Dawgen GLOBAL

2026 EDITION



Dawgen Global illustration

CYBERSECURITY SERIES · TECHNOLOGY & CYBER

Ransomware Readiness & Cyber Crisis Response

Be ready before the ransom note appears.

Ransomware risk assessments, backup and recovery testing, crisis playbooks and executive exercises that prepare your organisation to withstand and recover from an attack.

HARDEN. REHEARSE. RECOVER.

01 · THE BUSINESS ISSUE

Ransomware is the attack that stops everything.

Ransomware encrypts systems and data, and attackers increasingly steal data first and threaten to publish it. Organisations across the Caribbean, from public services to private companies, have lost days or weeks of operations to these attacks.

Operations stop

Billing, bookings, payroll, payments and public services can all halt at once.

Backups are targeted

Attackers search for and destroy backups before encrypting systems, so untested backups often fail when needed most.

Double extortion

Stolen data can be published or sold even if systems are restored, creating legal and reputational damage.

Decisions under pressure

Leaders must decide quickly about containment, communications, regulators and ransom demands, often without a plan.

QUESTIONS EVERY BOARD SHOULD ASK

- Could we keep operating if our systems were encrypted tonight?
- When did we last restore our backups in a test?
- Are our backups protected from attackers?
- Who decides what, and who do we call?
- How would we tell customers and regulators?
- Does our insurance cover us, and what does it require?

> **Organisations that rehearse their response recover faster and make better decisions under pressure.**

02 · OUR SERVICES

A complete ransomware readiness programme.

We assess your exposure, strengthen your defences and recovery, and rehearse your response with the people who will make the decisions.

Ransomware risk assessment

How exposed you are today.

- Review against common attack paths
- Privileged access and remote access review
- Prioritised hardening plan

Backup & recovery assurance

Backups that work when needed.

- Backup design and protection review
- Restore testing
- Recovery time and point objectives

Crisis playbooks

Clear decisions, agreed in advance.

- Ransomware response playbook
- Roles and decision rights
- Communication templates

Executive exercises

Rehearsing the worst day.

- Tabletop exercises for leadership
- Technical simulations for IT teams
- After-action reports

Crisis response support

Help when it happens.

- Incident response and forensics
- Containment and recovery support
- Regulator and insurer reporting support

WHO WE PREPARE

Public bodies and municipal services · utilities and energy companies · hospitals and clinics · hotels and resorts · financial institutions · manufacturers and distributors · schools and colleges.

Ransomware readiness connects with our business continuity work in the **Governance, Risk & Board Advisory** brochure.

03 · OUR APPROACH

Assess, harden, rehearse, recover.

Our programme is practical and process-driven. We focus on the controls that stop ransomware spreading and the recovery steps that bring you back online.

01

Assess

We review your systems, backups, access controls and incident plans against common ransomware attack paths.

02

Harden

We prioritise fixes such as multi-factor authentication, patching, privileged access controls and network segmentation.

03

Protect backups

We confirm backups are isolated, protected and restorable within your recovery targets.

04

Plan and rehearse

We write a ransomware playbook and test it through tabletop and technical exercises.

05

Respond

If an attack happens, our incident response team supports containment, investigation and recovery.

CONTINUITY AND CYBER TOGETHER

We combine cyber recovery with your hurricane and outage continuity plans, so one plan covers every disruption.

CONTROLS THAT MATTER MOST

- Multi-factor authentication
- Isolated and tested backups
- Patched internet-facing systems
- Limited administrator access

CERTIFIED TEAM

Our cyber specialists hold recognised certifications such as OSCP, CEH, CISM, CCSP and ECIH.

04 · TABLETOP EXERCISES

Rehearse the worst day in a safe room.

A tabletop exercise walks your leadership team through a realistic ransomware scenario, minute by minute, so gaps in plans, roles and communication are found before a real attack.

Realistic scenarios

Built around your systems, sector and regulators.

Real decisions

Containment, communications, legal and ransom questions.

Clear outputs

An after-action report with prioritised improvements.

HOW AN EXERCISE RUNS

01 **Design**

Scenario tailored to your organisation.

02 **Brief**

Participants and roles confirmed.

03 **Exercise**

Two to three hours of guided decisions.

