SPANNING
a Kaseya company

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:

	SMBs	MMEs
PHISHING/EMAIL FRAUD	53%	52%
RANSOMWARE	22%	25%
PASSWORD COMPROMISE	14%	15%
ACCOUNT TAKEOVER (ATO) ATTACKS	8%	6%
OTHERS, E.G., MALICIOUS INSIDERS	1%	2%

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 citing phishing awareness as their top security priority this year.

Other priorities include:

	SMBs	MMEs
PHISHING AWARENESS	37%	36%
SECURITY BEST PRACTICES, E.G., PASSWORD PROTECTION	27%	19%
DATA PRIVACY AND PROTECTION	21%	29%
COMPLIANCE	14%	15%

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 & **71% of MMEs**

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

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

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

Read **Data ASaaSsins: Threats That Can Cause Data Loss and Hurt Your Business** to learn about the various threats and the threat actors that cause SaaS data loss and be detrimental to your business.

www.spanning.com