The Commonwealth

Commonwealth Cybercrime Journal \ 111
ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cybercrime-journal

Data Security Concerns Raised by 'Bring Your Own Device' in Corporate Organisations' Hybrid and Remote Work Environments in Nigeria

Rotimi Ogunyemi[1] and Akintunde Idowu[2]

Abstract

The perceived benefits of increased productivity, employee efficiency and work flexibility have given rise to the phenomenon known as 'bring your own device' (BYOD), which permits employees of an organisation to complete their tasks or processes on their own personal devices. The COVID-19 pandemic accelerated this trend, particularly as the shift to hybrid and remote work intensified. Major organisations have pushed for the adjustment of their personnel, procedures and cultures to the new reality. The fact that employees can access organisational data from their own devices at any time and from any location increases the likelihood of unauthorised access to corporate data. Finding secure technologies for conducting confidential meetings in a remote workspace and managing confidential data outside of a remote location has been difficult. The vulnerabilities include, among others, phishing email attacks, unauthorised access through insecure remote-access tools and hacking of video conference tools. As remote work tools must be protected, periodic risk assessments and routine monitoring are required to safeguard the privacy and integrity of an organisation's information assets and resources. This paper seeks to investigate the role of cybersecurity in general; data privacy and security challenges posed by BYOD using Nigeria as a case study; cybersecurity policy recommendations for remote and hybrid work; and the implementation of a secure BYOD structure.

1 Technology Lawyer; Managing Partner, Johnson & Wilner LLP, Nigeria (Formerly Bayo Ogunyemi & Co.); President, Spindlar Cyberlaw Centre (Lagos, Nigeria). linkedin.com/in/rotimiogunyemi

2 Intellectual Property and Information Technology Lawyer, Johnson & Wilner LLP, Nigeria. linkedin.com/in/akintundeidowu

Introduction

According to available data, 83 per cent of companies allow employees to use their own devices, such as laptops, tablets and smartphones, for business purposes.[3] The results of a recent survey indicate that 95 per cent of employers have adopted 'bring your own device' (BYOD) due to technological advancements and the perceived costs of providing their workforce with secured devices, and that 57 per cent of employees prefer the convenience of keeping track of personal and work-related items on a single device.[4] It is, therefore, no surprise that the global BYOD market size is expected to grow by US$69.07 billion from 2021 to 2026.[5]

Bring your own device or BYOD is a policy in which employees use personally selected and purchased devices to perform work for their employer via remote intranet access.[6] This includes the use of mobile devices such as smartphones, tablets, laptops and personal computers. The goal of a BYOD scheme is to enable the employee to be more productive and efficient by selecting a device that best suits his or her preferences and work purposes, while ensuring data integrity and protecting the organisation's data from leakage and loss.[7]

According to joint research, approximately 88 per cent of all data breaches are due to employee error.[8] For example, it was reported that the personal information of about 30,000 customers of the South Korean cryptocurrency exchange Bithumb was recently exposed when a Bithumb employee's home computer was hacked.[9] A 2020 report[10] indicates that 62 per cent of businesses experienced **phishing and social engineering** attacks[11] and 91 per cent of this type of cybercrime is said to begin with malicious email

3 Zippia (2022), '26 surprising BYOD statistics [2022]: BYOD trends in the workplace', Zippia.com, 17 October, available at: https://www.zippia.com/advice/byod-statistics/ (accessed 2 November 2022).

4 Samsung (no date), 'Maximizing Mobile Value', White Paper, Samsung Business, available at: www.samsung.com/us/business/short-form/maximizing-mobile-value-2022/ accessed 11 September 2022. p.2. The survey was conducted between 2021 and 2022 with 500 executives and 1,000 employees in the United States.

5 Technavio (2022), 'Bring your own Device (BYOD) Market by End-user and Geography – Forecast and Analysis 2022–2026', Technavio.com. September, available at: https://www.technavio.com/talk-to-us?report=IRTNTR74271&type=sample&rfs=epd&src=report&utm_source=prnewswire&utm_medium=pressrelease+&utm_campaign=t42dtcs_rfs1_wk41_2022_007&utm_content=IRTNTR74271 accessed 2 November 2022.

6 Cavoukian, A (2013) 'BYOD: (Bring Your Own Device) Is Your Organization Ready?' Information and Privacy Commissioner Ontario, Canada, retrieved from https://silo.tips/download/byod-bring-your-own-device-is-your-organization-ready accessed 2 November 2022.

7 Ibid.

8 Tessian (no date), 'Understand the mistakes that compromise your company's security', available at: https://www.tessian.com/research/the-psychology-of-human-error/

9 Yonhap News Agency (2017), 'S. Korea probes cyberattack on digital currency exchange', 3 July, available at: https://en.yna.co.kr/view/AEN20170703010400320 accessed 1 November 2022.

10 T-Mobile for Business (2020) *The T-Mobile for Business 2020 Workplace Mobility Report*, available at: https://www.t-mobile.com/content/dam/tfb/pdf/T-Mobile-for-Business-2020-Workplace-Mobility-Report.pdf?icid=TFB_TMO_P_TFBFTRWRKS_7LCBNVDVYBXY27WF321599 accessed 1 November 2022.

11 See discussion of these terms on page 5.

links. Thus, although BYOD devices create business transformation, the phenomenon is at the heart of data breaches, cybercrime and network attacks and poses arguably the largest risk to enterprise security.

