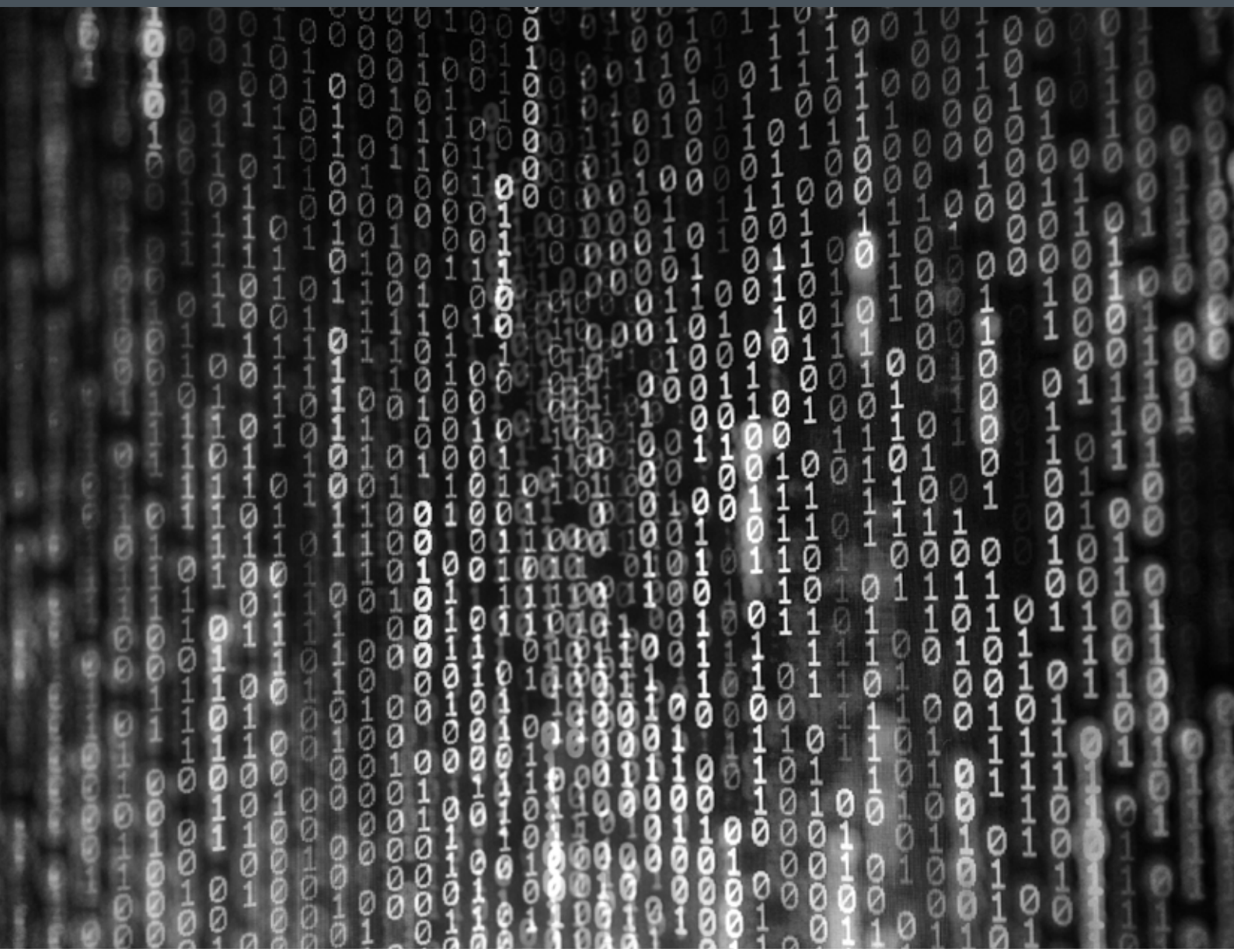


COVID-19 AND REMOTE WORKING - CYBER SECURITY AND DATA PRIVACY

As remote working becomes more and more mandatory across the globe so the prevalence of Covid-19 cyber security and data privacy issues is increasing commensurately.

We have previously commented on some of these issues in our financial lines updates[1]. In this briefing we now broaden this scope to cover business and commerce in general.

