Cyber-insecurity: What do Treasurers need to do?

Increasing numbers of high profile cyber-attacks mean that the risks of a data theft, serious outage or a ransom demand are risks that corporate treasurers cannot ignore. In addition, the incidents such as the CrowdStrike outage have exposed the global reliance on IT to run our businesses. We explore the risks facing boardrooms more broadly in detail here; in this briefing we consider how cyber-insecurity affects treasurers, their financings and derivative transactions.

Risk assessment from a Treasury perspective

In the event of a cyber-attack or a sustained IT outage, it will be important for corporate treasurers to quickly assess what impact the cyber-attack or outage has had on the corporate's treasury functions and whether there are any actual or potential breaches under their financings.

Have you lost access to bank accounts?

If access is lost to bank accounts as a result of a cyber-attack (or if funds are depleted by the incident itself, such as in funds redirection frauds), this may affect the ability to make payments which are due, such as payments to suppliers as well as payments owed under its principal financings. In financing agreements,

What happens when there is a cyber-attack?

There are many cyber threats affecting business, and many ways in which they can be attacked. However, very broadly the most common outcomes are:

- denial of access to systems or data; and
- theft, whether of data or of money;

coupled with a ransom demand.

there are commonly short grace periods for delays in payments as a result of a systemic technical disruption event which is outside the control of the company, but, at least for LMA-style loan agreements, this is likely to be no more than three business days.

Even where payments are not due under a corporate's principal financings, corporate treasurers should consider whether there is a risk of cross-default, with non-payment defaults under smaller financings aggregating to exceed applicable *de minimis* thresholds.

Similar considerations would apply in respect of any derivative transactions entered into under an ISDA Master Agreement, where the standard failure to pay grace period is one business day and which typically contain a cross-default provision.

Have you lost access to treasury systems and other data and information?

The affected corporate may also lose access to other treasury systems which would be required to comply with obligations under financings, for example:

1. systems may be required to perform calculations in relation to compliance with financial covenants or enable cash management processes to ensure sufficient liquidity in a particular group company to make payments due or effect certain transactions; or
2. those which would be required to upload documents by way of information, or to deliver notices to counterparties under financing documents.

Similar considerations may also apply in respect of derivative transactions, although typically these will not contain financial covenants that need to be calculated by the corporate.

Business disruption

A disruption to the business as a result of a cyber-attack or IT outage may have other consequences under the financing documents. Careful review of the contractual terms will be required to determine if any additional waivers will be required from lenders for defaults.

Material adverse effect

Depending on the severity of the cyber-attack or IT outage and the effect on the company's business, there could be a material adverse effect (**MAE**). Many finance documents have a separate material adverse effect event of default and many have numerous representations and undertakings which may be qualified by the likelihood of a potential breach of the underlying obligation having an MAE.

Whether these are at risk of being triggered or breached depends on the drafting of the relevant document.

1. The definitions of an MAE vary widely; in many cases it would be objectively determined, but in some markets it may be subjective (ie depend on the opinion of the creditors, with or without an obligation to act reasonably).
2. It may only apply where there is an event or circumstance which has a material and adverse effect on the corporate group, or the providers of credit support to the lenders.
3. It may encompass a range of effects, including the business, operations, property, condition (financial or otherwise) or prospects of the corporate group (or a subset thereof).

The bar to convince a court that an MAE has occurred is high, and creditors would likely only consider exercising rights of enforcement on the basis of a MAE event of default as a last resort. However, the occurrence of a MAE could come into play in relation to other provisions such as representations and covenants which are qualified by reference to an MAE. For example, the Loan Market Association investment grade document includes a representation that no litigation or other proceedings has occurred which, if adversely determined, *might* have an MAE. This representation may need to be repeated periodically, including on the date any funds are drawn under a revolving credit facility.

Force majeure

Where derivative transactions have been entered into under an ISDA Master Agreement, it is common for the ISDA Master Agreement to include the ISDA standard force majeure termination event, which will be triggered if, by reason of "force majeure or act of state", a party is prevented from making or receiving payments or complying with any other material provision of the ISDA Master Agreement or it becomes impossible or impracticable to do so.

