Why defending against hackers is an uphill battle

Cybercrime is a swamp of statistics. The Microsoft Digital Crimes Unit reported that 531,000 unique phishing URLs were taken down in 2022 and 70 billion email and identity threats were blocked.

Anna Collard | image supplied

Google reported that global cyberattacks increased by 38% in the same year, with a cost of $10.5 trillion expected by 2025. Cybercriminals have the advantage. They pick the time, the method and the vulnerability.

They only have to find one hole in a company's defences, or one person who falls for a phishing email, and they have won. For the organisation, says Anna Collard, senior vice president of content strategy and evangelist at KnowBe4 Africa, it can feel like a losing battle.

"But it is not," she emphasises. "Yes, the attackers can use automation, artificial intelligence (AI) and sophisticated attacks, but these tools are also available to those on the other side of the fence. Organisations can also benefit from AI and automation, and leverage their intelligence to filter attacks, prioritise responses and manage overall security. It is a cat and mouse game – sometimes the organisation wins, sometimes the hacker."

For Collard, the real challenge is not at the edge of the battle, at the wall where the onslaught takes place. It is the lack of skills. Security professionals are in short supply and the role itself tends to be thankless, challenging and stressful. If the company remains secure with no breaches and robust defences, security does not hear a word, but the moment something happens, all eyes are on the security team.

#EcomAfrica: Boardroom confidence in cybersecurity crucial for e-commerce success

Imran Salie 21 Apr 2023

“A lot of security professionals suffer from anxiety and health problems because it is a demotivating, stressful and demanding career,” says Collard. “There has to be a shift towards recognising the intense complexity that surrounds the cybersecurity role and focus on interventions to mitigate the high staff turnover and the resultant risks this introduces, and increase the number of skilled people entering the profession.”

The gap between talent and retention is widening, not least because security used to be about understanding networking, firewalls and anti-virus. Now it is a complex dance that asks for insight and understanding across multiple environments, stakeholders, service providers and solutions. This is made even more challenging with the influx of hybrid and remote working frameworks and human error.

“People have poor passwords, weak security on their home devices, click on phishing links, accidentally share passwords and so much more,” says Collard. “Yet the business still thinks that everything has to be handled by security or the IT person. They are expected to handle all the IT problems in the company and then security on top of that – it is an impossible ask.”

Winning the cybersecurity battle is more than just holding the digital fort against the invaders, it is a strategic investment into security systems, employee training and security personnel. One that aligns the people factor with the security factor so that those defending against the cyberattack are engaged, supported and prepared to mitigate the risks and manage the threats.