Given that data security is essential to information privacy, this poses a significant threat. Indeed, security is a prerequisite for privacy.[12] There should be no gaps in protection or accountability for secure storage or transmission, regardless of whether the information is stored on a mobile device, in a database or in the cloud. As organisations' operations have become more data-intensive, network-dependent and accessible than ever before, ensuring full lifecycle protection has become a formidable obstacle.[13] The proliferation of mobile devices such as laptops, smartphones, tablets, USB drives and portable storage media, as well as the increasing use of personal mobile devices for business purposes, necessitates a fundamental revaluation of how to best protect end-to-end the sensitive data of the modern enterprise.[14]

As information processing technologies, business practices and networked architectures become increasingly complex and critical for organisational operations, it is more important than ever to anticipate security risks as early as possible and to mitigate those risks by defaulting to strong policy, and technical, administrative and physical security practices. Several intersecting growth trends are pressuring companies to let employees use their own devices and connect them to corporate networks and systems. Consumer adoption of new mobile device brands, the rapid evolution of device capabilities, as well as of cloud and virtualisation technologies, the explosive growth of mobile applications, and a growing tech-savvy population adept at using mobile technologies are a few of these factors.[15] Although working on a mobile device offers many benefits to employees and employers, this blurring of personal and business use of BYODs raises many data security and cybersecurity concerns that, if not properly addressed, may result in data breaches, turning the many BYOD benefits into losses for organisations.[16]

Prior literature reviews suggest that data security issues in BYOD are under-researched, as they are relatively young compared to other data security issues. This paper draws the attention of corporate organisations to implications they should be aware of in order to increase safeguards against threats targeting BYOD initiatives. It also focuses on the legal implications of BYOD schemes on real-life business issues and as well as how the judiciary approaches the determination of BYOD cases in corporate organisations. This paper seeks to answer questions such as:

- What are the data security issues associated with the processing of employees' personal data on BYODs for work-related purposes?

12 Cavoukian, 'BYOD: (Bring Your Own Device) Is Your Organization Ready?' [2] (n 1).
13 Ibid.
14 Ibid.
15 Ibid, p.3.
16 Ibid.

- What is the judiciary's approach to determining BYOD cases in corporate organisations?
- What are the legal measures, including policies and strategies, for implementing BYOD schemes?

This paper will seek to produce an assessment of BYOD issues that can also serve as a template for organisations. It will begin with a conceptual analysis of the BYOD schemes by describing the relevant law and carrying out an analysis of previous literature. It will also examine the data security issues pertaining to the processing of employees' personal data for work-related purposes. Furthermore, it will attempt to provide an analysis of the judiciary's approach to determining BYOD cases in corporate organisations by comparing case laws in the United Kingdom (UK), the United States (US), Canada and Europe with Nigeria, outlining the challenges this approach presents and demonstrating inconsistencies in Nigerian jurisprudence. Just like Nigeria, the UK and the US are generally considered common law countries (while Canada and Europe have a mix of both common law and civil law systems) and therefore provide a suitable basis for comparison.

Conceptual analysis of BYOD schemes

The terms BYOD, CYOD, COPE, and COBO are encountered by anyone researching enterprise mobility (plus a few more). BYOD stands for 'bring your own device', CYOD for 'choose your own device', COPE for 'company owned/personally enabled', and COBO for 'company owned/business only'. There is little agreement on their meaning, but they are all similar concepts.[17] BYOD and CYOD involve smartphone-based integration and access, while COPE and COBO involve company-owned and -controlled devices.[18] The *Wired* blog[19] provides a helpful summary of the three factors that determine a device's category.

1. Who chooses the device, who pays for the device and the cellular connectivity service?
2. Who is responsible for managing and providing support for the device?
3. How crucial is the device's integration with daily workflow?

As will be discovered later in this article, the answers to these questions are useful for determining the numerous questions of liability for security and privacy risks associated with the use of BYOD devices for enterprise applications. Yet the issue of ownership may not be straightforward, especially when the employer contributes to the device's cost and/or compensates the employee for its use. Therefore, businesses must safeguard their data to reduce their liability exposure. Employers should consider the responses to

17 Wired (2018), 'BYOD, CYOD, COPE, COBO — What Do They Really Mean?', available at: https://www.wired.com/brandlab/2018/06/byod-cyod-cope-cobo-really-mean/ (accessed 2 November 2022).
18 Ibid.
19 Ibid.

the three factors when drafting policies that serve as a reminder to employees that all company data belongs to the employer, while the issue of device and content ownership must be made explicit.

Data security risks associated with BYOD in remote and hybrid work

Bring your own device is a trend with both risks and benefits. While the benefits may include potential cost savings as employees invest in their own devices, a solution to the 'two pocket problem' that allows employees to carry one device instead of two (one for work and one for personal use), an increase in employee engagement and productivity because employees use devices they desire and are familiar with, and enhanced recruitment strategies by attracting candidates with technological expertise, the risks for employers appears to far outweigh the benefits. Of many types of attacks affecting BYOD devices, the notable risks include: data loss due to device loss, phishing, spyware attacks and malware attacks, network attacks, and Zoom bombing.[20]

1. Data loss due to device loss

Smart devices contain large amounts of data covering different services such as emails, contacts, social media, credit card information, etc. When an employee connects his/her personal devices to a corporate network, he/she makes it easier for hackers to access employee information, company data and the corporate directory. If this device is stolen, it leaves the owner vulnerable and gives room for the exploitation of corporate networks and data. Once inside, a hacker can hide in the corporate network, steal desired information and monitor network activity, particularly outbound traffic. This eventually leads to the organisation suffering data loss or data breach.

