SLAUGHTER AND MAY/

SM TREASURY INSIGHTS

Treasury's Role in Cyber Resilience

March 2026

Treasury's role in cyber resilience

Recent high-profile cyber incidents underline how quickly operational disruption can translate into acute financial and liquidity challenges. The cyberattack on Jaguar Land Rover in late 2025 forced the shutdown of production across multiple UK plants for several weeks, disrupted supply chains and required rapid intervention to stabilise cash flows across the group and its suppliers, including emergency financing measures and close engagement with lenders and government stakeholders. Earlier in 2025, Marks & Spencer suffered a significant cyber incident that disrupted payment systems, online ordering and gift card functionality across its UK estate, with material impacts on sales and profitability and immediate implications for cash management, stakeholder communications and market disclosure.

In both cases, the incidents demonstrate that cyber events are not confined to IT or data issues: they can rapidly become treasury-critical events, requiring urgent focus on payment continuity, liquidity resilience, funding access and the management of financial counterparties.

In this article, we consider the specific impacts of a cyber incident that treasury teams might be called on to analyse and respond to, both in the initial phase of response to an incident and over the longer term as the business seeks to recover.

"Cyber security is now a matter of business survival and national resilience. With over half the incidents handled by the NCSC deemed to be nationally significant, and a 50% rise in highly significant attacks on last year, our collective exposure to serious impacts is growing at an alarming pace."

Dr Richard Horne, Chief Executive, National Cyber Security Centre, 14 October, 2025

Key areas of treasury involvement

Planning for, and responding to, a cyber incident requires organisation-wide input and coordination, including from treasury. Treasury will typically play an important supporting role, providing advice to the board and lead response team members and implementing aspects of the response strategy. For example, the costs of responding to a cyber incident and the potential credit implications of continuing disruption to production, sales or services make advice and analysis from treasury on matters such as the business's liquidity position and available financial resources a crucial component of any crisis response. Treasury may also be well-placed to manage key stakeholders such as banks, insurers and rating agencies where their involvement is required as part of an incident response.

Payment continuity

Ensuring that the business can make critical payments may be an immediate priority in the aftermath of an attack. How will payroll, tax and key supplier payments continue if enterprise resource planning (ERP) or treasury management systems (TMS) are unavailable? A related point is the efficacy of systems for flagging fraudulent payments. There have been instances of cyber breaches specifically aimed at implementing fraudulent payments. These include instances of attackers entering systems to target and divert large, known payment flows, including debt coupon payments.

Fallback and workaround arrangements must be agreed with banks and other counterparties, and properly documented and tested in advance. These arrangements might include alternative authorisation channels, payment templates and out-of-band verification protocols (for example, pre-agreed telephone or secure messaging confirmations used where normal digital approval routes are unavailable). It may be appropriate to streamline payment volumes temporarily, prioritising statutory obligations, payroll, the funding of operating entities, debt service, hedging obligations and payments to mission-critical suppliers.

Liquidity requirements

Boards and senior management will look to treasury for advice on the company's liquidity position. How long can the business operate if trading is disrupted? What emergency funding options are available if disruption persists longer than expected and what is the strategy for accessing that funding? In the early stages, all stakeholders will be working with imperfect information, so responses may be directional rather than precise or decisive. Treasury may be working with daily cash-burn ranges, scenario-based projections and

imperfect visibility over receipts and cash balances, particularly where access to TMS, cash-pooling platforms or internal reporting tools is disrupted.

Cyber incidents may also have implications under the terms of loan and other financing documentation. The analysis for treasury teams in this context is typically, broadly the same as applies to any crisis event which has, or could have, a sustained impact on business performance or financial position. Any liquidity assessment must involve a review of the contractual terms of the company or group's financing arrangements, to identify any constraints on utilisation that may come into play in relation to either the incident itself or a financial stress scenario. The potential for drawstops and defaults will need to be considered both in the short and over the longer term.

We take a deeper dive into the impact of a cyber incident on debt documentation below.

Communications with financial counterparties

Some cyber incidents, particularly those disrupting business as usual activities, may be in the public domain from an early stage, while others are highly confidential. In either event, there may be legal (regulatory and/or contractual) requirements to notify relevant regulators, the market and impacted individuals and counterparties. Where communications are required, providing relevant external stakeholders with calm, factual updates - focused on what is known, what is being assessed and how risks are being managed - can help preserve confidence while technical investigations and recovery efforts continue.

