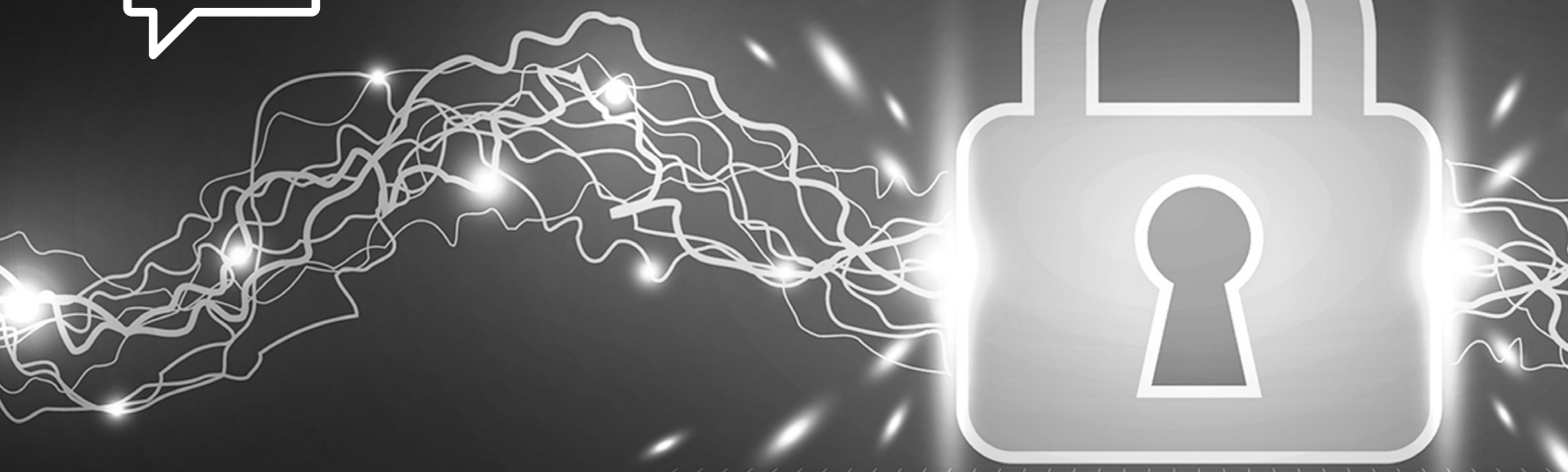
ITWEB'S 2018 INFORMATION SECURITY SURVEY

IN ASSOCIATION WITH VMWARE



vmware®

iTWeb events

iTWeb SECURITY SUMMIT 2018

Key findings

CISOs view insider attacks as the greatest security risk to their businesses, yet less than half have data leakage prevention solutions in place.

By Kirsten Doyle

Over three quarters of South African businesses experienced phishing or other impersonation attacks over the past year, proving this scourge is still rife and a favourite among cyber criminals.

In addition, 24% of CISOs said their organisations had suffered a DDoS attack in the same time period, and 18% said they had been affected by attacks on their Internet and telecoms traffic.

These are some of the findings of the ITWeb, VMware security survey, aimed at gauging the current state of cyber security readiness in South Africa, by polling the very people who are in charge of their companies' security – CISOs and equivalent C-level executives.

Top threats

In terms of security breaches, more than half the respondents (52%) said they had experienced malware attacks, and 46% said they had fallen victim to ransomware.

> "CISOs are recognising that by far the biggest risk is the insider.

Surprisingly, the main culprit was not the notorious WannaCry ransomware that brought companies across Europe to their knees last year. In fact, 76% said they were not affected by WannaCry at all, while 20% claimed they were somewhat affected, and only 4% said they experienced drastic effects.

"Whether it affected them or not, the majority of companies – 59% – have altered their security posture based on the 'wake-up call' that WannaCry presented," comments Gareth James, network and security sales specialist at VMware South Africa.

"We can see that a quarter of companies didn't have their patching up to date and were susceptible to the lateral attacks that WannaCry perpetuated using a weakness in the Microsoft Server Message Block protocol," he adds.

Gareth James, network and security sales specialist at VMware South Africa

The insider threats

Just over a third of respondents (37%) said they had suffered an internal, staff-related breach. The main way insiders did damage was through the loss or leakage of confidential data (44%), followed by unauthorised access at 38% and misuse of confidential data at 40%.

CISOs also view insider attacks as the greatest security risk to their businesses, with 73% citing this, followed by uncontrolled portable devices at 47%, malware at 46% and email viruses at 42%.

James says the insider threat is made up of an equal number of complicit or malicious employees who deliberately steal information or damage systems, and unintentional culprits, who do things such as write their passwords on a Post-It notes. "Nearly half of the respondents lost data last year – largely due to weak internal protections."

