ornico
KNOW HOW TO GROW

| Publication | | |
|---|---|---|
| JSE - SUPPLEMENT | | |
| **Page** | **Date** | **AVE (ZAR)** |
| 40-43 | Mon 01 Apr 2019 | 123305.54 |


# SAFETY CATCH

SA corporates must become far more proactive when it comes to securing data

**BY TONI MUIR**

**PHOTOGRAPHY** GALLO/GETTY IMAGES

Employee behaviour – whether accidental or malicious – is the biggest threat to data privacy and security in SA, says Dragan Petkovic, security product leader at ECEMEA Oracle. 'Industry estimates put nearly half of all security breaches down to inadvertent human error. These attacks are usually conducted through phishing, whaling and other attacks that rely on unsuspecting end-users to click on links to infected websites, or open attachments that install malware or ransomware.'

Rohan Isaacs, director and head of technology at Norton Rose Fulbright, agrees that people are at the centre of the problem. 'People, primarily employees, who don't receive proper training and awareness in cyber vigilance pose the biggest threat. Even employees who have been trained are human and make errors that cybercriminals exploit. Most cyberattacks occur through employees unintentionally giving cybercriminals access to systems.'

Wilmari Strachan, an executive in the technology, media and telecommunications department of ENSafrica, feels differently. 'The biggest threat to data privacy and security is the lack of compliance with data privacy legislation,' she says. This is because SA's data privacy legislation, the Protection of Personal Information [POPI] Act of 2013, is not yet fully operational, she adds.

The POPI Act affects how companies store, process and use personal customer data. While enforcement of the act is imminent (hopefully by 2020), businesses are already working to ensure compliance. Section 19, which pertains to security safeguards, stipulates that organisations take appropriate measures to protect personal information against loss, damage or unauthorised destruction, as well as unlawful access or processing. In short, the responsibility lies with the business to keep its security and data protection current and to ensure that anybody who handles data on its behalf does the same. The POPI Act is based on the EU's General Data Privacy Regulations and is therefore in line with international standards.

'Even though the right to privacy, including the protection of personal information, should be a known concept, companies often do not internalise the complexities of POPI in their organisation's design and processes. This is a core risk,' says Ahmore Burger-Smidt, director at Werksmans Advisory Services, head of its data privacy practice group and co-author of a Commentary on the Protection of Personal Information Act, published by LexisNexis. As well as a lack of understanding of the POPI Act's implications for business, the fact that cybercriminals 'do not stand still and are always looking for the next opportunity offered by a vulnerability in company systems' leaves companies exposed, she adds.

Danie Strachan, partner at Adams & Adams, believes that when the POPI Act does come into force, it will solve some but not all of SA's cybersecurity problems. 'Sure, it will set a standard for organisations when they process information, but the law is mainly aimed at corporates that process personal information – not criminals.' Companies have an obligation to deal with information responsibly so that criminals cann ot access it and thus, once the POPI Act is in place, it will be more difficult for criminals to access information because of those strengthened systems at company level, he adds. 'Responsible corporate citizens should, out of a moral obligation, look after their customers – and staff – by ensuring their information is protected. But there will probably be a huge, collective sigh when POPI is implemented, because then companies will realise they now have to do something about it.'

Elizabeth de Stadler, a founding director of Novation Consulting, believes companies are not adequately aware of the risks associated with insufficient data security. 'Most companies underestimate the cost of a data breach. They tend to focus on regulatory fines and legal costs, adopting a wait-and-see approach to POPI. But in fact, your biggest cost will be loss of profits, the cost of the investigation and reputational loss,' she says. 'Last year IBM did a security study in which they found that the average data breach costs R36.5 million. The lion's share of that figure is loss of goodwill, and that has nothing to do with whether legislation is in place or not.'

According to Oracle and KPMG's Cloud Threat Report 2018, which explores the security challenges faced across the globe and how businesses are

'DATA SHOULD BE ACCESSED ON A NEED-TO-KNOW BASIS ONLY, BACKED BY A LEGITIMATE INTEREST'

DRAGAN PETKOVIC, SECURITY PRODUCT LEADER, ECEMEA ORACLE

responding to these, as well as the technology solutions that are enabling them to resolve these threats, participating organisations reported experiencing a wide range of cyberattacks over the past 24 months. However, email phishing took the top spot as the attack vector that was experienced most often during that period. Of the companies surveyed in the report, two-thirds (66%) suffered a significant business operations interruption in the past two years, with 90% of firms saying that at least half of their data is sensitive information. In addition, 38% reported issues detecting and responding to cloud security incidents.

'Cloud adoption has expanded the core-to-edge threat model,' says Petkovic. 'An increasingly mobile workforce accessing both on-premises and cloud-delivered applications and data dramatically complicates how organisations must think about their risk and exposure.' He argues that more attention needs to be paid to practising minimum privileges. 'Data should be accessed on a need-to-know basis only, backed by a legitimate interest,' he says. 'These access rights should be reviewed periodically and revoked when not required.'

