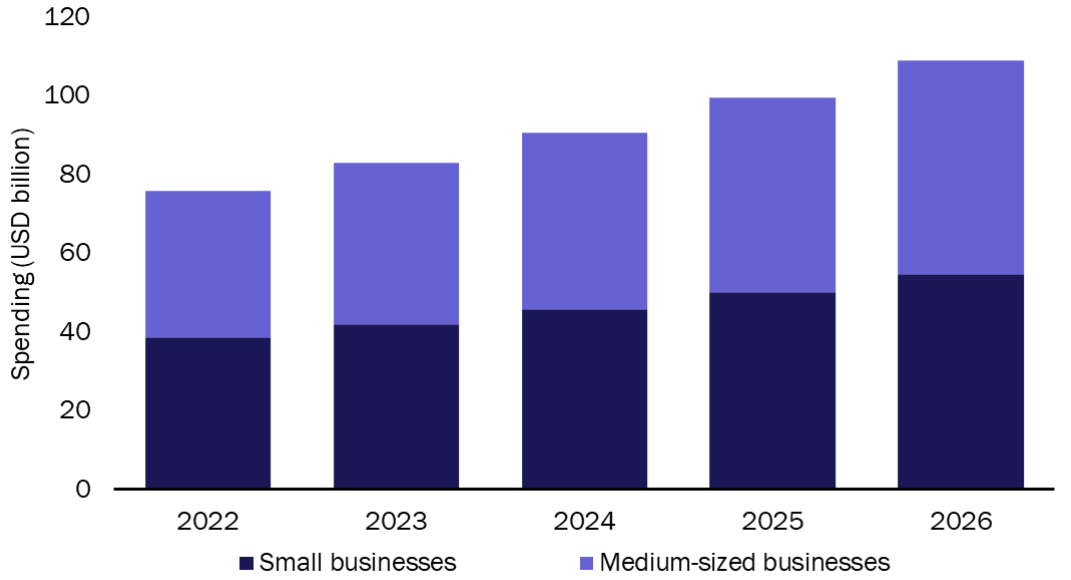
SMBs' spending on cyber security will increase at a 10% CAGR to reach USD109 billion worldwide in 2026

June 2023

Youngeun Shin

Analysys Mason's SMB Technology Forecaster estimates that small and medium-sized businesses (SMBs) spent USD76 billion on cyber security in 2022 and forecasts that this will rise to USD109 billion by 2026. Small businesses' spending on cyber security is expected to increase at a CAGR of 9.2% during this period and that of medium-sized businesses at a CAGR of 9.8% (Figure 1). This growth will result in SMBs accounting for 60% of the spending on cyber security worldwide in 2026.

Figure 1: SMB spending on cyber-security solutions and services, worldwide, 2022–2027



Source: Analysys Mason

The strong growth in SMBs' cyber-security spending is driven by a range of factors, including the heightened awareness of cyber risks, increased use of mobile devices and adoption of cloud-based solutions. SMBs are particularly vulnerable to cyber attacks because their IT environments are not as securely managed as those at large businesses. As a result, SMBs have become major targets of cyber criminals seeking to exploit their weaknesses.

We expect SMBs' cyber-security spending to continue to grow at a steady pace, driven by increasing regulatory compliance requirements and growing customer expectations around data privacy and security.

SMBs will mainly invest to improve the security of remote management systems, mobile devices and data

Remote management. Remote management will be one of the largest and rapidly growing categories of SMB cyber-security spending between 2022 and 2026. SMBs' spending on securing remote management systems is projected to exceed USD45 billion by 2026, growing a CAGR of 15%. Managed service providers or managed security service providers are expected to remain key partners for SMBs in managing these complex cyber-security measures.

Mobile devices. SMBs are projected to spend USD 9.5 billion on securing mobile devices in 2026, growing at a CAGR of 13.4% during the forecast period. The surge in mobile security spending can be attributed to the growing use of mobile devices on corporate networks.

Data. SMBs are expected to increase their spending on data security from USD3.2 billion in 2022 to USD4.3 billion in 2026, at a CAGR of 8.5%. SMBs will continue to invest in data security solutions to comply with regulations and safeguard their customers' data and intellectual property.

SMBs in Asia–Pacific are expected to spend more on cyber security than SMBs in the Americas from 2023 onwards

As of 2023, SMBs in Asia–Pacific (APAC) account for 38% of the total SMB cyber-security spending. We expect SMBs in APAC to increase their share in the coming years. By 2026, it is projected that SMBs in the APAC region will invest USD45 billion in cyber security, reflecting a CAGR of 12.6%.

This surge in cyber-security spending reflects the growing recognition among SMBs in the APAC region of the need to protect their businesses against cyber threats. SMBs in APAC have increasingly embraced digital technologies to drive growth and innovation, which inevitably brings with it an increased risk of cyber threats. The strong growth in spending is also indicative of the rapidly growing number of businesses in the region.

SMBs in the Americas are projected to spend USD 31 billion in 2023, accounting for 37% of the total SMB cyber-security spending. SMBs in the USA are increasingly focused on protecting themselves from cyber-security threats and are adopting more sophisticated solutions.

MSPs and SIs will become the dominant route to market for SMB cyber-security spending by 2025

In 2022, value-added resellers (VARs) accounted for 43% of SMBs' spending on cyber security, while managed service providers (MSPs) and systems integrators (SIs) accounted for 36%. However, this distribution is expected to change in the coming years. MSPs and SIs will account for 40% of SMB cyber-security spending by 2025, while VARs will account for a declining share (39%).

SMBs are increasingly recognising the risks associated with cyber attacks, leading to increased budget allocation towards cyber-security solutions. However, SMBs are not likely to build in-house security teams. Instead, they are expected to seek the assistance of MSPs and MSSPs to help to manage their cyber-security solutions. Moreover, as SMBs' needs evolve, many resellers and VARs are expected to transform into MSPs to cater to their clients' 'enterprise-lite' demands.

We also expect SMBs to increase (at a CAGR of 17%) their spending on cyber-security solutions with telecoms operators during the forecast period. This surge can be attributed to the operators' continued efforts to augment their cyber-security offerings and strengthen their association with the delivery of cyber-security solutions.

Key takeaways

In response to the increasing cyber threats, SMBs are investing in cyber security to protect their IT environments and data assets with spending expected to reach USD109 billion by 2026. The adoption of digital technologies, such as cloud-based solutions and mobile devices, has made SMBs particularly vulnerable to cyber attacks. SMBs have recognised the need to enhance their cyber-security posture to safeguard against potential data breaches and minimise business disruptions. SMBs are investing in a range of cyber-security solutions to mitigate these risks and protect their critical business assets.

APAC's SMB cyber-security market has emerged as the largest in the world and is expected to maintain its growth trajectory. The proliferation of digital transformation initiatives across industries and the growing adoption of cloud-based solutions have significantly increased the cyber-security risks faced by SMBs in the region, driving the demand for robust cyber-security measures. As a result, we expect that SMB cyber-security market in APAC will continue to expand in the foreseeable future, presenting lucrative opportunities for players in this space.

MSPs and SIs are projected to become the dominant route to market for SMB cyber-security spending. In-house security teams are not a practical option for SMBs. As a result, more are turning to MSPs and SIs to manage their cyber-security requirements. Additionally, several resellers and VARs are predicted to transform into MSPs to meet the enterprise-lite demands.