NORTON ROSE FULBRIGHT

Going viral

Heightened cyber and corporate crime risks in the COVID-19 pandemic

The COVID-19 outbreak has posed an unprecedented challenge – not just for individuals and governments, but also corporates seeking to navigate unchartered waters in the widespread disruption caused by the global pandemic. Operational challenges aside, the unique circumstances of the pandemic have also presented opportunities for cyber and corporate criminal activity.

In this article, we explain how the ongoing pandemic presents corporates with further risks from four key corporate crime threats, namely, (1) cyber scams, (2) cyber attacks, (3) corrupt activity and (4) fraudulent conduct. As corporates grapple with economic survival in this pandemic they should also actively inoculate themselves against these risks by continuing to educate their employees about fraudulent schemes and corruption risks, ensuring "compliance as usual" and undertaking fact-finding enquiries promptly.

Cyber scams

With the enforced closures of offices, various degrees of lock-down and remote working arrangements for employees in response to the COVID-19 outbreak, an organization may find that its existing anti-fraud controls and procedures are at greater risk of being compromised due to such controls and procedures not being fit for purpose in an enforced remote working environment, with limited employee interaction and compliance oversight and severe curtailment in resources.

The diminution in the efficacy of such controls and procedures can be exploited by opportunistic cyber fraudsters. In particular, we have seen an increase in Business Email Compromise (BEC) scams. BEC fraudsters are increasingly sophisticated and meticulous. They carry out careful surveillance of their corporate victims – analyzing organizational structures, identifying the names and titles of key officers, and studying detailed information on the company's products and services. The days when such scams can be easily spotted through typographical errors and clearly forged websites are fading away. BEC fraudsters have been known to compromise accounts in order to obtain access to email and IT systems to covertly read exchanges and obtain confidential company information. Armed with the intelligence gathered about their corporate victim, BEC fraudsters would then identify a target – often a mid-level employee with key access to company assets such as corporate bank accounts. They execute their scam by posing as a key senior officer of the company through email spoofing and instructing the target employee to take certain action – often on an urgent basis – such as the transfer of money to an account controlled by them.

Cyber scams such as BEC are not new. Where such scams could have been averted by popping over to a colleague's cubicle to verify purported instructions from a key senior officer of the company, this is no longer the case with an enforced remote working environment thereby providing fraudsters with greater opportunity to effectively carry out their fraudulent schemes.

Cyber attacks

Enforced remote working has placed a greater emphasis on the integrity and availability of enterprise IT systems of corporates. Cyber criminals are well aware of this and more motivated than ever to carry out their attacks on IT network systems.

In this regard, there has been a discernible increase in cyber incidents involving the use of ransomware – where threat actors deploy malware to encrypt files of their victims, making them inaccessible and demanding ransom payments in return for the provision of passwords. Ransomware first came into prominence in 2017 with the WannaCry ransomware attacks that spread viciously and indiscriminately across the world, affecting healthcare, manufacturing, telecommunications and financial systems. However, it was easier to ignore cyber criminals responsible for the WannaCry attacks if a victim had alternate means to access and recover their data, and there was little downside to ignoring their demands for ransom.

Recent attacks have seen sophisticated cyber criminals become bolder and more vindictive. In addition to simply obtaining access to, and encrypting, data belonging to their victims, cyber criminals now seek to exfiltrate valuable data

(e.g., personal data, business sensitive information, trade secrets) from the systems and encrypt the data so that it becomes inaccessible. These cyber criminals are also more selective, seeking to target large corporates, rather individual victims. These cyber criminals would then pile pressure on their corporate victims to pay the ransom by taunting and threatening to release the data if the ransom is not paid. In this regard, some of these cyber criminals have published "data shaming" websites, where they have leaked exfiltrated data stolen from their victims that have refused to accede to their demands – in effect making good on their threats, and setting off a series of consequences including civil claims, regulatory investigations and adverse publicity.

In addition to the increased threat posed by these cyber criminals, the enforced remote working environment also poses challenges to corporates in responding to these threats, as incident response teams are forced to grapple with logistical challenges of not being able to carry out response measures in close proximity onsite.

Corruption

The operational and business pressures brought on by the COVID-19 pandemic have meant that some corporates are more focused on financial preservation and operational continuity at the expense of compliance. This is myopic and may result in increased corruption risks in potentially the following ways.

First, corporates may be tempted to temporarily defer the implementation of scheduled compliance processes and initiatives. They may render them more vulnerable to corruption risks as it diminishes the ability of compliance controls to effectively safeguard against such risks. It may also send the wrong compliance message to employees – that compliance is "good to have" in good times and may be disregarded in bad times.

Second, the increased focus on financial objectives, including performance targets, is likely to result in greater pressure being placed on sales employees to perform and meet targets. Some of these targets may have been set in a pre-COVID-19 pandemic environment and may no longer be realistic. Such targets, coupled with employment anxiety, may tempt some employees to take risks and enter into corrupt transactions.