1 https://www.hfw.com/Financial-Lines-and-COVID-19-Mar-20

> **“As remote working widens, and for indefinite periods of time, so cyber criminals will continue to innovate threat vectors based on Covid-19.”**

Cyber security

With the rapidly expanding closure of physical premises, cyber criminals are increasingly targeting all manner of businesses whose staff are working from home. Covid-19 related phishing attempts are on the rise as staff, who may already be feeling vulnerable and anxious as the Covid-19 peril accelerates, find themselves in unfamiliar working conditions and increasingly reliant on resources that may be under pressure.

For some businesses, remote working may have already been in place to some extent prior to the pandemic. For other businesses, the switch to remote working may be something entirely novel. Regardless, if new or extended remote working strategies are hurried through on an emergency basis without full and 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, then the risk of security breach is greater.

Further, against operational systems that are under tension employees may seek to rely more heavily on personal devices with less stringent security controls than those of the company. There is then a risk that the line between company information and personal social media information becomes blurred, and in doing so opens up opportunities for cyber criminals.

Also, employees may, albeit unwittingly, become less vigilant and less diligent when working under less formal conditions than that provided by the structured office environment. Physically, the risk of misplaced devices is increased, as is the susceptibility to eavesdropping and the unsanctioned viewing of screen content.

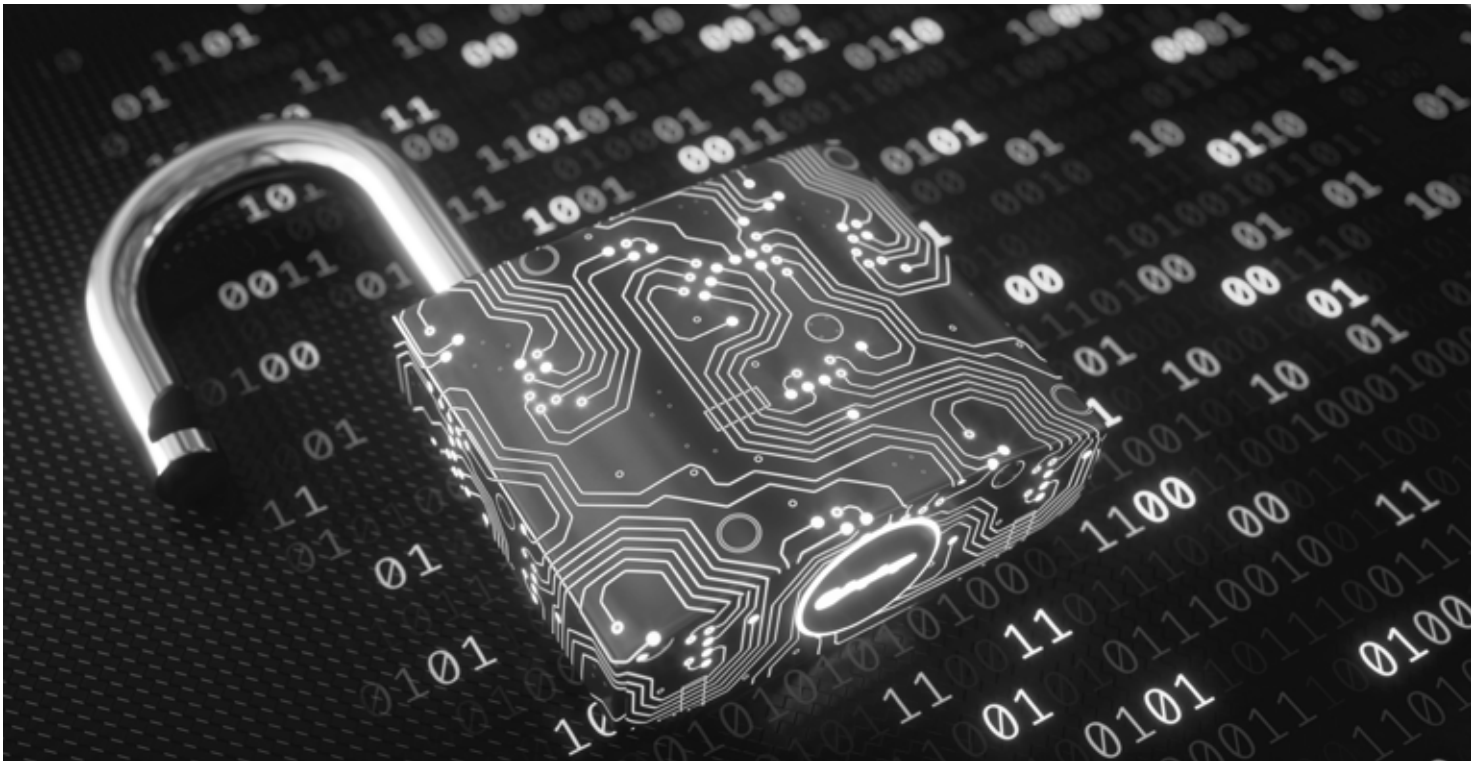
Cyber criminals are of course alive to, and looking to take advantage of, such weaknesses. As remote working widens, and for indefinite periods of time, so cyber criminals will continue to innovate threat vectors based on Covid-19. A single employee click on the wrong email can lead to unauthorised access to the company’s systems and result in significant losses arising out of, for example, liability, data breach, regulatory sanction and reputational damage, which can of course result in significant detriment to a company’s share value. In the event of such, policyholder businesses may well be faced with having to show to insurers the extent to which they had control over the computer network systems from whence the breach and loss emanated.