2. Phishing, spyware attacks and malware attacks

Phishing is a form of social engineering commonly used to steal user data, including login credentials and credit card information. It occurs when an attacker impersonates a trusted entity in order to deceive a victim into opening an email, instant message or text message. Phishing can have devastating consequences for employees if an attacker gains access to a company network as part of a larger attack and this may result in the attacker making unauthorised purchases, stealing funds and employee identity. In this scenario, employees are compromised as an attacker circumvents security perimeters, spreads malware within a closed environment or gains privileged access to secured data. This typically results in financial losses, and declines in market share, reputation and consumer trust in businesses.[21] Similar to phishing attacks are 'spoofing' attacks.

20 Rai, S, P Chukwuma and R Cozart (2016), *Security and Auditing of Smart Devices: Managing Proliferation of Confidential Data on Corporate and BYOD Devices,* Auerbach Publications, pp. 54–55.

21 Imperva (no date), 'Phishing attacks', available at: www.imperva.com/learn/application-security/phishing-attack-scam/ (accessed 4 November 2022).

Spyware, by comparison, allows an intruder to covertly obtain information from a user's computer. It can be acquired through a phishing attack. Once the user clicks on the link in the phishing attack, the spyware is installed and it monitors smart device usage, keystrokes, and is able to copy contact information or financial information. Where the smart device is connected to a corporate network, the spyware will collect all the necessary information that a hacker needs to break into the corporate network. When a single individual or corporation is targeted, the spyware attack becomes a surveillance attack. The surveillance attack may or may not be for criminal intentions. Some of these applications installed by employees contain trojan viruses, which are rogue applications that can be used to introduce advance persistent threats (APTs).

3. Network attacks

Network attacks generate additional traffic and bandwidth consumption, which can impede network performance. They include distributed denial of service (DoS), man in the middle attacks, network sniffing and ransomware. 'Ransomware' refers to software that can be maliciously installed on a computer or a network, and which is designed to block access to critical data, such as by encrypting files, until a ransom is paid. A recent report found that 71 per cent of Nigerian organisations were hit by ransomware in 2021, a higher number when compared to the previous year.[22] Another 2022 report reveals that 49 per cent of organisations that had their data encrypted paid ransoms to get their data back.[23]

4. Zoom bombing

Zoom bombing is a challenge that became prominent during the COVID-19 pandemic and has since naturalised in remote meetings. The increased use of Zoom and other videoconferencing platforms has given prominence to efforts of malicious users to sabotage classrooms and discussions in attacks that have been termed 'Zoom bombing'.[24] Some have defined this as 'gate-crashing tactics during public video conference calls' that often result in flooding the calls with disturbing images. A report by VMware Carbon Black, based on a survey of 1,002 respondents conducted in March and April 2020, estimated that 91 per cent of executives believed that cyberattacks on

22 Guardian Nigeria (2022), 'Ransomware hits 71% of Nigerian Organisations', 4 May, available at: https://guardian.ng/technology/ransomware-hits-71-of-nigerian-organisations/ (accessed 4 November 2022).

23 Sophos, 'State of Ransomware in Retail 2022 report', retrieved from https://www.sophos.com/en-us/whitepaper/state-of-ransomware-in-retail accessed 4 November 2023.

24 Oxford University News Science Blog, 'FBI follows Oxford academics' guide to beat Zoom bombers' (24 April 2020) https://www.ox.ac.uk/news/science-blog/fbi-follows-oxford-academics-guide-beat-zoom-bombers accessed 24 February 2023.

their organisation increased because of remote working during the pandemic.[25] Some 85 per cent believed that their own organisation was not adequately prepared to deal with a sudden shift to working from home.[26]

Existing statutory laws and security obligations applicable to BYOD in Nigeria

In Nigeria, the laws and policies affecting bring your own device (BYOD) are mainly governed by the Nigerian Data Protection Regulation, Nigerian Cybercrime Act, Electronic Transactions Act, and the Freedom of Information Act. These Acts set out the framework for the regulation of the information and communications technology sector in Nigeria, and include provisions related to privacy, security and the protection of personal data that have a bearing on the use of personal devices for work purposes.

1. Nigerian Data Protection Regulation (NDPR)

To ensure the protection of personal data, data controllers and processors have specific security obligations, including both technical and organisational measures that increase the level of information technology (IT) security directly or indirectly. These obligations can be grouped into seven main areas of data protection: (i) data minimisation and storage limitation; (ii) data confidentiality; (iii) risk assessment and security measures; (iv) data protection by design and by default; (v) regular assessment of the effectiveness of the security measures taken; (vi) notifications, reporting obligations and mitigation measures (data breaches); and (vii) business continuity, disaster recovery and resilience.

On data minimisation and data storage limitation, the Nigerian Data Protection Regulation (NDPR) requires data controllers to ensure that a limited amount of data is obtained and processed as strictly necessary[27] ('data minimisation'); and that no data may be collected unless the employee is informed of the purpose. Furthermore, employee data should not be retained for longer than necessary[28] ('data storage limitation'). A strategy based on data minimisation and storage limitation can help mitigate the effects of data breaches caused by cyberattacks or incidents, from the perspective of cybersecurity.[29]

25 The Daily Swig (2020), 'Remote working during coronavirus pandemic leads to rise in cyberattacks, say security professionals, 14 July; VMware (2020) *Carbon Black Global Threat Report June 2020 – Extended Enterprise under Threat*, available at: https://www.carbonblack.com/resources/global-threat-reportextended-enterprise-under-attack-index/

26 Ibid

27 Section 2.1 (b) NDPR 2019.

28 Section 2.1(1) (c) NDPR 2019; see also Section 38 of the Cybercrime Act, which stipulates that service providers must retain traffic data and subscriber information for at least two years. In addition, Section 5 of the Credit Reporting Act of 2017 mandates that a credit bureau should keep credit information for at least six years from the date it was obtained, after which it must be archived for an additional ten years before being destroyed.

