



10 Commandments of Cybersecurity for Caribbean Business Leaders





Stratos Cyber's 10 Commandments for Caribbean Business Leaders

What we are about to share comes from 25+ years in cybersecurity, not just advising but leading from inside organisations.

From our collective senior and executive roles in major institutions that include cybersecurity companies and countless conversations with business leaders, we at Stratos Cyber have seen what works, what fails, and regrettably, what many wished they had done earlier.

So today, from our Leadership to you, we are sharing what we call:

The 10 Commandments of Cybersecurity for Caribbean Leaders

No technical theory. No vendor talks. Just leadership truths—earned the hard way.



The 10 Commandments of Cybersecurity for Caribbean Leaders

I. Cyber Risk = Business Risk

Cybersecurity is no longer IT's problem.
It's revenue, reputation, and regulation.

If it's not discussed at the board table,
it's already unmanaged.





The 10 Commandments of Cybersecurity for Caribbean Leaders

II. Lead from the Top

Culture follows leadership.

If leaders bypass controls, delay training, or treat cyber as “IT’s job,” the organization learns that security is optional.





The 10 Commandments of Cybersecurity for Caribbean Leaders

III. Know What You Own and What Matters

Every leader should know:

- What data would cripple the business if exposed
- What systems must never go offline

We are a “too Small a market for attacks” creates big blind spots.



The 10 Commandments of Cybersecurity for Caribbean Leaders

IV. Invest Based on Risk, Not Fear

Cyber spending driven by panic is always more expensive.

Smart leaders invest early, proportionately, and strategically.





The 10 Commandments of Cybersecurity for Caribbean Leaders

V. Prepare for Breach—Don't Hope Against It

Hope is not a strategy.

Mature organisations assume breach and plan for it, testing response, leadership decisions, and communications.



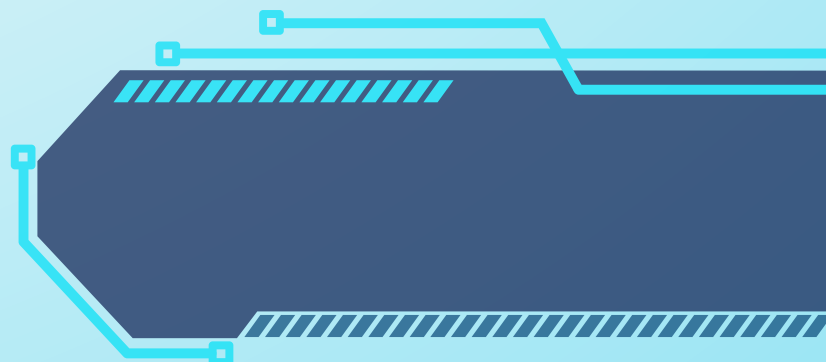


The 10 Commandments of Cybersecurity for Caribbean Leaders

VI. Cybersecurity Is a Human Discipline

Most incidents start with one click, not elite hackers.

Technology helps—but trained, empowered people are your strongest control.





The 10 Commandments of Cybersecurity for Caribbean Leaders

VII. Govern Third Parties Like Yourself

If a vendor touches your systems, data, or brand—they share your risk.

Outsourcing does not outsource accountability.





The 10 Commandments of Cybersecurity for Caribbean Leaders

VIII. Compliance Is the Floor, Not the Goal

Passing audits $\neq$ resilience.

Leaders must ask: Are we truly resilient, or just compliant?



The 10 Commandments of Cybersecurity for Caribbean Leaders

IX. Measure What Matters

Executives should see cyber risk in business language, with trends over time—not technical noise.

What gets measured, gets managed.





The 10 Commandments of Cybersecurity for Caribbean Leaders

X. Cybersecurity Is a Trust Obligation

Trust is now a business currency.

Customers, regulators, employees, and
shareholders expect resilience.

Cybersecurity is no longer optional, it's
fiduciary leadership.



The 10 Commandments of Cybersecurity for Caribbean Leaders

Final Thought

The Caribbean is digitizing faster than its cybersecurity maturity.

The leaders who build resilience won't be the most technical—but the most intentional.

Cybersecurity does not belong in IT.

It belongs with executives and in the boardroom—where strategy is set and accountability lives.

