ITWeb

ITWeb's 2019 Information Security Survey

IN ASSOCIATION WITH VMWARE

vmware®

ITWeb events

ITWeb SECURITY SUMMIT 2019

Business-driven compliance, risk determine security spend

The impact of traditional IT factors on security spend is diminishing amid an increasingly complex business risk landscape.

BY KIRSTEN DOYLE

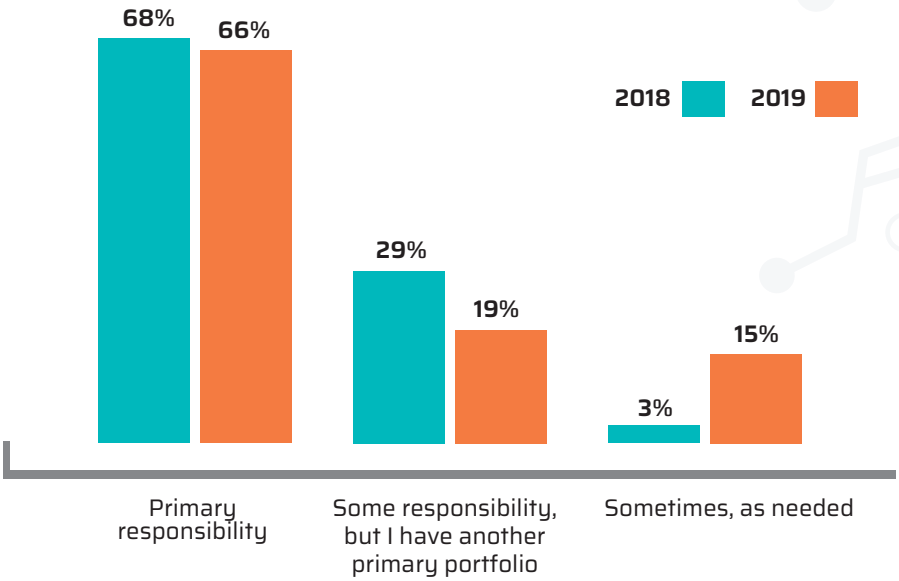
A staggering 57% of South African organisations participating in this survey suffered a phishing attack in the past year, with 39% falling victim to a malware incident. DOS or DDoS was an issue for 20% of CISOs, and ransomware attacks surprisingly plummeted to only 17%, from 46% in 2018.

However, when it comes to insider threats or staff-related incidents, under a third (28%) say they have experienced this threat. In fact, under half of respondents (42%) say they have not had any insider issues, and only 17% claim unauthorised access has been a problem.

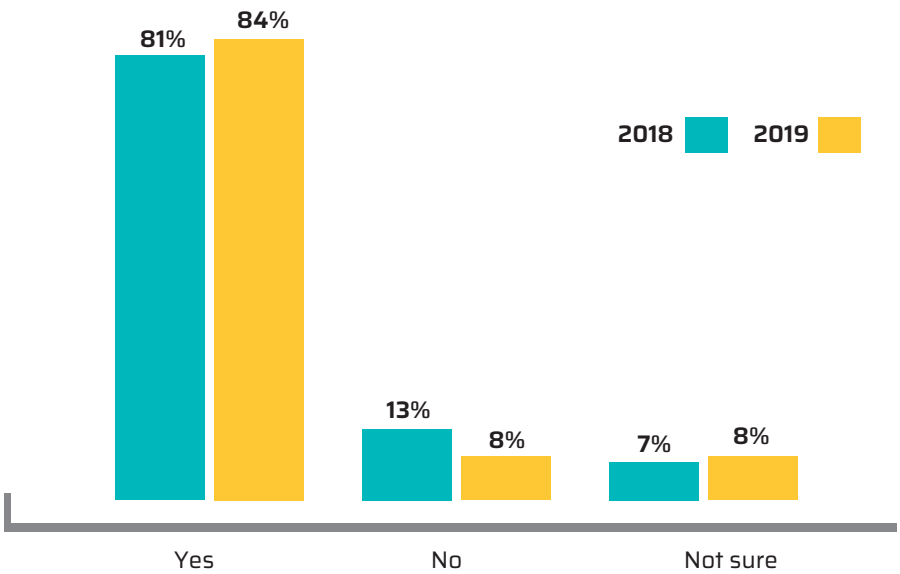
The survey also shows a marked improvement in preventing the loss or leakage of confidential data (13%, down from 44% in 2018), as well as the misuse of confidential data (12%, down from 40%)

Despite these positive findings, respondents still claim insider attacks remain their greatest security risks – however, the percentage plummeted to 29% from 73%. Next came e-mail viruses (14%, down from 42%) and uncontrolled portable devices with 13%, dropping from 47% previously.

To what extent are you responsible for oversight and day-to-day-operations of the cyber security programme at your organisation?



Do you carry out security risk assessments through a recognised framework or standard?



Cost, and lack of time, remain the top two factors that delay investment in IT security.

Driving spending

The effects of an increasingly stringent regulatory environment and the introduction of GDPR and PoPI are having an effect. When asked to single out the primary driver for security expenditure, 22% of CISOs cited compliance, versus only 14% in 2018. Protecting customer information dropped from 24% to 19%, as did maintaining data integrity, with only 9% citing this as opposed to 15% last year.