29 See also Mantelero, A and G Vaciago (2017), 'Legal Aspects of Information Science, Data Science and Big Data', in M Dehmer and F Emmert-Streib (Eds.), *Frontiers in Data Science,* CRC Press.

The regulation requires controllers and processors to perform a Data Protection Impact Assessment (DPIA)[30] and a Data Protection Audit[31] to identify and mitigate against any data protection-related risks arising from employees' performance of work projects on their BYODs ('risk assessment'). This goes beyond data security and takes a more holistic risk-based approach, focusing on the impact of data use on the rights and freedoms of employees and customers. If the DPIA reveals that the processing poses a high risk that cannot be mitigated by the controller, the National Information Technology Development Agency (NITDA) must be consulted. Thus, organisations are required to assess the impact of the proposed processing on employees, considering its necessity and proportionality, and to identify the risks posed by data processing to personal rights and liberties. Based on this assessment, organisations must then take appropriate measures to mitigate these risks. While the NDPR is silent on the content of the DPIA, the European Union (EU) Article 29 Working Party recommends that all DPIAs be reassessed every three years, or sooner if circumstances change rapidly.[32]

The NDPR contains provisions that mandate employers (as controllers and processors) to implement technical and organisational safeguards to ensure the confidentiality, integrity, and availability of employee data (that is, security measures).[33] The deployment of comprehensive organisational policies and processes – ranging from the configuration of devices in accordance with mobile device policies to the training of employees on procedures for handling incidents such as data breaches, and the adoption of technical measures such as encryption, setting up mobile and cloud firewalls, whitelisting of IP (internet protocol) addresses,[34] installation of intrusion detection systems, anti-virus protections, and malware detection systems – will all aid in the protection of sensitive data on BYODs during remote and hybrid work.

To protect personal data and prevent data breaches caused by the use of BYOD devices, employers should integrate data privacy features and data protection technologies directly into their business practices. These necessary safeguards must be applied to

30 Section 3.2 (viii) NDPR Implementation Framework.

31 Section 3.2 (i) NDPR Implementation Framework.

32 Data Protection Commission (DPC) Ireland (2022b), 'Data Protection Impact Assessments', *@dpcireland,* available at: https://www.dataprotection.ie/organisations/know-your-obligations/data-protection-impact-assessments

33 Section 2.6 NDPR 2019.

34 IP whitelisting is a security measure used to restrict access to a computer system or network based on a list of trusted IP addresses. This means that only computers or devices with an approved IP address can access the system, while all other IP addresses are denied access. For example, a company might use IP whitelisting to ensure that only employees on their corporate network can access their internal systems or to allow access only to trusted vendors or partners.

the processing, and any pre-existing configuration value must be adjusted in accordance with the principles of data minimisation and purpose limitation (that is, data protection by design and by default).[35]

2. Nigerian Cybercrime Act

The provisions of the Nigerian Cybercrime Act are relevant to bring your own device (BYOD) policies and practices. The Cybercrimes (Prohibition and Prevention) Act 2015, has a significant impact on cyber law in Nigeria. The Act creates a comprehensive legal, regulatory and institutional framework in Nigeria to prohibit, prevent, detect, prosecute and punish cybercrime.

The Act criminalises unauthorised access to computer systems, including personal devices used for work purposes as part of a BYOD policy.[36] Section 9 of the Act makes it a criminal offence to intercept communications transmitted over a computer system or BYOD devices.[37] Where, however, such interception of electronic communication is carried out pursuant to the order of a judge, because there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of criminal investigation, then such interception is decriminalised.[38] The Nigerian Cybercrime Act further requires that companies report any cybercrime incidents to the Computer Emergency Response Team (CERT) co-ordination, so that it can take necessary measures to tackle the issue.[39] Section 31 of the Act criminalises non-submission of access rights or codes to the employer after disengagement without any lawful reason. A relevant question, in this case, is whether the personal devices of employees used for work purposes fall under the access rights of employers, since they may contain corporate data. It remains to be seen how BYOD issues of this kind will be dealt with in litigation, but employers may put in place clear and comprehensive policies and procedures, providing employees with training and guidance on the use of personal devices for work purposes, and using mobile device management (MDM) software to help secure and manage the devices and data associated with BYOD.

3. Electronic Transactions Act

Section 2 of the Act defines an electronic transaction as any transaction that is created, recorded, processed, stored, retrieved or transmitted by electronic means.[40] This definition includes transactions conducted on personal devices used for work purposes as part of a BYOD policy. Electronic records on BYOD devices are admissible in evidence

35 Data Protection Commission (DPC) Ireland (2022a), 'Data protection by Design and by Default', *@dpcireland*, available at: https://www.dataprotection.ie/organisations/know-your-obligations/data-protection-design-and-default
36 Section 6 Nigerian Cybercrime Act (NCA).
37 Section 9 NCA.
38 Section 39 NCA.
39 Section 21 NCA.
40 Section 2 Nigerian Electronic Transactions Act (NETA).

in court proceedings, provided that the records are shown to be reliable and trustworthy.[41] Such records are necessarily meant to be made available to the parties who are entitled to access them. Under this Act, electronic signature shall be considered to be as valid as a handwritten signature, provided that the signature is reliable and trustworthy.[42]

The Act, notwithstanding, provides that electronic records be retained for the minimum period necessary, taking into account the type of record, the purpose for which it was generated and the legislation that requires its retention.[43] This includes records stored on personal devices used for work purposes as part of a BYOD policy. Therefore, employers are obliged under this Act to only retain information on personal devices as necessary and in accordance with the law. Under the Nigerian Cybercrime Act, such retention of traffic data shall be for a period of two years.[44]

4. Freedom of Information Act

The provisions of the Freedom of Information Act (FOIA) in Nigeria are relevant to bring your own device (BYOD) policies and practices. The Freedom of Information Act gives everyone the right of access to information, whether in written or electronic form, held by public institutions or officers. The person requesting the information does not need to show any specific interest in the information or justify his/her reasons for making the request.[45] Section 3 of the Act provides for the procedures for making a request for information. However, this request may be rejected on certain grounds, such as international affairs and defence,[46] law enforcement and Investigation,[47] personal Information,[48] trade or commercial secrets,[49] professional circumstances,[50] and for protection of course or research materials.[51] Notwithstanding, an applicant may apply to the court for judicial review within 30 days of rejection of such application.

