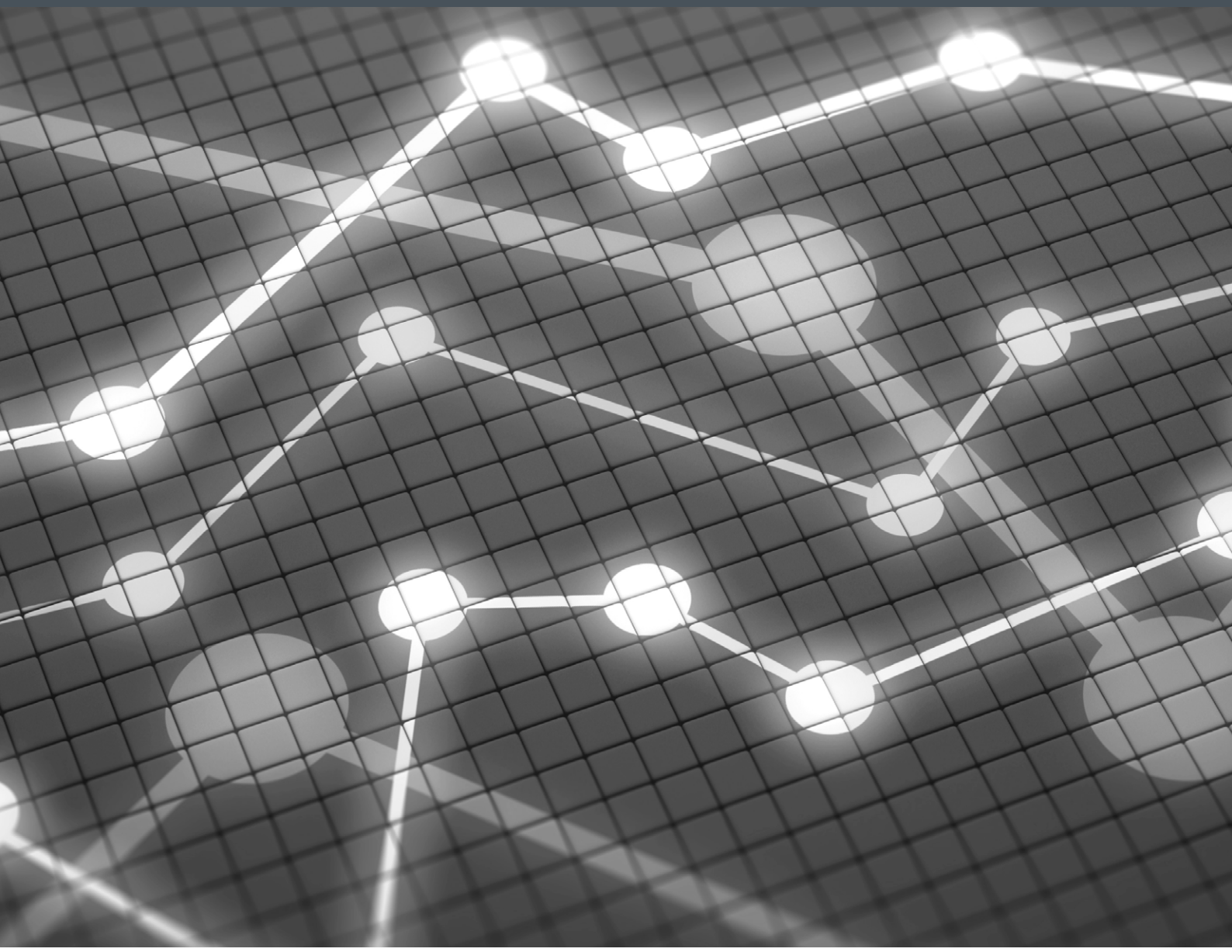

FINANCIAL LINES AND COVID-19

Whilst Central Banks are battling to prevent a worldwide recession caused by COVID-19, by cutting interest rates or injecting funds into their respective economies and banks are seeking to give customers some respite from their financial obligations, (re)insurers are likewise looking at their exposures and the underlying risks and how to manage them. From the Financial Lines perspective, the current circumstances throw up a number of issues.