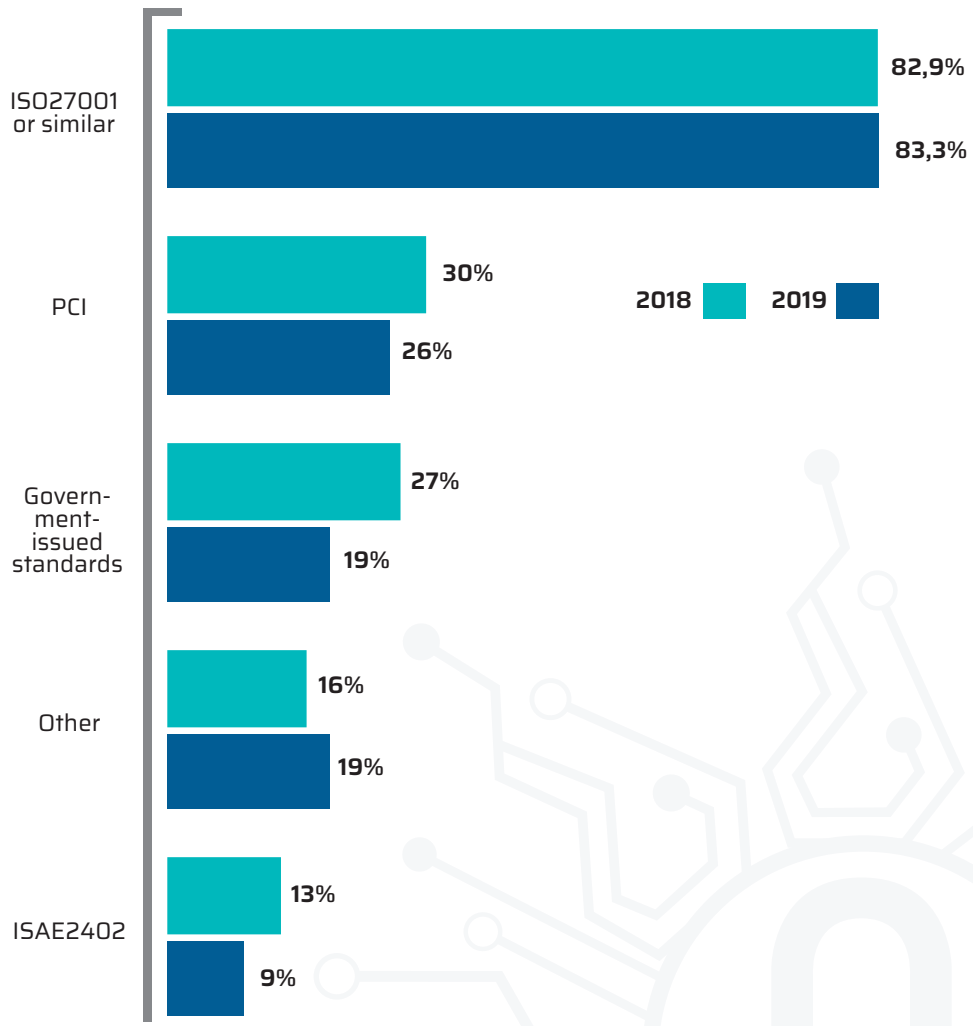
"Traditional IT drivers are down," comments Gareth James, network and security sales specialist at VMware South Africa. "Business driven compliance and risk are now driving spend."

However, when asked how confident they are that their business is ready to comply with PoPI, only 27% say they are 'very confident', with nearly a third (31%) being 'somewhat confident', while 11% are either highly concerned or somewhat concerned about their organisations' compliance readiness.

What governance and risk management practices do businesses have in place?

The vast majority (69%) say they have some formal cyber security policy in place, a marginal decrease from 71% last year. Most (70%) also cite having carried out a risk assessment within the

Which standards and good practice guides have you implemented?



past year. Just over a half of companies appear to have a CISO on board and, encouragingly, cyber risks have been promoted into the enterprise risk register by 58% of respondents (up from 52% in 2018.)

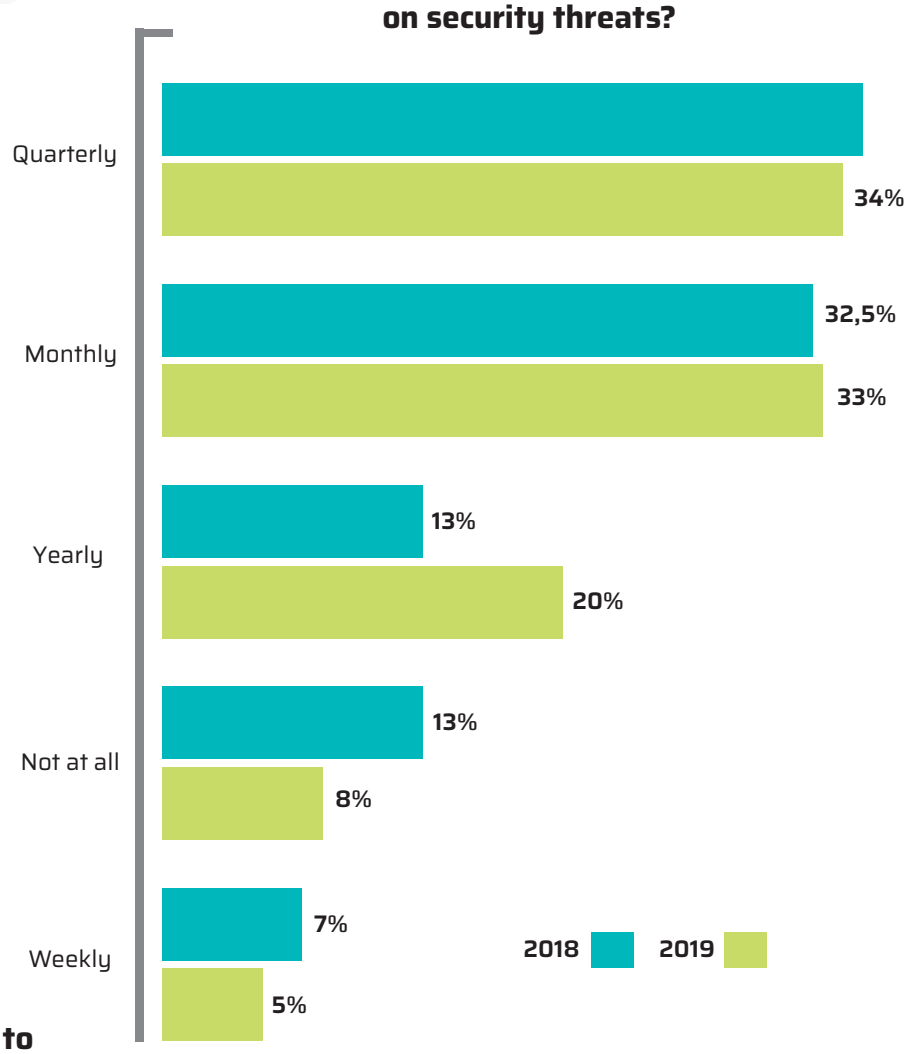
When asked which standards and good practice guides have been implemented within their organisations, ISO27001 remains the most popular choice, followed by PCI and government-issued standards.

