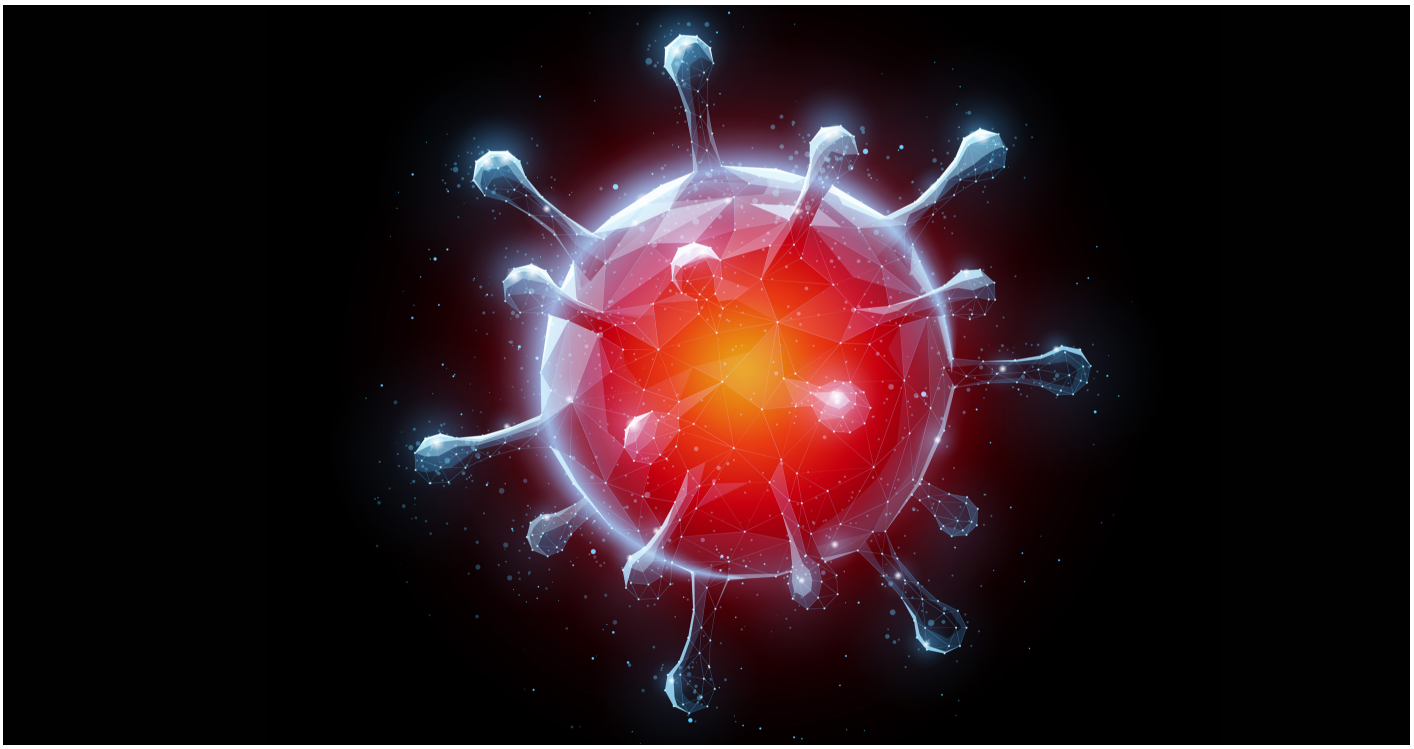
Deloitte.

March 2020



# COVID-19's Impact on Cybersecurity

All over the world, the COVID-19 pandemic has been the headline over the past few weeks. COVID-19 has also forced organisations and individuals to embrace new practices such as social distancing, hand washing/sanitizing and remote working. Governments are reconsidering ways to ensure that their countries are stable by developing and enforcing new economic plans. Nevertheless, while the world is focused on the health and economic threats posed by COVID-19, cybercriminals around the world undoubtedly are capitalizing on this crisis. In this article, are some of our thoughts on the impact of COVID-19 on cybersecurity.

