**The State of Email Security 2023**

**KEY FINDINGS IN SOUTH AFRICA IN THE LAST 12 MONTHS**

1. Email usage continues to rise at **86%** of companies. **44%** said it was a significant increase – higher than all other countries and against a global average of **29%**
2. **68%** of companies have experienced an increase in email-based threats.
3. **Two thirds** of survey respondents say cyberattacks are growing increasingly sophisticated.
4. **92%** of companies have been targeted by email-based phishing attacks.
5. **52%** of companies were harmed by a ransomware attack.
6. **Half** saw an increase in attempts to misappropriate their email domain
7. **93%** are using DMARC or plan to use it to thwart email spoofing and encouragingly **38%** have already deployed it.
8. **93%** agree that collaboration tools are essential to the well-ordered functioning of their companies
9. **70%** ofrespondents say collaboration tools are posing significant new security risks.
10. **61%** of companies expect to be harmed in 2023 by a collaboration-tool-based attack.
11. **72%** ofrespondents say their companies need to spend an average of 13.5% more on cybersecurity – the highest percentage globally
12. **97%** of companies either have a system to monitor and protect against email-borne threats or are actively planning to roll one out.
13. Respondents are divided on whether cyber insurance policies can serve as a substitute for developing a comprehensive cyber preparedness program:
	* **39%** would not see it as a comprehensive safety net
	* **56%** see them as worthwhile additions
14. **93%** of the organisations inclined to reduce their reliance on insurance agree they will need to compensate by investing more in their own cybersecurity defenses.
15. South Africans are most likely to increase investment in the following to address reduced reliance on cyber insurance:
	* DMARC protections – **59%**
	* Email security – **56%**
	* Use of APIs within cybersecurity – **54%**
16. **94%** of companies think they need stronger protections than those that come with their MS 365 and Google Workspace applications. **58%** *strongly* agreed (against a global average of 34%)
17. **93%** of companies are either using or plan to use AI and machine learning to bolster their cybersecurity. And more than **half** are already using these.
18. Respondents said the three main benefits of AI were:
	* An improved ability to block threats – **56%**
	* More accurate threat detection – **56%**
	* Reduced human error across the company (e.g. email warning banners) – **49%**
19. Almost all **(94%)** agree that [AI systems](https://www.mimecast.com/blog/artificial-intelligence-and-cybersecurity-separating-fact-from-fiction/) that provide real-time, contextual warnings to email and collaboration tool users would be a huge boon

A massive **32%** said that the benefits of such a system would revolutionise the ways in which cybersecurity is practiced– by far the highest globally

1. **52%** said insufficient employee awareness of cyber threats would be their organisation’s biggest security challenge in 2023.
2. **8** out of **10** respondents believe their company is at risk due to inadvertent data leaks by careless or negligent employees. **A quarter** said the risk was extremely high.
3. South Africans were also concerned about employees making serious security mistakes in the following activities:
	* **81%** - misuse of personal email
	* **78%** - using cloud storage and other shadow IT
	* **77%** - poor password hygiene
	* **69%** - using collaboration tools
4. **99%** of companies provide some form of cyber awareness training to their workforce.
5. More than a quarter **(28%)** train their staff on an ongoing basis