46% of respondents have fallen victim to ransomware

He says it is no coincidence, then, that CISOs are recognising that by far the biggest risk is the insider. Of the respondents, roughly three quarters have the insider as their greatest threat.

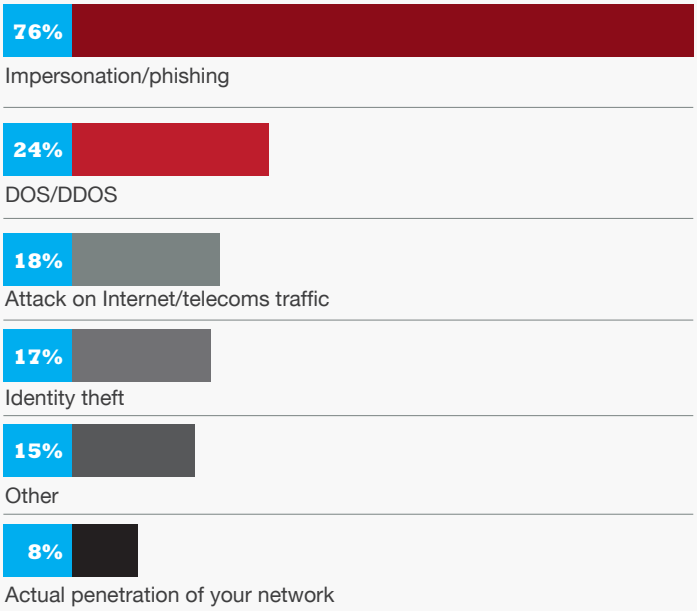
Tools and standards

Unsurprisingly, almost all of those surveyed have the expected anti-malware solutions (93%) and firewalls (94%) in place. An additional 94% have end-point protection solutions, 76% employ intrusion prevention software, and 53% have device protection in place. Less than half (49%) of those surveyed have data leakage prevention (DLP), and only 40% employ mobile device management solutions.

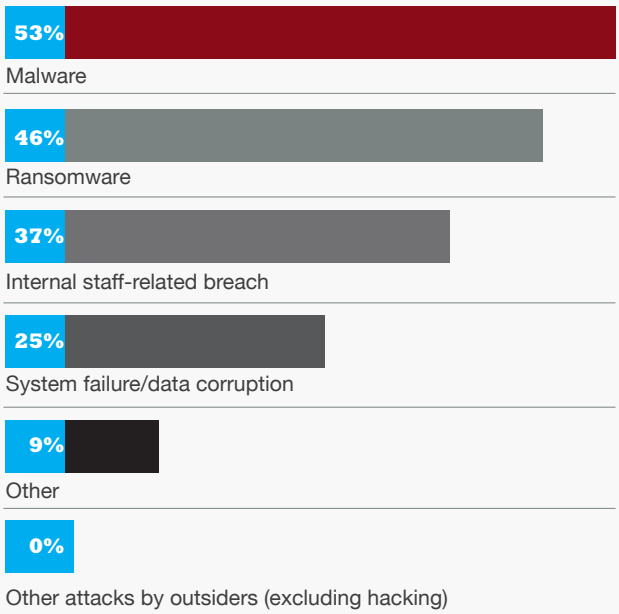
“Perimeter-based security and signature-based endpoint protections are the predominant solutions already in place. What is less prevalent are protections for the inside – tools such as micro segmentation and DLP. It is definitely better than a year ago, though. We have seen growth of internal controls, and newer technologies are now part of the roadmap, even if only a third of people have acted already,” adds James.

The survey shows that most organisations are trying to prevent lateral movement within their data centre, James notes.

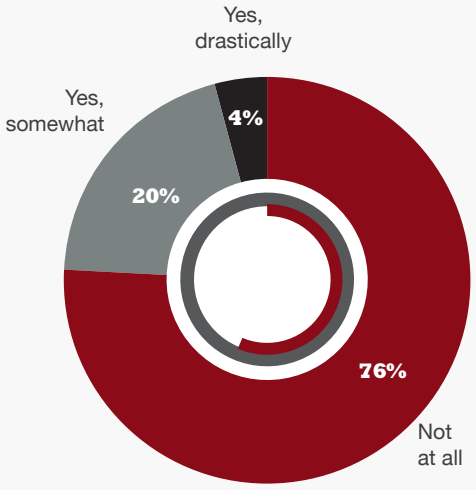
Did you suffer any of the following outsider attacks in the past year?



