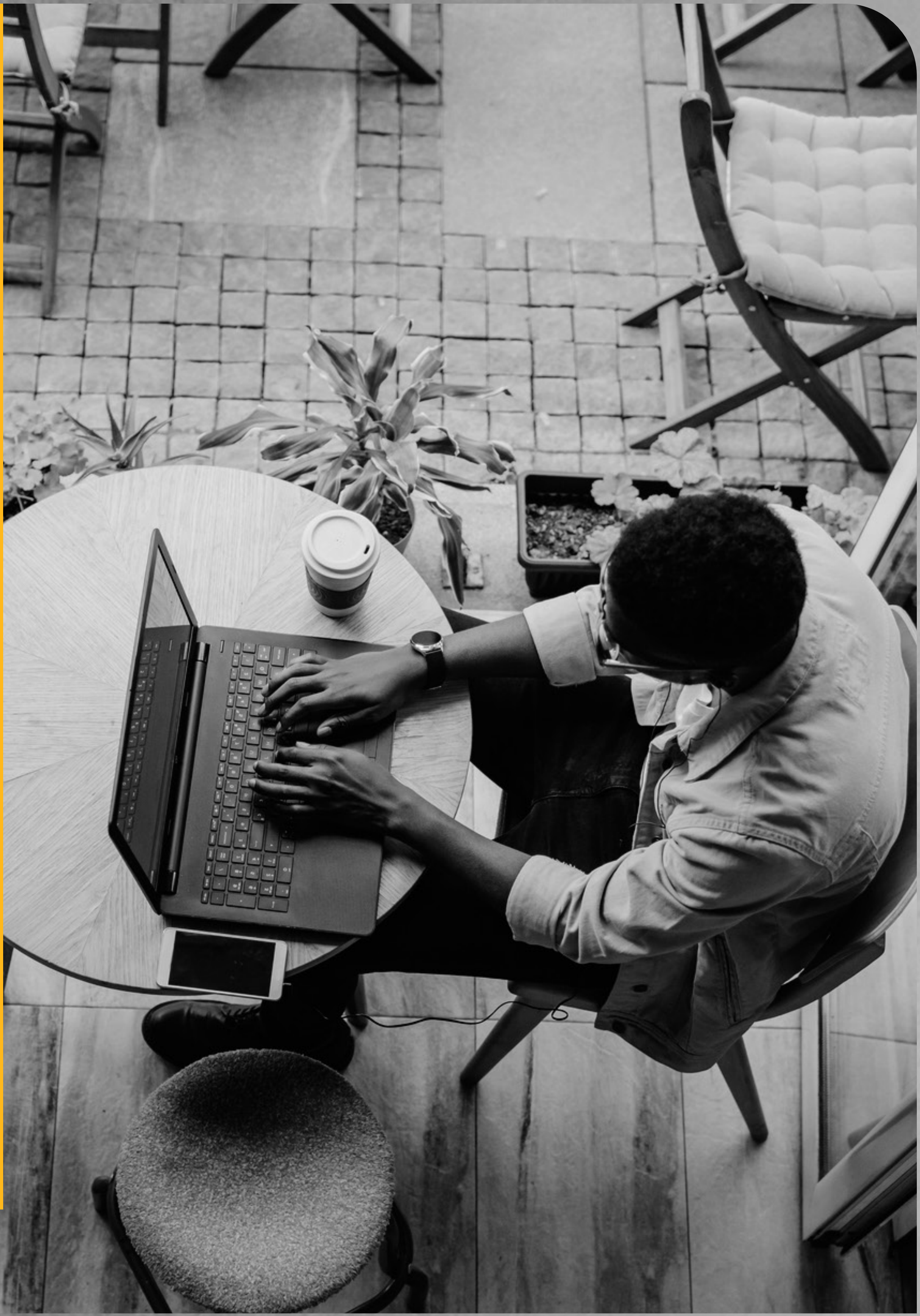
Business email platforms:

How well are South African organisations protected from email-borne attacks?



