ÆLEX

JULY 2020

DATA BACKUP AND SECURITY GUIDELINES AS IMPACT MITIGATION STRATEGIES IN LIGHT OF THE COVID-19 PANDEMIC

ARTICLE SERIES

INTRODUCTION

The COVID-19 pandemic hit the world in an unprecedented manner and, in just a few months, it has had such a profound impact on the world of work. The need to curb the spread of the COVID-19 virus forced governments of affected countries to issue lockdown orders and restrict movements. As a result, physical office premises were shut down and many employees engaged by organisations were forced to work from home with little or no security policy in place or a viable data backup and recovery plan.

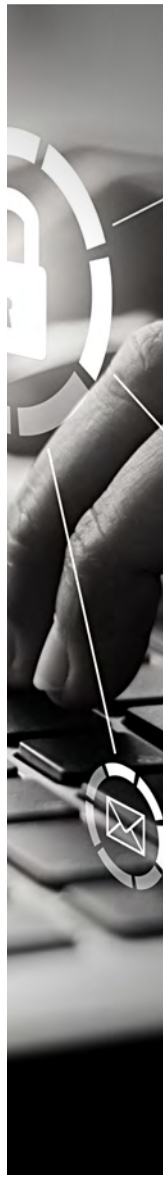
In addition, some organisations resorted to employees using their personal computers and other devices to carry out official assignments. The resulting effect is possible exposure to cyber-risks from the use of insecure Internet protocol (IP) addresses and the possibility of data not being backed up appropriately.[1] In this article, we examine data backup and other data security guidelines that may be useful in assisting Nigerian organisations during the pandemic.

DATA BACKUP AND RECOVERY

Data backup and recovery refers to the process of backing up data and setting up systems that allow data recovery in order to forestall loss of data.

Data backup and recovery is very important in running a business for many reasons. Computers may crash, human errors may occur, documents may get corrupted and several other issues might occur which the organisation may be ill prepared for.[2]

Backing up data requires copying and archiving computer data so that it is accessible in case of data deletion, corruption or a human-caused event such as a malicious attack (virus or malware).[3] Some popular data backup tools include Microsoft Outlook's OneDrive, SharePoint, Oracle Database Backup Service and Google Drive. It is, however, advisable that for every backup that is carried out, adequate security must be in place.



[1] Dan Dahlberg, 'Identifying Unique Risks of Work from Home Remote Office Networks' (2020) Bitsight <https://www.google.com/amp/s/www.bitsight.com/blog/identifying-unique-risks-of-work-from-home-remote-office-networks%3fhs_amp=true/ > accessed on 21 May 2020
[2] IT, 'Importance of data backup' (2019) Brickhost https://www.brickhost.com/importance-of-data-backup-and-recovery > accessed on 16 June, 2020
[3]'Backup and Recovery' (2017) Techopedia <https://www.techopedia.com/definition/24058/backup-and-recovery#:~:text=Backup%20and%20recovery%20refers%20to,of%20data%20deletion%20or%20corruption.> accessed via 16 June, 2020

RECENT INCIDENTS OF CYBERATTACKS

In 2018, it was reported that 60% of Nigerian firms suffered cyber-attacks, and that the country spent $270 million on cyber security.[4] There is also evidence to show heightened cyber attacks during the COVID-19 pandemic. Consequently, the Central Bank of Nigeria in a recent press release[5] alerted the general public of cyber-criminals taking advantage of the pandemic to defraud citizens, steal sensitive information or gain unauthorized access to computers or mobile devices using various techniques. However, the increasing trend is not peculiar to Nigeria. Other parts of the world have witnessed a rise in cyber-attacks. For instance, just recently, EasyJet[6] reported a phishing attack to the United Kingdom's Information Commissioner's Officer.[7] Similarly, it has been reported that a New York law firm used by A-list stars has been hacked by cybercriminals who claimed to have accessed clients' data including contracts and personal emails.[8]

It is pertinent to note that when employees are targeted by cyber criminals, employers of the organisation are often vicariously liable for the actions and inactions of employees whether done intentionally or negligently.

NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY'S POSITION

National Information Technology Development Agency ("NITDA"), the agency in charge of data protection regulation in Nigeria, issued the Nigeria Data Protection Regulation ("NDPR") which prescribes that[9] anyone involved in processing or controlling data shall develop security measures to protect data.

