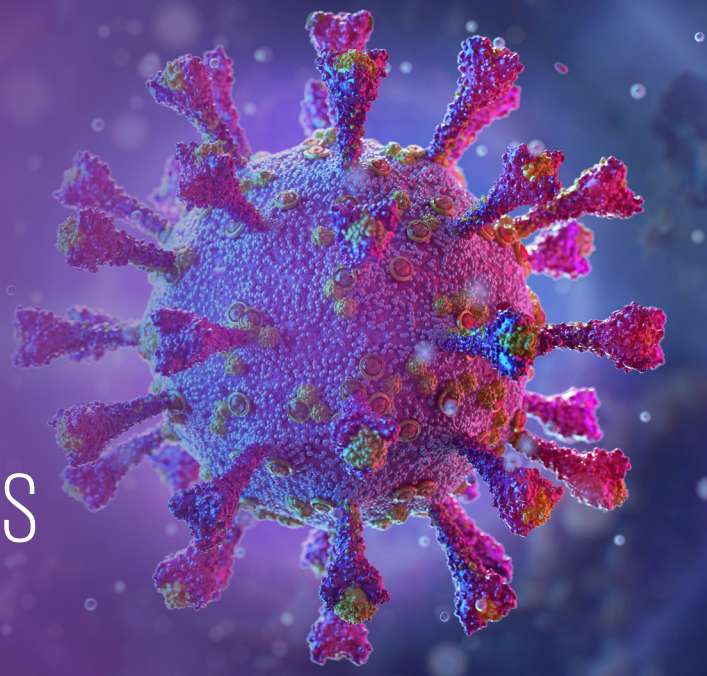
KPMG

COVID-19 Cyber Security Implications for Businesses



KPMG in Nigeria

April 2020

COVID-19 pandemic is changing our lives. People are concerned, and with that concern comes a desire for information, safety and support. Organized crime groups are exploiting the fear, uncertainty and doubt which COVID-19 brings to target individuals and businesses in a variety of ways.

The threat

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. The 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.

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. Some of these include:

- **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 organizations is ad hoc; and was never fully planned has increased the risk of loss of sensitive business and personal data. The 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 organizations 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.

The response

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

- 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.
- Share definitive sources of advice on how to stay safe and provide regular communications on the approach your organization is taking to the COVID-19 pandemic
- Make sure you set up strong passwords, and preferably two-factor authentication, for all remote access accounts; particularly for Office 365 access
- Provide remote workers with straightforward guidance on how to use remote working solutions including how to make sure they remain secure and tips on the identification of phishing
- 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
- Run a helpline or online chat line which they can easily access for advice, or report any security concerns including potential phishing
- Disable USB drives to avoid the risk of malware, offering employees an alternate way of transferring data such as a collaboration tool

Also, make sure that your finance processes require finance teams to confirm any requests for large payments during the COVID-19 pandemic. 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.

Ensure that you apply critical security patches and update firewalls and anti-virus software across your IT estate, including any laptops in use for remote working. You should expect organized crime groups to exploit any failures in the maintenance of IT systems during this pandemic.

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?
- Have you identified single points of failures (SPOF) in the security architecture and how do you plan to manage any resulting incident?
- Are you confident that your current cyber security awareness sufficiently and effectively covers your employees, third-party and customers

COVID-19 will drive significant changes in how you and your organization work, stay safe and stay secure.

If you have any questions or would like additional advice, please contact us.

Contacts

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

Samuel Asiyanbola
T: +234 802 501 3893
E: samuel.asiyanbola@ng.kpmg.com

Saheed Olawuyi
T: +234 803 403 5542
E: saheed.olawuyi@ng.kpmg.com

Tomi Ogunwole
T: +234 802 501 1431
E: Olutomilayo.Ogunwole@ng.kpmg.com

home.kpmg/ng
home.kpmg/socialmedia