CYBERSECURITY WEBINAR SERIES • 2026

When There's No Cyber Team:

Building an Incident Response Plan You Can Actually Use

Practical Guidance for Caribbean Financial & Business Leaders

STRATOS-CYBER INC.

SESSION OVERVIEW

Threat Landscape

IR Framework

3 Live Scenarios

Practical Checklists

SESSION AGENDA

01 **The Caribbean Threat Reality**

Why incident response is no longer optional

02 **Understanding Incident Response**

Framework, phases & what it means in practice

03 **Building Your IRP**

Plan, classification, playbooks & communication

04 **Evidence & Containment Basics**

What to do before your IR partner arrives

05 **Three Live Scenarios**

Ransomware · Business Email Compromise · Credential Theft

06 **Your Pre-IR Checklist**

Critical actions in the first 60 minutes

Cyber incidents are not a distant risk — they are happening across our region now

73%

of Caribbean SMBs have no formal IR plan

$1.2M

Average cost of a data breach in LATAM/Caribbean

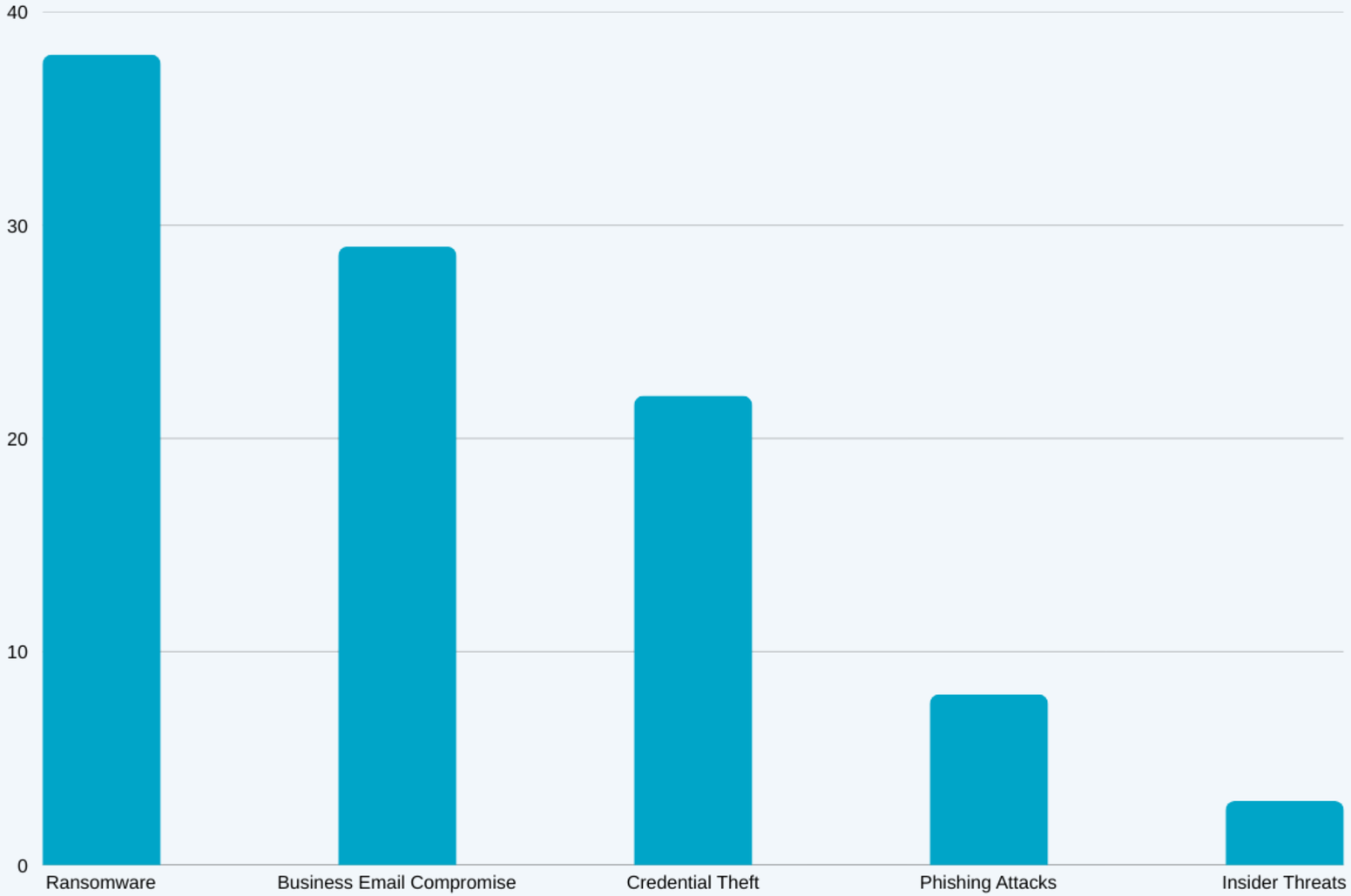
287

Days average breach goes undetected

Ransomware Attack	Email / Phishing Compromise	Ransomware / System Compromise	Ransomware
Curaçao Tax & Customs Administration 2025 Ransomware encrypted core systems, all services offline for 11 days, Dutch cybersecurity specialists flown in, ransom demand confirmed by Finance Minister	**Aruba Parliament** 2025 Official email accounts of multiple MPs hacked, used to send phishing messages to constituents	**Joint Court of Justice (Aruba, Curaçao, Sint Maarten, BES islands)** 2025 Malware hit IT systems, court shut down for multiple days, legal proceedings postponed, emails lost July 23–28	**Bahamas government** 2025 Ransomware attack, just weeks after Turks & Caicos was hit by a separate ransomware group

Sources: The Record / Recorded Future News · Curaçao Chronicle · Cybernews · CSIS Significant Cyber Incidents · LATAM CISO Report 2024 (Duke University)

Most common cyber incidents affecting Caribbean financial institutions and SMBs



Based on regional incident data and CARICOM cybersecurity reports 2023–2024

Ransomware is #1

38% of Caribbean incidents. Average ransom demand has tripled since 2022.