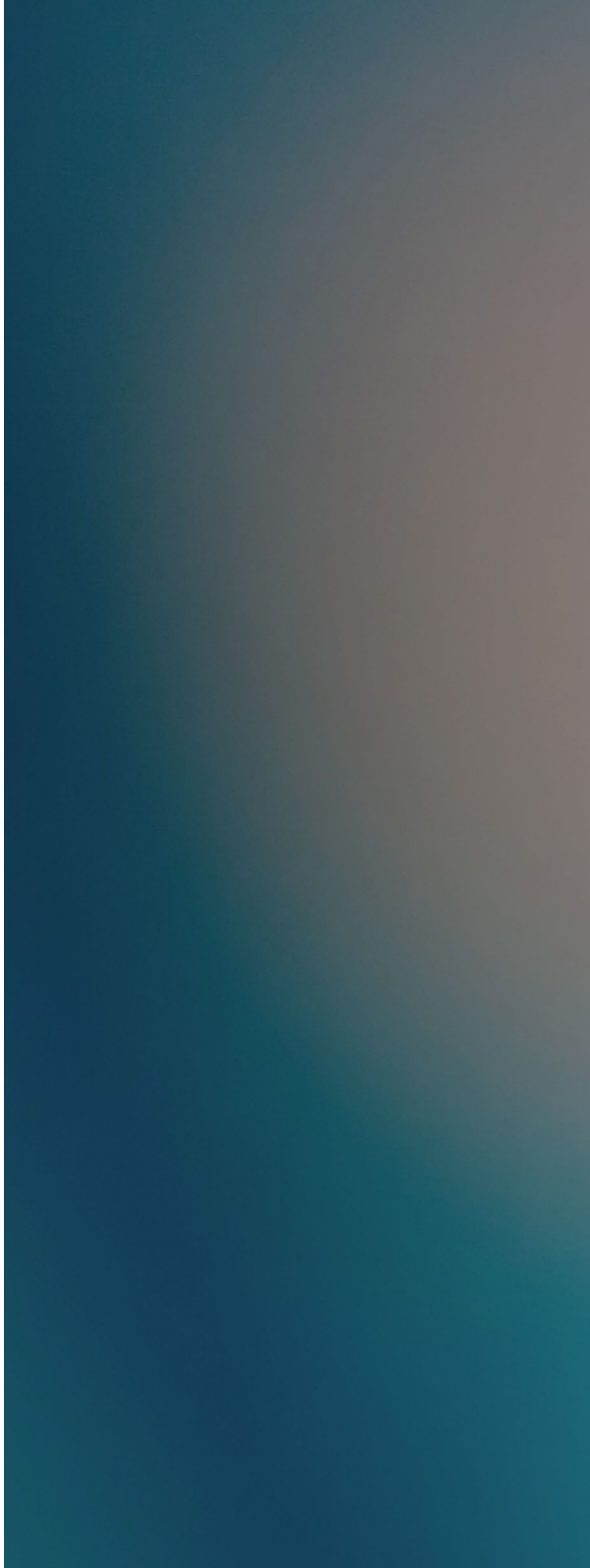
Communications are often managed through a structured 'cascade arrangement' where a small, senior group agrees core messaging at the outset of an incident – covering what is known, what remains under investigation and how key risks are being managed. That messaging is then passed through defined internal channels and, where appropriate, on to external stakeholders.

Limiting external communications to pre-approved, high-level factual updates, engaging only through designated channels, and taking comfort from existing confidentiality obligations and established counterparty relationships, enables organisations to reduce the risk of unintended disclosure during a cyber incident. Communications are typically sequenced carefully alongside regulatory notifications or market disclosures, recognising that investigations and internal assessments may still be ongoing.

Engagement with relationship banks and other key financial counterparties requires careful consideration. If a cyber incident is likely to impact payment capacity, liquidity headroom or reporting timelines, if financial fallback arrangements are being activated or if facilities may need to be drawn down to support the response (or indeed to pay a ransom), lenders and other financial counterparties will need to be engaged.

