DATA SECURITY
A UBDS GROUP COMPANY

DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR) SERVICES

For G-Cloud 15

January 2026

CONTENTS

1. INTRODUCTION

3B Data Security is one of the UK's only cyber security providers fully assured by the National Cyber Security Centre (NCSC) to deliver CHECK penetration testing, cyber incident response, cyber incident exercising, and cyber advisory services.

NCSC assured across the board, CREST accredited, and dual-approved by the PCI Security Standards Council as both a Qualified Security Assessor (QSA) and PCI Forensic Investigator (PFI), 3B Data Security is trusted by UK government, regulators, and critical national infrastructure organisations to deliver security assurance at the highest level.

Using the same reconnaissance techniques as threat actors and red teams, 3B Data Security's consultants uncover risks others miss, rigorously challenge assumptions, and deliver clear, action-oriented reporting that enables organisations to secure systems, data, and services that underpin the public sector. This approach is underpinned by **Check. Challenge. Secure.** 3B Data Security's proven method for ensuring defences hold under audit, attack, and public scrutiny.

Backed by over 20 years of real-world experience in digital forensics and incident response, 3B Data Security provides confidence that security controls operate effectively under real-world conditions - not just in theory.

CHECK

We uncover the risks others overlook, using deep expertise and the latest threat intelligence.

CHALLENGE

We rigorously test every control, critique every assumption, and simulate real attacker tactics so nothing is left to chance.

SECURE

We help you close every gap, validate every fix, and prove your defences hold under audit, attack, or public scrutiny.

CERTIFIED AT EVERY LEVEL THAT MATTERS.

Assured Service Provider
in association with National Cyber Security Centre
CHECK Penetration Testing

Assured Service Provider
in association with National Cyber Security Centre
Cyber Incident Exercising

Assured Service Provider
in association with National Cyber Security Centre
Cyber Incident Response: Standard Level

Assured Service Provider
in association with National Cyber Security Centre
Cyber Advisor (Cyber Essentials)

CREST MEMBER
CREST Penetration Testing
CREST Vulnerability Assessment
CREST Incident Response
CREST Incident Exercising

PCI Security Standards Council
PCI FORENSIC INVESTIGATOR™

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR™

CERTIFICATION BODY CYBER ESSENTIALS PLUS

IASME CYBER ASSURANCE

CERTIFICATION BODY IoT SECURITY ASSURED

CfA Centre for Assessment ISO 9001 Quality Management UKAS MANAGEMENT SYSTEMS 0120

CfA Centre for Assessment ISO 27001 Information Security UKAS MANAGEMENT SYSTEMS 0120

You can get in touch with us via: 3bframeworks@3bdatasecurity.com

Website: www.3bdatasecurity.ccom

LinkedIn: https://www.linkedin.com/company/3b-data-security

2. CYBER INCIDENT EXERCISING (CIE).

Cyber Incident Response Exercising tests an organisation's ability to handle real-world cyber incidents through realistic tabletop and live-play scenarios. Delivered by NCSC Cyber Incident Exercising (CIE) accredited experts, the service identifies gaps, improves coordination and strengthens resilience.

KEY FEATURES

- Bespoke cyber incident exercises
- Realistic attack scenarios for technical and leadership teams
- Cross-functional participation
- Delivered by NCSC CIR and CIE accredited specialists
- Clear objectives and measurable outcomes
- Incident communication and escalation drills
- Evidence handling and compliance scenarios
- Post-exercise debrief with improvement plan
- Alignment with existing policies and playbooks
- Regular scheduling for continuous readiness

KEY BENEFITS

- Identifies gaps in incident response processes
- Improves coordination under pressure
- Strengthens decision-making during incidents
- Reduces response time through rehearsal
- Builds confidence across teams
- Supports regulatory compliance
- NCSC-accredited expertise
- Improves resilience to evolving threats
- Measurable post-exercise improvements
- Reduces incident impact and cost

3. CYBER INCIDENT RESPONSE CONSULTING.

Cyber Incident Response Consulting supports organisations to prepare for, manage and recover from cyber-attacks. The service provides strategic guidance, readiness assessments and tailored response planning to reduce business impact and improve cyber resilience.