04 **Report**

Findings and actions presented to the board.

WHO TAKES PART

- Chief executive and senior managers
- IT and security leads
- Legal, communications and finance
- Board representatives where useful

REPEAT ANNUALLY

Annual exercises keep plans current as people and systems change.

05 · RECOVERY ASSURANCE

Prove you can recover.

Many organisations discover during an attack that their backups were incomplete, infected or deleted. Recovery assurance confirms you can restore critical systems within the time the business can tolerate.

Backup review

Are backups protected?

- Offline or immutable copies
- Separate credentials for backup systems
- Coverage of critical systems and data
- Monitoring of backup jobs

Restore testing

Do backups actually work?

- Test restores of critical systems
- Measured recovery times
- Recovery order agreed with the business
- Documented recovery runbooks

ON THE DAY OF AN ATTACK

Contain

Stop the spread and protect what is left.

Investigate

Find the entry point and data affected.

Recover

Restore systems safely, in priority order.

> **Paying a ransom does not guarantee recovery. Tested backups and a rehearsed plan are the most reliable route back.**

06 · WHO SHOULD CONSIDER THIS SERVICE

For organisations that must keep operating.

Public bodies delivering essential services

Utilities and energy companies running critical infrastructure

Hospitals and clinics where downtime affects patients

Hotels and resorts with guests to serve every day

Financial institutions with customer funds and data at stake

Boards wanting assurance on cyber recovery

07 · ILLUSTRATION

A public body and a backup that would have failed

Situation. A public body believed its nightly backups would allow recovery from any attack. Its board asked for assurance after a ransomware attack on a similar organisation in the region.

Our work. We assessed its ransomware exposure, tested restores of critical systems and ran a tabletop exercise with senior managers. The restore test showed backups were stored on the same network and used the same administrator accounts.

Outcome. Backups were moved to an isolated, protected location, multi-factor authentication was enforced for administrators, and the body now has a tested ransomware playbook.

Anonymised composite illustration based on regional experience.

WHAT YOU RECEIVE

- Ransomware risk assessment
- Prioritised hardening plan
- Backup and restore test results
- Ransomware response playbook
- Tabletop exercise and after-action report
- Board briefing

08 · ENGAGEMENT OPTIONS

Choose the support you need.

Readiness assessment

Exposure review and prioritised hardening plan.

Recovery assurance

Backup review and restore testing.

Tabletop exercise

Executive ransomware simulation and report.

Full programme

Assessment, recovery assurance, playbook and exercise.

Fees are tailored to each organisation and agreed in the engagement letter once scope and deliverables are confirmed.

WHY DAWGEN GLOBAL

- **Caribbean insight.** Over 24 years serving Caribbean business.
- **One desk, 35 territories.** Centrally managed from our Caribbean headquarters.
- **Certified specialists.** Offensive, defensive and forensic skills in one team.
- **Joined-up advice.** Cyber, audit, risk, legal and data protection together.

09 · START HERE

- Request a ransomware readiness assessment
- Book a tabletop exercise for your leadership team
- Ask about combining cyber and continuity planning

CONTACT

Email
info@dawgen.global

Web
https://www.dawgen.global/

Territory desks
Write to your territory desk at *territory*@dawgen.com (for example guyana@dawgen.com). Jamaica: info@dawgen.global

Headquarters
Dawgen Towers, 47-49 Trinidad Terrace, Kingston 5, Jamaica

AUDIT & ASSURANCE · TAX ADVISORY · TECHNOLOGY & CYBER · FINANCE & BPO · GROWTH & RECOVERY · HR & LEGAL

This brochure provides general information only and is not professional advice. Services are provided only under a signed engagement letter. The illustration is an anonymised composite and does not describe any single client.

Dawgen Global is an independent, integrated multidisciplinary professional services firm and is not a member of any international network. As a multidisciplinary firm, Dawgen Global offers some regulated services; in each case the head of the regulated division holds the appropriate professional practice licence in the respective jurisdiction. Some regulatory services are performed by affiliated firms, and clients are advised of this when a request is made.

BIG FIRM CAPABILITIES. CARIBBEAN UNDERSTANDING. · © 2026 Dawgen Global.