Understanding the SME Security Workload Crisis in a Changing World

Table of Contents

Executive Summary

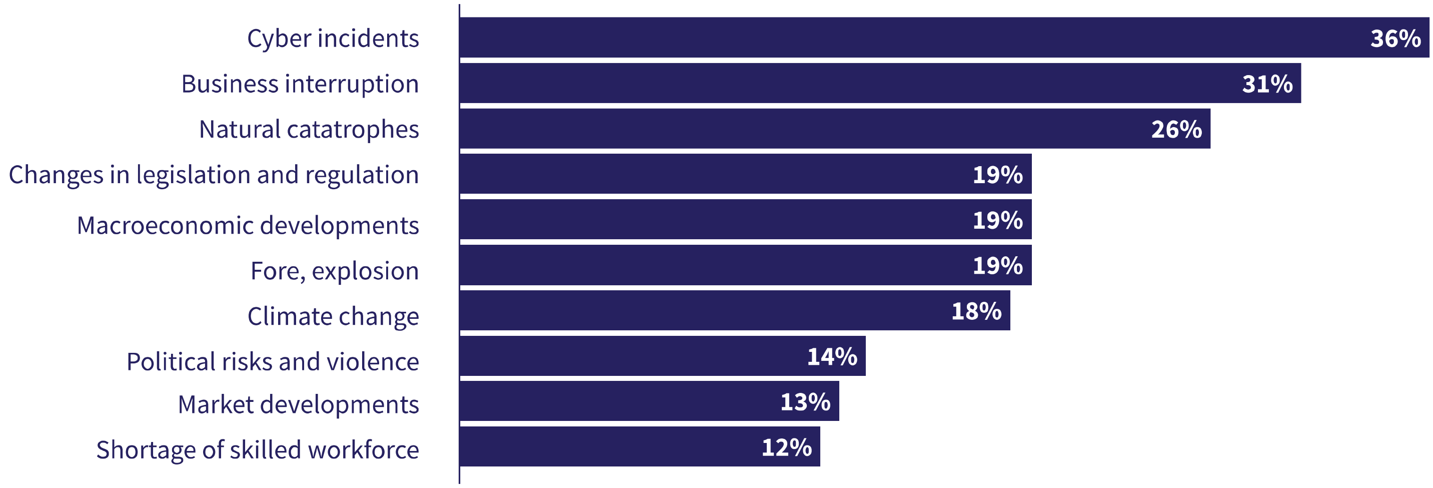
Small and medium-sized enterprises (SMEs) are at a critical juncture in the digital age. With an escalating number of cyber threats, many need more resources and expertise to protect themselves effectively. Findings presented in Coro's 2024 SME Security Workload Impact Report, supported by additional insights from the Coro-sponsored TechTarget Enterprise Strategy Group (ESG) research and other industry research, shed light on the overwhelming burdens SMEs face in managing cybersecurity. This white paper explores these challenges and offers strategic recommendations, emphasizing the need for modular, scalable solutions tailored to the specific needs of SMEs.

A Changing World for Businesses Globally

The Allianz 2024 Risk Barometer Report indicates the rise in cyber threats as a leading cause of destruction for businesses of all sizes. The report lists cyber incidents as the number one risk factor for businesses globally, surpassing disruption to business continuity in parameters such as financial damage, recovery capabilities, and ability to stay in business.

The top 10 global business risks for 2024

The top risks and mjor risers in this year's annual business risk syrvey reflect the big issues facing companies around the world right now - digitalization, climate change and an uncertain geopolitical environment. Many of these risks are already hitting home, with extreme weather, ransomware attacks and regional conflicts expected to test the resilience of supply chains and business models further.



A Changing World for SMEs

According to Accenture cybercrime study, while companies of all sizes have experienced a rise in cyberattacks, 43% of all cyberattacks in recent years have been directed at midmarket organizations (the study sets small businesses at 10-49 employees and medium-sized organizations at 200-499 employees).

Findings presented in the 2024 U.S. Small Business Administration (SBA) Summit confirm the reasons for SMEs' increased exposure to cyber threats. According to data presented at the summit, midmarket organizations endure a particular set of challenges unlike those of larger corporations, primarily:

- added exposure to the evolving threat landscape
- growing reliance on cloud-based data storage
- increased difficulties with the shift to remote and distributed work environments

Data collected from an SBA survey emphasizes that 88% of small business owners felt their business was vulnerable to cyberattacks, yet they lacked the budgets for advanced security solutions, had limited time to devote to cybersecurity, or didn't know where to begin. The Accenture study similarly concurs that only 14% of surveyed SMEs were adequately prepared to defend themselves against a cyberattack.