



HOWDEN

Cyber Resilience for Growth: A Strategic Roadmap for Caribbean Businesses

Building strong
defenses to protect
small business assets



Stratos Cyber
www.stratos-cyber.com



Howden Group
www.howdengroup.com



Welcome to Our Webinar

At Stratos Cyber, we work closely with small and mid-sized organizations across the Caribbean to turn cybersecurity from a confusing technical checkbox into a business advantage. In sectors like hospitality, financial services, education, healthcare, and professional services—where teams are lean, customer trust is everything, and the margins for error are razor-thin—resilience isn't optional. It's essential.

Today's session isn't about fear. It's about clarity. What's really happening in the threat landscape? Where are the hidden risks for SMBs in our region? And what can we do—practically and affordably—to protect the people, data, and operations that matter most?



Threat Landscape 2025: Global Forces & Caribbean Risk Surge

Global Perspective — These Are the Forces Redefining Risk

AI-Powered Phishing & Social Engineering

- Attackers now use generative AI to craft ultra-credible spear phishing, deepfake voice calls, and chatbots that mimic real employees.

Ransomware 3.0 Goes Mainstream

- Ransomware is no longer just encrypt + demand. Exfiltration, double extortion, and automation put SMBs in the crosshairs.

Cloud Attacks Now Focus on SMBs

- As more small businesses move workloads to cloud or SaaS, misconfigurations, identity theft, and ignored logging become entry points.



Threat Landscape 2025: Global Forces & Caribbean Risk Surge

Caribbean Context — Where the Risks Hit Harder

Cloud Misconfigurations Are a Leading Vector

- In our region, many breaches stem from poorly configured cloud access, overprivileged service accounts, and weak default settings.

Vendor & Supply Chain Breaches Are No Longer Theory

- SMBs in the Caribbean depend heavily on third-party platforms (reservation systems, POS, booking engines). Vendor compromise is effectively your compromise.

Data Residency, Bandwidth, and Backup Weaknesses

- Because many islands rely on external data centers or slow links, recovery is slower and cross-jurisdiction complexity is higher.



Cybersecurity – Confidence vs Reality

71% of SMB leaders are confident in cybersecurity, but only 22% have mature controls in place.

Global Cyberattack Frequency

Over 2,200 cyberattacks occur daily, averaging one attack every 39 seconds worldwide.

Ransomware Threat Prevalence

Ransomware accounts for 68% of cyber incidents, posing the most common threat to SMBs.

Financial Impact of Breaches

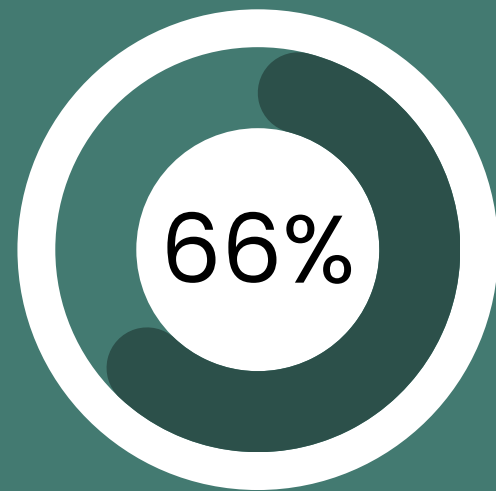
The average cost of a data breach is projected to reach \$4.88 million in 2025.



71%

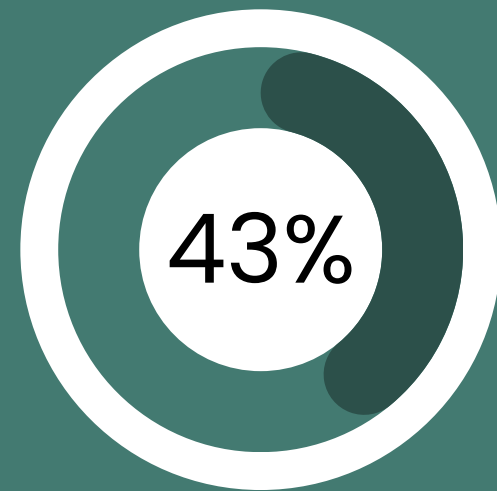
The 'Too Small to Hack' Myth

SMB Cyberattack Misconceptions



66% of SMBs believe they're too small to be targeted.

www.bdemerson.com



Yet, 43% of all cyberattacks target small/medium businesses.