## A rise in COVID 19 related phishing and ransomware attacks

From our Cyber Intelligence Centre, we have observed a spike in phishing attacks, Malspams and ransomware attacks as attackers are using COVID-19 as bait to impersonate brands thereby misleading employees and customers. This will likely result in more infected personal computers and phones. Not only are businesses being targeted, end users who download COVID-19 related applications are also being tricked into downloading ransomware disguised as legitimate applications.

Organisations should take proactive steps by advising their staff and customers to be more vigilant and cautious especially when opening links, emails or documents related to the subject COVID-19. Organizations should ensure their detection and alerting capabilities are functional while keeping an eye on the impact of having many remote workers.

## Increased security risk from remote working/learning

With many employees working from home and students learning virtually, enterprise virtual private network (VPN) servers have now become a lifeline to companies/schools, and their security and availability will be a major focus going forward. In a bid to achieve this, there is a possibility that an organisation's unpreparedness will lead to security misconfiguration in VPNs thereby exposing sensitive information on the internet and also exposing the devices to Denial of Service (DoS) attacks. In addition to this, some users may utilise personal computers to perform official duties which could also pose a great amount of risk to organisations.

Organisations should ensure VPN services are safe and reliable as there promises to be a lot more scrutiny against these services. Furthermore, employees should be advised against using personal computers for official purposes.

## Potential delays in cyber-attack detection and response

The functioning of many security teams is likely to be impaired due to the COVID-19 pandemic thereby making detection of malicious activities difficult and responding to these activities even more complicated. Updating patches on systems may also be a challenge if security teams are not operational.

Organizations should evaluate the security defences in place and explore the use of co-sourcing with external consultants especially for areas where key man risks have been identified.

## Exposed physical security

The enforcement of “work from home” policy by some companies in Nigeria, where stable power supply and fast Internet connection may be a luxury in some quarters, may see employees work from public spaces to utilise power and free internet facilities. This behaviour may inadvertently expose the computing facilities and confidential information it contains to theft or damage.

Organisations are hereby encouraged to sensitize their employees around information security outside of the office space. Working from public spaces should be restricted and organisation should utilize technologies that ensure confidential information remain secure on these devices in the case of theft or damage.

## Influx of cyber criminals

Globally, companies are downsizing their workforce to cope with the effects of COVID-19. Some people have also lost their means of livelihood due to the various restrictions of movement by governments across the world. This move would likely encourage the growth of cyber criminals as idle people with internet access who have lost their jobs from the effects of COVID-19 may see an opportunity to make a living out of this pandemic.

Organisations considering laying off staff should enforce proper exit plans. Also, we encourage all who have lost their jobs or currently being restricted to a location to consider taking this period to learn a new profitable skill and undertake online courses.

## Business Continuity Plans (BCP) to feature global pandemics

Many organizations have business continuity plans, but it is obvious the impact of a global pandemic like COVID-19 was not considered in many BCPs. With the widespread impact of the COVID-19, organisations need to re-visit their Business continuity program and incident response plans especially to feature such pandemics that affect many countries and critical elements of supply chains at the same time.

A revised risk assessment should be conducted on critical processes to identify the various options in ensuring these processes can still be maintained at an acceptable level and an effective fail over is achievable.

## Post COVID-19 Cyber Security Posture

The COVID-19 pandemic has caused a huge strain on the global economy with some experts predicting a recession as part of the after effects of the pandemic. Organisations Post COVID-19 pandemic strategy might include downsizing by cutting off business lines considered as non-critical which may include cyber security operations. This short term plan might however prove to be “penny wise and pound foolish” in the long haul as this will further increase the impact of attacks on the organization.

Organizations are advised to update at their BCPs and remote working policies/practices whilst prioritizing cyber security during post COVID-19 re-strategizing process.

In conclusion, COVID-19 will change our lives forever with new work styles, new cybersecurity issues, new proposed policies, personal hygiene and so on. The fight against COVID-19 is not just for the organisation, employee or customer but a joint effort from everyone. It is also apparent that Post COVID-19, organizations will need to rethink their cyber risk management measures.

## Contact

**Tope Aladenusi**
Cyber Risk Services Leader
Deloitte West Africa
taladenusi@deloitte.com.ng
+234 1 904 1730

www2.deloitte.com/ng

Deloitte Nigeria