COVID-19: A Business Impact Series

Cyber and Fraud Risk

Issue 4 | 20 April 2020

The COVID-19 pandemic has led governments and organisations to respond by taking unprecedented steps including lockdown measures which have had significant socio-economic impact. This impact on Nigerian businesses cuts across demand & supply, operations & business continuity as well as cyber and fraud risks. This edition of our newsletter will focus on the latter, i.e. cyber and fraud risks facing businesses as they navigate through this pandemic crisis and key considerations in managing such risks.

Overview

COVID-19 pandemic is changing our lives; from the way we interact to the way we work and communicate. Corporate entities and people are not just concerned but are working frantically to ensure safety and wellness of their employees, their loved ones, and at the same time, ensuring business continuity.

In a bid to control the spread of COVID-19, various governments have had to respond by restricting movement and enforcing lockdown measures across different locations. This has compelled both businesses and customers to opt for digital channels in performing operations and transactions. Similarly, to ensure business continuity, many businesses have adopted remote working, which in this context, is an uncharted territory for many organisations and their employees. This increase in internet and mobile app adoption has also created an opportunity for cyber attackers who have increased their efforts in performing various cyber attacks, particularly via social engineering.

Furthermore, it is understandable that there is a heightened level of concern and worry, and with that concern comes a desire for information, safety and support. Organised crime groups are exploiting the fear, uncertainty and doubt which COVID-19 brings to target individuals and businesses in a variety of ways.

Since mid-February, KPMG member firms have seen the rapid growth of infrastructure by cybercriminals used to launch COVID-19 themed spear-phishing attacks. These attacks continue to underscore the impact of cyber risk on businesses today, particularly in the face of a pandemic.

Cyber and Fraud Risk Implications

Business disruption

Data correlated across several threat intelligence platforms show that there has been an upward trend in attempted COVID-19 themed malware and spam campaigns. There have been several phony advisories purporting to provide updates on COVID-19 spread, health updates, fake cures, leading to malware download and ransomware attacks. Some of these attacks if successful could lead to unavailability of critical systems and data.

Fraud

COVID-19 themed spear-phishing attacks have lured customers and employees to fake websites seeking to collect customer banking details, credentials of critical systems such as Office 365. There have been cases of impersonation of bank staff in order to lure unsuspecting customers to give out sensitive information such card details, one-time-passwords (OTP), etc. in order to perpetrate fraud. CEO and CFO fraud is also a key risk area, where a cyber attacker claims to be the CEO or CFO of the company and is under high time pressure to get an important payment through.

Critical data breach

The remote working arrangement, which for many organisations is ad hoc; and was never fully planned has increased the risk of loss of sensitive business and personal data. This arrangement has led to an increase in the use of virtual meeting platforms, some of which may contain vulnerabilities that can be exploited by cyber attackers. Other key risk factors include use of personal devices with limited or no security protection

for business, inadequate awareness amongst staff, inadequate remote access security for critical systems. Breach of business and personal data can lead to reputational damage as well as regulatory sanctions.

Third-party failures

As organisations across the world adopt remote working arrangement, there is a widening of the attack surface due to third-party risk. Many vendors providing support for critical services also have their employees provide support to clients from home, while some have to engage ad hoc staff to perform services due to unavailability of certain employees. The impact of third-party failures may lead to business disruptions, data breach, amongst others if not properly managed.

Changing fraud landscape

The immediate concern regarding the current situation is that traditional fraud controls are being challenged, with more focus being shifted to cyber fraud.

Corporate entities should therefore pay more attention to the following, among others:

Increase in use of e-signatures

Contracts, invoices and sensitive documents that are usually printed and physically signed now have to be processed electronically with e-signatures and electronic letter heads. This may result in some fraud risks for organisations; such risks include:

- easy and unauthorized reproduction of the organisation's letterheads and relevant e-signatures.
- reduced ability to authenticate documents.

Relaxed segregation of duties and controls

The current situation is not business as usual and fraudsters may want to exploit this to their advantage by creating perceived emergency situations that may result in relaxed controls or disregard for existing segregation of duties.

Possible increase in records falsification

Due to the restricted movements, employees and third parties in remote locations may take advantage of this to falsify records such as:

- Billing hours
- Stock delivered/Service provided
- Expense reports

How businesses can respond

There are some key steps you should take to reduce the risk to your organisation, your customers and your employees, particularly as you move to remote working:

- Minimise sharing sensitive information in the virtual meetings, as you can still use your secure email platform, for sharing sensitive information.
- Minimise sharing sensitive information in the virtual meetings, as you can still use your secure email platform, for sharing sensitive information.
- Raise awareness amongst your team warning them of the heightened risk of COVID-19 themes phishing attacks.
- Enhance security awareness to your customers via email and text messages, providing tips on safe use of your digital channels.
- Make sure you set up strong passwords, and preferably two-factor authentication, for all remote access accounts; particularly for Office 365 access.
- Assess third-party risks of vendors who provide support for critical systems, digital interfaces and channels.
- Ensure that all provided laptops have up to date anti-virus and firewall software.
- Ensure that your critical IT infrastructure are fully patched with up-to-date security fixes
- Run a helpline or online chat line which they can easily access for advice, or report any security concerns including potential phishing.
- Ensure that your finance processes require finance teams to confirm any requests for large payments. This confirmation can help to guard against the increased risk of business email compromise and CEO frauds. Ideally, use a different channel such as phoning or texting to confirm an email request.
- Confirm invoices and sensitive information received from third-parties against previous communication with the third-parties before they are treated.
- Make certain that you back up all critical systems and validate the integrity of backups, ideally arranging for off- line storage of backups regularly. Expect an increased risk of ransomware during the COVID-19 pandemic as organized crime groups exploit COVID-19 themed phishing.

