

From industry concern to practical action: the value of working with regulators

How industry, the NCSC and the FCA worked together to help organisations share information while protecting market integrity

Sharing cyber incident information quickly, whilst responding to an incident, is an important contributor to UK cyber resilience.

High-profile incidents in the retail sector highlighted the value of timely cyber incident information sharing, not just within the retail sector but with other sectors too. Organisations often rely on the same technologies, suppliers and digital supply chains, meaning an incident affecting one organisation or sector may expose similar vulnerabilities elsewhere. Sharing information enables organisations to learn, adapt and defend themselves against common threats before they cause further harm.

Organisations can share cyber incident information with the NCSC and through trusted information-sharing communities. However, information sharing often takes place under significant operational, legal and commercial pressures. For some organisations, questions about regulatory obligations can create hesitation at exactly the point where timely information may be most valuable to others.

This blog describes how industry, the NCSC and the Financial Conduct Authority (FCA) worked together to better understand one such challenge, and how that collaboration helped provide greater clarity for organisations seeking to share cyber incident information responsibly.

The challenge

Organisations recognise the value of sharing information about cyber threats, incidents and mitigations. They understand that doing so can help other organisations protect themselves and strengthen resilience across an entire sector. However, for publicly listed organisations, cyber incidents can also raise questions about market-sensitive or ‘inside’ information and the obligations that come with it.

Some organisations were uncertain about when information could be shared with the NCSC or through trusted information-sharing communities while continuing to meet their obligations under the UK Market Abuse Regulation (MAR), which is overseen by the FCA.

The issue wasn't a lack of willingness to share information; it was uncertainty about how to do so while meeting legal and regulatory obligations.

Bringing the right expertise together

Rather than treating this solely as a cyber security issue, we brought together the people best placed to understand it from different perspectives.

Industry brought the operational reality of responding to cyber incidents and the practical challenges organisations face when deciding what information can be shared. The NCSC contributed expertise in incident response, trusted information sharing and how the information we receive is used. The FCA – the regulatory body responsible for market-abuse requirements – provided both regulatory expertise and insight into how existing obligations apply in practice during cyber incidents.

Together, we focused on a shared objective: helping organisations understand how they can share cyber incident information while continuing to meet their legal and regulatory obligations.

The discussions showed how collaboration between industry, regulators and cyber security experts can help turn uncertainty into practical guidance. They also demonstrated the role regulators can play in making complex requirements easier to understand and apply.

This work ultimately led to a practical outcome designed to provide greater clarity for organisations seeking to share cyber incident information while meeting their regulatory obligations.

A practical short-term solution

The [FCA's guidance on disclosing inside information relating to cyber incidents](#) helps organisations assess their disclosure obligations when responding to a cyber incident.

Importantly for cyber resilience, it also addresses when organisations may share information with government departments, law enforcement, regulators and trusted information-sharing communities.

The guidance explains that sharing cyber incident information with the NCSC – as part of the NCSC's work to help protect UK critical systems and online services, and support incident response – may be compatible with an organisation's regulatory obligations. This is because such sharing may be consistent with an organisation acting in the normal exercise of its employment, profession or duties.

It also recognises NCSC-led information-sharing communities where sharing information can help others prevent or mitigate cyber threats.

Individual organisations remain responsible for assessing their own circumstances and meeting their legal and regulatory obligations. However, providing clearer regulatory guidance aims to remove uncertainty that might otherwise discourage appropriate information sharing.

Continuing the conversation

The publication should not be the end of the conversation.

The NCSC and FCA will continue engaging directly with industry, legal advisers and other stakeholders to explain the guidance and understand how it works in practice.

This feedback is important. Cyber incidents don't respect organisational or regulatory boundaries, and building national resilience depends on organisations being able to share information quickly and confidently.

This work is one example of what can be achieved when industry, regulators and cyber security experts come together to address a shared challenge. Sharing cyber incident information with the NCSC and through trusted information-sharing communities remains an important contributor to UK cyber resilience, and we encourage organisations to continue raising any barriers to sharing so they can be better understood, addressed and where possible removed.

Mark K

Senior Resilience Lead and Cyber Consultant, NCSC

WRITTEN BY



Mark K

Senior Resilience Lead and Cyber Consultant, NCSC

PUBLISHED

27 October 2026

WRITTEN FOR

Cyber security professionals

Large organisations

Public sector

PART OF BLOG

