Cyber-criminal activity in Africa is a reality

Advances in technology across industries are yielding significant opportunities for cyber criminals, both organised and otherwise, said KPMG.

Image: Free Digital Photos

Said Kajen Subramoney, associate director of KPMG in South Africa and specialist in Forensic Technology Services: "Considering the evolution in technology and the digital age we now find ourselves in, the traditional 'stick-'em-up' bank robbery, for example, has evolved into a far more sophisticated crime - often resulting in lower risk, greater anonymity and even greater financial rewards for such cyber criminals than before. Today, organised criminals tend to focus on the use of an array of services offered in what we call the 'cyber underground' - a criminal cyber network and syndicate that needs to be recognised by both consumers and business alike to mitigate risk."

For financial institutions, bank accounts and credit cards are the main targets of such crime. In fact, one such financial crime, committed in 2013, simultaneously targeted multiple locations throughout the world, pointing to how criminals relied upon a combination of unrivalled knowledge of ATM systems, processes and the technological prowess of a criminal network.

Continued Subramoney: "Here, hackers gained access to the bank's databases to compromise hundreds of credit cards linked to seemingly legitimate bank accounts. Apparently with the help of insiders, the hackers were able to gain remote access to a terminal to increase the daily ATM withdrawal limits on each of the cards to more than US$100 000.

By exploiting this weakness in the bank's IT security, the hackers essentially created the availability of "fake money", which could then be accessed through magnetic strip cards with appropriated codes, via ATMs around the world. You can imagine the amount of money withdrawn here and all the while unchallenged."

A foretaste of things to come

According to KPMG, this type of robbery is a foretaste of things to come. "We know that criminals are not only acting unilaterally, but today are buying and leasing the services of cyber criminals, and expanding their networks far and wide, using tactics and tools where the criminal literally becomes invisible."

Mirroring this sentiment, Jason Gottschalk, associate director of KPMG said: "Africa has the strong potential to become a hotspot for cyber-crime, especially now that the continent is well recognised on the global map and investment in Africa is becoming rife. This reality could pose a threat on critical infrastructures. In fact, KPMG feels strongly that the cyber security issue is the 'invisible war' that should be a top-of-mind priority for local businesses now, in order for them to protect themselves."

Globally, KPMG has seen that cyber-criminal activity and security is on the rise, where the topic is now on almost on all board agendas. Continues Gottschalk: "These discussions should be leading businesses, in particular, to an outlook of approaching cyber security proactively. Organisations need to undertake internal business IT security infrastructure audits, defining what their security strategies should be and then taking steps forward to implement this."

According to KPMG, one of the biggest concerns within the local environment around IT security is the "reactive" versus the "proactive" approach that the brand sees among businesses. Said Subramoney: "This has to change. Cyber-criminals are becoming smarter and, with this, are finding new ways are performing such criminals attacks daily - ways that we wouldn't think could be possible, yet can cause severe damage."