

Cyber crime a national crisis

Cyber crime is a national crisis costing the country a billion rand a year, a law firm said on Wednesday, 23 October.

The FBI in the US listed South Africa as the sixth most active country where cyber crime took place.



Cyber crimes are a major threat to South Africa.
Image: chanpipat [Free Digital Photos](#)

Informal consensus within the private sector saw South Africa ranked third, behind Russia and China, Dave Loxton head of business crime and forensics at Werksmans, told reporters in Johannesburg.

He said that within the next two to three years the proceeds from cyber crime would outweigh those from all other forms of white-collar crime combined, as it had grown exponentially and would continue to do so.

"Cyber crime is any crime involving a computer or the Internet. South Africa had proven to be a particularly fertile ground for cyber crime as it is a lawless society," he said. "Cyber crime syndicates know that law enforcement was paper-thin, and the chances of being arrested and successfully convicted were low," said Loxton.

He said it was rare for cyber criminals to operate alone as they were normally part of a syndicate being run like a business. "Cyber crime is linked to other illegal activities such as drug running and human trafficking," he said.

Law enforcement lax

Loxton said that comparing the FBI's cyber crime enforcement to that of the South African police was like comparing "chalk and cheese".

"We are generally dealing with highly intelligent, sophisticated people. It is a national crisis," Loxton said, adding that the syndicates find it quite easy to operate in South Africa because of a lack of law enforcement resources.

The government and private sector needed to recognise that there was a problem and, following that, throw resources into combating cyber crime. Citizens needed to recognise that the threat of cyber crime exists and use their own common sense when working online.

He said the government needed to train police and prosecutors to know how to successfully investigate, arrest and prosecute cyber criminals.

"The private sector needed to have the necessary skills in-house to deal with potential threats and implement policies to reduce their exposure to crime," he said.



David Loxton. Image: Werksmans

Billions stolen each year

The Norton security firm estimates that about US\$110bn was lost worldwide to cyber crime.

"It started off with guys hacking for fun and the people started realising they could make a fortune. Suddenly the whole process changed," Loxton said.

One of the new trends people needed to be aware of was the abuse of social media.

He estimates that about 600,000 Facebook accounts worldwide are compromised daily. "About 1.5m people are victims of cyber crime daily, equivalent to 18 people a second," he said.



Passwords need to be strong. Image: Stuart Miles
[Free Digital Photos](#)

Password crackers

"The big concern is that the compromise is taking place because of a lack of common sense," Loxton added.

He advised people to stop using simple passwords based on birthdays, surnames and other information readily available to cyber criminals. "These criminals know that people chose passwords which were easy to remember," he said.

"The software [to crack passwords] is there. One needs to have strong, strong passwords," he added.

He conceded that while people were using Internet security and anti-virus software on their computers, they neglected their smartphones, tablets and other mobile devices used for social media, business and communication.

"Often someone buying a new smartphone, for example, would ask about the screen size, but not about its security features," he said.

Loxton said South Africa's banking sector was "superb", as the major banks had strong internal forensic services.

"I think our banks are superb. However, they can't provide answers for their customers stupidity," Loxton said.

Source: Sapa via I-Net Bridge

For more, visit: <https://www.bizcommunity.com>