Third, the COVID-19 pandemic may result in interruptions to supply chains due to border closures, transport disruptions and lockdown restrictions. The pressure on corporates to deliver their services on time to avoid paying liquidated damages, despite such restrictions, may result in new third parties having to be engaged without proper due diligence in order to meet contractual obligations. These high-risk third parties may expose the corporates to corruption risks, e.g. when making facilitation payments to government officials in order to expedite operations.

Fraud

The emphasis on financial performance may tempt individuals into engaging in corrupt behavior if they consider it necessary to protect their jobs and ensure the continued viability of the business. This similarly holds true for fraudulent behavior.

The pressure to deliver revenue targets may find employees more likely to manipulate books and records, or enter into fictitious or sham transactions in order to create the appearance of a healthy financial position.

Inoculation – Preventing a fraud and corruption pandemic

In such uncertain times, it is important for organizations to bolster their safeguards against fraud and corruption risks, and to utilize the challenges posed by the COVID-19 pandemic as a springboard to better prepare against such risks.

Educate and raise awareness among employees of new risks

Keep employees attuned to the heightened risks of fraudulent schemes (including digital fraud such as phishing attacks and account takeover fraud, in addition to BEC scams) and corruption risks. Prompt and focused training on these practices should be provided to employees so that they are cognizant of the steps they would need to take to reduce these risks and sharpen detection and prevention of such practices. Employees should also be reminded of their obligations to comply with company policies and applicable laws, as well as the ramifications of their failure to do so. Significantly, leaders in organizations should clearly set the 'tone from the top' on the importance of this training and to emphasize the organization's commitment to vigilance against fraudulent and corrupt acts.

Ensure compliance as usual

Given the unprecedented business challenges faced by organizations, compliance programs will be placed under tremendous pressure to adapt to the economic issues created by the pandemic. Organizations should consider if their compliance frameworks need to be re-tooled to adapt to the new circumstances. While it may be tempting to cut corners to meet demands, it is crucial that compliance controls are carried out as rigorously as before. An assessment of the new risk environment and the appropriate tailoring of available resources to protect business, reputation and employees will assist organizations in circumventing fraud and bribery exposure.

Undertake fact-finding enquiries promptly

In addition to encouraging employees to report acts of fraud or corruption, organizations should ensure that necessary fact-finding investigations are promptly undertaken to preserve relevant information and documentation, and to stop the continuation of the alleged wrongdoing. It is vital for the organization to demonstrate that it takes allegations of misconduct seriously, instilling a strong culture of ethics and integrity within the organization.

While the primary focus of organizations has pivoted to financial viability and preservation in weathering the extraordinary circumstances of COVID-19, it is imperative that these challenges do not distract them from the elevated exposure to cyber scams and attacks as well as fraud and corruption risks which have emanated from the crisis. Now more than ever, organizations should be prepared to respond to these risks by ensuring that compliance functions are adequately resourced.

Contacts

Wilson Ang
Partner
Tel +65 6309 5392
wilson.ang@nortonrosefulbright.com

Jeremy Lua
Associate
Tel +65 6309 5336
jeremy.lua@nortonrosefulbright.com

Marianne Chew
Associate
Tel +65 6309 5452
marianne.chew@nortonrosefulbright.com

Global resources

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 3700 lawyers and other legal staff based in Europe, the United States, Canada, Latin America, Asia, Australia, Africa and the Middle East.

People worldwide

7000+

Legal staff worldwide

3700+

Offices

50+

Key industry strengths

- Financial institutions
- Energy
- Infrastructure, mining and commodities
- Transport
- Technology and innovation
- Life sciences and healthcare

Our office locations

Europe

- Amsterdam
- Athens
- Brussels
- Frankfurt
- Hamburg
- Istanbul
- London
- Luxembourg
- Milan
- Monaco
- Moscow
- Munich
- Paris
- Piraeus
- Warsaw

United States

- Austin
- Dallas
- Denver
- Houston
- Los Angeles
- Minneapolis
- New York
- St Louis
- San Antonio
- San Francisco
- Washington DC

Canada

- Calgary
- Montréal
- Ottawa
- Québec
- Toronto
- Vancouver

Latin America

- Mexico City
- São Paulo

Asia Pacific

- Bangkok
- Beijing
- Brisbane
- Canberra
- Hong Kong
- Jakarta[1]
- Melbourne
- Perth
- Shanghai
- Singapore
- Sydney
- Tokyo

Africa

- Bujumbura[3]
- Cape Town
- Casablanca
- Durban
- Harare[3]
- Johannesburg
- Kampala[3]
- Nairobi[3]

Middle East

- Dubai
- Riyadh[2]

1 TNB & Partners in association with Norton Rose Fulbright Australia
2 Mohammed Al-Ghamdi Law Firm in association with Norton Rose Fulbright US LLP
3 Alliances

NORTON ROSE FULBRIGHT

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 3700 lawyers and other legal staff based in Europe, the United States, Canada, Latin America, Asia, Australia, Africa and the Middle East.

Law around the world

nortonrosefulbright.com