Assessments, insurance

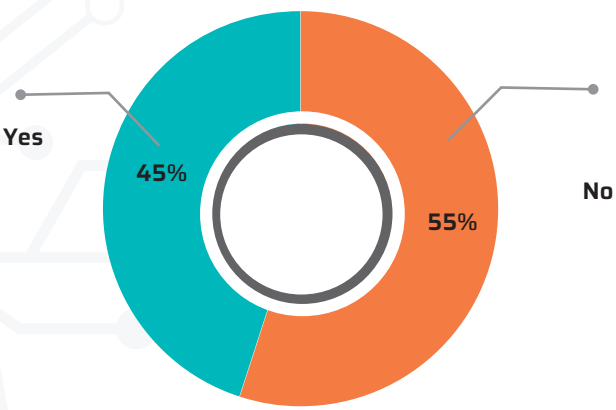
In terms of security assessments, most South African companies perform these once a year or once a quarter. Only 15% claim to do an assessment once a month, and 3% say they do no assessments at all.

On the plus side, when it comes to the speed of remediating security breach events in general, almost half (48%) say they could do this 'fairly quickly', while 16% say 'extremely quickly'.

How frequently do you provide training to staff on security threats?

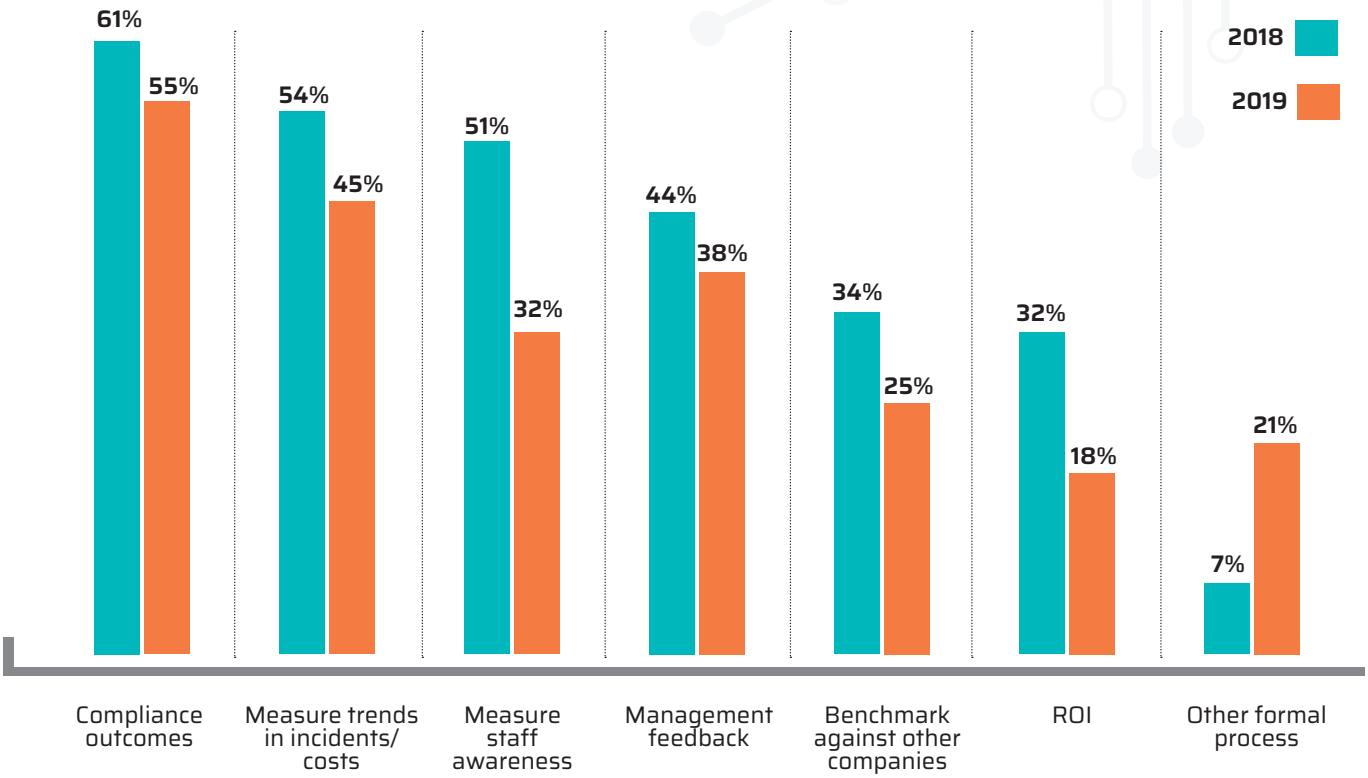


Do you have a formal process to measure the effectiveness of your security expenditure?