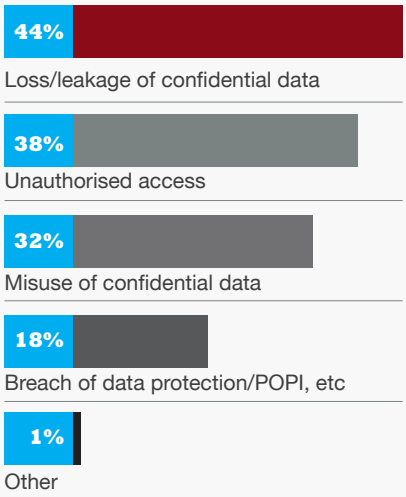
Did you suffer one or more of the following information security breaches in the past year?



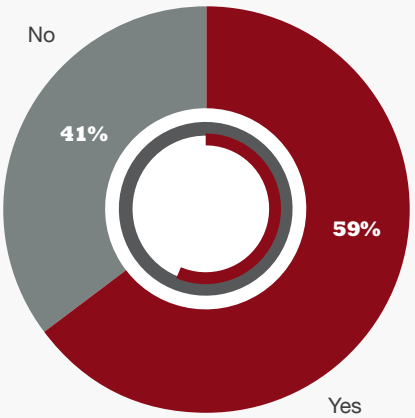
Did last year's WannaCry attack affect you?



What staff-related incidents did you suffer in the past year?

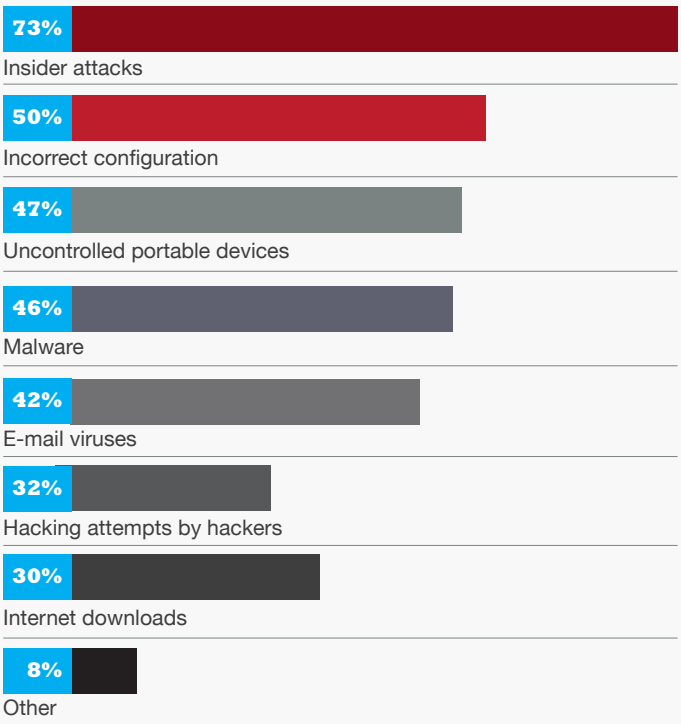


If yes, have ransomware attacks changed your security posture?



+ Ransomware attacks have changed business' security postures

What do you consider to be your greatest security risk?



Almost a quarter of the respondents are doing traffic flow analysis; more than a third have installed data centre intra-departmental firewalls to reduce exposure; and 19% have implemented micro-segmentation – granular, per-application firewalling.

When asked whether or not they carry out security risk assessments through a formal or recognised framework or standard, 81% said yes, 12% said no, and 7% were unsure.

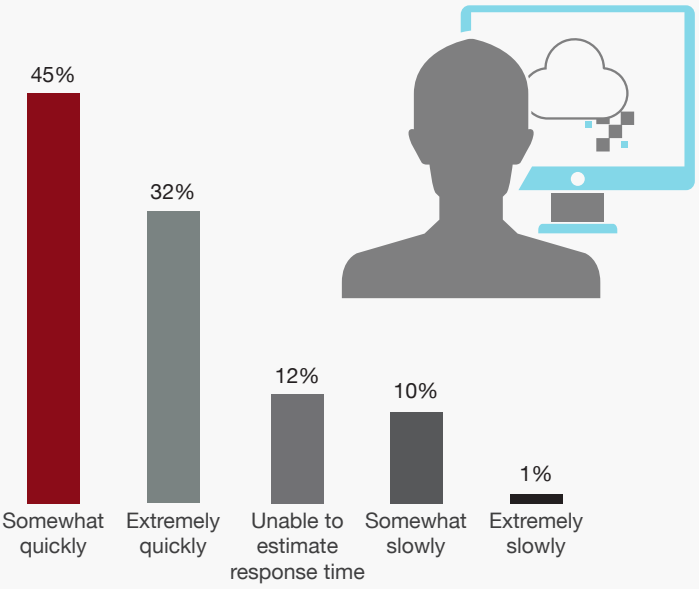
In terms of standards implemented, ISO27001 was the most popular, with 85% citing this, followed by PCI at 29% and government-issued standards at 27%.