While it remains unusual for debt documentation to contain specific provisions requiring notification or other action by the borrower in the event of cyber incidents specifically, a cyber incident or its fallout may trigger general contractual requirements to notify or otherwise engage with lenders or other financial counterparties.

A cyber incident may also attract attention from rating agencies. A single cyber incident is unlikely, of itself, to trigger a ratings action. However, repeated incidents, a poorly managed response, or an incident impacting an organisation facing financial pressures, can influence outlooks and qualitative assessments over time.



Treasury's day-to-day relationships with key financial counterparties (which may also include insurers), and understanding of the relationship dynamics, their confidentiality expectations and information sensitivities mean treasury input is relevant to an organisation's cyber preparedness plans. In particular, treasury will want to ensure that information flows to all relevant financial counterparties are taken into account by the relevant decision-makers and, in the aftermath of the attack, when the cascade is activated.

Insurance arrangements

Many organisations will take out specific cyber insurance policies. These typically require that insurers are notified promptly of the occurrence of an incident and may provide assistance (technical, legal, ransomware negotiation etc.) as part of the policy. They may also place constraints on communications and requirements around the documentation of remediation activity. Whether any other insurance arrangements might be relevant in the context of the incident should also be considered. For treasury teams with responsibility for group insurance, familiarity with notification requirements and evidencing standards is critical. Missteps in the first days can materially delay recoveries.

Whether or not responsible for insurance cover, treasury will often be responsible for tracking insured versus uninsured costs and, crucially, for managing the timing mismatch between cash outflows and insurance proceeds. In practice, proceeds may only be received after a prolonged period of forensic investigation, loss quantification and insurer approval. Even where coverage is robust, that mismatch can have real liquidity implications, making advance planning and regular stress-testing an important part of liquidity resilience.

A related analysis that is likely to fall to treasury in the context of insurance, is whether insurance claims or recoveries trigger any obligations or restrictions under financing arrangements. These might include, for example, requirements to notify lenders or any creditor rights or controls over the application of proceeds. This will not be the case in all facilities, but it is important to consider whether any relevant facility terms exist and if so, their extent.

Impact on loan documentation

In relation to loan facilities, the key issues to consider (in addition, as highlighted in section 1 above, to any provisions relating to insurance) include those detailed below.

Ability to pay on time

A delay in meeting payments due to lenders is likely to trigger a default, subject to the expiry of any applicable grace periods. Grace periods for non-payment generally are not widespread. If they exist, they are typically very short. The LMA templates do, however, provide specifically for non-payment due to a technical/systems related disruption which is beyond the control of the paying party (a "Disruption Event"). This mechanism provides for a grace period during which an alternative method for making payments while the disruption subsists can be negotiated. The grace period that is agreed in this context is also typically very short, underlining the need to notify lenders as soon as possible if payments by normal channels are likely to be disrupted.

Disruption to information flows

Undertakings relating to conduct of business or delivery of information are usually subject to grace periods and therefore not usually breached merely because systems are unavailable or information flows are temporarily

constrained. However, delays may trigger a drawstop and will need to be reviewed if (for example) the production of reports or financial information is likely to be problematic while systems are unavailable or compromised.

Financial covenant pressure

If significant adverse impacts are starting to be felt or anticipated, treasurers will be monitoring the business's ability to comply with any financial covenants in its loan facilities. Reduced revenues, increased costs and working-capital volatility can erode covenant headroom, and this assessment may be further complicated where access to TMS or underlying financial data is disrupted, limiting real-time visibility over covenant performance. Covenant capacity is generally considered and stress-tested as part of broader cyber resilience and contingency planning. A specific point to pay attention to may be whether the proceeds of business interruption or any other applicable insurance proceeds are permitted to be taken into account in EBITDA-based covenants.

Cross-default

If payment delays or defaults may arise under any other financing or hedging arrangements as a result of the cyber incident, there may be cross-default implications. Understanding how grace periods, payment thresholds and cure mechanics interact across the capital structure is an important part of the documentation analysis.

Cessation of business

Sustained disruption which prevents the business or key parts of it from resuming trading in the ordinary course may prompt consideration of cessation of business provisions. Experience during the COVID period illustrates that the wording of these types of provisions and the scope of any exceptions can vary quite widely.