BEC Attacks Rise

Business Email Compromise causes the highest financial loss per incident — avg $50K.

Credential Theft

Often the entry point for both ransomware AND BEC. MFA can stop 99% of these.

What it is — and why the first hour matters most

> *"By failing to prepare, you are preparing to fail."*
>
> — Benjamin Franklin

Without an IR Plan

- ✗ No one knows their role
- ✗ Evidence is destroyed accidentally
- ✗ Attacker remains undetected for weeks
- ✗ Regulators & members lose confidence
- ✗ Business never fully recovers

With an IR Plan

- ✓ Clear roles activated immediately
- ✓ Evidence preserved for legal/insurance
- ✓ Attacker contained within hours
- ✓ Transparent, controlled communication
- ✓ Faster recovery, lower total cost

THE INCIDENT RESPONSE LIFECYCLE

Six phases that turn chaos into a controlled, documented response

1 — PREPARATION

- IRP documented
- Roles assigned
- Tools ready

2 — DETECTION

- Alert received
- Verify incident
- Scope impact

3 — ANALYSIS

- Collect evidence
- Identify vector
- Timeline built

4 — CONTAINMENT

- Isolate systems
- Block attacker
- Preserve data

5 — ERADICATION

- Remove malware
- Patch vectors
- Clean rebuild

6 — RECOVERY

- Restore systems
- Monitor closely
- Resume ops

↻ *Continuous Improvement Loop — each incident improves the plan*

Seven core elements every organization must have documented before an incident

01

Response Charter

Formal mandate: authority to act, budget, executive sponsorship, and legal boundaries.

02

CSIRT Roles & Contacts

Named individuals (primary + backup) for IT, Legal, HR, PR, and Executive communications.

03

Incident Classification

Severity tiers (Critical/High/Moderate/Low) with defined escalation thresholds for each.

04

Communication Plan

Pre-approved templates for staff, regulators, members, media, and law enforcement.

05

Incident Playbooks

Step-by-step procedures for each incident type. Not improvised — written and rehearsed.

06

Evidence Procedures

Chain of custody, log retention policy, forensic contacts, and insurance notification steps.

07

Training & Testing

Annual tabletop exercises. At least one simulated incident per year. Document gaps found.