Further investments

When it came to what prevents or delays investment in IT security, cost was the biggest factor for 78% of respondents, with the difficulty in determining ROI at 42%. Shockingly, a full quarter of respondents said they do not perceive security as a risk to the company.

As data regulations tighten for South African businesses, the primary driver behind security expenditure was protecting customer information at 26%, maintaining data integrity at 16%, and compliance at 11%. In addition, nearly half (42%) of CISOs surveyed said they had specific cyber insurance in place, and another 20% said they would like it, but cannot justify the cost.

How quickly can you remediate security breaches? *By remediate, we mean stopping attacks so that no further damage can occur.*



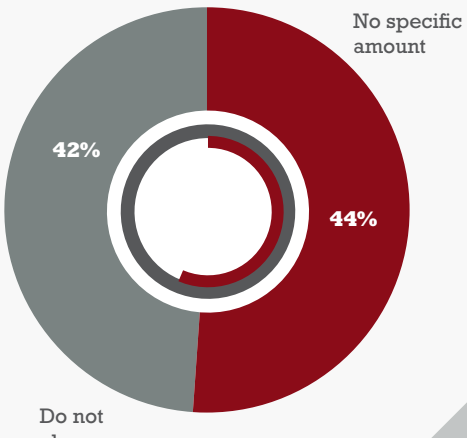
What security tools/solutions has your organisation implemented?

- 94% End-point protection
- 94% Firewall
- 93% Anti-malware
- 76% Intrusion prevention
- 58% SIEM
- 54% Device protection
- 49% Data leakage prevention
- 41% MDM
- 32% Microsegmentation

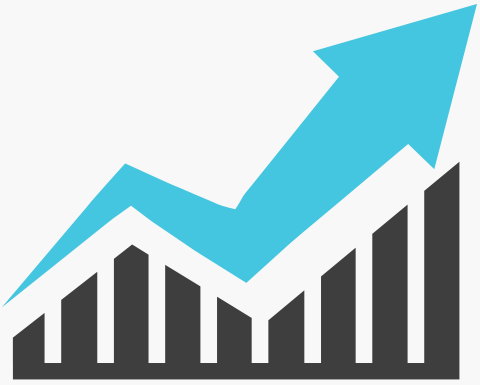
What prevents, or delays, investment in IT security?

- 78% Costs involved
- 42% Difficult to determine ROI
- 33% Lack of security management skills
- 25% Do not perceive security as a risk to the company
- 23% Not enough time
- 19% Difficult to integrate into the existing infrastructure
- 9% Do not know where to start
- 7% Too complex

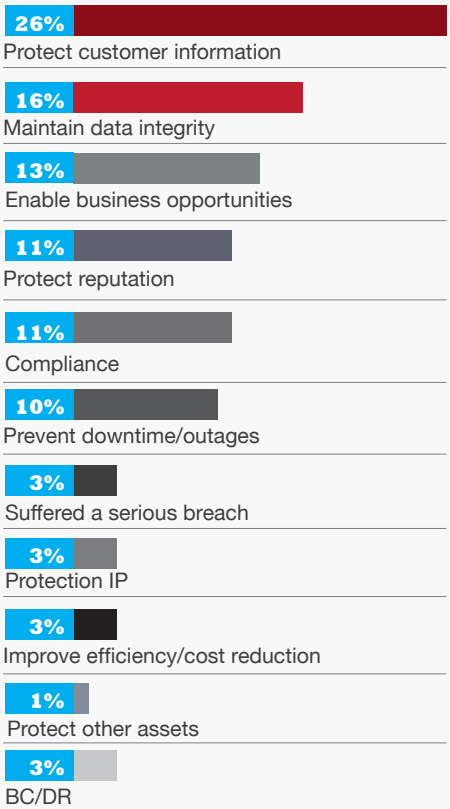
What percentage of your organisation's current budget is allocated to cyber security?



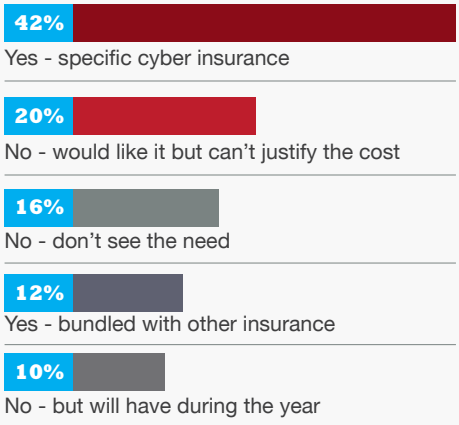
Phishing and DDoS are the most common major threats to South African businesses