MAC and insolvency events

A crisis event tends to engage an immediate consideration of material adverse change (MAC) provisions. While this analysis is always necessary and worthwhile, trigger thresholds are typically relatively high. In the early days, if disruption is expected to be temporary and the business remains solvent, the MAC may not be a material risk factor. However, MAC provisions, together with insolvency-related events of default, tend to come into sharper focus as the commercial and financial impact of a cyber incident becomes clearer over time. Prolonged disruption, rising remediation costs, asset impairments or regulatory exposure can all create pressure points.

There are examples of businesses that have gone into insolvency proceedings as a result of a cyber incident (Travelex and the Heritage Company for example). In the context of insolvency provisions, if creditor relationships come under strain, this is the risk of engaging creditors' process events of default.

Impact on derivatives documentation

The above considerations are focussed on loans, but similar considerations may arise under other financing arrangements. This includes derivative transactions documented under ISDA master agreements.

Derivatives terms may provide for short grace periods for payment failures, and force majeure termination events may apply in limited circumstances. These mechanisms are tightly framed and their application, fact-specific. Even where a cyber incident prevents the relevant company's performance

under an ISDA, relief is typically temporary and does not displace the need for active engagement with counterparties. As with loan facilities, treasurers should not assume that contractual mechanics alone will absorb prolonged disruption, reinforcing the importance of early assessment, communication and contingency planning.

Ransomware and sanctions

Where a ransom demand has been made, the starting point must be whether any payment would be lawful, including whether it could breach sanctions or other financial crime restrictions. Legal, dark web/specialist ransomware advisers will typically be engaged to assess these issues and to help the organisation get comfortable, for example, that any payment would not be made to a sanctioned person or entity.

Where a ransom is paid, this is often effected in cryptocurrency, most often bitcoin, and typically through specialist ransomware negotiators and advisers who operate their own wallets and payment infrastructure. A small, specialist team will usually manage the ransomware negotiations themselves, which may not involve treasury. However, in some cases, input from treasury may be required on what funding is realistically available to meet a demand.

In practice, it may be difficult to obtain new financing for this purpose, given financial institutions' sensitivity to sanctions, AML and reputational risk. Where funds need to be released from existing bank accounts, treasury may often be central to those discussions, reflecting its relationships with relationship banks and understanding of payment mechanics.

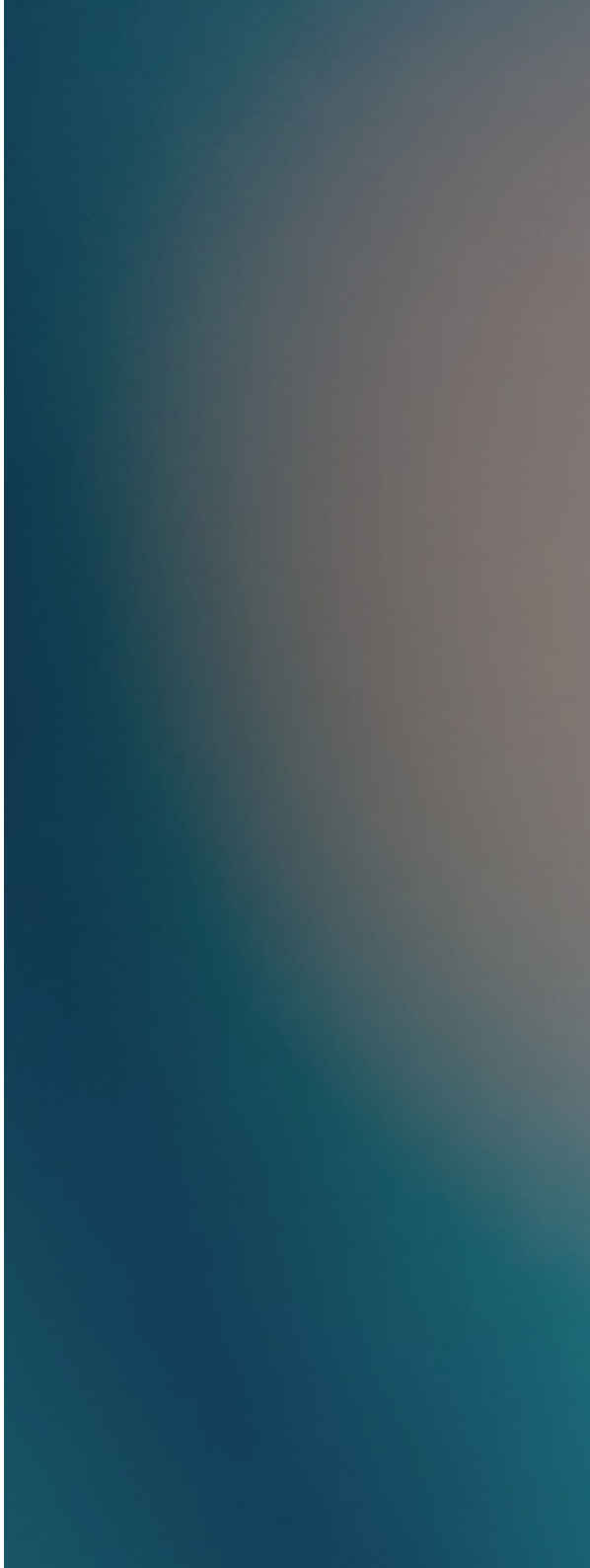
From operational engagement to strategic involvement?