Introduction

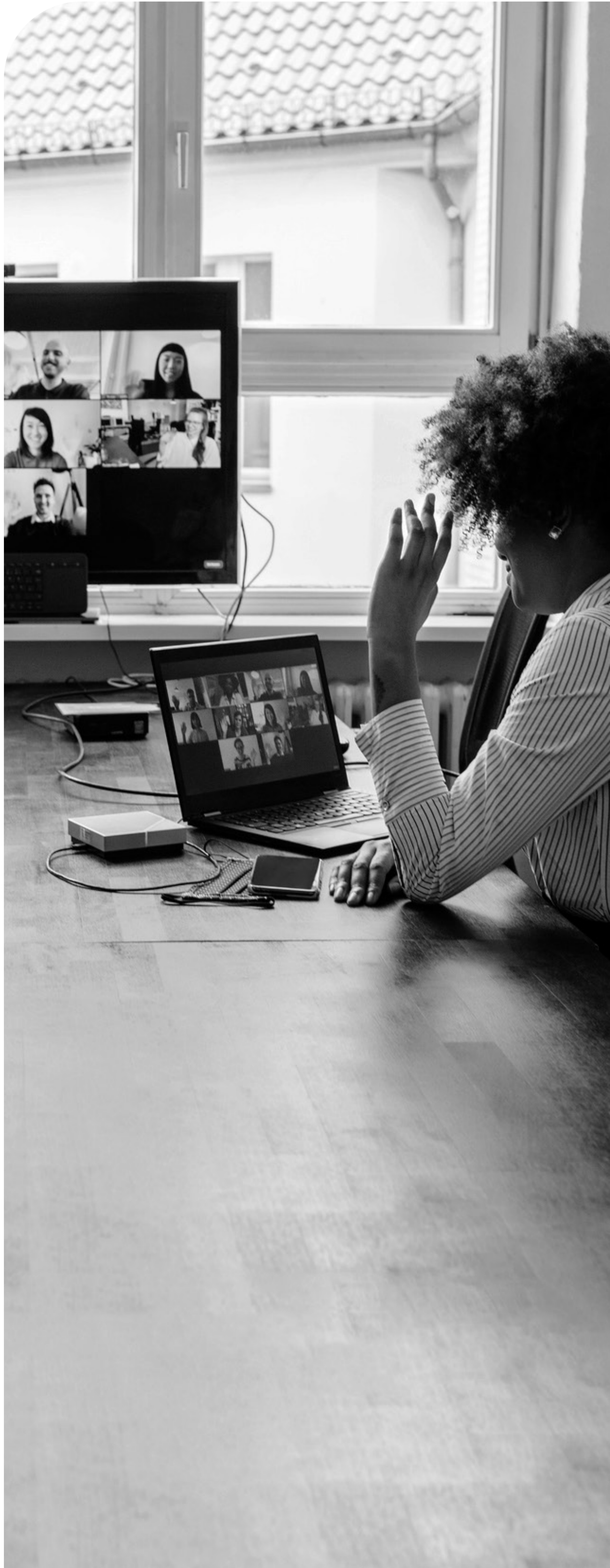
Organisations are more reliant on their business email providers than ever before. Work-from-home and hybrid work models have become the norm as organisations first adapted to the pandemic and associated lockdowns, and quickly realised the positive productivity gains of enabling remote work models. However, an escalation in global cybercrime activity has created new challenges for South Africa's IT decision-makers – challenges we are only just beginning to fully understand.

South Africa's public and private sector organisations have never been more dependent on email and other collaboration tools such as Microsoft 365 to stay connected with customers, partners and colleagues. The proliferation of hybrid and remote work environments has exposed potential new vulnerabilities, and attempts by opportunistic cybercriminals continue to grow in volume and sophistication.

New regulations – specifically the Protection of Personal Information Act (POPIA) – are adding further pressure and complexity on organisations to improve their defences. As of July 2021, organisations are at full risk of fines and penalties for non-compliance.

The current landscape has given rise to several important questions. Are South African organisations confident that business email platforms are secure? Do IT decision-makers trust the security bundled with their business email services, or is there a need for additional supplementary solutions? How well are organisations implementing layered security strategies to protect them against various forms of cyberattack? And which attack types are they most worried about breaking through their email perimeters?