INCIDENT CLASSIFICATION FRAMEWORK

Not all incidents are equal — your response must be calibrated to the severity

CRITICAL	Examples: Active ransomware • Domain Controller compromised • Mass data exfiltration Response: Immediate CEO/Board notification • Invoke IRP • Contact IR partner • Regulatory filing within 72 hrs	**SLA: < 15 minutes**
HIGH	Examples: Confirmed BEC • Credential breach • Malware detected on servers Response: Dept head + IT lead notification • Contain systems • Preserve evidence • Assess scope	**SLA: < 1 hour**
MODERATE	Examples: Phishing email opened • Unauthorized access attempt • Failed login spike Response: IT team investigates • Log collection • User password reset • Monitor 48 hrs	**SLA: < 4 hours**
LOW	Examples: Policy violation • Lost device (unconfirmed access) • Spam campaign Response: Ticket logged • Standard remediation • Review at next security meeting	**SLA: < 24 hours**

Who communicates what, to whom, and when — pre-written before you need it

⚠ **CRITICAL RULE: During an active incident, STOP using corporate email. Assume attacker has access. Use personal mobile phones only.**

Audience	When to Notify	Channel	Key Message Content
Executive / Board	**Within 1 hour**	Personal call	Incident confirmed, severity, initial actions taken, decision needed
Staff / All Employees	**Within 2–4 hours**	SMS / In-person	Do not use email/Teams. Follow IT instructions. Do not discuss externally.
Regulator / Central Bank	**Within 72 hours**	Official letter / Portal	Nature of breach, data affected, steps taken, point of contact
Members / Customers	**After containment**	Website / SMS / Post	What happened, data involved, what you're doing, what they should do
Law Enforcement	**Critical incidents**	Direct contact	Evidence package, timeline, known indicators. Do not delay.
Media / Public	**As needed**	Prepared statement	Brief, factual. CEO or designated spokesperson ONLY. No speculation.

EVIDENCE PRESERVATION — BEFORE YOU TOUCH ANYTHING

Actions taken in the first 30 minutes can make or break your legal and insurance claim

✓ DO THESE THINGS

- Photograph ransom notes / screen messages before closing
- Export firewall, VPN, Active Directory, and email logs to a USB drive
- Hibernate (not shut down) machines that are actively running
- Document the timeline: who noticed what, and when
- Notify your cyber insurer immediately — do not delay this
- Use personal phones for all response communications

✗ NEVER DO THESE

- Do NOT power off an encrypted machine — you lose volatile RAM evidence
- Do NOT run antivirus scans that may overwrite artifacts
- Do NOT wipe or reimage any machine before imaging it first
- Do NOT communicate via corporate email/Teams/Slack
- Do NOT pay ransom without legal and executive approval
- Do NOT post on social media or speak to press unilaterally

Live Scenarios

What does incident response look like in practice? Let's walk through three real-world cases.

Severity: CRITICAL • Assumption: Limited security staff • Objective: Stop the spread, preserve evidence

PHASE 1: IDENTIFICATION — Confirm & Scope

Signs to Look For

- Files renamed (.locked, .enc extensions)
- Ransom note on desktops / wallpaper changed
- Server services (SQL, File Shares) crashing
- Users locked out of accounts suddenly

Immediate Scope Questions

- Are Domain Controllers encrypted?
- Are backup servers affected?
- Is internet connection still active?
- How many machines showing symptoms?

PHASE 2: CONTAINMENT — Stop the Bleeding

Network Kill Switch

Unplug ISP cable OR disable WAN interface on firewall. This stops C2 traffic and data exfiltration.

Segment Internally

Isolate infected VLANs. Disconnect switch uplinks. Shut down corporate Wi-Fi SSID.

Isolate Endpoints

Unplug network cables (not power). Hibernate if possible — do NOT power off (RAM evidence lost).

Identity Lockdown

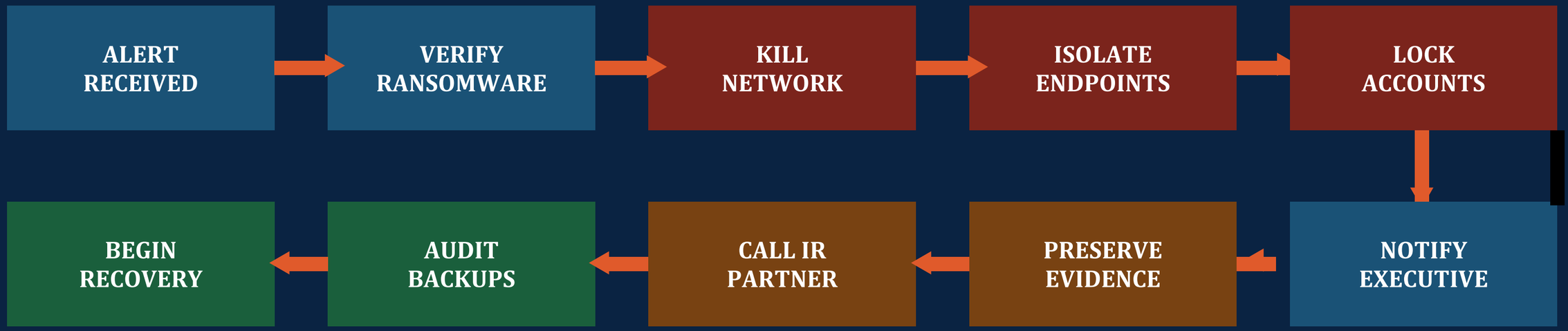
Reset Domain Admin + krbtgt passwords (twice). Disable the 'Patient Zero' account immediately.