Public institution employers in Nigeria should be aware of these provisions and should take steps to ensure that they are in compliance with the FOIA when implementing a BYOD policy. This may include putting in place clear and comprehensive policies and procedures, providing employees with training and guidance on the use of personal devices for work purposes, and using mobile device management (MDM) software to help secure and manage the devices and data associated with BYOD. Additionally, employers

41 Section 7 NETA.
42 Section 11 NETA; Section 17 of the Nigerian Cybercrime Act (NCA).
43 Section 10 NETA.
44 Section 38(1) NCA.
45 Sections 1 and 2 Freedom of Information Act (FOIA).
46 Section 11 FOIA.
47 Section 12 FOIA.
48 Section 14 FOIA.
49 Section 15 FOIA.
50 Section 16 FOIA.
51 Section 17 FOIA.

should be mindful of the provisions of the FOIA when responding to requests for information and should be prepared to provide access to information in accordance with the provisions of the Act.

Data security issues associated with BYOD in remote and hybrid work

The Nigerian Data Protection Regulation (NDPR)[52] regulates the processing of personal data. All obligations under the NDPR fall on the 'data controller' – typically the employer – who determines the purpose and way data is processed. 'Processing' involves obtaining, storing and utilising data, as well as modifying or erasing it. Employers should not assume that they are the data controller of all information on an employee's personal device merely because the device is used for business purposes. Such an assumption could lead to the employer processing (including erasing) the employee's personal information (as well as the information of the employee's friends and family). Depending on the circumstances, this could constitute a violation of the NDPR and would technically necessitate an assessment of the identity of the data controller in relation to each class of personal data on the device prior to accessing, processing or deleting the data.

In the workplace, BYOD devices will primarily contain two types of data: company data and employee personal data.[53] Company data consist of any sensitive, confidential information about the organisation or its clients. Employers must ensure that employee privacy is protected, so it is essential that company data and employee personal data remain separate and that employers do not have access to employee personal data. Several issues have been identified and analysed against the legal position.

1. Can the employer access personal emails and text messages (SMS), the browsing history, and other data on a personal smartphone or tablet used for work?

Employees may be reluctant to hand over their own devices and allow their employer to review their content, especially if the employer requires access to the device to conduct an investigation into an allegation of misconduct.

As a condition of their participation in the BYOD scheme, employers should consider requiring employees to submit their device and password for periodic inspection. If the employee refuses to co-operate, the employer may discipline (and possibly terminate)

52 The Nigerian Data Protection Regulation (NDPR) 2019, is the main data protection regulation in Nigeria. Some other laws and regulations that contain provisions on data protection: the 1999 Constitution (as amended); the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 ('the Cybercrimes Act'); the National Identity Management Commission Act 2007 ('the NIMC Act'); the NDPR; the National Cybersecurity Policy and Strategy 2021; the Draft Data Protection Bill 2020 (which is currently going through the legislative process); the Consumer Protection Framework 2016; the Framework and Guidelines for Public Internet Access 2019; Guidelines for the Provision of Internet Service; and the Nigeria Data Protection Regulation 2019: Implementation Framework 2020.

53 GVZH, 'Data Protection Implications of a Bring Your Own Device Policy', 18 Oct. 2019, https://gvzh.mt/insights/data-protection-implications-bring-your-own-device-policy/ accessed 1 November 2022.

him or her for failing to comply with a reasonable management directive. Whether or not a dismissal under these conditions would be just depends on the facts. If an employer uses an employee's username and password without the proper authorisation to access their personal device, it is extremely unlikely that the employer will process the employee's personal data 'fairly and lawfully', as required by the NDPR.[54] In addition, this would be a violation of the Cybercrimes (Prohibition and Prevention) Act 2015. This is because under the Cybercrimes Act, it is a crime to gain unauthorised access to any computer or its data.[55] A 'computer system' is defined in the Cybercrimes Act as any device or group of interconnected or related devices that process data automatically or interactively.[56] It includes computers, mobile phones and other data-processing devices. The hardware and software device may include input, output and storage components that stand alone or connect to a network or other devices, including computer data storage media. Therefore, if an employer gains unauthorised access to a bring your own device (BYOD), the employer may be subject to a fine.

2. Can employees be compelled to let the company inspect their device when they leave the company, to ensure that all confidential information has been deleted?

Employers may wish to wipe an employee's device upon employment termination or if it is lost or stolen. If the employee's personal data and company data are not separated on the device – for example, by a sandbox – all data on the device will be deleted. If the employee has not recently backed up their personal data, the wipe could result in the employee losing significant, potentially irreplaceable data. Employers should ideally consider using software that separates company data and personal data on the device, as well as requiring employees to consent to the deletion of all data on the device as a condition of their participation in the BYOD programme by including a section on remote wipes.[57] This will serve as a waiver.

