

Tech Trends
& Insights:The State
of IT Security

Summary of Top Findings

 Surveyed over
650 IT professionals
worldwide.

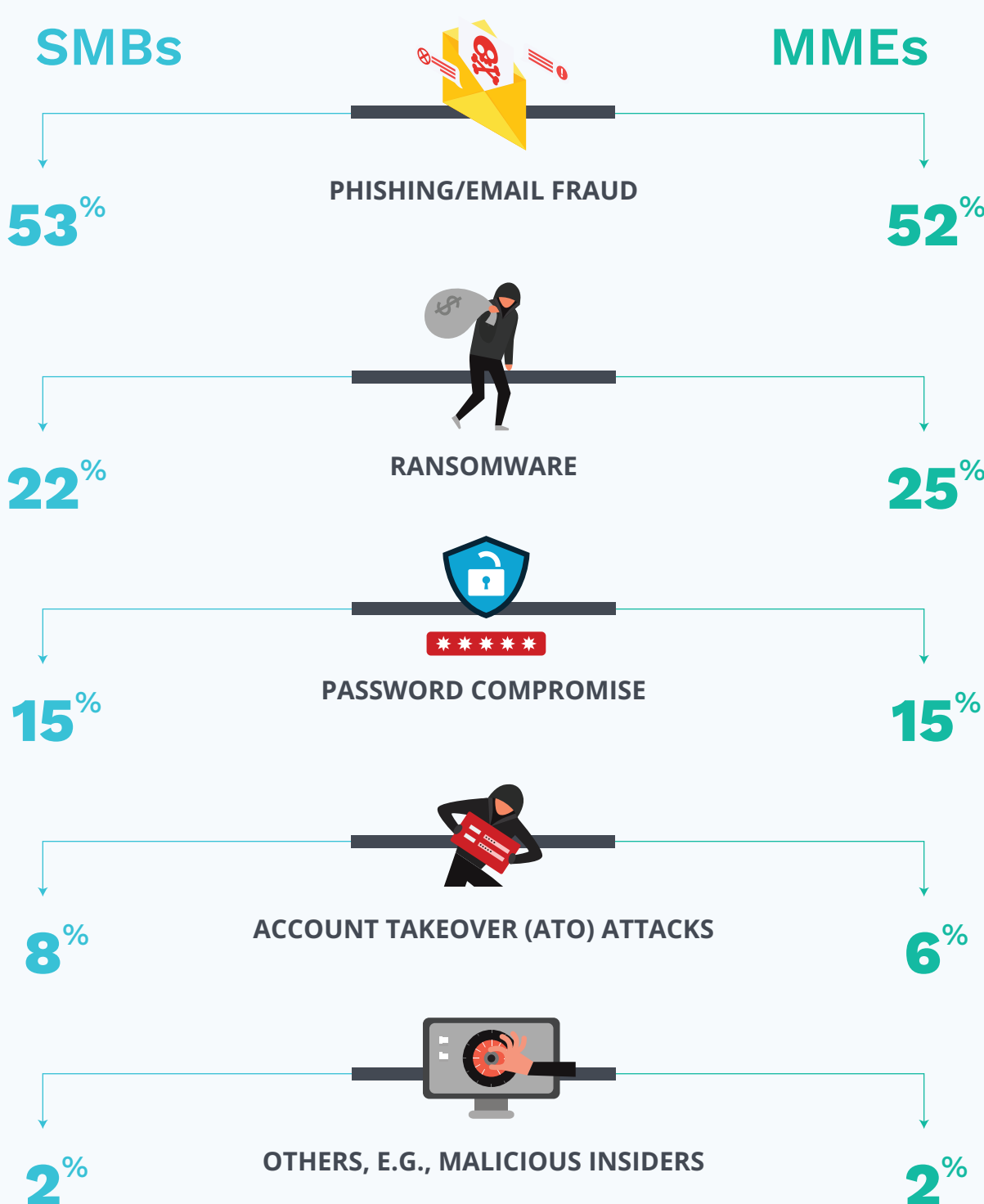
Respondents were divided into two groups: small and midsize businesses (SMBs) with 1,000 employees or less, and mid-market enterprises (MMEs) with more than 1,000 employees.

Shifting to a hybrid business model introduced new threat vectors and galvanized others that had fallen out of prominence. Cybercriminals quickly exploited the vulnerabilities caused by this transition, and today, threats loom larger than ever.

The following infographic explores respondents' sentiments with regard to their current state of IT security.

Top Threats Organizations Face Today

Respondents consider the primary cyberthreat to their business to be:



Top IT Security Priority

Organizations today are largely aware of and are addressing the high risk the phishing threat vector presents. We see this reflected by both SMB and MME respondents most frequently citing phishing awareness as a top security priority.

Other priorities include:



Phishing attacks are primarily designed to target unsuspecting and unsophisticated users. To that end,

77% of SMBs & **81%** of MMEs

reported they conduct regular security awareness training.



Tools Businesses Use to Mitigate the Risks of Phishing Attacks

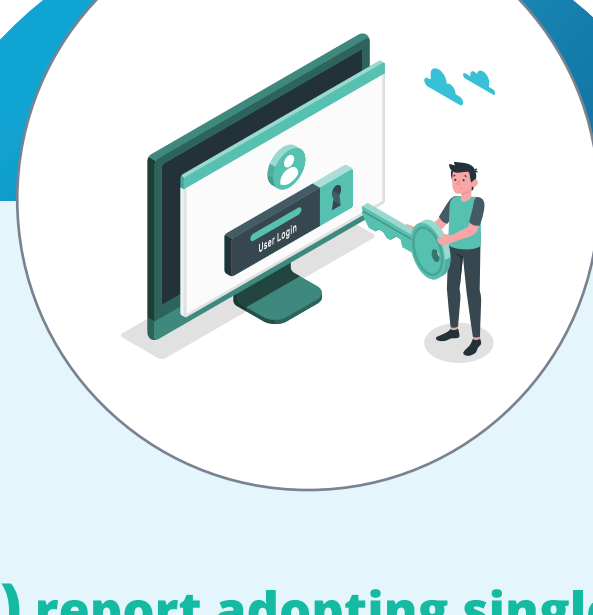
Phishing represents a significant security risk, emerging as one of the top threat vectors this year. Similarly, organizations of all sizes are equipping themselves with additional tools to help minimize the risks of the human element.

64% of SMBs & **79%** of MMEs

have tools to detect network changes that may indicate insider threats.

68% of SMBs & **72%** of MMEs

have implemented multifactor authentication (MFA) or two-factor authentication (2FA).



MMEs (64%) report adopting single sign-on (SSO) 48% more frequently than SMBs (43%).

Among respondents who suffered a data breach last year, only **15%** of SMB breaches and **12%** of MME breaches occurred against organizations utilizing MFA, SSO and a password manager.

As cyberthreats evolve and become more sophisticated, a layered approach is necessary to tackle them head-on. In a layered defense approach, even if an attacker penetrates through one layer, they will be thwarted by a subsequent layer.

[Download](#)

Get the **State of Cyberattacks infographic** to learn about the current state of cyberattacks and data breaches.

[Learn More](#)

Check out our blog on **Top 5 Cyberattacks and How They Happen** to better protect your business and data against the ever-growing cyberthreats.