Out-of-Band Comms

STOP using corporate email/Teams. Switch to personal phones. Create a WhatsApp response group.

RANSOMWARE: DECISION FLOW

Follow this sequence in order — deviation can compromise recovery



RECOVERY SEQUENCE (in order)

1. Clean Network

Reinstall/update firewall config

2. Rebuild Identity

Clean DC install or restore from verified backup

3. Restore Data

Scan backups in isolated environment first

4. Harden & Monitor

Deploy EDR, enable MFA, monitor anomalies 30 days

CASE 2: BUSINESS EMAIL COMPROMISE (BEC)

Severity: HIGH • Attacker impersonates executives or vendors to redirect payments or harvest data

HOW A BEC ATTACK WORKS

1 — Recon

Attacker researches org via LinkedIn, website, social media

2 — Compromise

CEO/CFO email hacked via phishing or password spray

3 — Impersonate

Fake invoice or wire request sent to Finance staff

4 — Transfer

Funds wired to attacker-controlled account

5 — Cover Tracks

Rules set to auto-delete replies. Detection delayed.

RESPONSE STEPS

- Block the compromised account immediately
- Search mailbox for inbox rules hiding replies
- Notify bank to recall any wire transfers made in last 48 hrs
- Audit email forwarding rules for all executives
- Review all sent items for data exfiltration
- Enable MFA on all email accounts immediately

PREVENTION (Your Best Defense)

- ✓ Enable MFA on ALL email accounts — especially executives
- ✓ Implement email authentication: DMARC + DKIM + SPF
- ✓ Require two-person approval for wire transfers > threshold
- ✓ Train staff to verify payment changes by phone (known number)
- ✓ Use separate, verified channels for payment authorization

CASE 3: CREDENTIAL THEFT & ACCOUNT TAKEOVER

Severity: HIGH • Often the entry point for both ransomware and BEC — and the most preventable

INDICATORS OF COMPROMISE

- Login from unusual geography (VPN or foreign IP)
- Spike in failed authentication attempts
- Account active outside business hours
- Unexpected password reset requests
- New MFA device added to executive account
- Service account suddenly querying many systems

RESPONSE SEQUENCE

1. **Force Password Reset**
   Immediately reset the affected account(s) and revoke all active sessions.
2. **Audit Access Logs**
   Review what systems the account accessed in the last 30 days. Map lateral movement.
3. **Disable & Investigate**
   Disable account until cleared. Examine email rules, file access, and API tokens.
4. **Scope the Breach**
   Were other accounts accessed? Was data exfiltrated? Check cloud storage too.
5. **Enable MFA Everywhere**
   This incident is your mandate. Enable MFA on all systems before re-activating accounts.

BEFORE YOU CALL YOUR IR PARTNER

Critical actions your team can execute in the first 60 minutes — while help is on the way

0–10 min

- Confirm the incident is real (not a test)
- Activate your CSIRT contact list
- Switch to personal phones for all comms
- Notify the CEO / Executive on call

10–30 min

- Isolate affected systems from network
- Photograph all visible evidence on screen
- Export logs to USB (firewall, VPN, AD)
- Notify your cyber insurer immediately

30–60 min

- Brief all department heads via phone
- Prepare regulatory notification timeline
- Document everything with timestamps
- Do NOT restore or wipe anything yet

POST-INCIDENT: TURNING A BREACH INTO RESILIENCE

Every incident is a paid lesson. The question is what you do with it.