To help answer these questions, Mimecast commissioned research in the first half of 2021 to find out from more than 330 South African IT and security directors in the public sector, financial services, healthcare, manufacturing, utilities and professional services industries. This report contains the key findings from our research and highlights how South African organisations are bolstering their business email defences against an array of cyber threats.



How confident are South African organisations in their email platform's security?

44%

Just over **four in ten** don't believe there's a real need for additional email security solutions on top of their organisation's email platform.

South African organisations have apparent high levels of confidence in the security of their business email services.

In fact, compared to other markets, South African organisations believe they are well-suited to protecting against a wide range of email-borne cyberattacks.

Respondents who say their email platform are designed to offer Business Email Compromise (BEC) protection:

South Africa
80%

UK
32%

Respondents who say their email platform are engineered to offer zero-day threat protection:

South Africa
77%

UK
40%

However, some of the findings indicate there is a disconnect between security decision-makers believing there is no need for additional layers of security, and to what extent they are indeed implementing additional security.

That’s because, despite high levels of confidence in built-in email platform security and perhaps being overly trusting of hyperscale vendors, nearly all (95%) deploy third-party solutions for their underlying email solution. This points to a growing awareness of the need for greater resilience, and highlights the prevalence of having a defence in depth strategy.

Perhaps if the more than nine in 10 organisations were to actually remove their additional security solution, confidence in built-in platform email security alone would wane.

95%

of all respondents deploy third-party solutions for email, despite high levels of confidence in built-in email platform security

How confident are South African organisations in their email platform's security? *cont.*

29% Nearly a third (29%) of all South African organisations said they don't trust their email platform to stop all cyberattacks.

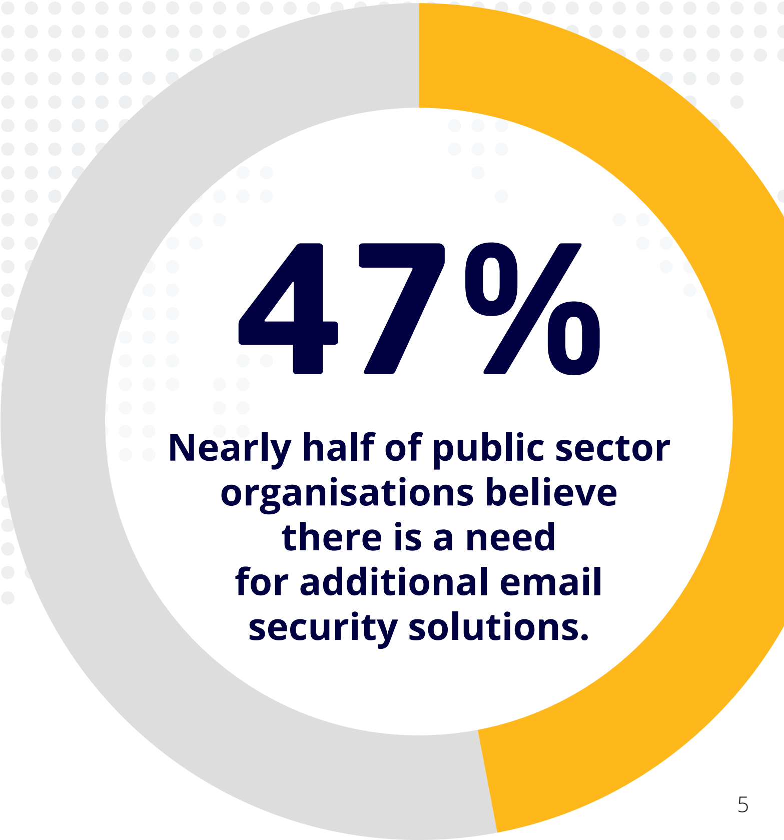
36% In the financial services and public sectors, this rate rises to 36%.

35% of all respondents said their email platforms do not offer adequate anti-phishing tools.

38% of all respondents said their email platforms don't offer adequate ransomware protection.

The last year has seen a major shift in the threat landscape; the rise in ransomware has been particularly worrying for security leaders.

So, while email platforms such as Microsoft 365 might have provided adequate security in the past, the increase in sophistication of attacks is making it harder for organisations to justify not being adequately protected.