[4] Jumoke Akiyode-Lawanson 'SMEs hardest hit by cyber attacks, as 60% of Nigerian business suffers attack (2019) Businessday <https://businessday.ng/technology/article/smes-hardest-hit-by-cybercrime-as-60-of-nigerian-businesses-suffer-attacks/> accessed on June 11 2020

[5] Isaac Okorafor ' Alert, Beware of Covid-19 cyber-attacks fraud' (2020) CBN <https://www.cbn.gov.ng/Out/2020/CCD/CBN%20Press%20release%20-%20COVID-19%20-%20Cyber%20Security.pdf> accessed on June 11 2020

[6] 'EasyJet Airline Company Limited - Company Profile, Information, Business Description, History, Background Information on easyJet Airline Company Limited' Reference for Business <https://www.referenceforbusiness.com/history2/7/easyJet-Airline-Company-Limited.htm>l accessed on 21 May, 2020

[7] Jane Wakefield'EasyJet admits data of nine million hacked' (2020) BBC<https://www.google.com/amp/s/www.bbc.com/news/amp/technology-52722626> accessed on 20 May, 2020

[8] Joe Tidy 'Hackers hit A-list law firm of Lady Gaga, Drake and Madonna' (2020) BBC < https://www.google.com/amp/s/www.bbc.comnews/amp/technology-52632729> accessed on 20 May, 2020

[9] Article 2.6 of the NDPR

Such security measures include protecting the systems from hackers, setting up firewalls, storing data securely with access to authorised individuals, employing data encryption technologies, developing organisational policy for handling personal data (and other sensitive or confidential data), protection of emailing systems and continuous capacity building for staff. Furthermore, while celebrating the World Backup Day on 31st March 2020, NITDA advised Nigerians on Data Backup as impact mitigation strategy in light of COVID-19. The following are the basic guidelines that NITDA has recommended:

1. Ensure that you backup your data frequently and at relevant intervals;
2. Consider using remote storage for your backups;
3. Ensure that the files containing your data backups are encrypted and protected; and
4. Use multiple methods and multiple media for your data backups.[10]

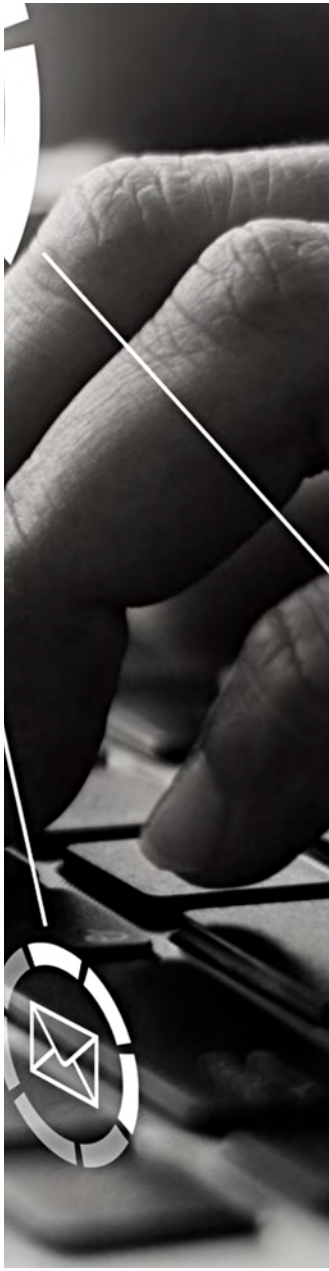
The above guideline is mostly premised on the principles of the NDPR, which include storage, security and accuracy.

RESPONSIBILITY FOR DATA SECURITY

Organisations have a duty of care to protect clients' information and/or documents. Within the organisation, the data controller has the responsibility for providing data security[11]. Consequently, in order for organizations to adequately protect themselves, it might be advisable that they encrypt their data and/or set up passwords on emails or documents sent. Overall, organisations should be conscious of cyber security issues and probably develop a security policy.

CONCLUSION

Data Controllers should always remember that actions and inactions of their employees rise and fall on them. Hence, organisational and technical controls should be put in place to protect information of the clients in its possession from the risks of unauthorised disclosure, hacking, corruption, etc. while trying to store data, backup and or recover information.



[10]Ugo Onwuaso 'COVID-19: NITDA advises Nigeria on data backup as impact mitigation strategy' (2020) Nigeria Communications Week https://nigeriacommunicationsweek.com.ng/covid-19-nitda-advises-nigerians-on-data-backup-as-impact-mitigation-strategy/ accessed on 16 June, 2020
[11] Article 2.1(d) of the NDPR

ÆLEX

Florence
Bola-Balogun

Opeyemi
Adeleke

ÆLEX is a full-service commercial and dispute resolution firm. It is one of the largest law firms in West Africa with offices in Lagos, Port Harcourt and Abuja in Nigeria and Accra, Ghana. A profile of our firm can be viewed here. You can also visit our website at www.aelex.com to learn more about our firm and its services.'

DISCLAIMER: This publication is not intended to provide legal advice but to provide information on the matter covered in the publication. No reader should act on the matters covered in this publication without first seeking specific legal advice.
Contact us at:

4th Floor, Marble House,
1 Kingsway Road, Falomo Ikoyi,
Lagos, Nigeria

Telephone: (+234-1) 4617321-3, 2793367-8, 7406533,

If you need additional information, please contact fintech@aelex.com.

Click here www.aelex.com
to follow our social media handles click below

@aelexpartners