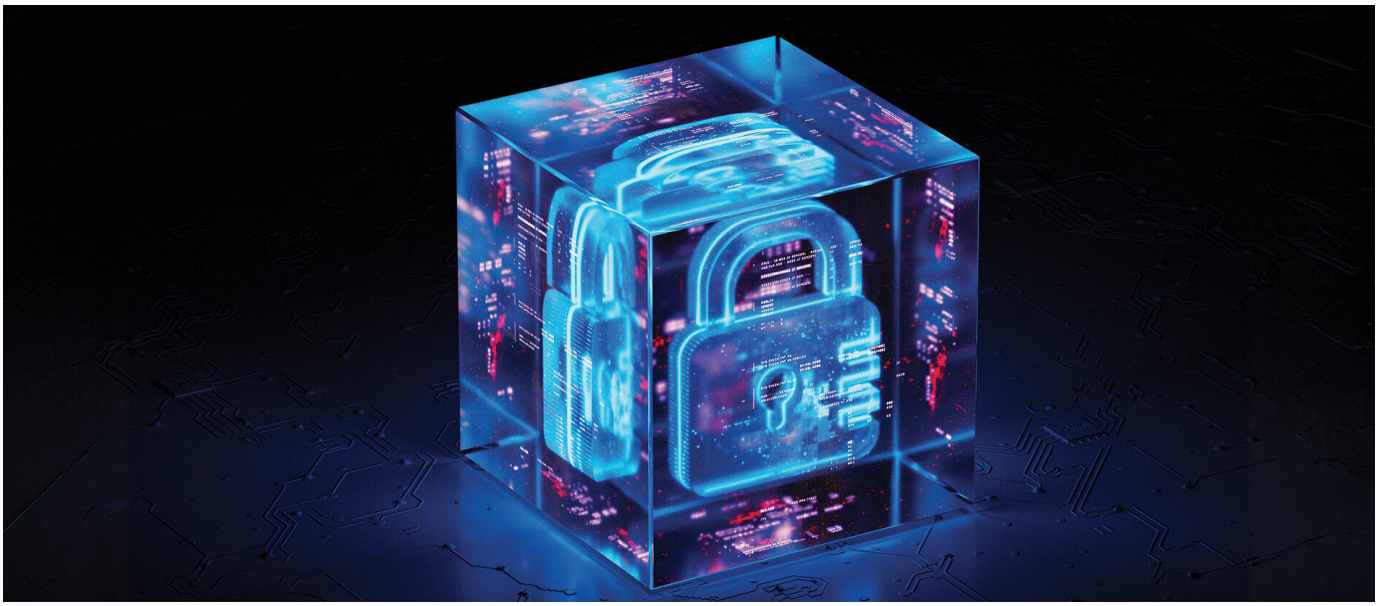
Cyber controls: tax risk governance

General Features | Management of taxes | Large Corporate



19 February 2026

After a sharp rise in ‘nationally significant’ cyber attacks, we ask how tax professionals can support cyber incident preparedness.

Key Points

What is the issue?
Cyber attacks are rising sharply and can severely disrupt tax functions, exposing organisations and advisers to financial loss, compliance failures and regulatory penalties.

What does it mean to me?
Tax teams and firms face real risks to filing obligations, data security and client trust, particularly as digitalisation and AI increase dependence on interconnected systems.

What can I take away?
Tax professionals must be embedded in cyber incident planning, ensure robust

controls and testing are in place and treat cyber resilience as a core part of tax risk governance.

Cyber attacks are having a significant impact on both UK citizens and the economy. Whether you are part of an in-house team or work in a professional tax firm, it is vital to understand what a cyber attack could mean for your organisation and for taxpayers.

Recent figures from the National Cyber Security Centre (NCSC) show a sharp rise in ‘nationally significant’ cyber incidents, which can cause significant business disruption and financial loss. These attacks have more than doubled already in the last year alone. Between September 2024 and August 2025, the NCSC recorded 429 cyber incidents, of which 204 were classed as ‘nationally significant’ – a 130% increase on the previous year. The scale and frequency of these incidents underline the growing sophistication of threats and the widening range of organisations affected.