Ransomware Impact

Ransomware hits SMBs hard: average cost per attack is \$255,000–\$1.24 million. [lgcybersec.co.uk]

Phishing as an Attack Vector

Phishing is now the #1 entry point for ransomware, used in 35% of cases often exploiting human vulnerabilities to breach security. [[Markets Insider](#)]

Emerging AI Threats

AI-powered phishing and ransomware-as-a-service are lowering barriers for attackers. [www.akamai.com]



Caribbean SMB Cybersecurity Posture

Evolving Threat Landscape

Caribbean SMBs face increased cyber threats due to limited resources, rapidly adopted Digital Transformation initiatives, and outdated infrastructure.

Regional Cybersecurity Initiatives

CARICOM countries and Trinidad and Tobago have launched strategies and mandates to improve cybersecurity, yet this will take time to adopt

Cyberattack Trends on the Rise

Jamaica recorded around 4 million attempted cyberattacks in early 2024, showing regional risks.

Improving Cybersecurity Posture

Caribbean SMBs need capacity building, awareness, and investment to strengthen defenses.



Caribbean SMBs are also targeted

SMBs in the Caribbean are increasingly targeted and exploited due to:

- Low awareness and belief they're not targets.
- Weak endpoint protection and lack of encryption.



Ransomware attacks have hit key sectors:

✓ Finance (Jamaica FSC, Trinidad and Tobago – Credit Union)

✓ Energy (Belize, Aruba Electricity)

✓ Government (Bermuda)

✓ Telecoms (Trinidad and Tobago)

Regional efforts include public education, incident response frameworks, and capacity building.

Build a Cyber Resilience Roadmap That Actually Works for SMBs

Small doesn't mean unprepared — but it does mean focus.

To build resilience, SMBs should prioritize visibility, critical asset protection, and simple but effective controls. Global frameworks like NIST CSF and ISO 27001 aren't just for enterprise — they scale down if you know where to start.

Map what Matters

Identify your most valuable systems and data — from hotel booking platforms to customer databases.

Assess gaps, not everything

Use free tools like CIS Controls or a guided assessment to pinpoint real risks.

Start Small, Protect Smart

MFA, asset inventory, and logging are low-cost, high-impact.

Document and Adapt

Even a simple risk register or incident checklist helps shift your team into a proactive mindset.

Leverage Regional & Global Support

Many SMBs in the Caribbean feel like they're fighting this battle solo. But there are valuable resources built exactly for your context.

Who Can Help:

- TT-CSIRT & OECS Cybersecurity Unit – for timely alerts and regional threat updates
- CARICOM IMPACS – for cyber policy alignment and public-private coordination
- Cybersecurity incentives – Trinidad & Tobago offers up to TTD 500,000 in tax-deductible security investments
- Cybersecurity Service Providers with global and regional experience that can customise their services to your needs

How to Take Advantage:

- Sign up for your national CSIRT bulletins
- Request basic threat assessments via regional units
- Consult your tax advisor about available deductions, where applicable



The Ecosystem Challenges

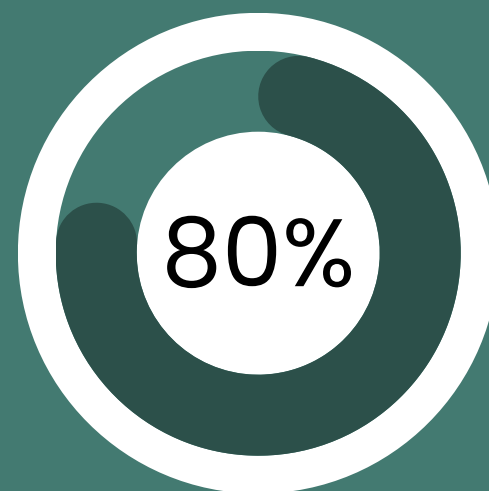
Your Security is Only as Strong as Your Weakest Link
The Reality:



