Dawgen GLOBAL

2026 EDITION



Dawgen Global illustration

CYBERSECURITY SERIES · TECHNOLOGY & CYBER

Digital Forensics & Incident Response

Uncover the digital traces. Contain the damage. Recover with evidence.

Rapid incident response, forensic investigation and expert reporting when a cyber attack, data breach or insider misconduct strikes.

CONTAIN QUICKLY. INVESTIGATE THOROUGHLY. REPORT CREDIBLY.

01 · THE BUSINESS ISSUE

The first hours after an incident decide the outcome.

When a breach, ransomware attack or insider incident happens, decisions made in the first hours affect how much is lost, how quickly operations resume and whether evidence survives for legal or insurance purposes.

Evidence is fragile

Rebooting systems, wiping devices or restoring backups too early can destroy the evidence needed to understand what happened.

Attackers come back

Without finding how an attacker got in, the same weakness can be used again, sometimes within days.

Reporting duties apply

Data protection laws, regulators, card schemes and insurers may require timely, accurate breach reports.

Disputes need proof

Insurance claims, employment action and court proceedings depend on evidence collected to proper standards.

INCIDENTS WE RESPOND TO

- Ransomware and destructive malware
- Business email compromise and payment fraud
- Data theft and suspected leaks
- Insider misconduct and policy breaches
- Account takeover and unauthorised access
- Website defacement and compromise

> **A well-run investigation answers four questions: how they got in, what they did, what was taken, and how to stop it happening again.**

02 · OUR SERVICES

Response and investigation, end to end.

Our forensic and incident response team follows a recognised three-phase approach: prepare, respond and follow up.

Incident response

Containing the threat fast.

- Isolation of infected systems
- Malware identification and removal
- Recovery guidance

Digital forensics

Recovering and preserving evidence.

- Computer, mobile and server forensics
- Memory and log analysis
- Chain of custody and evidence handling

Breach investigation

Understanding what happened.

- Attack vector and root cause
- Data loss assessment
- Dark web checks for stolen data

Reporting & expert support

Findings others can rely on.

- Breach reports for regulators and insurers
- Reports for card schemes and banks
- Expert witness support

Incident readiness

Prepared before it happens.

- Incident response plans and playbooks
- Incident response retainers
- Tabletop exercises

WHO WE HELP

Financial institutions · insurers and their policyholders · law firms acting for clients · hotels and retailers · public bodies · employers investigating misconduct.

Financial fraud investigations are covered in our **Forensic Services** brochure.

03 · OUR APPROACH

Prepare, respond, follow up.

Our incident response work follows a structured three-phase method. Every step is documented, and evidence is handled so it can support legal, regulatory or insurance processes.

01

First response

We assess the incident, advise on immediate containment and secure systems to protect evidence.

02

Identify and preserve

Devices and data involved are identified, isolated and preserved using forensic methods.

03

Acquire and analyse

Evidence is collected without altering it, then analysed to reconstruct events and find the attack path.

04

Contain and recover

Malicious code and access are removed, weaknesses closed and systems returned to service safely.

05

Report and learn

A clear report sets out findings, data affected, root cause and recommendations, and we support any testimony.

EVIDENCE FIRST

We balance getting you back in business with preserving the evidence you may need later.

OUR FORENSIC PHASES

- Identification
- Preservation
- Analysis
- Documentation and presentation

CERTIFIED RESPONDERS

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

04 · INCIDENT RESPONSE RETAINER

Help on call before you need it.

An incident response retainer agrees terms, contacts and response times in advance, so our team can start immediately when an incident is reported.

Agreed response

Defined response times and a 24/7 contact route.

Pre-agreed terms

Engagement terms in place, so no time is lost on paperwork.

Readiness work

Unused hours can go towards plans, exercises and assessments.

WHEN YOU CALL

01 **Triage**

We assess the situation by phone.

02 **Mobilise**

Responders start remotely or on site.

03 **Contain**

Immediate steps to limit damage.

04 **Investigate**

Forensic work and reporting begin.

RETAINER CLIENTS RECEIVE

- Priority response
- Incident response plan review
- Annual tabletop exercise
- Quarterly threat briefing

INSURER-FRIENDLY

Retainers support cyber insurance requirements for a named response provider.

05 · IN THE EVENT OF A BREACH

What we do when you are under attack.

When a breach happens, our team works alongside your IT staff, insurers and legal advisers to limit damage and restore operations.

Technical response

Stopping the attack.

- Identify the attack vector
- Analyse and isolate malicious software
- Check for dormant malware and backdoors
- Secure data for later analysis

Business response

Managing the consequences.

- Assess possible data loss
- Prepare breach reports
- Advise on regulator and customer notification
- Identify insider involvement where present

AFTER THE INCIDENT

Root cause

Why it happened and how to prevent a repeat.

Remediation

Closing the gaps the attacker used.

Lessons learned

Plan and control improvements.

> **Calling for help early is not an admission of failure. It is the fastest route to recovery.**

06 · WHO SHOULD CONSIDER THIS SERVICE

For organisations facing an incident, or preparing for one.

Organisations under attack needing immediate response

Insurers and brokers needing independent investigation

Law firms needing forensic evidence for clients

Employers investigating misconduct or data misuse

Financial institutions meeting regulatory reporting duties

Boards wanting an incident retainer in place

07 · ILLUSTRATION

A distributor and a fraudulent payment instruction

Situation. A distributor's finance team paid a large supplier invoice to a new bank account after receiving what looked like a genuine email from the supplier.

Our work. Our investigators found that a staff mailbox had been compromised weeks earlier, traced the attacker's activity, confirmed which data was viewed and preserved evidence for the bank, insurer and police.

Outcome. The bank recovered part of the funds, the insurer accepted the claim on the strength of the report, and mailbox security was strengthened across the company.

Anonymised composite illustration based on regional experience.

WHAT YOU RECEIVE

- Immediate containment guidance
- Forensically preserved evidence
- Investigation report and timeline
- Data loss assessment
- Breach reports for regulators or insurers
- Remediation recommendations

08 · ENGAGEMENT OPTIONS

Choose the support you need.

Emergency response

Immediate help when an incident is under way.

Incident response retainer

Agreed response times and readiness work.

Forensic investigation

Evidence recovery and analysis for a specific matter.

Readiness package

Plans, playbooks and tabletop exercises.

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

- Report an incident to info@dawgen.global
- Request an incident response retainer proposal
- Book a tabletop exercise for your leadership team

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. In an active incident, contact us immediately and do not switch off, wipe or restore affected systems until advised.

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.