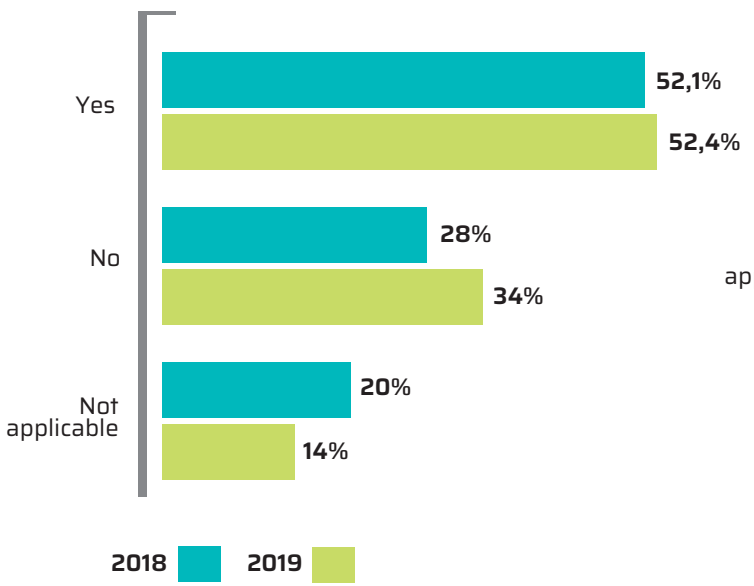


69% say they have a formal cyber security policy in place.

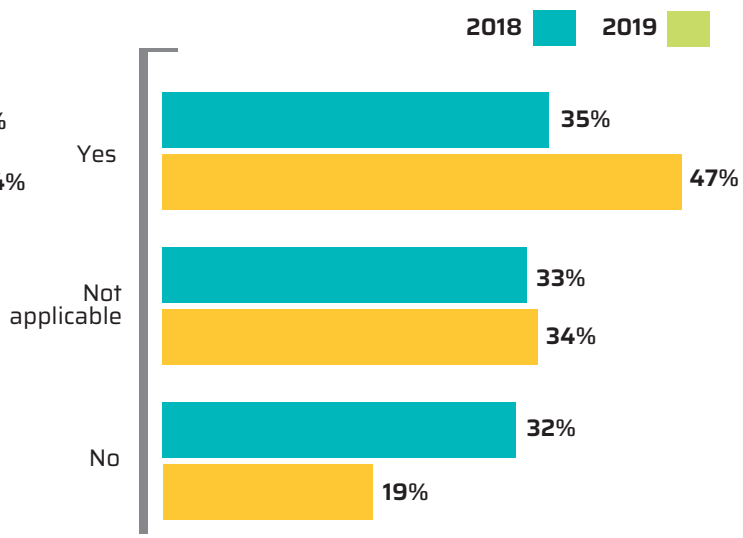
How do you measure the effectiveness of your security expenditure?



Does server virtualisation limit the visibility of traffic flows in your data centre? (In other words, can you see VM to VM network traffic?)



Does SD-WAN factor into how you do branch security planning?



Cyber risks have been promoted into the enterprise risk register by 58% of respondents.

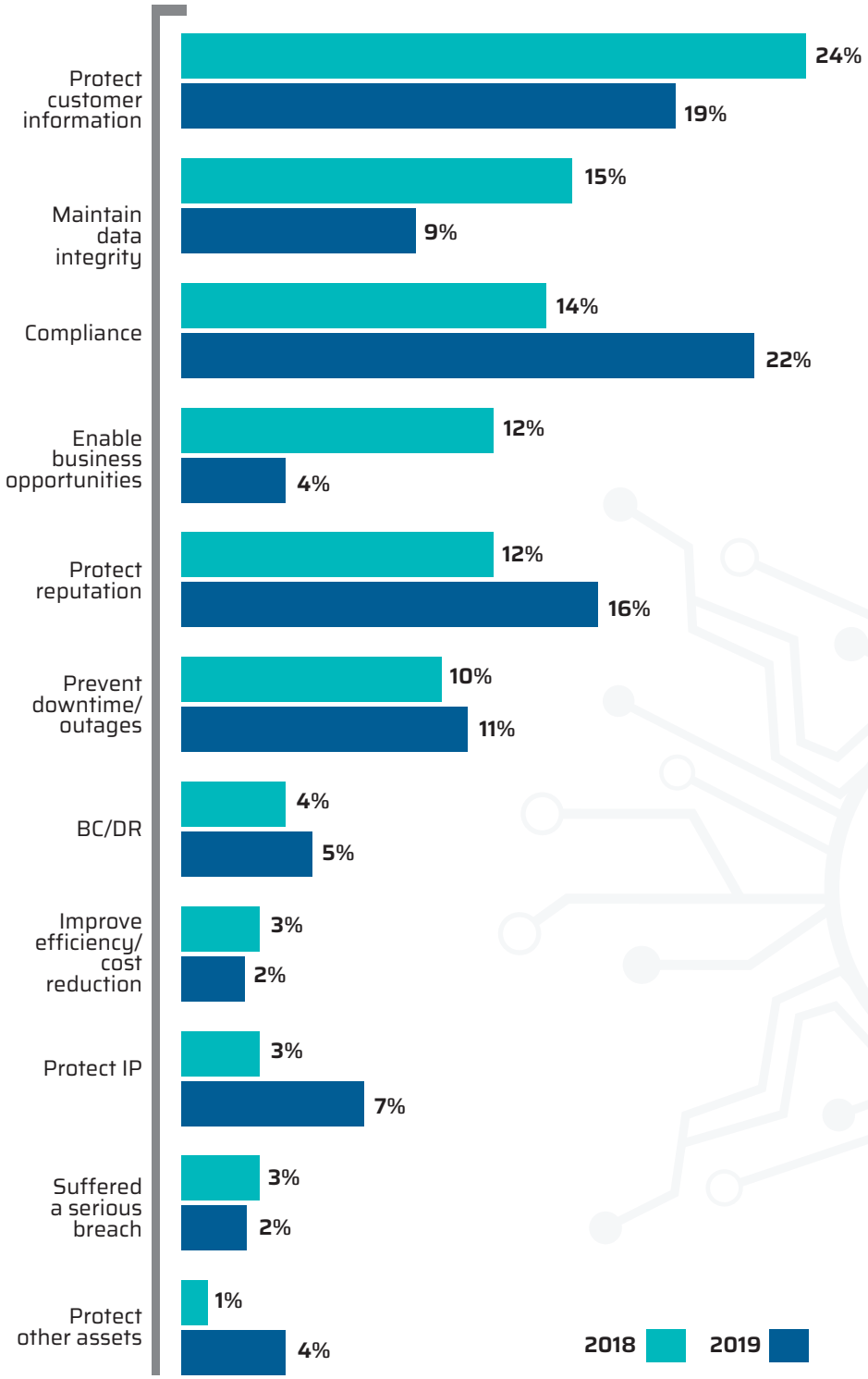
In terms of cyber insurance, fewer organisations appear to be seeing the value, with only 30% this year saying they have specific cyber insurance in place, a drop from 42% last year. A quarter of respondents say they would like it, but can't justify the costs, and 11% simply don't see the need.