The BYOD policy should state that employees may use their own devices to access work data, but that if those devices are stolen or lost, the employer has the authority to remotely wipe them. Any deletion should be limited to company data whenever possible, but policies should seek to exclude liability if an employee's data are lost. The employees

54 See Section 5(1)(a) of the NDPR, which states that personal data must be collected and processed in accordance with the data subject's consent to a specific, legitimate and lawful purpose. Note that these fairness, specificity, legitimacy and lawfulness requirements are in addition to any other procedures outlined in the regulation or any other instrument.

55 See Section 6 of the Cybercrimes (Prohibition and Prevention) Act 2015. See also Sections 12, 13, 14 and 16 of the same Act.

56 See Section 58 of the Cybercrime Act, 2015

57 On this approach, there are two schools of thought, the first being that every company has the ability to restrict access for employees who bring their own device and, therefore, must sign a written remote work policy. The alternative approach is for a remote work policy to outline what the company expects of remote workers and what the workers can expect from the company.

should be made aware of any onerous requirements of the BYOD policy, such as wiping the device. This may aid in managing employee expectations and reduce the risk of withdrawal of consent.

3. To what extent can the employer monitor and control the smartphone, laptop or tablet?

Remote employees may keep irregular hours and use their devices for both personal and professional purposes, making it nearly impossible for employers to distinguish between monitoring work and private time. Many employers deploy software tools on employee devices to monitor employee activities, such as hidden cameras, data loss protection (DLP) tools, and mobile device monitoring (MDM) tools, to combat this challenge. This software logs keystrokes and tracks mouse movements, which frequently constitutes a violation of employees' right to privacy and the NDPR. A PressReader blog[58] cites a similar case of employee monitoring in which the chief executive officer (CEO) of a furniture store installed four cameras in the store's headquarters to monitor employees without their knowledge and viewed the store's activities via an app while he was in London. This raises questions regarding consent and legitimate interest.

The NDPR[59] recognises consent as a legal basis for processing personal data and includes information on how consent must be obtained and how it can be withdrawn. The NDPR does not recognise a data controller's legitimate interests as legal grounds for processing.[60] Prior to collecting personal data from a data subject, the controller must provide the data subject with information regarding the legitimate interest pursued by the controller or a third party. In addition, the right to erasure and the right to restrict processing apply when there are no overriding legitimate grounds for the processing. In the scenario described in the PressReader blog, this means that the CEO unlawfully processed employee data.

Recent events have demonstrated that excessive employee monitoring and a failure to respect employee privacy are violations of data protection laws. For example, following a recent investigation, the Information and Data Protection Commissioner in Malta fined HSBC 5,000 euros (€) for monitoring an employee's bank.[61] In addition, a Dutch court ordered a Florida-based software development company to pay a former remote employee €75,000 for wrongful termination after he refused to leave the webcam on while he worked. According to the court, the employee's right to privacy was violated

58 Pressreader, 'Nigerian employers and employee monitoring', 14 June 2021, www.pressreader.com/nigeria/business-a-m/20210614/282029035175985 accessed 1 November 2022.

59 Section 6 of the Nigerian Data Protection Regulation 2019. In Nigeria, data protection is a constitutional right founded on Section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended).

60 Section 6 of the Nigerian Data Protection Regulation 2019.

61 Times of Malta (2019), 'HSBC fined €5,000 for monitoring employee's bank account', 15 August, available at: https://timesofmalta.com/articles/view/hsbc-fined-5000-for-monitoring-employees-bank-account.728921 (accessed 4 November 2022).

by the instruction to leave the camera on.[62] As a solution, employers could consider requiring employees' consent to monitoring or surveillance activity as a prerequisite for participation in the BYOD programme, with them terminating an employee's network access if consent is withdrawn. However, this will not necessarily comply with the NDPR, as the employee's consent may not have been freely given and is easily revocable.

While there are no specific provisions for the enforcement of workplace privacy in Nigeria, the right is protected by constitutional and statutory provisions. The Constitution of the Federal Republic of Nigeria 1999 (as amended) is a fundamental right that prohibits unreasonable searches and seizures of employees' electronic devices, homes, correspondence, telephone conversations and telegraphic communications. Although the National Industrial Court is also authorised to apply international treaties and covenants, such as International Covenant on Civil and Political Rights, which guarantees the right to privacy, and to consider foreign judgments, it leans toward protecting the human rights of employees in the workplace. The tort of breach of confidentiality and misuse of information are common law remedies to a grievance that an employee may have against his or her employer for the improper use or misuse of his or her personal information.

An employee's right to privacy in the workplace is guaranteed, albeit with limitations. Employers are permitted by law to monitor their employees' internet usage, but they are also required to inform their employees of the monitoring and to not misuse the information obtained. A policy in this regard has therefore proved to be essential, as has its dissemination to the employee.

Analysis of the judiciary's approach to determining cases of BYOD in corporate organisation: a comparative analysis of the BYOD cases in the UK, the US, Canada and Europe with Nigeria

The judiciary's approach to determining cases related to bring your own device (BYOD) varies, depending on the specific legal issues involved and the jurisdiction in which the case is heard. In general, the judiciary tends to approach BYOD cases with a focus on balancing the rights and interests of employees, employers and other stakeholders. The legal system, however, has been slow to address the problems brought on by BYOD policies.[63] In Nigeria, there exists a lack of statutes and case laws addressing BYOD policies. This paper's authors, therefore, aim to draw on the steadily evolving case law in the US, UK, Canada and Europe to illustrate some of the legal issues related to BYOD in corporate organisations. These jurisdictions have growing importance for BYOD-related legal issues in the modern business landscape and the comparative analysis of their approaches can provide valuable insights into best practices and innovative solutions.