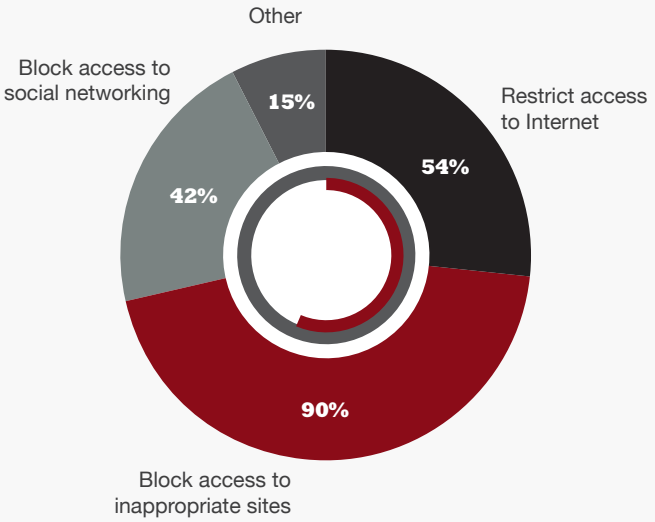
What is the primary driver for your security expenditure?



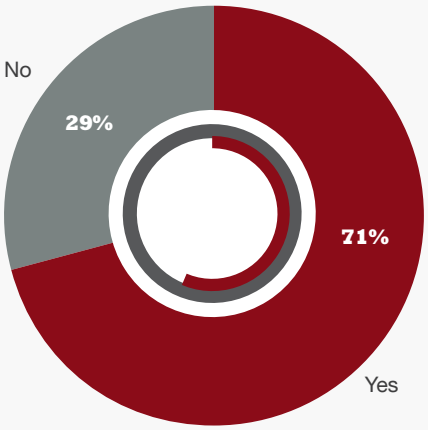
Do you have cyber insurance?



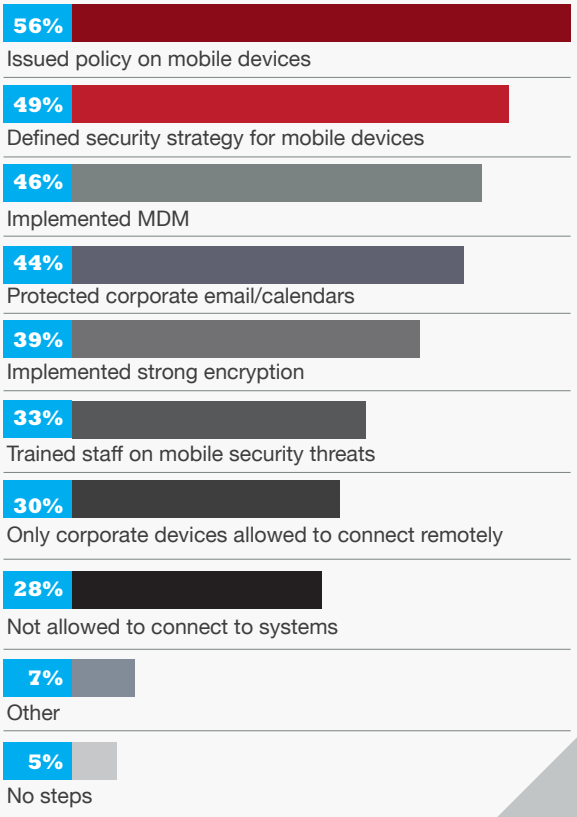
How do you prevent staff misuse/abuse?



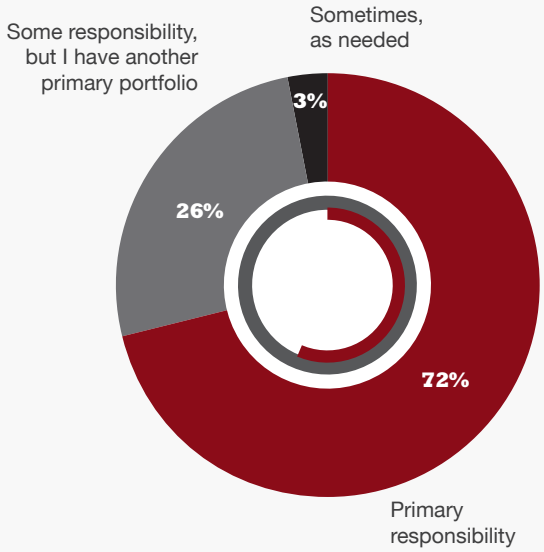
Have you taken any steps to mitigate mobile device risk?



If yes, what steps have you taken to mitigate mobile device risk?