Tools, solutions

As for security tools being used, it seems most South African businesses have a smorgasbord of solutions on board, although almost all (98%) make use of a firewall, 88% have endpoint protection, and 86% have anti-malware in place.

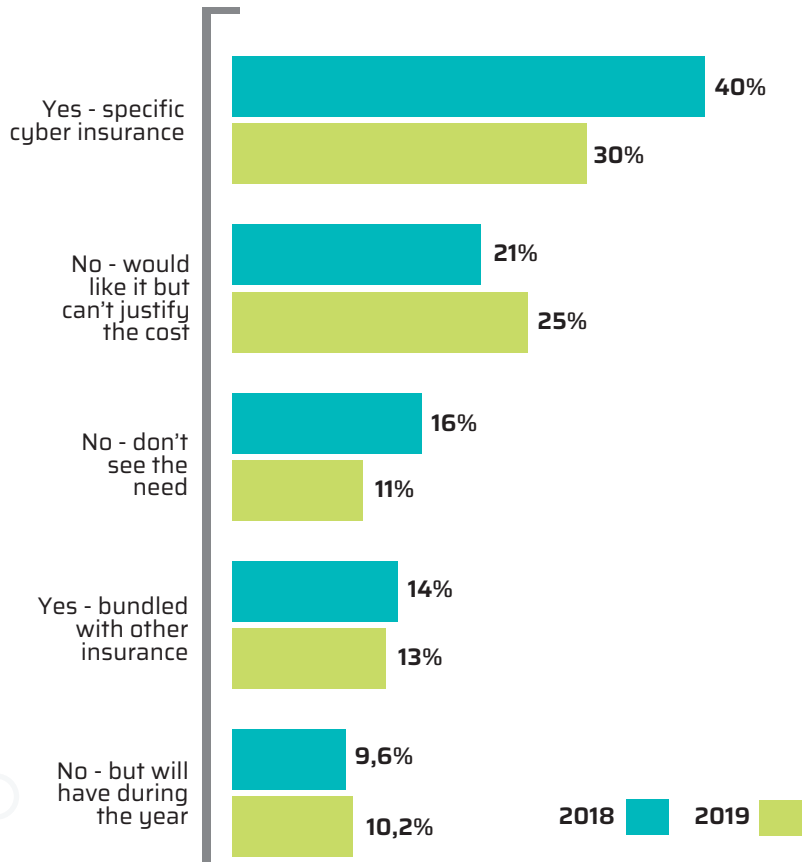
Speaking of measures businesses have taken to mitigate mobile device risk, 54% say they have issued a policy on mobile devices, and a further 45% say they have a defined strategy in place.

What is the primary driver for your security expenditure?