62 NL Times (2022), 'Dutch employee fired by U.S. firm for shutting off webcam awarded €75,000 in court', available at: https://nltimes.nl/2022/10/09/dutch-employee-fired-us-firm-shutting-webcam-awarded-eu75000-court

63 Blair, L (2018), 'Contextualizing bring your own device policies', *Journal of Corporation Law*, Vol. 44, 153.

The authors' goal is to understand how local laws and regulations are adapting to these developments and to illustrate the different approaches taken by these legal systems to address the BYOD challenges.

One of the most complex and noticeable issues arising with BYOD policies is when a business is facing litigation (Ibid), especially around e-discovery issues. E-discovery issues can arise in legal proceedings involving bring your own device (BYOD) as personal devices may contain electronically stored information that is relevant to a legal case. In such cases, the process of identifying, collecting and producing relevant electronic information can become complex, costly and present various legal challenges. Such challenges could include: determining what electronic information on personal devices is relevant to the legal proceedings and preserving that information to prevent destruction or alteration of evidence; balancing the right to privacy with the right to discover relevant evidence; collecting and producing electronic information when stored on personal devices that are owned and controlled by employees; and the significant cost of collecting, preserving and producing electronically stored information in BYOD cases where many personal devices are involved. A few cases have been decided across various jurisdictions, laying down some principles on how e-discovery issues in BYOD are handled.

In the case of *Zubulake v UBS Warburg LLC,*[64] the court held that a party was required to preserve electronic information stored on personal devices if it was relevant to the legal proceedings. This case established the standard for reasonable and proportionate discovery of electronic information in the context of civil litigation in the United States. In *O'Grady v Superior Court,*[65] which involved the production of electronic information stored on personal devices in the context of a criminal trial, the court established the principle that personal devices may contain information that is relevant to legal proceedings and may need to be produced as part of the discovery process. In *Jivraj v Hashwani,*[66] the court dealt with the issue of whether a party was required to disclose electronic information stored on personal devices if it was relevant to the legal proceedings. The court held that the party was required to produce the information, but emphasised the importance of balancing the right to privacy with the right to discovery. There was also the case of the warrant to search a certain Apple iPhone cellular telephone,[67] which dealt with the issue of whether the US Government could force Apple to unlock a suspect's personal iPhone in a criminal investigation. The court held that the government's request was reasonable and that Apple was required to assist in the unlocking of the phone.

From the above cases, the courts in various jurisdictions appear to prioritise the importance of the preservation and production of electronically stored information (ESI) on personal devices in legal proceedings. However, the case of *Jivraj v Hashwani* highlights

64 *Zubulake v UBS Warburg LLC*, 217 FRD 309 (SDNY 2003).
65 *O'Grady v Superior Court*, 139 Cal.App.4th 1423, 44 Cal. Rptr. 3d 72 (Cal. Ct. App. 2006).
66 [2010] EWCA Civ 712, [2010] 2 Lloyd's Rep 534, [2010] IRLR 797, [2010] ICR 1435.
67 In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, 17-mj-02814 (CD Cal. 2016).

the importance of balancing the right to privacy with the right to discovery. There have not been many specific case laws in Nigeria that address BYOD specifically, but the Federal High Court has jurisdiction to hear cases involving e-discovery and the production of electronic information in the context of civil litigation. While Nigerian law Section 7 of the Electronic Transactions Act provides for the admissibility of electronic evidence in court, copies of ESI have been tendered as evidence in court without any clear protocol for their authentication or admissibility. This was the case in *FRN v Femi Fani Kayode,*[68] where the court rejected a computer print-out in a banker's book as inadmissible. The court opined that this was secondary evidence that was not authenticated and thus inadmissible under the Evidence Act. Thus, it is important for organisations to be aware of the e-discovery rules in Nigeria and to have processes in place to preserve and produce ESI in the event of a legal proceeding. This can include having policies and procedures for the preservation of ESI and the management of electronically stored information, as well as having technology and resources in place to assist with the production of ESI in a legal context.

Lindsey Blair identifies two primary concerns of BYOD policies on e-discovery as accessibility and control.[69] The concept of 'control' refers to the extent to which an organisation can manage and regulate the use of personal devices for work purposes. This includes the ability to access, monitor and secure the data stored on personal devices, as well as the ability to enforce compliance with company policies and regulations (Sophos 2021). A party's duty to deliver to its opponent discoverable information is limited to that information that is within its custody and control.[70] The two relevant questions then are whether an employer is in 'control', since BYOD is not within the immediate control/possession of the employer, and whether an employer's monitoring and management of personal devices used for work purposes is reasonable and in accordance with relevant laws and regulations. Courts have addressed this matter in various ways. For instance, in the case of *Bărbulescu v Romania,*[71] the European Court of Human Rights (ECHR), in determining the balance between employees' and employers' rights, held that an employer's monitoring of an employee's personal communications, even if the monitoring was carried out in accordance with company policy, was a violation of the employee's right to privacy. This decision was similar to that in *R v Cole* (Canada),[72] a case that dealt with the issue of whether the search of an employee's personal laptop by his employer, without a warrant, was reasonable. The court held that the search was unreasonable and violated the employee's privacy rights. Furthermore, in *Ontario (Public Safety and Security) v Criminal Lawyers' Association (Canada),*[73] the court dealt with the

68 (2019) LPELR-46796(CA).
69 Blair, L (2018), 'Contextualizing bring your own device policies', *Journal of Corporation Law*, Vol. 44, 153.
70 *Jirak v Abbott Labs., Inc.*, 712 F.3d 351, 360 (7th Cir. 2013).
71 *Barbulescu v Romania* (61496/08) [2016] I.R.L.R. 235.
72 *R v Cole*, 2012 SCC 53 (CanLII), [2012] 3 SCR 34.
73 *Ontario (Public Safety and Security) v Criminal Lawyers' Association*, 2010 SCC 23 (CanLII), [2010] 1 SCR 815.

issue of whether an employer's policy of searching personal devices of employees, including those brought from home, was reasonable. Here, the court held that the policy was overbroad and unjustified, and violated the employees' privacy rights.