**60% of breaches
involve third-party
vendors**



**82% of attacks
use stolen
credentials**



**80% exploit known
vulnerabilities with
available patches**

Ransomware spreads laterally through unsegmented networks

Caribbean Context: Increasingly interconnected regional supply chains = shared risk

Key Message: You can't protect what you can't see or control



Four Ecosystem Security Pillars



VENDOR RISK MANAGEMENT

Audit third-party access, enforce security standards

NETWORK SEGMENTATION

Contain breaches, limit lateral movement

MULTI-FACTOR AUTHENTICATION

Block 99.9% of credential attacks

SYSTEMATIC PATCH MANAGEMENT

Close vulnerability windows consistently

**Key Principle:
Layered defenses
—attackers must
overcome all four**

Vendor Risk + Network Segmentation

Manage External & Internal Risk

VENDOR RISK MANAGEMENT:

Quick Actions:

- Inventory all vendors with system/data access
- Classify by risk: Critical – Elevated – Standard
- Require security questionnaires for critical vendors
- Include security clauses in all contracts (breach notification, audit rights)

NETWORK SEGMENTATION:

Essential Segments:

- Guest WiFi → Internet only (isolated)
- Point-of-Sale → Payment processor only
- Office → Internal apps + controlled internet
- Servers → Critical data and applications
- Admin → All segments (MFA required)

Impact: Segmentation reduces ransomware spread by 70–90%



Multi-Factor Authentication (MFA)

The Single Most Effective Control

The Problem:

- 82% of breaches involve stolen credentials
- Passwords alone are inadequate
- Users reuse passwords across sites

The Solution:

- MFA Something you know + Something you have + Something you are

The Impact:

- MFA blocks 99.9% of automated credential attacks



MFA Methods Compared

Choosing the Right MFA Approach

Recommendation:
Authenticator apps or push notifications for most users; hardware

Method	Security	User Experience	Cost	Recommendation
SMS/Text codes	⚠ Medium	★★★ Easy	\$ Free	Better than nothing
Email codes	⚠ Medium	★★★ Easy	\$ Free	Non-critical systems
Authenticator Apps	✅ Strong	★★ Moderate	\$ Free	Standard choice
Push Notifications	✅ Strong	★★★★ Very Easy	\$ Low	Best user adoption
Hardware Tokens	✅✅ Very Strong	★★ Moderate	\$\$ Medium	High-security roles
Biometrics	✅ Strong	★★★★ Seamless	\$ Varies	Mobile/modern devices

Patch Management

Close the Vulnerability Window

The Problem:

- 80% of breaches exploit known vulnerabilities
- Patches available for months or years before exploitation
- Attackers scan for unpatched systems continuously

Examples:

- Log4Shell (2021): Massive exploitation within hours
- MOVEit vulnerability (2023): Zero-day to mass exploitation in weeks

Caribbean Impact: Limited IT staff + competing priorities = delayed patching = increased risk

The Goal: Systematic, prioritized patching process



What Needs Patching?



Automation Strategy:

- Auto-patch: Workstations, non-critical systems
- Staged deployment: Production servers, critical apps
- Compensating controls: Legacy/unpatchable systems
- What to Patch: ✓ Operating systems ✓ Applications ✓ Network devices ✓ Web applications ✓ Firmware/IoT devices

Caribbean Context: Schedule large updates for off-peak hours (bandwidth)

Severity	Asset Criticality	Timeline
Critical (9-10)	High	24-48 hours
Critical (9-10)	Medium/Low	7 days
High (7-8.9)	High	7 days
High (7-8.9)	Medium/Low	30 days
Medium (4-6.9)	Any	90 days

Invest Smartly: The Investment Challenge

The Caribbean Cybersecurity Paradox

Key Challenges:

Cyber threats are
growing
exponentially

Budgets remain
constrained

Technical talent is
scarce

24/7 monitoring is
cost-prohibitive

The Solution: Strategic investment
in force-multiplier technologies



What are the Investment Pillars?