After Action Report (AAR)

- → Document the complete timeline
- → Identify root cause — how did they get in?
- → Record what worked and what failed
- → Estimate total business impact

Policy & Technical Hardening

- → Mandate MFA on all VPN and mail accounts
- → Remove local admin rights from end users
- → Segment network — isolate critical systems
- → Implement email authentication (DMARC/SPF/DKIM)

Plan & Playbook Updates

- → Update IRP with lessons from this incident
- → Revise playbooks based on gaps discovered
- → Update contact lists and escalation paths
- → Schedule next tabletop exercise within 60 days

Regulatory & Stakeholder Close-out

- → File final regulatory incident report
- → Issue member/customer notification if required
- → Brief Board of Directors with executive summary
- → Close cyber insurance claim with documentation

KEY TAKEAWAYS

What every Caribbean business should walk away knowing

01

Incidents are inevitable. Unpreparedness is a choice.

Caribbean organizations are actively being targeted. Having no plan is the most expensive option.

02

The first 60 minutes determine the outcome.

What your team does before the IR partner arrives — isolation, evidence, communication — is the difference between weeks or months of recovery.

03

Your IRP does not need to be perfect. It needs to exist.

A documented, rehearsed plan — even a simple one — outperforms improvisation every time. Start with classification and a contact list.

04

MFA alone stops 99% of credential-based breaches.

The single highest-ROI security control available. Enable it on email, VPN, and admin accounts today.

05

Evidence determines your insurance payout and legal outcome.

Never wipe a system before imaging it. Preserve logs. Document everything with timestamps.

Free, immediately usable resources to start building your incident response capability today

Ransomware Identification

ID Ransomware
id-ransomware.malwarehunterteam.com

Upload a ransom note to identify the variant and check for free decryptors

No More Ransom
nomoreransom.org

European law enforcement initiative — may have free decryption keys for your variant

Threat Intelligence

Have I Been Pwned
haveibeenpwned.com

Check if your domain's emails appear in known breach databases

Shodan
shodan.io

See what your organization exposes to the internet — from an attacker's perspective

IR Frameworks & Templates

NIST SP 800-61 Rev 2
nvlpubs.nist.gov

The standard IR guide. Free PDF download. Use as your IRP template baseline.

SANS IRP Templates
sans.org/score/checklists

Free incident handling checklists by scenario type

Caribbean Regulators

CARICOM IMPACS
impacs.org

Regional security coordination — escalation path for nation-state or cross-border incidents

Your Central Bank / FSC
Let’s review them together

Know your notification obligations and timelines before an incident occurs

Free, immediately usable resources to start building your incident response capability today

Jurisdiction	Primary financial regulator	Privacy / data protection	FIU / AML authority	National cyber authority
ECCU / OECS banks under ECCB	**Eastern Caribbean Central Bank (ECCB)** — https://www.eccb-centralbank.org/	Varies by member state	Varies by member state	Varies by member state
Jamaica	**Bank of Jamaica (BOJ)** — https://boj.org.jm/ / **Financial Services Commission (FSC Jamaica)** — https://www.fscjamaica.org/	**Office of the Information Commissioner** — https://opm.gov.jm/the-office-of-the-information-commissioner/	**Financial Intelligence Division / FIU** — https://www.fid.gov.jm/about-us/the-financial-intelligence-unit-fiu/	**JaCIRT** — https://www.cirt.gov.jm/
Barbados	**Central Bank of Barbados** — https://www.centralbank.org.bb/ / **Financial Services Commission Barbados** — https://www.fsc.gov.bb/	**Data Protection Commission** — https://www.gov.bb/General/data-protection-commissioner	**Barbados Financial Intelligence Unit** — https://www.barbadosfiu.gov.bb/	National cyber reporting is less centralized on a single public reporting portal than in Jamaica/TT
Trinidad and Tobago	**Central Bank of Trinidad and Tobago** — https://www.central-bank.org.tt/	**Office of the Data Protection Commissioner** — https://www.odpc.gov.tt/	**Financial Intelligence Unit of Trinidad and Tobago** — https://fiu.gov.tt/	**TT-CSIRT** — https://ttcsirt.gov.tt/
The Bahamas	**Central Bank of The Bahamas** — https://www.centralbankbahamas.com/ / **Securities Commission of The Bahamas** — https://www.scb.gov.bs/	**Office of the Data Protection Commissioner** — https://www.bahamas.gov.bs/office-of-the-data-protection-commissioner	**Financial Intelligence Unit** — https://www.fiubahamas.org.bs/	National cyber routing may also involve law enforcement / national cyber channels depending on incident type
Cayman Islands	**Cayman Islands Monetary Authority (CIMA)** — https://www.cima.ky/	**Office of the Ombudsman (Data Protection)** — https://ombudsman.ky/data-protection	**Financial Reporting Authority (FRA)** — https://fra.gov.ky/	National cyber coordination may also involve Cayman national security / police channels depending on impact
Guyana	**Bank of Guyana** — https://bankofguyana.org.gy/	Privacy authority framework is less mature / more fragmented	**Financial Intelligence Unit** — https://fiu.gov.gy/	National cyber reporting may route through state cybercrime / law-enforcement structures

