Data breach readiness

Key trends and how to spot red flags

Digital and Data Legal team

July 2025

Introductions

PwC Digital and Data team

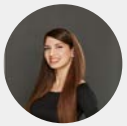
Our role

Our team advises clients on digital laws and regulations, including those in relation to personal data. We are thought leaders with a strong track record of working with governments, regulators and businesses to accelerate thinking around the responsible use of data and technology.

We provide support to clients on a broad range of matters, which is reflective of our diverse client base (many of whom operate in multiple jurisdictions worldwide).

Our team of lawyers include SMEs across numerous fields and sectors including UK & EU GDPR, direct and digital marketing, commercial contracts, data subject rights handling, and artificial intelligence.

Chris Cartmell
Director
Head of Digital & Data, Solicitor
chris.cartmell@pwc.com
+44 7483 353965



Lili Elenoglou
Senior Manager
Senior Digital & Data Lawyer
theofili.elenoglou@pwc.com
+44 7483 422515

Shivani Shenoy
Senior Associate
Solicitor
shivani.x.shenoy@pwc.com
+44 7483 924570

PwC Cyber Incident Response team

Our role

Our cyber incident response team is a NCSC CIR Enhanced provider, supporting organisations with incident response and digital forensics services since 1998. We advise and assist organisations facing a broad spectrum of incidents - from suspected malicious activity to large-scale ransomware attacks - offering expert-led digital forensics, technical investigation, threat intelligence, and crisis management support.

We work closely with law firms, regulators, and cross-functional client teams to deliver strategic, and operational response. Our global network of over 3,400 security professionals, including a dedicated UK team with access to over 60 forensics labs worldwide, enables rapid mobilisation and scaled support.

We combine frontline threat intelligence, business acumen, and a technology-agnostic approach to support clients to respond to cyber incidents with confidence.

David Cannings
Cyber Incident Response Lead

david.cannings@pwc.com
+44 7483 434287

Elaine Sands
Cyber Incident Response Manager

elaine.m.sands@pwc.com
+44 7483 424238

Agenda

1. Why being proactive matters
2. The evolving threat landscape
3. Spot and tackle the red flags
4. What's on the regulatory agenda
5. Key takeaways

Why being proactive matters

Why being proactive matters

With cyber incidents increasing across all sectors, my decision today is a stark reminder that organisations risk becoming the next target without robust security measures in place

Source: UK Information Commissioner commenting on a fine issued following a ransomware attack.

£600,000

Source: National Audit Office reporting on the British Library's assessment of costs attributable to a cyber attack in October 2023, by March 2024.

43% of UK businesses have experienced a cyber security breach or attack in the last 12 months

Source: UK Cyber security breaches survey 2025 (commissioned by the Department for Science, Innovation and Technology and the Home Office)

The evolving threat landscape

The evolving threat landscape

1. Geopolitical landscape
2. Types of threat actor
3. Ransomware as a service
4. Commoditisation of cyber tools
5. Move from traditional defences
6. Supply chain dependencies (MSPs)

Spot and tackle the red flags

Scenario 1 Spot the red flags

A university is considering using a third-party provider to deliver training to its students. The third party would hold student data.

During discussions about the services, it is revealed that the service provider uses single-factor authentication (e.g., password only), hosts data in the cloud, and system logs are reviewed manually once per week.

Scenario 1 Spot the red flags

How to tackle them

Due Diligence

- Data protection framework
- Security framework
- Assign risk

Contracts

- Pre-emptive
- Post incident

Audits

- Data protection clauses
- Audit rights
- Allocation of liability
- Termination rights

Technical controls

- Preventative
- Detective
- Response

Scenario 2 Spot the red flags

An employee works for a retail company. The company advises its employees to update their passwords regularly.

This employee makes only slight changes to their password each time (for example, by adding a letter).

One morning, while checking their emails, the employee notices that their inbox is loading slowly and that emails have been sent from their account to customers, urgently requesting payment to confirm orders.

Believing it to be a bug, the employee deletes the sent emails.

Scenario 2 Spot the red flags

How to tackle them

Awareness Training	Policies	Incident Response
• Annual training • Flyers/prompts • Champions	• Data Protection • Security • Breach Response	• Response structure • Escalation • Roles & Responsibilities • Documentation • Exercising

Other tools for breach prevention

1	Implement appropriate policies (e.g., access management)
2	Embed data protection into product lifecycle / processes
3	Cross functional playbooks
4	Documented strategy for regulatory notifications, evidence preservation and liaising with law enforcement
5	Regular review and table top exercises

What’s on the regulatory agenda

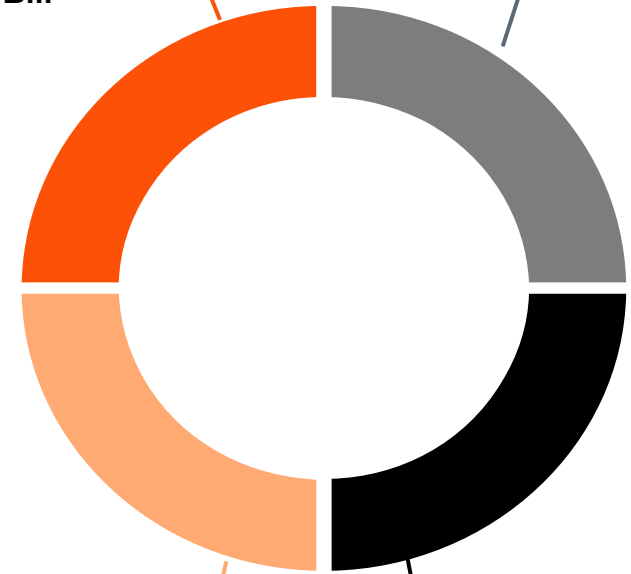
What's on the regulatory agenda

UK Cyber Security and Resilience Bill

- Wider scope (MSPs)
- Expanded reporting requirements
- Increased powers for regulators

Ransomware related proposals (UK)

- Prevent payments by government bodies and CNI providers
- Guidance on making payments
- Mandatory reporting



EU Digital Operational Resilience Act

In force

- Financial entities & ICT service providers caught in scope
- Governance and control
- ICT risk management
- Reporting & notification requirements
- Testing

EU Network Information Security Directive 2 (NIS2)

In force

- "Essential" & "important" entities
- Risk management measures & incident reporting
- Personal liability for management for NIS2

5

Key takeaways

Three lines of defence

1

Process

- Governance
- Risk
- Response

2

Technology

- Platforms & Infrastructure
- Tools

3

People

- Roles and responsibilities
- Training
- Not just an IT problem!

Any questions

Thank you