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



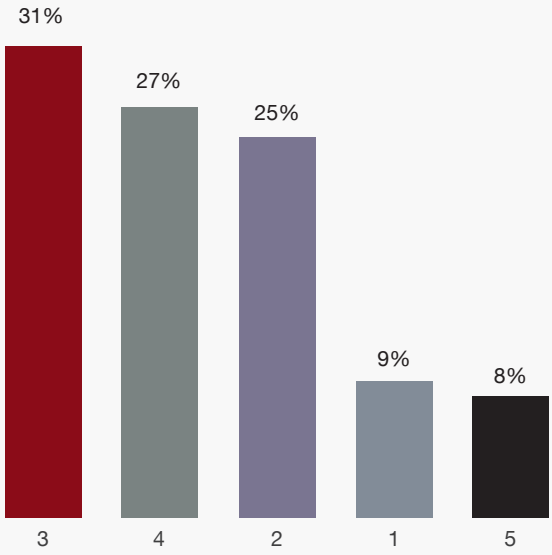
+ Cost remains the biggest stumbling block to improving IT security

CISOs view insider attacks as the greatest security risk to their businesses

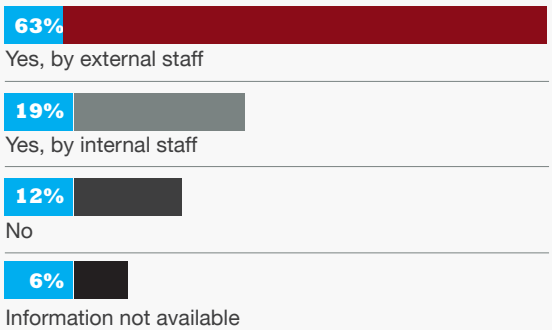
How frequently are security risk assessments conducted at your organisation?

What maturity level is your organisation's cyber security programme currently?

1 = Lowest, 5 = Highest



Has penetration testing ever been performed in your organisation?



View from the top

Do CISOs think differently?

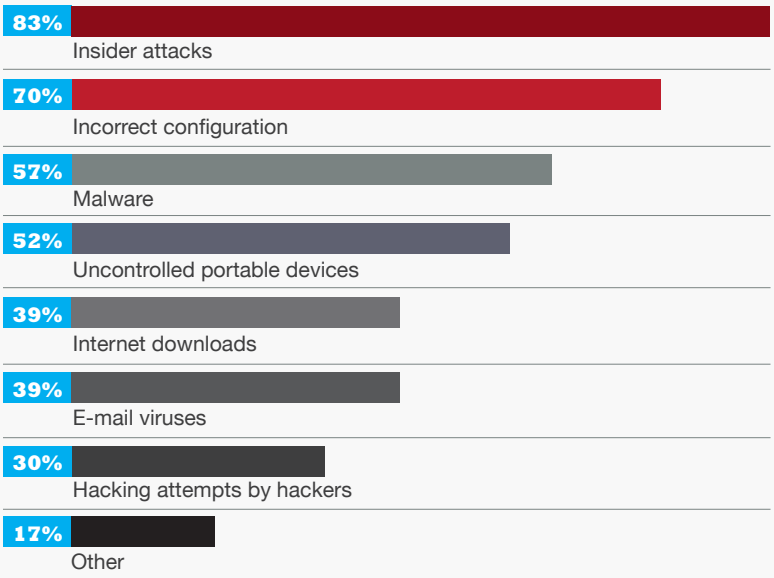
The survey also looked at responses from executive level / CISO respondents, who made up 31% of the sample, vs the entire sample, which included other security practitioners.

More CISOs (46%) expressed confidence that their organisation can respond ‘extremely quickly’ to security incidents vs their general counterparts (32%).

However, on the whole, exec level responses mirrored the general sample, indicating that businesses across the board share security concerns, and employ similar methods to defend themselves against today’s threats and maintain good governance.

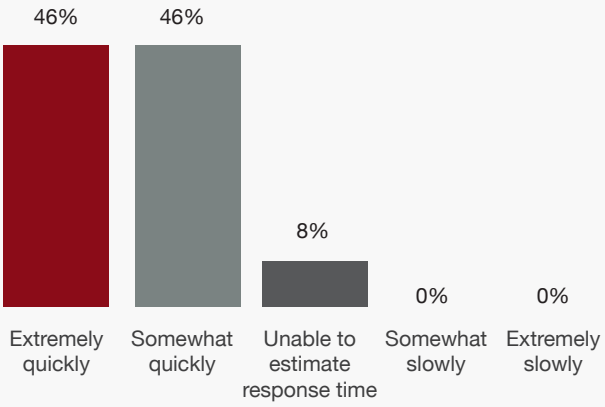
What do you consider to be your greatest security risk?