> **"Increased self-isolation, quarantine, business meeting cancellation and travel restriction inevitably results in increased remote working. This increases cyber security risks on a number of levels."**

Bank operational risk policies

- From an operational risk point of view, financial institutions are no different from other corporates in that the reduction of employee strengths (whether through illness or through flexible working or working from home arrangements) does potentially increase the risk of frauds occurring through/lack of supervision oversight etc.
- Whilst policies do not cater to numbers of employees, clearly a lack of resources, for example, in supervisory or back office staff may render financial institutions more susceptible to fraud. An obvious example, dual control requirements under BBB (Crime) policies. Likewise, the failure to execute transactions or customer mandates may result in claims being made under Professional Indemnity/Civil Liability policies. Whilst bank losses in the region are rising (although there has not been a commensurate increase in levels of cover), one can expect this upward trajectory to steepen in these times.
- Increased self-isolation, quarantine, business meeting cancellation and travel restriction inevitably results in increased remote working. This increases cyber security risks on a number of levels. Technically, employees may seek to rely more heavily on personal devices with less stringent security controls than those of the company, particularly if work is performed in a public place or via a home network. The risk is amplified if remote working strategies are rushed through on an emergency basis without proper implementation controls, for example if the company has not secured all endpoints and ensured that remote access to the corporate network is properly secure.
- Employees may also, albeit unwittingly, become less vigilant and less diligent when working under less formal conditions than that provided by the office environment. Physically, the risk of misplaced devices is increased as is the susceptibility to eavesdropping and unsanctioned viewing of screen content.
- Cyber criminals are of course alive to such increased vulnerabilities. Unauthorised access to the data held and processed by a business can result in significant losses arising out of, for example, liability, data breach, regulatory sanction and reputational damage.

Data privacy

- Given the nature of COVID-19, banks may also expect increased processing of sensitive personal health related data. This can arise from monitoring the health and welfare of not only employees but also, for instance, individuals with whom employees have close contact. From a regulatory perspective, health-related data is generally classified as special category personal data, with additional regulatory requirements above and beyond that of ordinary personal data. From a monetised "commodity" perspective, health-related personal data attracts a higher premium than ordinary personal data. Further, where data privacy regulations exist breaches of such regulations result in sanctions. The increased processing of health-related data increases the risk of regulatory breach. Companies may expect scrutiny from insurers as to the policies and procedures in place around the processing of such special category data.

Trade finance/credit policies

- Market sentiment is that trade finance/credit insurers are reducing their exposures to, at the very least, Chinese corporates

overnight (often to zero). Whilst insured risks prior to the taking down of these limits remain insured (and losses are likely to rise given the likely slowdown in manufacturing (q.v. the motor industry), there is little appetite for capacity going forward.

- Where delays in payment have occurred the ability of insureds to manage and/or recover payments within those jurisdictions is likely to be having circumscribed and constant mandatory (and reporting) to insurers is the best way of managing these losses on a wait and see approach. In addition, waiting periods may serve to mitigate these forms of risks.

D&O policies

- Any large organisation, particularly with public shareholders, are expected to have some form of disaster recovery plan in place (particularly to cater for operational risks). Failure to have the necessary procedures in place (given the more litigious/ regulatory environment) will mean that senior management may well be exposed to claims brought by shareholders, particularly where share prices fall (as they are now doing); thus, triggering D&O policies. In addition, the failure to have other risk transference products in place, such as cyber liability policies, and adequate insurance coverages (for example suitable crime covers and limits) may exacerbate the exposure of senior management to claims.

For further information, please contact:

SAM WAKERLEY
Head of GCC Insurance
T +971 50 654 4508
E sam.wakerley@hfw.com

JOHN BARLOW
Head of Financial Lines
T +44 (0)20 7264 8397
E john.barlow@hfw.com

JUSTIN WHELAN
Head of Cyber Lines
T +44 (0)20 7264 8397
E justin.whelan@hfw.com

HFW has over 600 lawyers working in offices across the Americas, Europe, the Middle East and Asia Pacific. For further information about our insurance and reinsurance capabilities, please visit hfw.com/Insurance-Reinsurance-Sectors.

hfw.com

Americas | Europe | Middle East | Asia Pacific