BCS’ Response to Ransomware: proposals to increase incident reporting and reduce payments to criminals

April 2025

Table of Contents

Introduction

The BCS Information Security Specialist Group members responded to a government consultation on proposals to crack down on the ransomware demands of cyber criminals. The government said that hospitals, businesses, and critical services could be protected under the measures, such as banning payments from Critical National Infrastructure. Ransomware is estimated to cost the UK economy millions of pounds each year, with recent high-profile ransomware attacks highlighting the severe operational, financial, and even life-threatening risks.

Key Consultation Responses

1. *Targeted Ban on Ransomware Payments (Proposal 1)*

- BCS **strongly supports** a ban on ransomware payments for **critical national infrastructure (CNI)** operators and the **public sector**, including **local government**.

The organisation believes this will be **somewhat effective** in reducing criminal incentives and encouraging stronger cyber resilience in essential services.

- Members of the **BCS Information Security Specialist Group** added:

  "Whilst we tend to strongly agree, we acknowledge that there will need to be a process for making exceptions to the rule."

- Our members emphasised the need to raise resilience standards across all sectors, supported by the **Cyber Security Code of Practice**, which would be more effective if more of it were **mandatory**.

  "We are still seeing the impact on the British Library and Synnovis attacks—hopefully this will drive better cyber security practices."

- On enforcement, BCS was cautious about **criminal or financial penalties** for public sector bodies:

  "Fines for public bodies waste taxpayer money, and criminal penalties are unrealistic. Reputational accountability, enforceable action plans and tailored support are more appropriate."

---

2. Ransomware Payment Prevention Regime (Proposal 2)

- BCS expressed **reservations** about a broad payment prevention regime requiring organisations to report an intention to pay a ransom before doing so. It **neither agreed nor disagreed** with the general approach and **tended to disagree** with all proposed models (economy-wide, threshold-based, organisations-only).
- **Rationale:**

  "Determining which firms this would apply to would be incredibly complex. We recommend starting with the public sector, CNI and their third-party suppliers."

- **Effectiveness in reducing ransomware payments:**
  - **Economy-wide** and **threshold-based** regimes: seen as **"somewhat effective"**
  - **Organisation-only** models: viewed as **less effective** or **somewhat ineffective**
- **Effectiveness in aiding law enforcement:**
  - All options rated as **"somewhat effective"** in enabling investigations and interventions.
- **On thresholds (Q22):**
  BCS selected **"don't know"**, reflecting concern over fair and workable criteria.
- **Supporting compliance (Q23):**
  - Recommended:
    - **Clear guidance**
    - **Post-attack support**
    - **Stronger internal accountability for cyber resilience**

- **Tailored measures (Q24):**
  BCS strongly supports tailoring compliance measures based on organisation size, sector and capacity.

3. Mandatory Ransomware Incident Reporting Regime (Proposal 3)

- BCS supports the introduction of a **mandatory ransomware incident reporting regime**, seeing it as vital to improving the UK's understanding of the threat and strengthening the national response.
- **Voluntary reporting (current system):**
  Rated as **ineffective** in increasing understanding and only **somewhat effective** in supporting the government response.
- **Preferred reporting options:**
  - **Economy-wide mandatory reporting** (all organisations and individuals): rated **effective** for understanding, though impact on response was marked as **"don't know"**
  - **Mandatory reporting for all organisations, excluding individuals:** supported as **effective** for understanding but again marked **"don't know"** for response
  - **Threshold-based models (with or without individuals):** received **mixed or neutral** responses
- **Compliance support (Q33–34):**
  - Backed:
    - **Additional guidance**
    - **Post-incident support**
    - **Tailored approaches** based on organisation size and capability
- **On non-compliance penalties (Q35–36):**
  - BCS selected **"don't know"**, noting challenges in enforcing fines or criminal penalties
  - Recommends:
    - **Transparency about breaches**
    - **Reputational accountability**
    - **Enforceable action plans with targeted support**
- **Business impact (Q37):**
  Uncertain whether foreign firms or investors would change decisions based on the regime (**"don't know"**).
- **Incident reporting timeframe (Q38):**
  Agreed **72 hours** is a reasonable period to report a suspected ransomware incident.
- **Support services for victims (Q39):**
  BCS strongly supports:
  - **Cyber expert support** (e.g. NCSC/law enforcement)
  - **Guidance documents**
  - **Threat intelligence**
  - **Operational updates** on enforcement activity
- **Scope of regime (Q40):**
  BCS supports extending mandatory reporting to include **all cyber incidents** (e.g. phishing, hacking), not just ransomware.

- **Additional comments (Q41):**

  “We advocate for greater transparency regarding outages in the public sector and essential IT services. The IT profession must design more resilient systems and be accountable for reliability.”
  “Professionalism and ethical leadership—reflected in Chartered status for IT leaders—are essential to restoring public trust.”

Who we are

BCS, The Chartered Institute for IT is the professional body for information technology. Our purpose as defined by our Royal Charter is to promote and advance the education and practice of computing for the benefit of the public. We bring together industry, academics, practitioners, and government to share knowledge, promote new thinking, inform, and shape public policy. BCS has over 70,000 members including businesses, entrepreneurs, public sector leaders, academics, educators, and students, in the UK and internationally.

BCS
The Chartered Institute for IT
3 Newbridge House,
Newbridge Square,
Swindon SN1 1BY
BCS is a registered charity: No 292786