Corporate South Africa still not taking cybercrime seriously enough

Business's growing reliance on technology is driving an exponential growth in cybercrime—but companies in both the public and private sectors are not taking the threat seriously enough, says David Loxton, Partner at law firm Dentons SA in Johannesburg, specialising in corporate investigations and compliance.

"Technology drives the world, which means business and government need to invest not only in systems but also in the capabilities to keep those systems safe from increasingly sophisticated and well-funded criminal syndicates," Loxton says. "By and large, corporate South Africa is not making the investment needed, so it is vulnerable. When clients consult me about fraud, cybercrime (and their vulnerability to it) is the common denominator."

Although cybercrime is often unreported, research shows it is growing alarmingly. Figures from Symantec, a leading software security company, indicate that in 2015 more than 500 million personal records were stolen or lost, phishing attacks targeting employees increased by 55 percent while the use of ransomware increased by 35 percent.[1] South Africa suffered the most cyberattacks on the African continent in 2014, with losses estimated to be in the region of R50 billion, according to Norton, Symantec's parent company.[2]

Surveys typically list theft (of money and assets), financial-statement fraud and corruption as the top three white-collar crimes globally, and in South Africa. "In my experience, however, because technology is the transactional platform for most – if not all business – cybercrime cuts across these boundaries, making it the most prevalent category of corporate fraud," says Loxton.

Challenges in curbing cybercrime

Shortcomings in the justice system pose a particular challenge when it comes to cybercrime. The Dark Web is faceless and borderless, and police lack both the resources and specialist skills to take on complex, multi-jurisdictional investigations. Another factor is the fact that the legal framework is very much on the back foot when it comes to cybercrime; because the world of technology is moving so fast, the laws under which to prosecute criminals often do not exist or are inadequate, both nationally and internationally.

"For all these reasons, prevention is definitely better than cure when it comes to cybercrime," he argues. "Companies should be proactive about using technology to protect themselves and at least limit any damage. Thus, for example, intelligent software exists that analyses all financial transactions as they occur, so anomalies are immediately flagged for investigation. This kind of software can also provide deep analysis of company data to uncover some of the common white-collar frauds that can cost companies millions over long periods of time. The multinationals are definitely investing heavily in protective technologies but I fear South African companies are not, a short-term approach with potentially devastating long-term consequences."