AI-DRIVEN SECURITY: 24/7 automated detection & response

Reduces detection time
from days to hours

One analyst does the
work of three

CLOUD-NATIVE SECURITY: Enterprise- grade protection built in

Encryption, IAM,
compliance included

500K+ on-prem security =
cloud subscription

OUTSOURCED MONITORING (MSP/MDR) : 24/7 SOC without hiring 24/7 staff

\$36K-\$180K/year vs.
\$200K+ for in-house team

Immediate expertise, no
training curve

**ROI: Preventing one breach pays
for years of investment**

AI-Driven Security : The Equalizer

Artificial Intelligence –
Your 24/7 Security Analyst

Why AI Matters for Caribbean Businesses:

- Works continuously without fatigue
- Analyzes millions of events per second
- Learns and adapts to new threats
- Compensates for limited staff

Key Stat:

AI reduces threat detection time from days to
hours



AI Security – Quick Wins

Deploy AI Where It Matters Most

Priority 1: Email Security (90% of breaches start here)

- AI-powered phishing detection
- Business email compromise prevention
- Natural language processing for social engineering

Priority 2: Endpoint Behavioral Analytics

- Detects ransomware before encryption
- Identifies compromised credentials
- Automated threat response

Priority 3: Vulnerability Management

- Continuous scanning + risk prioritization
- Tells you what to patch first
- Automates remediation workflows

Start Small: Email security + endpoint protection = 70% risk reduction



Cloud Security Benefits

Cloud Platforms: Enterprise Security for Everyone

Built-In Security Features:

Identity & Access Management

- Centralized authentication and MFA
- Role-based access control

Data Protection

- Automatic encryption (rest & transit)
- Managed key services

Network Security

- Virtual private clouds with isolation
- Built-in firewalls and DDoS protection

Compliance & Monitoring

- Automated logging and audit trails
- Pre-configured compliance frameworks



Smart Sourcing Strategy



Key Selection Criteria:

- ✓ Regional presence or Caribbean experience
- ✓ Response time SLAs (<1 hour critical)
- ✓ Local compliance expertise
- ✓ Transparent pricing, no hidden fees

Business Size	Recommended Model	Monthly Cost
<50 employees	MSP + Email Security	\$500-\$2K
50-200 employees	MSP + Focused MDR	\$3K-\$8K
200+ employees	Full MDR Partnership	\$8K-\$20K



LOWDEN

About Howden

Howden is a global insurance group with employee ownership at its heart. We're experts in helping clients adapt and thrive in a changing world. We provide insurance broking, risk management and claims consulting services, offering scale with the experience to deliver.

22,000

Colleagues

\$38bn

Premium under management

32.2%

Employee owned

110+

Territories



Howden at the forefront of
insurance innovation



Broker of the Decade
British Insurance Awards 2024

Global Reach, Local Expertise

Having operated in the Caribbean for 13 years we can provide local expertise to help you navigate your ever evolving risk landscape.

13 years

In the Caribbean

10+ years

Partners of Caribbean
Association of Banks

\$22m+

Claims paid into
the Caribbean

80+

Team members
focused on Financial
Lines

180

Banks worldwide

\$1.5bn

Premium placed into
the Financial Lines market

Cyber Threats to Watch in 2025: An Insurer's Perspective

Ransomware

Ransomware remains the top cyber threat, responsible for 68% of incidents with advanced extortion techniques.

Phishing and AI-driven Attacks

Phishing is the most common entry point, intensified by AI-driven tactics increasing attack sophistication.

Supply Chain Vulnerabilities

Supply chain attacks target third-party relationships, posing significant challenges for cyber resilience.