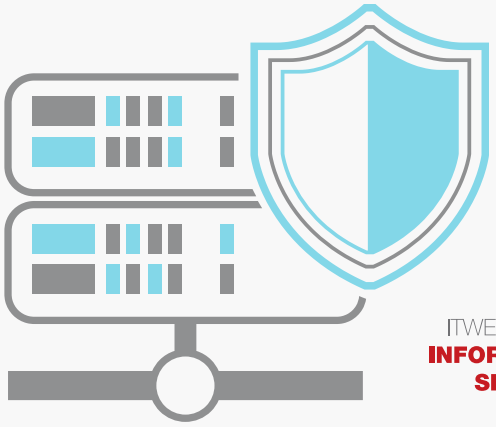
Surveyed: 22 (executive level respondents)



How quickly can you remediate security breaches?

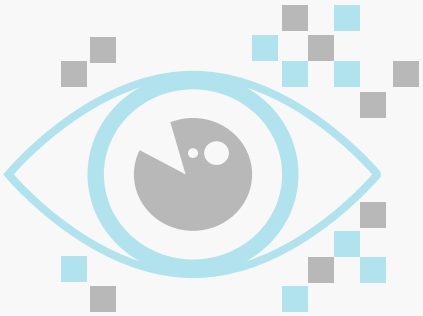
By remediate, we mean stopping attacks so that no further damage can occur.
Surveyed: 22 (executive level respondents)

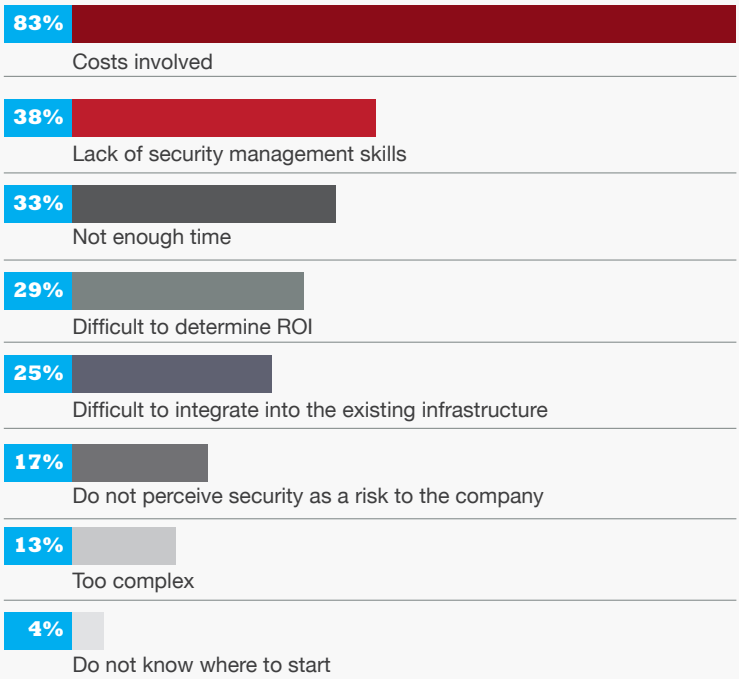




What prevents, or delays, investment in IT security?

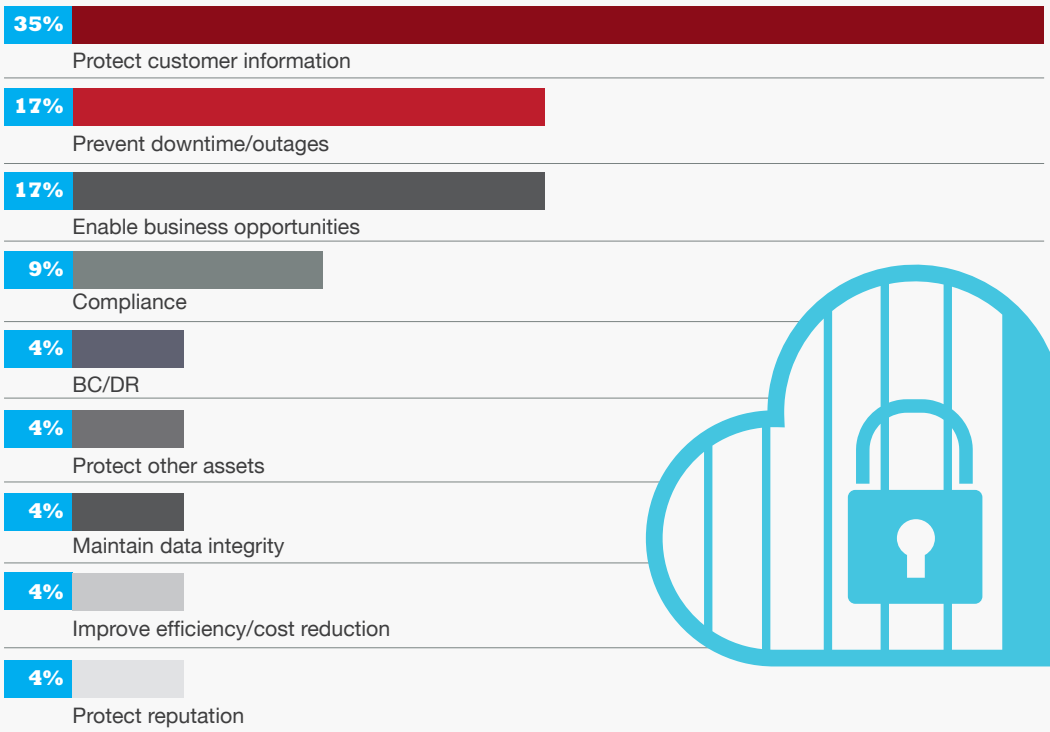
Surveyed: 22 (executive level respondents)