In summary, here are key points to consider:

- Have you assessed the cyber posture of new and existing systems being exposed for remote access?
- Can the current security incident monitoring mechanism support your organisation in case of increased attack on critical platforms?
- Are you confident that your current cyber security awareness sufficiently and effectively covers your employees, third-party and customers.

Economic and Regulatory Updates

Points from President Muhammadu Buhari's Speech to Extend the Lockdown

President Muhammadu Buhari, on the 13th of April, 2020, issued formal regulations to back his decision to extend the lockdown on two major cities (Lagos, Ogun) and the federal capital territory for another two weeks to curb the spread of the coronavirus.

With the signing of the Regulation (No.2) of 2020 by the president, there will now be restriction of movements on residents of the affected areas till April 28. A few points worthy of note are enumerated below.

- The approach to the virus remains in 2 steps – First, to protect the lives of our fellow Nigerians and residents, and second, to preserve the livelihoods of workers and business owners.
- The number of confirmed COVID-19 cases globally was over one million, eight hundred and fifty thousand.(1,850,000) This figure is more than double in two weeks since the lockdown.
- Nigeria had 323 confirmed cases in twenty States with ten (10) fatalities. Lagos State remains the center and accounts for 54% of the confirmed cases in Nigeria. When combined with the FCT, the two locations represent over 71% of the confirmed cases in Nigeria.
- Using our resources and those provided through donations, adequate equipment will be provided in the coming weeks. Already, healthcare workers across all the treatment centres have been provided with the personal protective equipment that they need to safely carry out the care they provide.
- Over 7,000 Healthcare workers have been trained on infection prevention and control while deploying NCDC teams to 19 states of the federation.
- The massive support from traditional rulers, the Christian Association of Nigeria (CAN) and the Nigerian Supreme Council for Islamic Affairs (NSCIA) during this pandemic is duly recognised.

Nigeria's Health Minister, Osagie Ehanire, Shares Strategies for Containment of COVID-19

One of the strategies for the containment of COVID-19 is to increase awareness among doctors who underrate the highly infectious potential that the virus possesses, in order to prevent their patients from the high risk involved. Currently, there are thirteen public laboratories that are in a position to handle tests for the Coronavirus. For the private sector to participate, certain criteria must be met in addition to having an accreditation to treat highly infectious diseases. This outbreak has allowed the opportunity to reshape the system, both in the public health sector and other health delivery spaces. Procurement plans and processes to revamp the entire health sector has been put in place. Various messaging channels including social media have been adopted to inform and educate people. A house to house collection of test samples, particularly in Lagos and Abuja has commenced. Travelers' were the first targets because of the potential of imported pathogens; right now, the next phase is to move into community transmission. This entails engaging traditional rulers and other gate keepers of society to encourage community members to test for the virus.

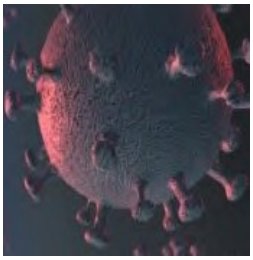
Our Latest Publications

Corona Virus: Global and Domestic Impact

Considering the global stance of the coronavirus source country (China) and its spread to other activity-driven economies such as the U.S., India, Russia, UK among others, it is important to examine the pass-through effect of the pandemic disease from global and Nigerian perspective. Follow the link for more details: xxxxxxx

Impact of COVID-19 on the Banking Sector

COVID-19 is in the first place, a pandemic with potential serious implications for people'shealth. It is an unprecedented challenge for our modern societies and health systems. Theconsequences of the pandemic for our global economy and financial sector are unpredictable. Follow the link for more details: xxxxxxxxxx



Tackling Fraud Opportunities Arising from Working Remotely

The COVID-19 pandemic has altered everything around us; from the way we interact to the way we work and communicate. Corporate entities and people are not just concerned but are working frantically to ensure safety and wellness of their employees, their loved ones, and at the same time, ensuring business continuity. This has resulted in the increased adoption of remote working. Follow the link for more details: xxxxxx

For feedback and enquiries, please contact:

John Anyanwu
T : +234 803 975 4061
E : john.anyanwu@ng.kpmg.com

Olusegun Zaccheaus
T : +234 703 417 0139
E : olusegun.zaccheaus@ng.kpmg.com

Omolara Ogun
T: +234 808 200 0128
E: omolara.ogun@ng.kpmg.com

Ebenezer Ibeneme
T: +234 808 313 3019
E: ebenezer.ibeneme@ng.kpmg.com

David Okwara
T : +234 708 383 3853
E : david.okwara@ng.kpmg.com
home.kpmg/ng
home.kpmg/socialmedia