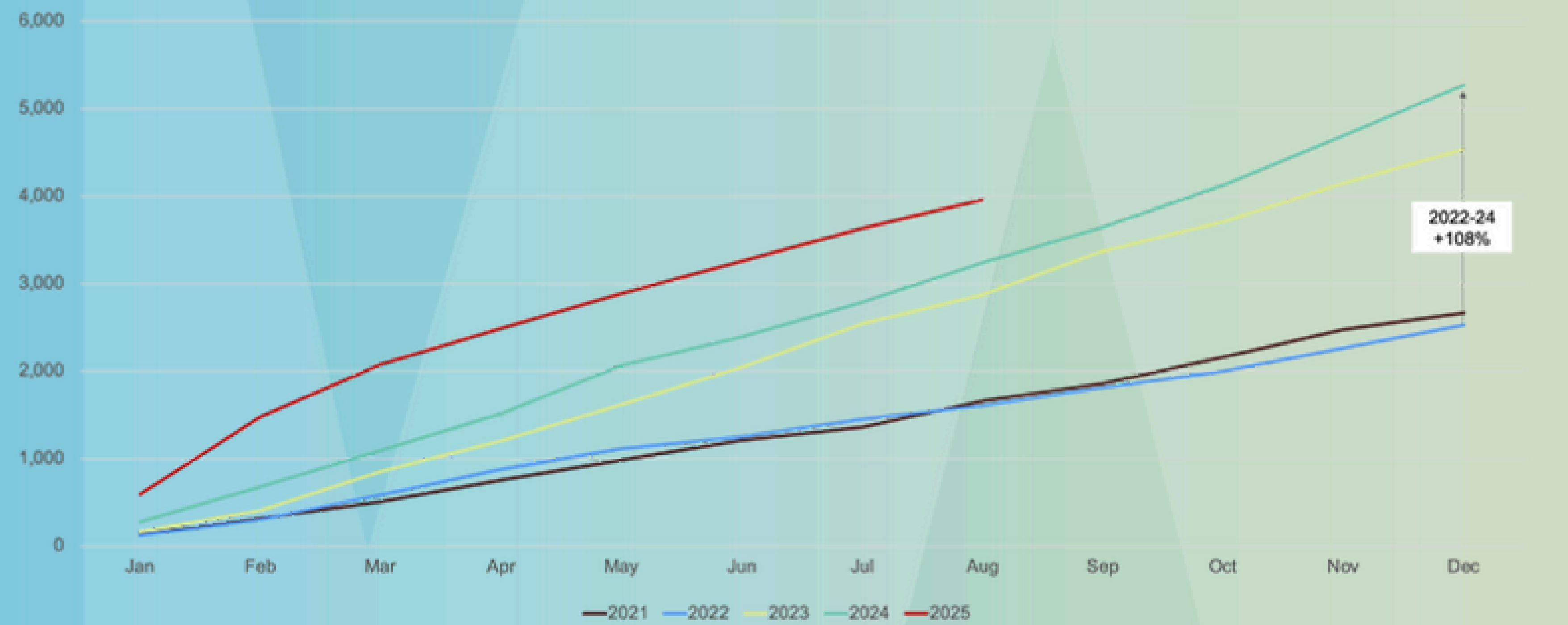
Nation-State and AI-enabled Threats

Nation-state actors and AI tools enable advanced persistent threats targeting critical infrastructure.



Ransomware persists as a leading threat, with every year since 2022 seeing more global incidents than the last

Cumulative global ransomware activity (number of attacks) – 2021 to 3Q25



Note: NCC Group tracks ransomware groups operating the hack and leak double extortion tactic by monitoring leak sites and scraping victims' details as they are released. Source: Howden analysis based on NCC data

Recovery costs, although down in 2025 vs 2024, nonetheless apply additional burden on businesses, often exceeding quantum of ransom payments

Mean recovery costs from ransomware attacks – 2021 to 2025



Note: Recovery costs include downtime, people time, device costs, network costs, lost opportunities and exclude ransom payments. Source: Howden analysis based on Sophos data

What does Cyber Insurance Cover?