The scale of cyber attacks

The impact of cyber incidents varies but businesses can lose all access to systems and data, including enterprise resource planning and payroll systems, resulting in severe disruption. In extreme cases, systems can be down for weeks, causing huge financial losses, as well as serious reputational damage and loss of trust.

For tax teams, system outages can prevent the submission of returns, particularly for VAT and payroll. This is an even bigger problem now that Making Tax Digital for VAT is dependent on direct data links, and could lead to HMRC penalties, missed claim windows and large backlogs of work once systems are restored. The corruption of underlying data can also compromise audit trails. It should be noted that HMRC generally accepts that computer or software failure may amount to a reasonable excuse in relation to late-filing penalties.

Cyber incident planning must consider how an attack could affect the services you provide – including the ability to file returns and safeguard taxpayers’ data. Firms should also prepare for how to communicate any data breaches of sensitive information and manage the regulatory and reputational consequences for your business.

Data protection failures may attract penalties from the Information Commissioner's Office, potentially compounded by other regulatory regimes. For example, where fraud is involved, a company could face criminal liability under the Economic Crime and Corporate Transparency Act 2023.

The evolving threat landscape

The rapid adoption of generative AI means that safeguarding data is now even more vital – no business can assume that it is safe. Businesses must adopt a mindset of 'when, not if' about cyber attacks, ensuring their cyber risk and anti-fraud measures are robust. This includes regular training for staff to ensure that they understand the most common risks and the red flags to look out for.

Most cyber attacks rely on social engineering – in other words, tricking someone into granting access to their systems – so tax advisers need to be trained on what to look out for and how to report any risks. Cyber incident plans need to be tested regularly – ideally through simulated cyber attack exercises – to ensure that they work effectively in practice.

Tax teams and cyber incident planning

In-house tax teams should coordinate with their Chief Information Officer or senior leadership team to ensure that the tax function is fully integrated into the organisation's cyber incident response planning. The cyber incident plan should include a prioritised list of critical systems, clearly setting out which need to be restored first following an attack.

Although many organisations already have a cyber incident plan, some have yet to consider all potential cyber risks from a tax perspective, meaning that exposure in this area may not have been quantified. Tax is increasingly an area where many in-house teams and firms are adopting the use of AI for elements of their work, further expanding the organisation's cyber footprint. Without sufficient awareness of AI-related vulnerabilities and safeguards to address them, businesses could find themselves exposed to heightened cyber risk.

Plans should set out clear roles and responsibilities, internal and external communication strategies, and the specific procedures or 'playbooks' to be followed

when systems are compromised. They must also take into account the wider regulatory landscape, relevant reporting requirements, and any dependencies on third-party suppliers. Since many cyber attacks and data breaches stem from weaknesses in third-party systems, organisations should also assess supper cyber resilience to ensure adequate protection.

Strengthening resilience and recovery

A detailed, well-tested cyber incident response plan is vital for quick recovery following an attack, helping to protect taxpayers, limit downtime and minimise financial losses. In line with recent NCSC guidance, businesses should maintain accessible paper-based copies of their plans in case digital systems are unavailable. Regular testing and staff training are equally important.

In addition to forming part of the wider cyber incident response plan, the risk of cyber attack should be recognised within the overall tax risk environment – for instance, by including it in the tax risk and controls matrix. Strong cyber controls can be a key factor in how HMRC responds to penalty appeals under the ‘reasonable excuse’ grounds. In practice, a cyber attack may provide such a defence; however, as HMRC’s focus on governance strengthens, and as cyber preparedness becomes standard practice, it will become harder to argue ‘reasonable excuse’ if cyber controls are inadequate.

Traditionally, many tax functions have regarded cyber security as the responsibility of the IT department. Yet those working in tax know that it is often one of the last areas to be considered when response plans are drawn up. Raising it on the agenda now will help to ensure the function is properly protected – and reduce the risk of serious surprises in the future.