Cyberfort

Service Overview

An introduction to Cyberfort Crisis Simulation exercises

Cyberfort regularly executes crisis scenario events for customers, where we work with leadership and technical teams to simulate a major incident and assess responses.

We base our events on real incidents we've responded to for a similar size and sector company, and target them to each customer's specific need, providing all resources, materials and media.

Following the event we run a full 'lessons learned' review, with recommendations for improvement. This brochure outlines the different types of crisis simulations we provide, and the key outcomes organisations can achieve by undertaking an exercise of this nature.

01304 814800 cyberfortgroup.com info@cyberfortgroup.com

Board-to-Keyboard

Cyber Incident Response

Cyberfort

This immersive crisis scenario simulation guides your organisation through a coordinated, high-impact cyberattack based on a real-world incident. The exercise is tailored to engage technical responders, executive leadership, and board members, each with scenario-driven materials and decision points aligned to their role.

Simulation Basis

SolarWinds Supply Chain Attack (2020)

A sophisticated, multi-stage breach affecting thousands of organisations globally.

Demonstrates adversary persistence, lateral movement, and the consequences of compromised trusted software.

Highlights the importance of visibility, vendor risk, and internal escalation workflows.

Who's Involved

Stakeholder Group	Role in this Simulation
Technical Teams (IT/SecOps)	Detect, triage, contain, and investigate the compromise. Simulated alerts and logs provided.
Executive Leadership	Manage internal comms, legal, regulatory exposure, and business continuity decisions.
Board Members	Make strategic calls on disclosure, reputational risk, and investment in cyber capabilities.

What's Included

Technical simulations
Simulated telemetry (EDR, SIEM, firewall, identity logs), IR playbook testing, Red Team prompts.

Executive Scenarios
Media inquiries, legal/regulatory pressure, client escalation paths, insurer updates.

Board-Level Briefings
Decision-making simulations on breach notification, public statements, and future risk posture.

Format & Duration

- 3-hour live simulation with optional pre-reading and post-exercise reporting.
- Delivered remotely or on-site, with a facilitator-led briefing and debrief.

Outcomes

Validate real-time collaboration and escalation pathways.

Assess organisational readiness against a high-severity attack.

Identify communication gaps, policy misalignment, and tooling weaknesses.

Generate actionable recommendations aligned to NIST/ISO27035 and regulatory expectations (e.g. DORA, GDPR, SEC).

Private Equity

Ransomware at Portfolio Scale

Based on: Capita ransomware breach (2023) + Kaseya VSA supply chain attack (2021)

PE firms face unique exposure due to centralised IT oversight and interdependencies across portfolio companies. This simulation prepares your fund to respond when multiple assets are simultaneously targeted in a ransomware campaign.

Cyberfort

Crisis Simulation

Coordinated Ransomware Across Portfolio Companies

Audience

Group	Focus
Investment Teams	Risk to asset value, M&A impact, public market reactions
CISOs / CTOs (Portfolio Companies)	Triage, containment, data restoration and negotiations
Managing Partners	Stakeholder assurance, reputational control, investor relations

Materials Provided

- **Simulated encrypted systems and ransom demands**
- **Comms templates for LPs, insurers, and regulators**
- **Decision trees for disclosing material cyber incidents pre/post-IPO**

Outcomes

- Assess cyber resilience across portfolio holdings
- Practice strategic decision-making at the fund level
- Clarify roles between central PE firm and asset leadership

Critical Infrastructure

Operational Downtime & Data Breach

Cyberfort

Based on: Colonial Pipeline Attack (2021)

Targeting fuel, transport, and energy networks, this simulation focuses on blended OT/IT disruption, public panic, and regulatory urgency. Ideal for utilities, logistics, or national infrastructure operators.

Crisis Simulation

Nation-State Compromise of OT & IT Systems

Audience

Group	Focus
OT Engineers / Incident Responders	ICS/SCADA isolation, failover procedures
Executive Crisis Management	Business continuity, media strategy, regulator engagement
Board / CNI Risk Committees	National impact decisions, public trust, long-term resilience

Materials Provided

Simulated SCADA outage with cascading IT effects

Government directives and regulator calls

Public narrative exercises under social media pressure

Outcomes

Stress-test NIS2, ISO 27019, and critical asset protection strategies

Strengthen IT/OT crisis collaboration

Practice with hostile attribution and geopolitical risk

Healthcare

Data Theft, Ransomware & Care Disruption

Based on: NHS & HSE Ireland ransomware attacks (2021)

Patient safety is the priority in this simulation where electronic health records (EHRs) are encrypted and patient data is stolen. This tests your ability to recover systems, communicate with stakeholders, and ensure continuity of care.

Cyberfort

Crisis Simulation

Patient Data Breach & Hospital Service Outage

Audience

Group	Focus
IT & Cyber Teams	EHR recovery, triage, and isolation under pressure
Clinical Operations / Risk	Managing patient care during IT downtime
Executives & Board	Legal/regulatory action, public confidence, ICO/OIC engagement

Materials Provided

- **Simulated EHR lockout and data leak on dark web**
- **Care backlog impacts and patient safety scenarios**
- **Briefing packs for Data Protection Authorities & insurers**

Outcomes

- Validate cyber incident protocols for clinical settings
- Test escalation from hospitals to trust/group/board levels
- Prepare for regulatory, press, and patient response under real-time stress

Financial Services

Insider Access & Market Disruption

Cyberfort

Based on: Morgan Stanley client data breach (2021) + Bangladesh Bank SWIFT heist (2016)

This simulation focuses on the real-time pressure of a compromise involving internal credentials, SWIFT/transaction systems, and client data — testing your ability to respond to both operational and reputational threats.