Cyber Breach Response

- Credit Monitoring Costs
- Cyber Extortion Costs
- Data Restoration Costs
- Forensic Costs
- Legal Representation Costs
- Notification Costs
- Public Relations Costs

Business Interruption Loss – Cover for your loss of net profit during the period of interruption, as well as the costs to avoid or mitigate effects of the system outage, network interruption or degradation.

Network Security & Privacy Liability – Damages, Regulatory Investigations fines and penalties (where insurable by law) awarded against you as a result of a data breach or unauthorised access .



Insurance Market Conditions

Is it a good time to purchase Cyber Insurance?

Rate Reductions

New entrants in the market helping to drive down premium rates – average rate reductions of 22%

Policy Enhancements

Competition in the market has resulted in Insurers enhancing coverage to give them an edge i.e Lower deductibles, shorter waiting periods for Business Interruption.

Abundance of Capacity with strong financial rating

Numerous Lloyd's of London Insurers wanting to insure Caribbean businesses



IT Security Requirements

What IT security do you need to purchase cover?

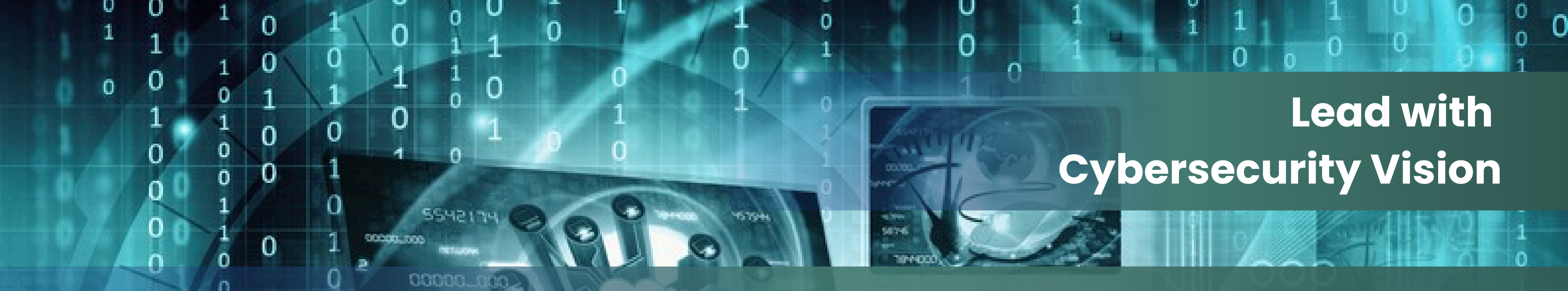
Minimum

- Multifactor authentication (MFA) required for all remote access to applications and servers
- Endpoint detection and response (EDR) deployed on all parts of the environment able to carry an agent
- Back-ups disconnected from and inaccessible through the organisations network and/or using a dedicated cloud storage provider Back up critical data regularly (minimum once per week)
- Email filtering is used and that the system is activated for all email accounts

Recommended

- Robust Continuity Plan which is regularly tested
- Do you conduct penetration tests of your network at least annually
- Encryption on all portable media, including phones and tablets
- Processes are in place to identify and apply patches within 30 days of release





Lead with Cybersecurity Vision

Cybersecurity as Business Priority

Make cybersecurity a board-level priority integrated into the core business strategy for company-wide impact.

Role of vCISO and Security Champion

Engage a virtual Chief Information Security Officer or appoint a security champion to guide SMB security posture.

SMART Cybersecurity Actions

Define and communicate cybersecurity vision by earliest Qtr. and assess security posture within 90 days for accountability.



Strategic Cybersecurity Leadership



Building Awareness and Vigilance

- **Security-First Culture**

Your staff and customers are your first line of defense and interestingly, your most vulnerable interface for attacks. Equip them with knowledge and tools to identify and respond to cyber threats effectively. e.g. Education campaigns, special help lines.