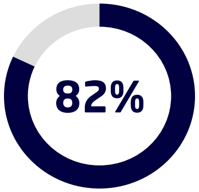
Nearly half of public sector organisations believe there is a need for additional email security solutions.

Business email threat landscape: What are SA organisations worried about?

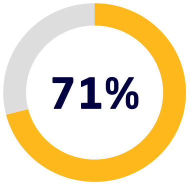
It’s no secret that cyber threat actors have dramatically ramped up their activities since the start of the COVID-19 pandemic. As normal ways of life and work were disrupted during the early stages and millions of people around the world started working from home, cyberattacks grew in both volume and sophistication.

In fact, according to the Mimecast’s State of Email Security 2021 report, 64% of global respondents saw an increase in email threats in 2020, and nearly two-thirds (65%) of South African respondents said they believe their organisation will be harmed by email attacks in the next year.

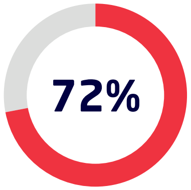
Our research found that:



More than four in five IT decision-makers say cyber attackers have become **more sophisticated in their attacks** since the start of the pandemic.



Seven out of ten respondents also stated that the number of **cybersecurity issues involving email has increased**.



found that email-borne attacks are **more likely to find some measure of success**.

South African IT decision-makers are typically concerned about the following cyber threats:

55%
Phishing

48%
Spam

47%
Ransomware

46%
Impersonation

South African organisations are meeting these challenges by ramping up digital transformation and cyber resilience.

85%

Eighty-five percent of respondents said the pandemic **has accelerated their digital transformation plans**.

55%

The most common reason? More than half say it is to be **better protected against cyber threats**.

The regulatory landscape also poses challenges.

With POPIA in force, organisations are under greater regulatory pressure than ever before to protect their systems and data against compromise.

40%

IT decision-makers '*strongly agreed*' their business email systems are fully POPIA compliant.

While most IT decision-makers said they have at least some confidence that their business email platform is designed to be POPIA-compliant, **one in five (20%)** of those surveyed don't believe they can reach being compliant. This may expose the organisation not only to potential regulatory risks and penalties, but any breach of personal data - where the organisation is found to have **not** implemented all reasonable measures to protect that data - may seriously damage its reputation and undermine customer trust.

Bolstering defences: the role of third-party solutions in improving business email resilience

South African organisations are doing well in their efforts to protect against email-borne attacks by leveraging third-party solutions and adopting a multi-layered security approach.

95% The rate of South African IT decision-makers who deploy third-party solutions for email

The general consensus over implementing additional layers of security solutions on top of standard business email platforms points to growing recognition that additional tools are necessary in the current threat landscape, and that built-in email platform security is likely insufficient to adequately protect against increasingly sophisticated email-borne attacks.

The main reasons South African organisations use third-party security solutions:

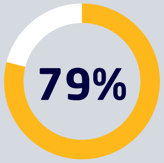
38% **To help halt attempted phishing attacks**

34% **To promote increase organisational resilience**

31% **To help stop ransomware attacks**

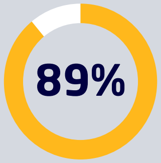
Considering the high prevalence of layered email security strategies among South African organisations, it is perhaps not surprising that IT decision-makers display high levels of confidence in their email security stacks. **Eight out of ten** respondents said they can identify and stop most cyberattacks before they breach the email perimeter.

If the perimeter defences are breached,



of organisations

and



of public sector respondents

believe they can identify and counter the attack before it does further damage to their network. In addition, **77%** of organisations say they would be able to recover email data within 24 hours following a successful breach.

Awareness and continuity: enabling safe hybrid work environments

As the number one business productivity tool, email is vital to the effective operations of any organisation. In the last year it's become even more critical as businesses swapped face-to-face interaction for digital communication. However, our research found that South African organisations suffer frequent outages on their email platforms, which interrupts business productivity and may open the door for opportunistic threat actors.