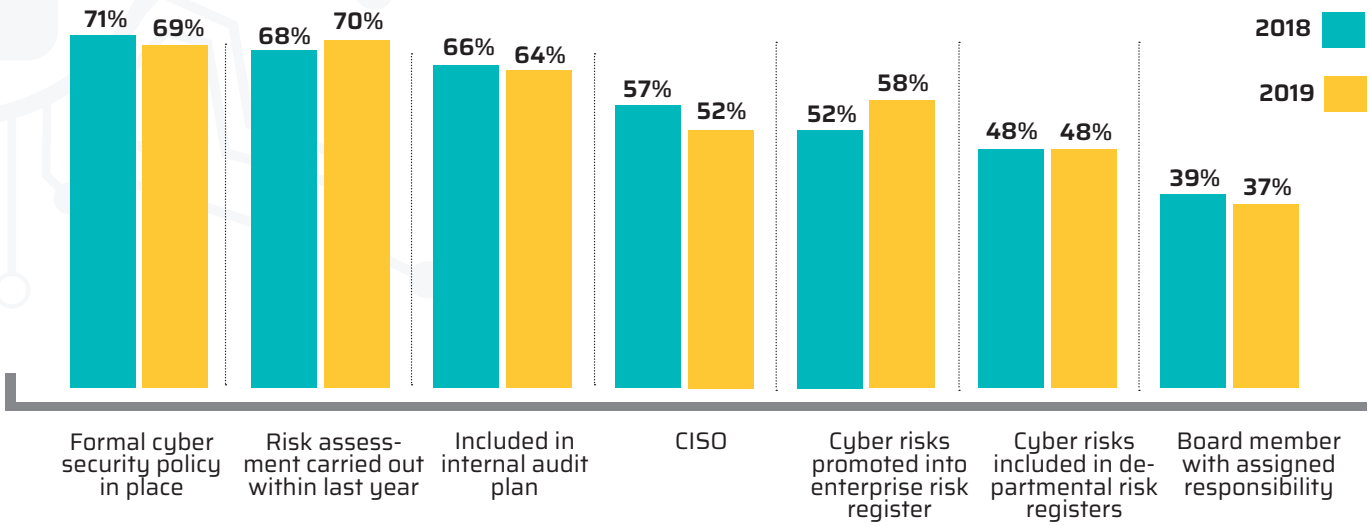


There's been a marked improvement in preventing the loss or misuse of confidential data.

Do you have cyber insurance?



What governance and risk management do you have in place?



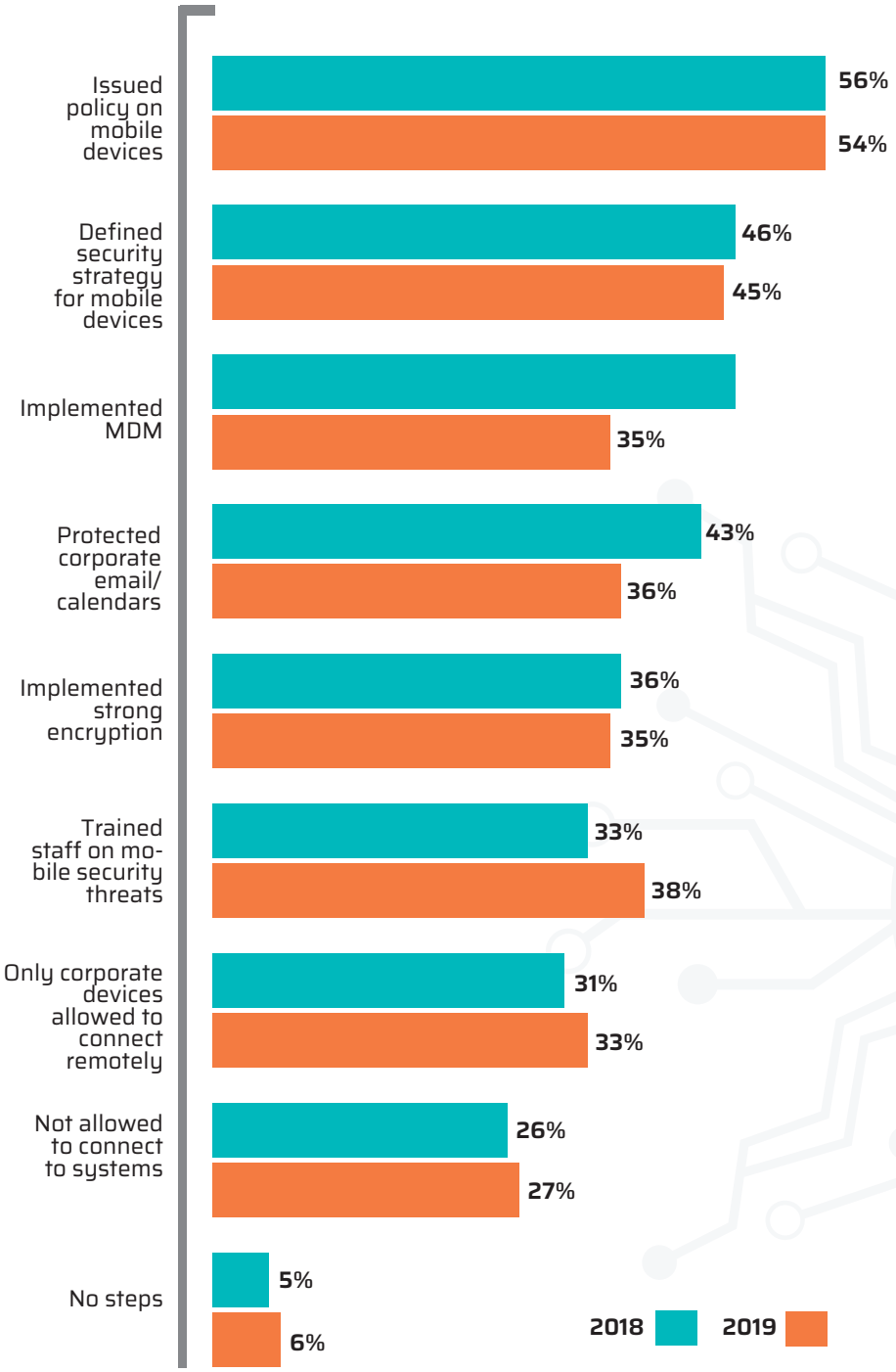
48% of CISOs claim they could remediate a security breach 'fairly quickly'.

Those who have implemented MDM dropped from 46% in 2018 to 35% this year. When it comes to encryption, not much has changed, with 35% having this measure in place. Similarly, only one third of respondents say they train their staff on mobile security threats.