- **Simulated Attack Exercises**

Conduct attack simulations to assess defenses and improve security posture based on threat exposure and communicate findings to key stakeholders and adjust plan if needed. Summary report should be tabled to Board and Executive levels.

- **Encouraging Vigilance**

Promote reporting of suspicious activities and reward employees for maintaining security awareness.

- **SMART Security Actions**

Implement quarterly trainings, phishing simulations, and security reward programs to reinforce security culture. Provide Quarterly reports to the Board – Transparency is your friend!

Addressing Cyber Resilience Challenges



Challenges to Cyber Resilience

Caribbean SMBs face threats like rising cyber-attacks, budget limits, talent shortages, and overconfidence in security.

Budget and Capability Gaps

Only 22% of SMBs have advanced capabilities while many allocate less than 5% of IT budgets to security.

Talent Shortages Impact

A global shortfall of cybersecurity professionals affects SMBs as skilled workers prefer larger enterprises.

SMART Actions for Resilience

Increasing security budgets to at least 7-10% and partnering with providers (services, and information respective CSIRTs) boost SMB cyber resilience.
Protect your cashflow – Evaluate Cyber Insurance Coverage.



At the very beginning of Stratos Cyber, our commitment or our WHY is to empower our clients to thrive in the challenges businesses are facing in the Caribbean. To achieve this we understood the need to deliver our cybersecurity services as a **business commodity** from a customer-centric perspective.

In essence, essential services that customers expect to be available with minimal friction, much like electricity, internet, or cloud storage.

Stratos Cyber focuses on the following pillars:

Simplicity & Accessibility

- Offer **plug-and-play solutions** that are easy to deploy and manage.
- Provide clear onboarding and **self-service portals** for customers to monitor and control their cybersecurity posture.

Transparent Pricing

- Use **flat-rate or usage-based pricing models** to make costs predictable.
- Provide **value comparisons** to show ROI and cost-effectiveness.

Standardization

- Package services like **endpoint protection, firewall management, threat detection**, and **incident response** into tiered bundles.
- Use **industry-standard frameworks** (e.g., NIST, ISO 27001), innovation, and strategic partnerships, to ensure consistency and trust.

Reliability & Trust

- Ensure **99.9% uptime, 24/7 monitoring**, and **rapid incident response**.
- Offer **SLAs** (Service Level Agreements) that guarantee performance.

Scalability & Flexibility

- Enable customers **to scale up or down** based on their needs.
- Offer customised or **modular services** that can be added or removed without disrupting operations. Bringing our global and regional experience to a local/company business context.

Customer Support & Education

- Provide **human-centric support** with fast response times.
- Offer **educational resources** to empower customers to understand and manage their cybersecurity risks.



Final Takeaway: Resilience is a Strategy, Not a Slogan

Cyber resilience isn't about avoiding every attack — it's about building a proactive, informed culture that can detect, respond, and recover faster than the threat can spread.

For small and mid-sized organizations, this means:

- Knowing what matters most
- Making smart, risk-based investments
- And building muscle memory through training, frameworks, and partnerships

It's not about perfection.

It's about preparation — and protecting the people, data, and operations that drive your mission.



Q&A



Contact us for more details:



BLAIR BUCHANAN
Head of Financial Institutions



MARY POPO
Consultant



RICHARD MILVERTON
Divisional Director

[LinkedIn](#)



Howden Group
www.howdengroup.com



ANTHONY SUBERO
Chief Executive Officer

[LinkedIn](#)



MICHEL-ANGE ZAMOR
Chief Technology Officer

[LinkedIn](#)



ANA ZAVGORODNIA
Chief Operating Officer

[LinkedIn](#)



Stratos Cyber
www.stratos-cyber.com





HOWDEN

October 2025

Thank You For Your Attention



Stratos Cyber
www.stratos-cyber.com



Howden Group
www.howdengroup.com