The relationship between cyber risk and credit risk is increasingly apparent, bringing the topic further into the treasury sphere. This is reflected in the prevalence of risk factors relating to cyber risk and IT security in capital markets issuance documentation, which are becoming ever-sharper and more issuer-specific. It is also reflected in ratings agency research suggesting that the costs of shoring up cyber resilience are viewed as a credit strength. In other words, effective cyber risk management is a topic to emphasise in communications with relationship banks and other debt investors.

These factors, combined with the range of areas where the board may look to treasury teams for analysis and input as they formulate cyber preparedness and incident response strategies, suggest that cyber risk is an increasingly important area for finance and treasury not simply to be involved in – but, in some cases, to have a role in formulating and steering.

The prominence of cyber resilience in risk registers is set to rise as the emphasis on cyber resilience as a governance matter is further embedded in the evolving regulatory backdrop, whether that's in the form of management body liability in the EU's cyber law for critical services (the NIS2 Directive) or changes to the UK's Corporate Governance regime, where cyber risk is referenced for the first time in the Code's guidance.

For further information on the regulatory environment and the broader implications of a cyber incident, please refer to the publications prepared by our Cyber team linked at the end of the briefing.



Key Contacts

Our Cyber Hub has the multi-disciplinary expertise and industry knowledge to advise clients across the full spectrum of preparedness, incident response and investigations. Our hub is made up of legal experts from our corporate, data privacy, digital and technology, dispute and investigations, financial services, financing, and IP teams. They have access to a network of cyber industry experts, regulator contacts and relationship firms across the world which means we can assemble a global team to tackle your cyber crisis, whatever your sector.

We help our clients understand and mitigate cyber risks, both in their business-as-usual operations, and when engaging in activities which raise specific cyber concerns. We build trust with senior stakeholders and create a roadmap to help prevent, and (where necessary) navigate a cyber attack, within each client's own corporate risk appetite.

Links to all of our publications on Cyber matters, including our blog "The Lens", are available on our website.

SLAUGHTER AND MAY/

Financing

Ed Fife
Partner

+44(0)20 7090 3662
Edward.Fife@Slaughterandmay.com

Caroline Phillips
Partner

+44(0)20 7090 3884
Caroline.Phillips@slaughterandmay.com

Kathrine Meloni
Special Advisor and Head of Treasury Insight
+44(0)20 7090 3491
Kathrine.Meloni@slaughterandmay.com

Peaches Stanforth
Associate

+44(0)20 7090 4183
Peaches.Stanforth@slaughterandmay.com

Cyber

Richard Jeens
Partner

+44(0)20 7090 5281
Richard.Jeens@slaughterandmay.com

Laura Houston
Partner

+44(0)20 7090 4230
Laura.Houston@slaughterandmay.com

Duncan Blaikie
Partner

+44(0)20 7090 4275
Duncan.Blaikie@slaughterandmay.com

Natalie Donovan
Head of Technology Digital Data and IP Knowledge
+44(0)20 7090 4058
Natalie.Donovan@slaughterandmay.com