CLOSING THE GAP

How Stratos Cyber Addresses Every Gap We Discussed Today

RISE™ = Resilience · Intelligence · Security · Empowerment — every gap we discussed today maps to a solution below

01

PERIMETER IQ™ — External Attack Surface & Threat Visibility

Continuous discovery of exposed systems, shadow IT, and vendor risks. Real-time alerts on open ports, misconfigured services, and domain misuse — before attackers act.

02

INSIGHT IQ™ — Threat Intelligence & Strategic Advisory

Dark web monitoring, leaked credential alerts, and Caribbean-specific threat intelligence. Monthly briefings calibrated to regional financial sector attack patterns.

03

GUARDIAN IQ™ — 24/7 Managed Detection & Response (MDR)

Round-the-clock SOC operations — detect, investigate, and neutralize threats at speed. Powered by advanced analytics and automation. Your always-on defence.

04

AURA IQ™ — AI Governance & Security Readiness

Ensure AI adoption is safe and compliant. Aligned to ISO 42001, NIST AI RMF, and EU AI Act. Address risks across model integrity, bias, and data sourcing.

05

GOVERN IQ™ — Security Architecture · GRC · vCISO · vDPO

Policies, risk assessments, and audit preparation aligned to Basel, CBTT, BOJ, ISO 27001, and ECCB requirements. Board-ready reporting that satisfies examiners.

06

ASSURE IQ™ — Offensive Security & Adversarial Simulation

Penetration testing, red/blue/purple teaming, and tabletop exercises. Validates defenses under real adversarial pressure — evidence your regulator and insurer will accept.

07

AWARE IQ™ — Cyber Awareness & Workforce Enablement

Role-based training, phishing simulations, and security culture campaigns tailored for finance teams, operations staff, IT, and executive leadership.

08

RESILIENCE IQ™ — Risk-Aligned Security Posture Assessment

Independent pre-coverage or maturity assessments that identify gaps, benchmark resilience, and deliver actionable roadmaps — before your next audit or exam.

YOUR NEXT STEP WITH STRATOS CYBER

Three Ways to Start — Every Path Leads to Resilience

Every service. Every step. One RISE Framework™. Contact us at stratos-cyber.com · info@stratos-cyber.com · +1 514 299 2015

01 START WITH VISIBILITY

PERIMETER IQ™ + INSIGHT IQ™

Know your exposure before anything else

- External attack surface scan — see exactly what attackers see
- Dark web check — are your credentials already compromised?
- Caribbean-specific threat briefing for your leadership team
- Executive summary report delivered within 2 weeks

Ideal for companies that don't yet have a clear picture of their digital exposure

02 ACTIVATE PROTECTION

GUARDIAN IQ™ + GOVERN IQ™

24/7 coverage + regulatory alignment

- 24/7 SOC activation — monitoring and response from day one
- IR plan development scoped specifically to your bank
- vCISO engagement — regulatory gap assessment and roadmap
- Basel / CBTT / BOJ / ECCB compliance mapping

Ideal for companiesthat need to close regulatory gaps before their next examination

03 VALIDATE & ASSURE

ASSURE IQ™ + RESILIENCE IQ™ + AWARE IQ™

Test your defences — train your people

- Penetration test with bank-specific scope using today's scenarios
- Tabletop exercise — ransomware, insider threat, vendor breach
- Phishing simulation measured across all departments
- Board-ready findings report for audit and insurance evidence

Ideal for companies that have controls in place but have never tested them under pressure

READY TO BUILD YOUR INCIDENT RESPONSE CAPABILITY?

We partner with Caribbean financial institutions and businesses to build practical, executable security programs — without the enterprise price tag.

- → Incident Response Plan Development
- → Tabletop Exercise Facilitation
- → Security Awareness Training
- → IR Retainer & On-Call Support

Stratos Cyber Inc. · www.stratos-cyber.com · info@stratos-cyber.com

Find us

→ LinkedIn

→ YouTube

→ Facebook

→ Spotify

Join our Cybercesurity Advisory

Stratos Cyber Inc. · www.stratos-cyber.com · info@stratos-cyber.com