KEY FEATURES

- Incident response plans and playbooks
- Readiness and preparedness planning
- Scenario-based tabletop exercises
- Crisis communications and PR planning
- Stakeholder notification planning
- First responder and breach management training
- Review of existing IR documentation
- Actionable improvement roadmaps
- Flexible standalone or retained delivery
- Delivered by experienced responders and forensic specialists

KEY BENEFITS

- NCSC CIR Level 2 accredited support
- CREST-accredited incident response expertise
- Reduced business risk through planning
- Improved regulatory compliance
- Stronger organisational resilience
- Reduced downtime and disruption
- Clear, structured decision-making
- Faster investigations
- Long-term cost savings

4. CYBER INCIDENT RESPONSE FIRST RESPONSE TRAINING.

First Responder Training prepares teams to act decisively during the critical first hour of a cyber incident. Delivered by NCSC CIR and CREST-accredited experts, the training improves confidence, compliance and incident handling through practical exercises.

KEY FEATURES

- Role-specific first responder training
- Clear first-hour actions and escalation
- Incident communication best practices
- Organisation-specific tabletop exercises
- Realistic simulations
- Evidence handling guidance
- Threat awareness and triage fundamentals
- Cross-team coordination drills
- Post-training review and recommendations
- Delivered by accredited specialists

KEY BENEFITS

- Faster containment and escalation
- Reduced downtime
- Improved regulatory compliance
- Increased organisational confidence
- Reduced risk of costly mistakes
- Stronger cross-team coordination
- Accredited assurance
- Improved resilience
- Faster recovery
- Measurable training outcomes

5. CYBER INCIDENT RESPONSE POLICY PLANNING AND PLAYBOOKS.

This service develops clear, actionable cyber incident response policies and playbooks. Delivered by NCSC CIR and CREST-accredited experts, it improves readiness, compliance and coordinated response during cyber incidents.

KEY FEATURES

- Custom incident response policies
- Clear escalation and decision frameworks
- Role-specific playbooks
- Regulatory and compliance alignment
- NCSC and CREST best practice guidance
- Incident categorisation templates
- Communication protocols
- Evidence handling procedures
- Review and update recommendations
- Delivered by accredited specialists

KEY BENEFITS

- Faster response times
- Improved regulatory readiness
- Reduced business disruption
- Stronger team coordination
- Consistent response across functions
- Accredited expertise
- Reduced recovery cost
- Improved resilience
- Simplified training
- Long-term policy value

6. CYBER INCIDENT RESPONSE RETAINED SERVICES.

Retained Incident Response Services provide 24/7 priority access to expert responders. With pre-agreed terms and rapid mobilisation, organisations benefit from faster recovery, reduced impact and ongoing resilience improvement.

KEY FEATURES

- Guaranteed priority access to responders
- 24/7 emergency availability
- Pre-agreed response times
- Dedicated Cyber Incident Manager
- Digital forensics and evidence handling
- Rapid containment and remediation
- Regulatory and breach reporting support
- Post-incident analysis
- Clear communication and updates
- Custom response plans

KEY BENEFITS

- Peace of mind through 24/7 cover
- Faster mobilisation and recovery
- Predictable costs
- NCSC CIR Level 2 assurance
- CREST-accredited responders
- Reduced downtime
- Tailored response
- Reduced financial loss
- Improved resilience
- Lower regulatory risk

7. CYBER INCIDENT RESPONSE SERVICES.

Cyber Incident Response Services provide expert support to detect, contain and recover from cyber-attacks. The service includes investigation, remediation and recovery to minimise impact and restore operations.

