Editor's Note:

Cybersecurity is Everybody's Business

IN 2025, the digital world is as much a part of our daily lives as the physical one. From smart homes and online classrooms to business networks and government systems, our dependence on technology has never been greater—and neither has our exposure to cyber-risk. Cybersecurity is no longer the sole responsibility of IT departments or security agencies; it is a shared duty across every sector, every business, and every individual.

This supplement, *Cybersecurity is Everybody's Business*, explores the evolving landscape of digital protection and resilience. It features expert insights and practical guidance on safeguarding data, from "Cybersecurity Awareness in 2025" to "Ten AI-Powered Cyber Threats Caribbean Businesses Can't Ignore".

It also examines the transformative role of education through "AI and Cybersecurity for Education" and the Finnish model of advanced cybersecurity learning, where universities are leading national collaboration to build the next generation of cyber-professionals.

The common thread is clear: awareness, education and vigilance are the strongest defences in an age of intelligent threats. Whether you're a small business owner, a student or a public servant, cybersecurity begins with personal responsibility—using strong passwords, questioning suspicious links, and updating systems regularly.

Protecting data means protecting trust, productivity, and the future. In an interconnected Caribbean and global community, cybersecurity truly is everybody's business.

— Sharon Ali Aziz

—Photo: rawpixel,

Cybersecurity Awareness in 2025

By George Whyte
Managing Director
Calibra Solutions Ltd

In 2025, the global business environment is more connected—and more exposed—than ever before. Digital transformation, hybrid work models and artificial intelligence (AI) have revolutionised how organisations operate. The change is for the better. However, conversely, the level of exposure to cybercriminals simultaneously skyrockets.

Cyberattacks today are more organised, more persistent, and increasingly powered by AI. Cybercriminals have strategically organised their operations and have come up with complex ways to commit any of the many cybercrimes.

Threat actors exploit automation and social engineering to target even the smallest vulnerabilities. Ransomware, phishing, and data breaches remain dominant, but emerging threats—such as supply-chain compromises and AI-driven deception—are changing the game.

For Caribbean-based enterprises and financial institutions, this challenge is especially urgent.

As regulations strengthen and digital service expectations grow, these organisations must prove they can protect data, ensure continuity and maintain customer confidence. Cybersecurity awareness, supported by disciplined action, is now both a compliance necessity and a competitive advantage.

Building a Resilient Cybersecurity Framework

Cybersecurity is no longer limited to a technical check-box; it is a strategic enabler of trust, resilience, and long-term success. Companies and organisations are encouraged to consider a holistic approach that unites technology, process, and people.

CREDITS

Advertising Manager:
Michelle Lee-Joseph

Sales Manager:
Nadine Hall

Content Producer:
Sharon Ali Aziz

Design and Layout:
Cindy Sankar