3.2

The average number of outages a year reported by all South African IT decision-makers (compared to only 1.3 in the UK)

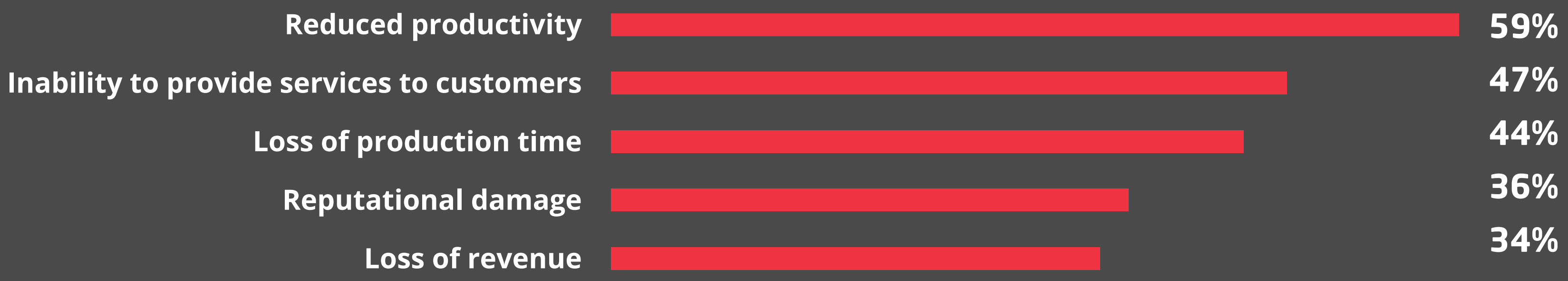
3.8

In the public sector, the rate of outages is even higher at 3.8 per year.

Considering the vital importance of public services - particularly during times of crisis such as an ongoing COVID-19 pandemic – having regular email outages could seriously undermine delivery of essential services to those in need.

When the majority of organisations also rely on the dominant Microsoft 365 as their business email platform – **75%** of respondents say they have implemented it - any interruptions or downtime hold the risk of not only affecting the productivity of single organisations, but entire economic sectors, which may have devastating consequences for economic growth.

How business email service outages affect South African organisations:



As the last line of defence against cyberattacks, employees have a critical role to play in protecting business email platforms from threat actors. South African organisations are generally aware of the role employees play in securing the business from cyber threats.

82%

The percentage of South African organisations that are aware that internal emails can represent a cybersecurity threat

27%

However, more than a quarter (27%) weren't confident that employees within their organisations are sufficiently trained to identify email-based cyberattacks

68%

Despite 68% saying employees are their organisation's biggest cybersecurity vulnerability

Considering that **71%** of organisations reported seeing an increase in the number of cybersecurity issues involving business email since the start of the pandemic, South African IT decision-makers would do well to prioritise more robust and ongoing cybersecurity awareness training to ensure every employee can identify, avoid and prevent potentially risky behaviour.

Key Takeaways

Add layers

Don’t rely on only Microsoft 365 to secure your business email.
Organisations need layers of security solutions that work to supplement the protections of the number one threat vector – business email – from an array of cyber threats.

Help empower employees

Turn your employees into effective support for the organisation’s overall resilience.
IT decision-makers are well aware of the risks their employees pose to the organisation’s overall business email security posture. Organisations should conduct regular, effective cybersecurity training to empower employees with the knowledge and awareness to prevent common attack types from breaching email perimeter defences.

Choose best-of-breed

Deploy the best solutions to address different security concerns and priorities.
Despite high levels of confidence in their business email platforms, 95% of organisations still deploy additional solutions to help protect against phishing, ransomware, spam and impersonation. Having specialised security solutions that offer the best-in-class protection against specific attack types gives organisations greater overall resilience. And by adopting Application Programming Interfaces (APIs) to automate data integration and exchange across multiple security tools, security teams can enable best-of-breed security for all their technology solutions, and help reduce the burden on overstretched IT security teams.

Help ensure continuity

Don’t be left twiddling thumbs when your business email platform experiences an outage.
South African organisations experience regular business email downtime that affects their productivity, reputation, and revenue. Having fall-back solutions that can keep the business running can help prevent damage to the organisation when there’s an inevitable outage.

mimecast®

Relentless protection. Resilient world.™