# The journey of cyber defence

Cybercrime has become a global epidemic from which Africa has not been spared, leaving companies counting losses which range from money to credibility. Corporates across the continent need to take urgent action to prevent these outcomes, but too few are yet making the management changes needed to ward off the threat.

©weerapat kiatdumrong via 123RF

“The vast majority of successful attacks are a result of an absence or lack of a well-defined cyber security strategy or poor implementation of such a strategy,” says Derek Schraader, risk advisory Africa leader of cyber risk services at Deloitte.

“For African organisations to be vigilant, resilient and secure, a holistic pro-active approach to the evolving cyber threat landscape is required,” he says, “and in developing a cyber-security strategy and framework, special care should be taken to make provision for current and evolving threats.’’

## Arms race with hackers

Schraader says cyber security involves far more than just understanding the capabilities and exposure of existing and emerging information technologies. Extensive Deloitte research reveals it involves understanding that you are in an arms race with hackers and it is imperative that you understand everything about the business and know exactly what your greatest assets and biggest risks are so that you can focus and manage your investments to address relevant cyber threats.

“Improving cyber security is not a one-time solution,’’ he says. “It’s a journey – for IT leaders and business decision makers alike. Figuring out which steps to take can sometimes prove to be challenging decision for any organisation, however there are essential steps that all organisations must take to improve their online security.’’

A report by Deloitte identifies five steps that could help create an organisation that operates securely, that remains vigilant in the face of cyber threats, and that can show resiliency when attacked. The staggered approach emphasises pragmatic solutions, that are industry-specific and that deploy the right people, processes, and tools to address known and emerging cyber threats.

## Steps to transformation

Businesses that take these five critical steps can transform themselves to become more secure, vigilant and resilient.

- Focus on what matters: Understand critical assets and interactions.
- Proactively assess your cyber risk: Know how to detect threats whether conventional or emerging.
- Build a multi-layered defence: Your cyber strategy must address a combination of defenses for all stakeholders.
- Fortify your organisation: Patch holes, develop stronger software and ensure physical security.
- Prepare for the inevitable: Focus on incident management for various test cases.

Becoming a secure and resilient organisation not only requires these five big, important steps, but also constant and consistent assessment to mitigate any clear and present threats to the organisation.

“Economic conditions are very tough and it is understandable many corporates are focusing on the bottom line. However, they are falling into perilous waters if they do not take the cyber threat just as seriously," says Schraader.