Cyber attacks are a growing risk to South African economy

With the expansion of broadband services and increasingly widespread Internet access, however, the country is becoming incredibly attractive to cyber criminals

JOHANNESBURG, SA, SOUTH AFRICA, February 14, 2014 /EINPresswire.com/ -- Nowadays cyber-space is a part of everyday South African life. Internet access can be found in schools, hospitals, government offices, public and private organisations and households. With the expansion of broadband services and increasingly widespread Internet access, however, the country is becoming incredibly attractive to cyber criminals: South Africa has been ranked as one of the least protected online countries in the world. Cybercrime has a very negative effect on the South African economy, affecting its productivity, national security and its appeal as a place for investment.

IT Governance SA, the global leader in information security and ISO27001 compliance products and services, highlights the fact that the South African government is not doing enough to regulate cyber security or to decrease cyber risks for South African organisations. Although the Electronic Communications and Transactions Act 2002, which enforces cyber security in South Africa, is now being rewritten, there is uncertainty about when it will become law.

IT Governance SA says that ISO27001 addresses the gap in cyber security that has arisen in South Africa. ISO27001 is the best-practice specification for an Information Security Management System (ISMS), which helps companies protect their assets, improve efficiency, identify vulnerabilities, and also strengthen and develop information security best practice.

According to the South African Cyber Threat Barometer 2012/13, the lack of cyber security knowledge or a national internet security policy in South Africa is making the country vulnerable. It is unsurprising that the country ranks as the most targeted globally for cyber-attacks (after Russia and China) according to the Norton Cybercrime Report of 2012: South Africa suffered numerous high-level cyber attacks in 2013, including the hacking of SANRAL in which 1 million e-tag users' full names, car registration numbers, mobile phone numbers, physical addresses, PIN's and other sensitive information were stolen. The city of Johannesburg's municipal government billing system was also hacked and thousands of citizens' bank account details had been found to be accessible to the public.

Nine steps to success: An ISO27001 Implementation Overview outlines the nine essential steps to an effective ISMS implementation and provides effective advice for an ISO27001 project. IT Governance also suggests downloading the free Information Security and ISO27001 Green Paper, which will increase information security knowledge for organisations that want to avoid cyber threats.

Ilenia Vidili
IT Governance
448450701750
email us here