Whether a cyber-attack or IT outage constitutes a force majeure event under any contract is a matter of contractual

interpretation and the ISDA Master Agreement does not specifically define what constitutes a "force majeure or act of state". Even if the cyber-attack or IT outage did constitute a force majeure or act of state, each of the following must also occur before the force majeure event provision applies:

1. the relevant event must prevent performance or make it impossible or impracticable to do so;
2. the event must have been beyond the party's reasonable control (which, among other things, may require an evaluation of whether the corporate's IT and cyber risk systems and controls, and its business continuity plans were reasonable and in line with industry standards); and
3. such party could not, after using all reasonable efforts (which will not require such party to incur a loss, other than immaterial, incidental expenses), overcome such prevention, impossibility or impracticability.

If the above elements are met, then there are various consequences under the ISDA Master Agreement, but the key ones being that: (i) payments and deliverables under any impacted transactions are suspended until the event is no longer continuing but up to a maximum of eight business days (the "**Waiting Period**"), meaning that the corporate could avoid a payment default during such period; and (ii) either the corporate or the hedge counterparty will, at the end of the Waiting Period and assuming the relevant event is continuing, be permitted to terminate transactions affected by the relevant event, but on a mid-market basis.

One complicating factor of cyber incidents is attribution – in other words working out who is behind the incident. In some cases, nation state actors can be implicated (or thought to be implicated). It remains to be seen what bearing, if any, this will have on force majeure and "act of state" in particular.

Other financing terms to consider

There may be other relevant financing terms to consider which relate to the disruption of business that will need to be considered. The loss of data or money may be a breach of a preservation of assets undertaking or lead to litigation which in turn may breach representations or undertakings regarding litigation (as mentioned above). Other corporates may also be required to comply with certain laws or licence requirements which may be breached as a consequence of the business disruption or loss of data.

Ransom payments

The logistics of making the ransom payments are complicated but a quick response time is key. Where ransom payments are made, it is common to do so via third parties who specialise in ransom negotiations and the logistics of converting sums of money into Bitcoin or other cryptocurrency.

Perpetrators of cyber-attacks will have committed criminal offences and may be subject to sanctions. Undertaking due diligence prior to any payment is crucial. Given ransom payments usually involve large sums of money, corporates may wish to use the proceeds of financing arrangements to make the relevant payments. The mechanism of making any payments will need to be carefully considered to ensure that there is no breach of laws or regulations (in particular, anti-money laundering and sanctions laws), or of the terms of any financing documents where there are commonly prohibitions against use of proceeds in breach of sanctions or, in some cases, prohibitions against use of proceeds for ransom payments (whether or not in breach of sanctions).

Additionally, many banks, due to the application of anti-money laundering laws and other legislation, will wish to understand the purpose underlying significant withdrawals, so time must be factored into the process to enable these checks to be completed and any objections overcome.

Mitigation of damage

In the event of a cyber-attack or IT outage, the affected corporate and its creditors could seek to agree alternative financing terms, but it may not be possible to effect the necessary changes in time to prevent a default under the finance documents. It is more likely that creditors will need to be notified (under information undertakings which require borrowers to report material litigation or other proceedings and the occurrence of any default, for example) and temporary waivers sought. In such a case, creditors will likely expect to receive periodic information on the continued effects on the business but the disclosure of such information will need to be monitored so as not to prejudice or jeopardise any ongoing insurance investigation or claim.

If you would like to discuss any of this in more detail, please do contact:

Gabrielle Wong
Partner
T +44 20 7466 2144
gabrielle.wong@hsf.com

Stacey Pang
Of Counsel
T +44 20 7466 2514
stacey.pang@hsf.com

Emily Barry
Professional Support Consultant
T +44 20 7466 2546
emily.barry@hsf.com

Kristen Roberts
Managing Partner
T +44 20 7466 2807
kristen.roberts@hsf.com

Nick May
Partner
T +44 20 7466 2617
nick.may@hsf.com

Andrew Moir
Partner
T +44 20 7466 2773
andrew.moir@hsf.com

Peter Dalton
Partner
T +44 2074 662 181
peter.dalton@hsf.com

Nicholas Rutter
Of Counsel
T +44 20 7466 7523
nicholas.rutter@hsf.com

For a full list of our global offices visit **HERBERTSMITHFREEHILLS.COM**