Crisis Simulation

Credential Compromise & Real-Time Trading Risk

Audience

Group	Focus
Security Operations & IT	Credential forensics, fraud detection, isolation of financial systems
Compliance, Risk & Legal	Regulatory response (FCA, SEC), customer communications
Executives & Board	Market stability, investor assurance, long-term recovery strategy

Materials Provided

- **Simulated internal alerting (e.g. unusual SWIFT activity, failed MFA)**
- **Injects from regulators (e.g. FCA/SEC queries) and media**
- **Customer panic scenarios including high net-worth clients and trading desk impacts**

Optional Enhancements

- Integrate real-world telemetry from SIEM/XDR/SWIFT monitoring
- Include AML and fraud risk team in cross-functional engagement
- Add tabletop walk-through of Section 166 (UK) or NY DFS Part 500 requirements

Outcomes

- Assess readiness for high-velocity financial cyberattacks
- Validate breach disclosure processes and regulatory engagement
- Improve coordination between SOC, risk, legal, and C-level leaders
- Test public and client-facing communications in volatile market conditions

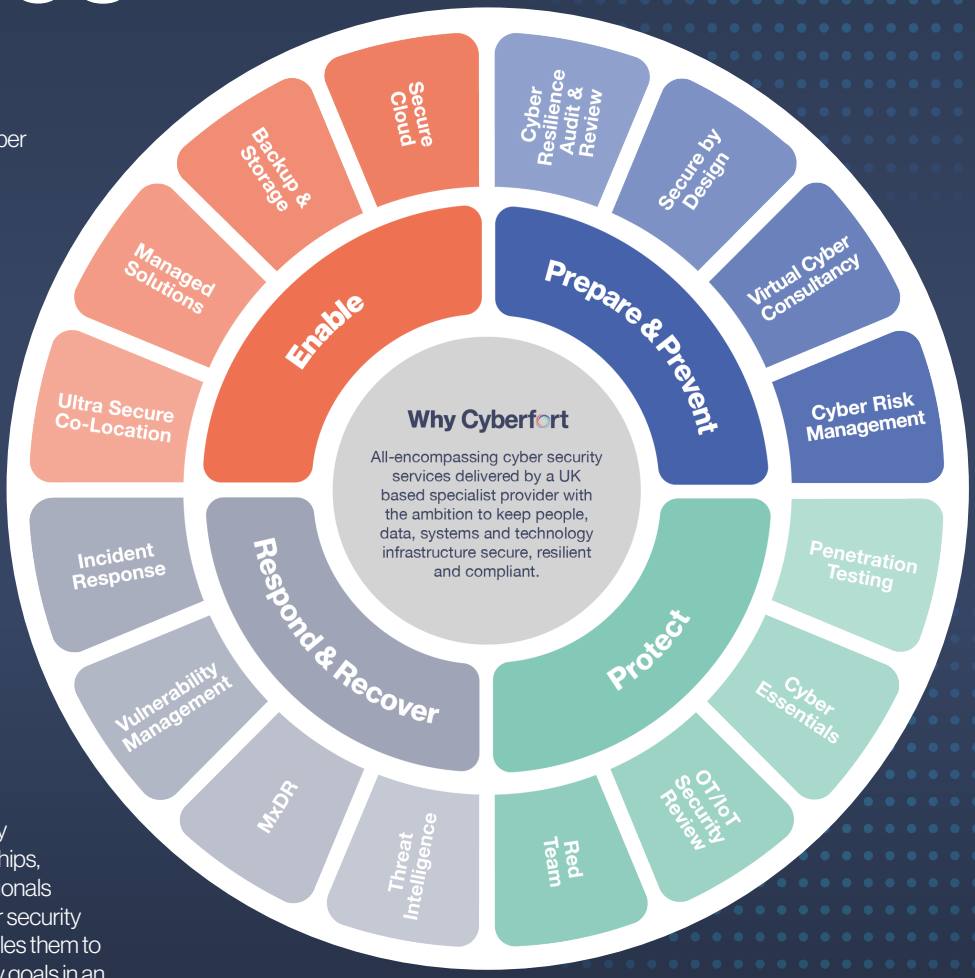
Cyberfort

Discover more about Cyberfort's Services

At Cyberfort we provide a range of customers with all-encompassing Cyber Security services. We are passionate about the cyber security services we deliver for our customers which keeps their people, data, systems and technology infrastructure secure, resilient and compliant.

Our business offers National Cyber Security Centre assured Consultancy services, Identification and Protection against cyber-attacks, proactive Detection and Response to security incidents through our security operations centre and a Secure and Recover set of Cloud solutions which keeps data safely stored, managed and available 24/7/365.

Over the past 20 years we have combined our market leading accreditations, peerless cyber security expertise, strong technology partnerships, investment in our future cyber professionals and secure locations to deliver a cyber security experience for customers which enables them to achieve their business and technology goals in an ever-changing digital world.



For more information on our Crisis Simulation services please contact us at the details below:

01304 814800 | cyberfortgroup.com | info@cyberfortgroup.com

We look forward to working with you!