Every person should think like a hacker

It is the individual who plays the single most important role in keeping the company secure.

Relevant cybersecurity isn't perpetuated exclusively through investment and systems, it is reliant on people and their understanding of the cyber threat. A leading ethical technology hacker in Europe, Jamie Woodruff, gained access to a well-known financial institution by simply posing as a pizza delivery man. He was quoted as saying that it is the mistakes that people make that are the true threat to the business.

That said, it is people like Woodruff who can provide the organisation with the insight required to pre-empt attacks, find hidden loopholes and educate employees. These ethical hackers know how to play the game of cybersecurity thrones. They understand the methodologies and the mindsets of those who make a living from penetrating business defences unlawfully and use this understanding to reshape security infrastructure and investment.

"The role of the ethical hacker has evolved considerably over the past few years," says Karien Bornheim, CEO of Footprint Africa Business Solutions (FABS).

"In the past, they would be hired by organisations to ensure that their security was capable of withstanding a concerted

attack and, in some cases, find out if they had already been breached. Many organisations only discover that they've had a breach years after it has taken place. Today, the ethical hacker has added to their arsenal - their skills have evolved and so have the methods they use. Not only are they penetrating the front lines of defence, but they are also launching attacks from the inside of the organisation."

There has been a subtle shift from the slide in and out pentesting of the past when ethical hackers would attack organisations over a period of a few days or weeks. Now, many undertake long-term undercover assignments that embed them into the company. These are the ethical hackers that become part of the culture so they can identify the insider threats that are affecting the organisation, and even identify the source of ongoing security challenges.

Many ethical hacker training courses specialise in undercover training into very specific technology skill sets that allow them to find the bigger threats to the organisation, particularly those perpetrated by employees.

Inside threats

The insider threat is a very real problem. According to CA's Insider Threat 2018 Report, 90% of organisations feel that they are vulnerable to an insider attack, 53% have had confirmed insider attacks, and 27% have seen an increase in frequency. This has sparked significant internal investment into insider threat programmes that focus on deterrence, forensics and user behaviour monitoring.

"Ethical hackers are capable of immersing themselves into the culture of the business. They use this to detect behaviour that could potentially indicate if someone is an insider threat," says Bornheim. "Their skills allow them to find digital proof of misdeeds and rapidly detect certain system issues or behaviours. Those who take on these roles can spend months or even years at an organisation protecting it both from within and without."

That said, in spite of their security expertise and experience, many organisations remain reluctant to hire external ethical hackers and grant them access to their information. It's an understandable concern. Many ethical hackers have moved from the so-called black hat (criminal) side of hacking to the white hat (legal) side and bring with them a suitcase of smart skills that few companies want to see thrown at their cybersecurity walls. However, this discomfort is the precise reason why the business should be paying attention and the bill.

"These individuals do command high salaries but what they offer the organisation in terms of reputational and cost-saving benefits, cannot be understated," says Bornheim. "Should they discover a bug, a loophole, an existing piece of dangerous code, or any other threat to the company, they can save it millions."

The average cost to the company, according to IBM's study - Costs of Data Breaches Increase Expenses for Businesses, is around $US3.86 million for a data breach. This cost has risen since 2016 by 6.4% and will likely increase again over the next 12-24 months. Any company facing that reckoning at the end of a cybersecurity hack from a black hat will suddenly see the bill that comes from a certified white hat like a missed opportunity.

"Certified ethical hackers operate under very strict ethical controls," concludes Bornheim. "They report any issues or information they find and help the organisation to put more stringent or relevant controls in place. The ethical hacker is ultimately a weapon, one that can be safely wielded by the untrained to defend the organisation against future attacks, to rebuild systems and security platforms, and to uncover insider threats. Their role is as critical to the development of a robust cybersecurity stance as the software, solutions and training that are embedded into the human, machine, server, and system."