KEY FEATURES

- 24/7 incident detection and response
- Dedicated Cyber Incident Manager
- Emergency CSIRT mobilisation
- Digital forensics and evidence preservation
- Immediate containment actions
- Root cause analysis
- Regulatory reporting support
- Custom response playbooks
- Threat intelligence integration
- Business continuity planning

KEY BENEFITS

- Reduced downtime
- Accredited NCSC CIR Level 2 support
- CREST-accredited expertise
- Clear regulator-ready reporting
- Improved cyber resilience
- 24/7 support
- Business-aligned response
- Reduced financial impact
- Fewer disruptions
- Targeted, intelligence-led response

8. CYBER INCIDENT RESPONSE TESTING AND MOCK TABLETOP EXERCISES.

Cyber Incident Response Testing and Mock Tabletop Exercises assess organisational readiness to manage real-world cyber incidents. Using realistic, facilitated scenarios, the service tests people, processes and decision-making to identify gaps, improve coordination and strengthen cyber resilience before an incident occurs.

KEY FEATURES

- Realistic cyber incident tabletop exercises
- Bespoke scenarios aligned to organisational threat profiles
- Mock cyber-attack simulations for technical and executive teams
- Facilitated by experienced incident response specialists
- Testing of escalation and decision-making processes
- Crisis communication and management scenario testing
- Validation of incident response plans and playbooks
- Evidence handling and regulatory response scenarios
- Structured debriefs with measurable outcomes
- Actionable improvement roadmap after each exercise

KEY BENEFITS

- Identifies weaknesses in incident response capability
- Improves coordination between technical and leadership teams
- Strengthens decision-making under pressure
- Reduces response times during real incidents
- Increases confidence across response teams
- Improves readiness for ransomware and major attacks
- Delivered by NCSC CIE accredited experts
- Improves communication during high-impact incidents
- Reduces business disruption
- Builds long-term organisational cyber resilience

9. DIGITAL FORENSIC INVESTIGATIONS.

Digital forensic investigations preserve, collect and analyse electronic evidence to reconstruct incidents, support litigation and strengthen security. Services are delivered by experienced investigators with emergency and retainer options.

KEY FEATURES

- End-to-end evidence handling
- Corporate and cybercrime investigation experience
- Forensic imaging and artefact reconstruction
- Defensible legal reporting
- 24/7 investigation availability
- Digital forensics retainer
- Forensic readiness planning
- Integration with incident response
- Accredited CREST and NCSC capability

KEY BENEFITS

- Rapid fact-finding
- Supports litigation and regulatory needs
- Reduced business impact
- Root cause identification
- Improved security posture
- Enhanced forensic readiness
- Accredited response capability
- Flexible support options
- Broader investigation coverage
- Clear, auditable reporting

10. EDISCOVERY.

eDiscovery services identify, preserve and investigate electronic data for litigation, regulatory matters and internal reviews. Combines forensic analysis with Nuix-powered processing to deliver defensible, cost-effective outcomes.

KEY FEATURES

- Global data collection
- Defensible data preservation
- Forensic analysis
- Nuix-powered processing
- Efficient indexing and culling
- Discovery of concealed information
- Tailored data strategies
- Secure audit trails
- Delivered by forensic specialists

KEY BENEFITS

- Reduced legal risk
- Faster case preparation
- Improved evidential integrity
- Lower review costs
- Enhanced investigation outcomes
- Regulatory compliance support
- Better legal-technical coordination
- Transparent audit trails

11. THIRD-PARTY ASSURANCE – CYBER INCIDENT RESPONSE FOR CRITICAL SUPPLY CHAIN PARTNERS.

This service strengthens cyber incident readiness across critical suppliers by assessing, uplifting and validating their incident response capabilities, ensuring faster containment, controlled communications and improved recovery.

KEY FEATURES

- Risk-based supplier tiering
- Supplier IR due diligence
- Contract and SLA alignment
- Joint incident playbooks
- Breach notification templates
- Supplier tabletop exercises
- Evidence handling procedures
- Continuous assurance dashboards
- Remediation tracking
- Delivered by accredited specialists

KEY BENEFITS

- Reduced supply chain cyber risk
- Faster containment across partners
- Improved compliance evidence
- Reduced downtime
- Stronger third-party resilience
- Lower financial impact
- Increased stakeholder confidence
- Faster recovery
- Improved visibility
- Measurable risk reduction