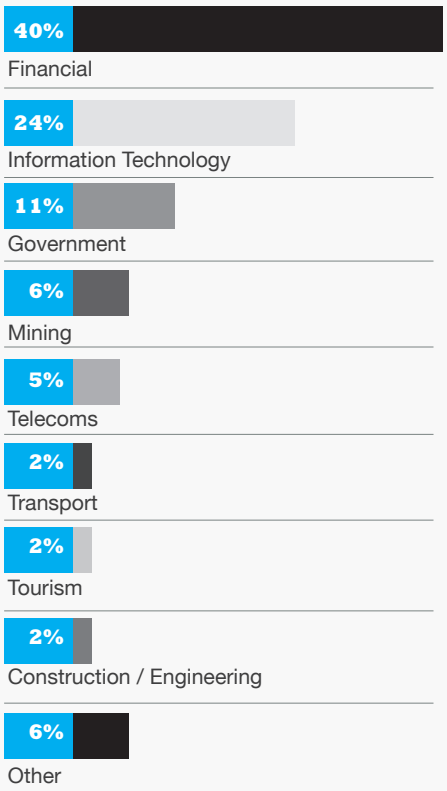


What is the primary driver for your security expenditure?

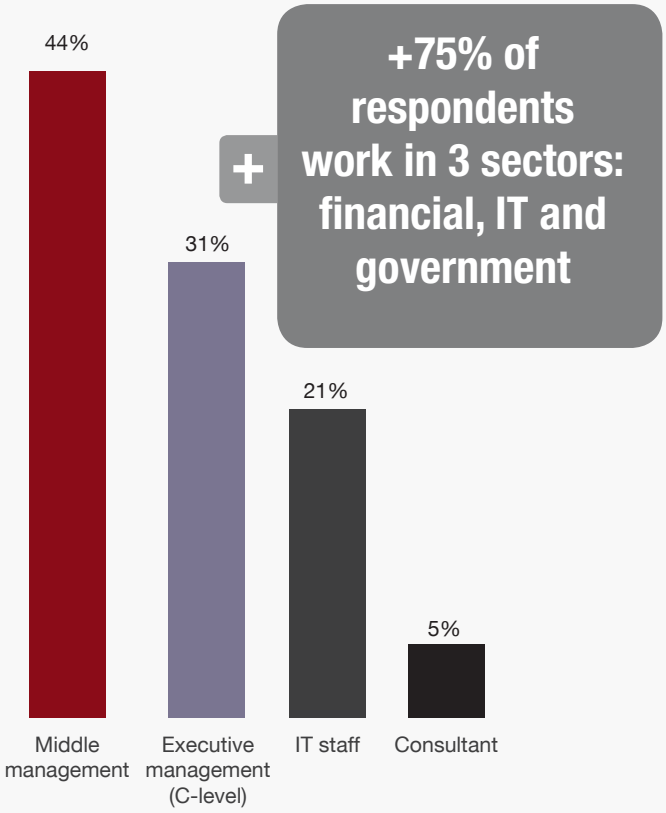
Surveyed: 22 (executive level respondents)



Industry sector



Role in the organisation



ABOUT THE SURVEY

ITWeb's first comprehensive Information Security Survey, in partnership with VMware, was run online during April 2018.

It was by invitation only, targeting predominantly chief information security officers (CISOs) and equivalent C-level decision makers in public and private sector organisations.

The objective of the survey is to establish an annual 'State of Cyber Security Report' – a first of its kind in South Africa.

The full research report will be available from ITWeb in July 2018.

WHO RESPONDED

- The survey captured input from **62** cyber security professionals.
- Almost 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.

ITWEB'S 2018 INFORMATION SECURITY SURVEY

IN ASSOCIATION WITH VMWARE

Publisher

Jovan Regasek

Survey development, research and analysis

ITWeb's technical and editoral teams

Editorial director

Ranka Jovanovic

Writer

Kirsten Doyle

Project manager

Allyson Towle

Sales director

Debbie Visser

Production

Sindiso Khupe

Layout and design

Ana Golijanin
Ontiretse Ngolwane

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