back from a sabbatical at Oxford University's newly established Global Centre for Cyber Security Capacity Building, Von Solms said that research at the UJ Centre for Cyber Security in some instances exceeds work being undertaken in the UK. "South Africa had the ability to be playing in the big league of cyber security," he stated.