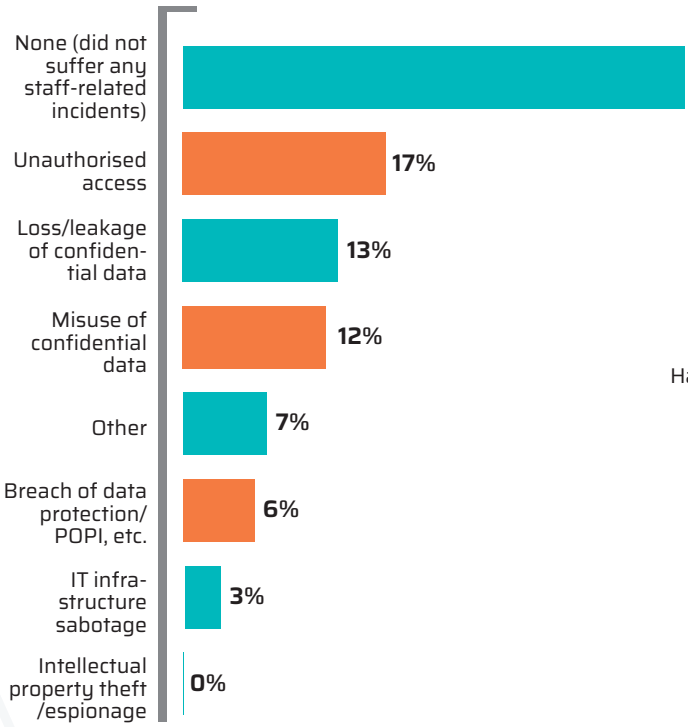
Unsurprisingly, time and money remain the greatest barriers to security investments, with the costs involved being cited by 72% of respondents, the difficulty in determining ROI by 45% and not enough time by a further 27%.

Though the 2019 survey shows cyber security programmes are improving, says Garth James, network and security sales specialist at VMware South Africa, most respondents (48%) still give it only a 'three' out of 'five'. Only 6% of the respondents rate their programme as being fully mature. ■

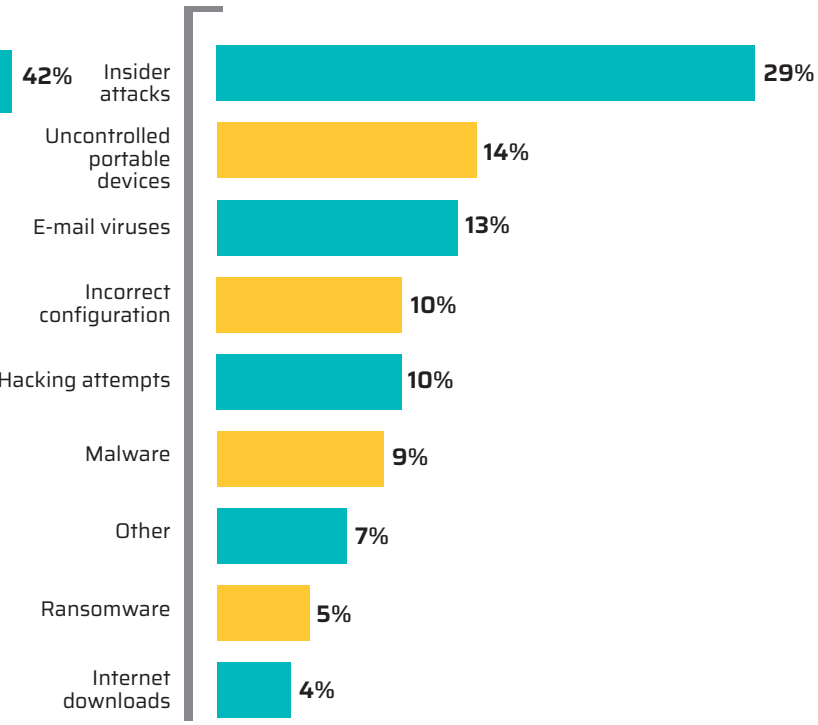
What steps have you taken to mitigate mobile device risk?



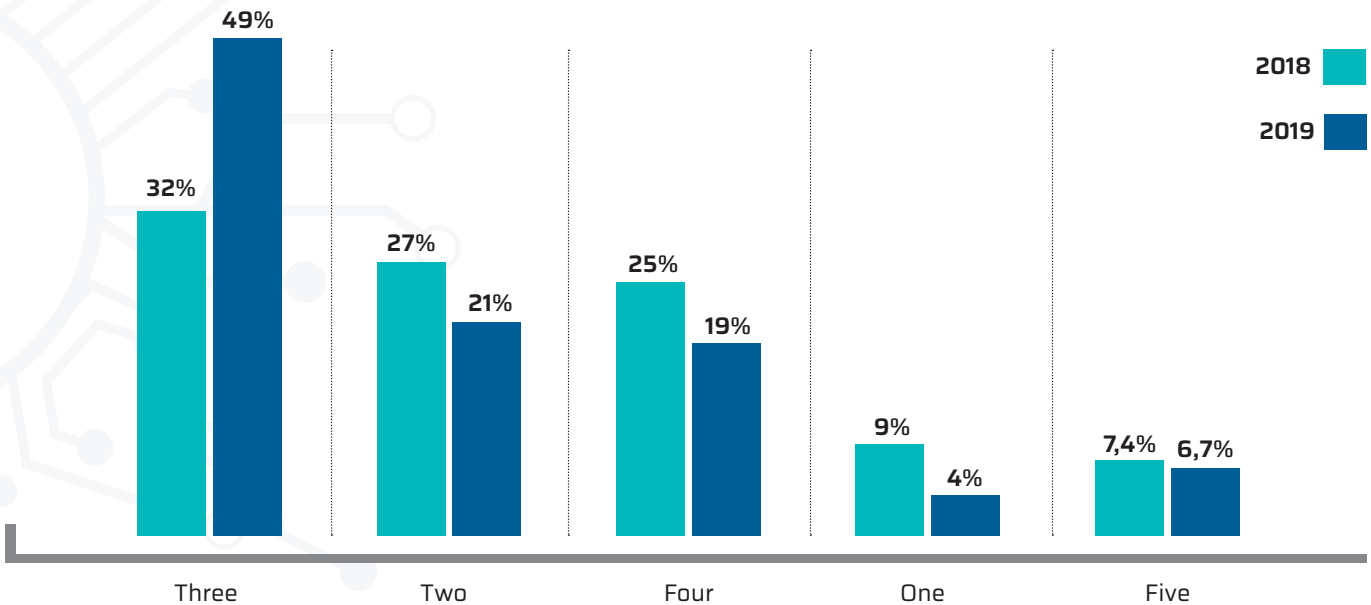
What, if any, staff-related incidents did you suffer?



