Is your company protected from cyber crime?

South African enterprise is no stranger to the phenomenon of cybercrime. In light of numerous high-profile data breaches, it is evident that digital espionage is on the rise.

Alex Roberts, Regional Director of Sales and Operations at CURA Software Solutions,

In fact, the South African Banking Risk Information Centre (Sabric) estimates that South Africans lose R2.2bn to internet fraud and phishing attacks annually. As cybercriminals are getting smarter, and employing more insidious means to get their hands on your valuable intellectual property, it is a business's imperative to implement constant controls against potential cybercrime - or run the risk of catastrophic consequences.

Failure to adapt or adequately police controls could be costly to an organisation on multiple levels. Aside from the cost of recovering stolen information, data loss could result in potential fines, penalties or litigation for the company.

In the event of a breach, the business may experience a drop in stakeholder confidence and dwindling trust.

Companies don’t only lose customers during a cyber-attack; a tarnished brand reputation also diminishes their potential to acquire new ones along the line. Worse still, capturing your IP could result in the elimination of a competitive advantage that has historically set the business apart.

Alex Roberts, regional director of sales and operations at CURA Software Solutions, stresses that the damage of cybercrime depends largely on how resilient a company is, and how comprehensive their cyber-risk strategy is.

“It is crucial to test how robust your controls are continuously, and in the event of any controls failing, an airtight business continuity plan must be in place. Security is no longer just an IT function; it is a fundamental business process that should be aligned to business objectives. As such, it is essential that cybersecurity is embedded and upheld across the entire organisation.”

It is critical to note that even if businesses have the most stringent systems and processes in place, a lack of security awareness among employees can be a serious risk. Seventy percent of all cyber-attacks are enabled by human error, so it is important to create a business culture which prioritises cybersecurity.

“Cybercrime doesn’t start with IT, it starts with people. It is the responsibility of all departments to be vigilant, and this requires educating your employees consistently through training, awareness and maintaining active conversations. It is also important to educate employees on best practices for passwords and to turn on features such as multi-factor authentication.”

The simplest of security steps must be upheld, such as regularly updating operating systems, backing up files regularly, implementing advanced authentication and encrypting all sensitive data. Cybersecurity should be discussed often at the highest levels while regimentally measuring controls against potential outcomes.

Further to this, a communications strategy to clients, employees and the general public in the event of a data breach should be disseminated. When it comes to cybersecurity, the old adage applies: prevention is better than cure.