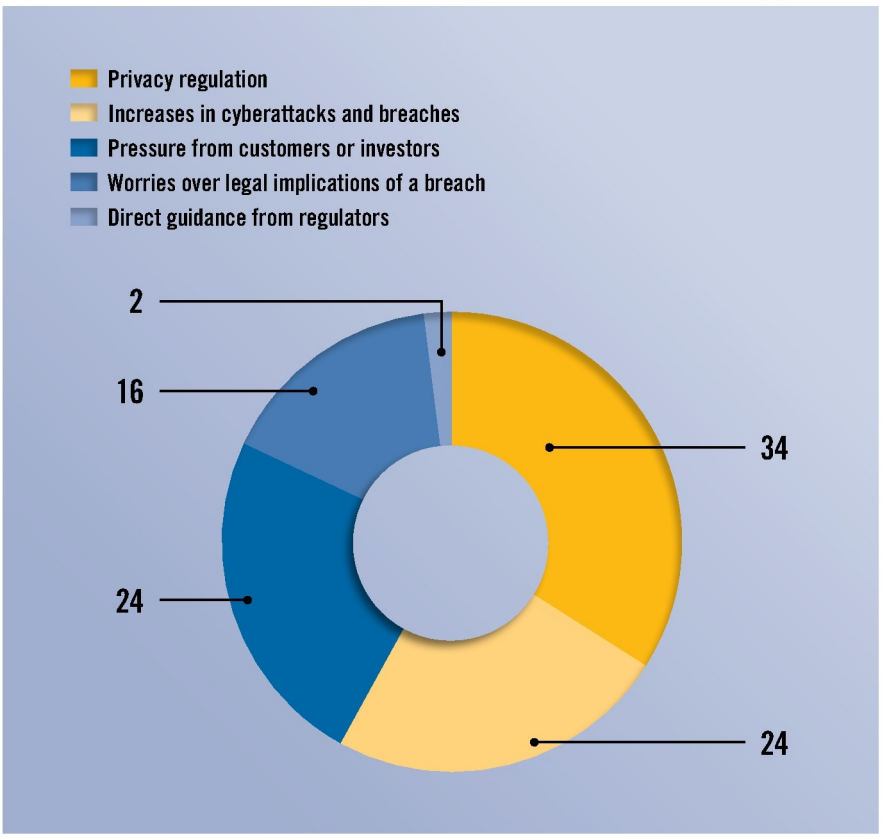
Strachan agrees, adding that companies should carefully consider who has access to customer files, what files and sensitive information staff members take out of the office, and what might lie around on workstations or at reception, as these are also vulnerable areas. He highlights that the more information a company collects from its customers, the higher its risk of exposure should it suffer a security breach. 'The bottom line is this: companies should not be collecting information that they do not need,' he says.

Strachan argues that insufficient data security has less to do with awareness and more to do with complacency. 'Companies think data breaches won't happen to them,' he says. 'This is an ignorant approach. People think of a hacker as someone sitting in their garage bent over a computer, but that's not the case these days – just think of the ransomware type of cybercrime. If you get locked out of your systems you won't be able to pay suppliers or staff, or access your data, without first paying a ransom.'

Another problem is that while companies know these threats exist, they do not fully comprehend the extent of the risks they pose, he says. 'They might think hacking is a threat to big corporates only. But ransomware can happen to anyone and it can shut down your entire business. Cyber breaches happen in various forms.'

## DRIVING FORCES

**THE FACTORS INFLUENCING CYBERSECURITY SPENDING BY SA ORGANISATIONS (%)**




*Source: FICO*

Experts agree that to adequately protect the data they hold, companies should ensure that their employees receive proper training and that they fully understand the importance of complying. Companies must also establish what information they process, how they process it, how they store it, what they do with it, how they share it and how long they retain it, as well as who has access to it and under what circumstances. Passwords and encryption, along with strong IT systems, should be non-negotiable.

In late 2017, the private personal data of up to 60 million South Africans, some deceased or no longer living in the country, was compromised when a database named 'masterdeeds' was publicly leaked online, exposing identity numbers, contact details, addresses and income estimates. Last May, close to 1 million records of SA citizens were exposed online, including similar information to the 'masterdeeds' leak, but this time revealing plain-text passwords. In international news, data breaches at behemoths Google and Facebook made headlines for months.

'Data breaches can happen at any company, no matter its size, geographical location or industry,' says Petkovic. 'Businesses have to be far more proactive when it comes to protecting data, especially customer data.' And when it comes to 'closing the holes attackers exploit', the value of penetration testing to find them and expedited patching to close them is well understood. 'In fact, penetration testing and patching more frequently are the two actions cited most often as having had the most positive impact on an organisation's cybersecurity posture.'

Firms can make every effort, but laws must still prevail. 'When POPI is brought into force this will be a major step forward for data privacy,' says Isaacs. 'The Cyber Crime Bill, which is also not yet law, will be a significant advance on current laws dealing with cybercrimes. Until these pieces of legislation are in force though, legal protection in South Africa remains patchy. Until then, there are limited legal consequences for data breaches and limited ability to investigate and prosecute cybercrimes.' ■