Data privacy

Whilst most, if not all, data has a monetary value, health-related data is very highly sought. Businesses may expect increased amounts of sensitive, personal health-related data processing, not least from monitoring the health and welfare of employees. Increased volumes of health-related data increases the risk of theft, loss and inadvertent disclosure of such data. For healthcare providers in particular, such a breach has the potential to also result in harm to health and safety.

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. 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. In the event of a breach, policyholder businesses may expect scrutiny from insurers as to the policies and procedures in place around the processing of such special category data.

Financial data is of course also highly sought and heavily targeted by cyber criminals. The objective remains to obtain company and personal



information such as passwords and bank account details etc. and ultimately to obtain money. As remote working broadens, and the aforementioned associated issues manifest, businesses should remain alive to the need to maintain and monitor the security of their own and their employee's personal financial data.

In the current climate, home-based data controllers and data processors are no doubt experiencing a demanding time as they strive to stay on top of the requirement to collect, process and share additional amounts of data borne out of Covid-19 related issues.

Mitigation

There are however a number of basic steps which businesses can take to mitigate such risks:

- Ideally, create a home environment for key employees that resembles the office environment and equipment as much as is possible.
- Establish remote working protocols and include cyber security into crisis management procedures.
- Ensure that IT and security employees are readily and easily contactable and have the appropriate bandwidth and capability to cope remotely with an increased workload.
- Heighten data access controls and restrict access where possible.
- Provide adequate training to staff and remind of the need to be vigilant in the face of increased phishing/malware attempts and the need to report hacking attempts.
- Ensure that home devices and networks are adequately protected, with clear advice on which anti-virus and email-filter software employees may install if required, and via implementing multi-factor authentication.
- Ensure that data that is required to be transported is also done so via protected mechanisms.
- Ensure that data is adequately backed up and capable of recovery and reconstitution, particularly essential data.
- Test such back-up and recovery systems and test incident response plans.
- Regularly install updates to include new patches against evolving threats.
- Log identified malicious attempts and alert employees with regular updates.

Our take

Remote working is here and it is likely to be so for the foreseeable future. There are increased cyber security risks arising from it with the potential for increased data breach, loss and theft resulting in financial losses. Bad actors are aware of the vulnerabilities of business and individuals in such testing times, and will look to increasingly exploit such weaknesses. At a time of worldwide uncertainty with emergency fiscal measures being implemented across the globe, many businesses are finding themselves in a vulnerable economic position. It is prudent therefore to implement cyber risk mitigation measures in seeking to protect and bolster resilience.

For further information on this briefing, please contact the authors or your usual HFW contact.

JUSTIN WHELAN
Partner, Abu Dhabi
T +971 2 235 4913
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