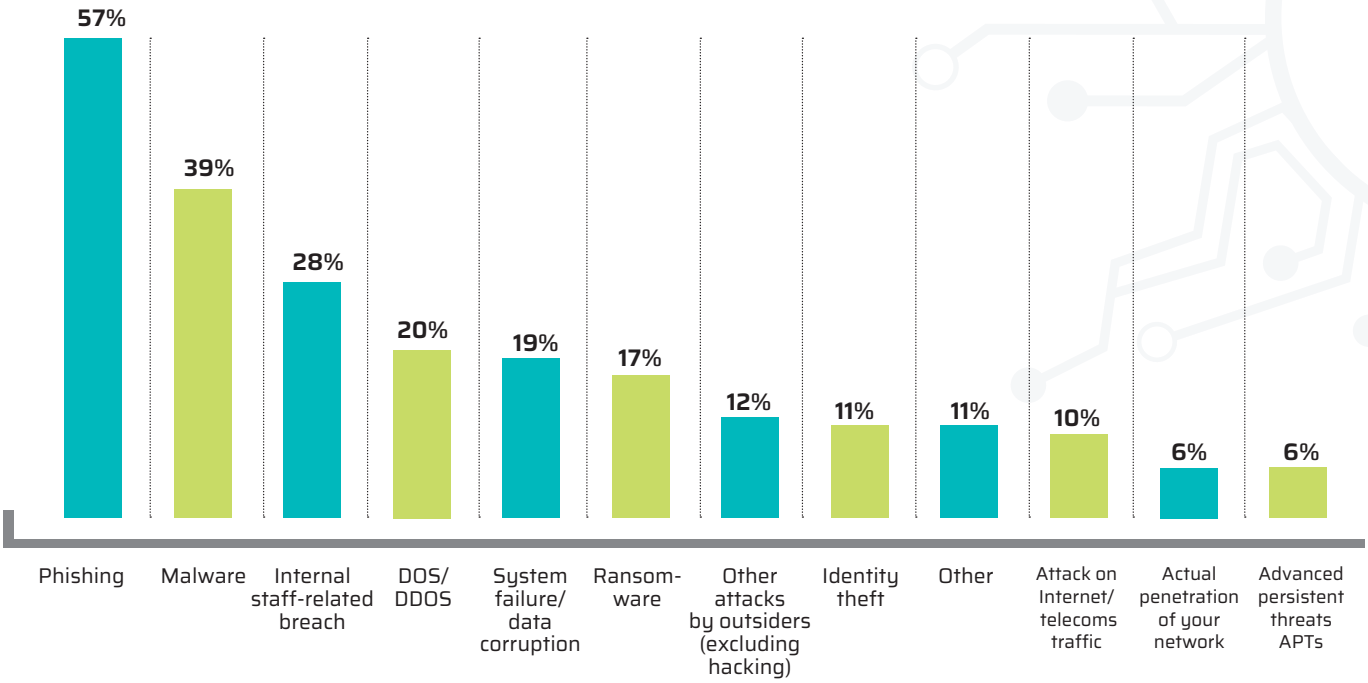
What do you consider to be your greatest security risk?



What maturity level is your organisation's cyber security programme currently? (1 = Lowest, 5 = Highest)



Which of these security breaches/outsider attacks did you suffer in the past year?



35% have strong encryption in place to mitigate mobile device risk.

About the survey

ITWeb's second comprehensive Information Security Survey, in partnership with VMware, was run online during April 2019. It was by invitation only, targeting predominantly chief information security officers (CISOs) and equivalent C-level decision-makers in South Africa's public and private sector organisations.

- The survey captured input from 118 cyber security professionals, up from 62 last year.
- One third are C-level execs and a further 44% are mid-level managers.
- Most respondents work in the financial sector, followed by IT and government.

The full research report 'The State of Cyber Security in South Africa' will be available from ITWeb in July 2019.

Credits

Publisher
Jovan Regasek

Survey development, research and analysis
ITWeb's technical and editoral teams

Editorial director
Ranka Jovanovic

Writers
Kirsten Doyle
Ranka Jovanovic

Sales director: ITWeb Events
Debbie Visser

Production
Sindiso Khupe

Layout and design
Sane Louw

PUBLISHED BY
ITWeb Limited
www.itweb.co.za
326 Rivonia Boulevard,
Rivonia, 2128
TEL +27(0)11 807-3294
FAX +27(0)11 807-2020