However, there are cases where the court has held that an employee cannot reasonably expect privacy where specific communications on personal devices are work related. In *Garamukanwa v UK,*[74] the European Court of Human Rights ruled that it was not a breach of the right to privacy when an employer used, during a disciplinary hearing, material found by the police in the employee's notebook and phone, and emails sent to another individual's account. The UK employment tribunal reasoned that since the email was sent to work email addresses and dealt with work matters in part, Mr Garamukanwa could have no reasonable expectation of privacy in relation to the materials used as evidence against him. In Mintz v. Mark Bartelstein & Assoc.,[75] the court dealt with the production of electronic information stored on personal devices used for work purposes and established the principle that employees may have a limited expectation of privacy in information stored on personal devices used for work purposes, subject to certain limitations. Specifically, the court held that any intrusion into an employee's privacy interest must be justified by a significant need, and that the intrusion must be limited to the extent necessary to achieve the legitimate objective. In the case of *City of Ontario v Quon,*[76] the US Ninth Circuit Court of Appeals dealt with the issue of whether an employer's review of an employee's text messages sent on a government-issued pager was a violation of the employee's Fourth Amendment rights. The court held that the employer's review of the text messages was reasonable, given the employer's policy on the use of pagers for work purposes.

The other primary concern is accessibility. 'Accessibility' in the context of bring your own device (BYOD) refers to the ability of employees and other users to access the data and applications they need to perform their work using their personal devices. This can include issues related to compatibility, security and privacy.[77] The relevant questions then are whether an employee is entitled to reimbursement or compensation for expenses related to the use of personal devices for work purposes and whether an employer is liable for damage to personal devices caused by work-related activities.

There have been several cases that have addressed the issue of accessibility. In *Doe v XYZ Corp*.,[78] the question was whether an employer's policy of requiring employees to use their personal devices for work purposes was reasonable. The court held that the policy was reasonable, but emphasised the importance of ensuring that the employees had access to the information and applications they needed to perform their work.

74 (70573/17) [2019] 6 WLUK 109.

75 *Mintz v. Mark Bartelstein & Associates, Inc.,* 885 F. Supp. 2d 987 (C.D. Cal. 2012)

76 Quon, 560 US 746 (2010).

77 TechTarget, 'BYOD (bring your own device)', (TechTarget, 2023) https://www.techtarget.com/whatis/definition/BYOD-bring-your-own-device accessed 24 February 2023.

78 887 A.2d 1156 (NJ 2005).

Also, in *King v Canadian National Railway Company (Canada),*[79] the court examined the issue of whether an employee was entitled to compensation for the cost of a personal device that was used for work purposes. The court held that the employee was entitled to be reimbursed for the cost of the device, as well as for other expenses related to accessing and using the data and applications they needed to perform their work. Furthermore, in *Commonwealth Bank of Australia v Barker,*[80] the court dealt with the issue of whether an employee was entitled to be reimbursed for the use of his personal device for work purposes. Here, the court held that the employee was entitled to reasonable compensation for the use of his device.

In *Digital Rights Ireland and Seitlinger et al.,*[81] the Court of Justice of the European Union (CJEU) issued a ruling dealing with the issue of data protection in the context of BYOD. The court held that an employee's personal data processed on a personal device used for work purposes must be protected against unauthorised access and that the employer is responsible for ensuring that appropriate technical and organisational measures are in place to protect these data.

These cases illustrate the challenges and complexities in BYOD cases and demonstrate the need for clear and comprehensive BYOD policies to help address the various legal issues associated with the use of personal devices for work purposes. They also demonstrate the importance of ensuring that employees have access to the information and applications they need to perform their work, regardless of whether they are using personal or company-owned devices. This can include ensuring compatibility with the necessary software and systems, providing necessary security measures, and protecting privacy.

Conclusion

The BYOD culture is advancing rapidly and changing work environments have accelerated this trend. This has exacerbated the data security and data privacy threat landscape. Organisations will need to rethink their data management strategies. This article examines the issues around BYOD ownership and the risks associated with such devices. It also analyses some data protection and security practices associated with BYOD and highlights the role of regulatory bodies in Nigeria in establishing proper compliance standards. The paper further recommends policy interventions to balance the rights and interests of employees, employers and other stakeholders. The article looks at the legal and regulatory framework in Nigeria and the need for organisations to adhere to regulatory standards and self-governing best practices. Very importantly, it evaluates the approach taken by courts in handling cases related to bring your own device (BYOD), drawing from principles established by US, UK, Canadian and European courts and the lessons that can be taken from these by Nigerian courts.

79 1922 CanLII 31 (SCC).
80 [2013] FCAFC 83.
81 C-293/12 (2014) ECLI:EU:C:2014:238.

References

Books, journals and blogs

Blair, L (2018), 'Contextualizing bring your own device policies', *Journal of Corporation Law*, Vol. 44, 151.

Cavoukian, A (2013) 'BYOD: (Bring Your Own Device) Is Your Organization Ready?' Information and Privacy Commissioner Ontario, Canada, retrieved from https://silo.tips/download/byod-bring-your-own-device-is-your-organization-ready accessed 2 November 2023.

Data Protection Commission (DPC) Ireland, 'Data protection by Design and by Default' available at: www.dataprotection.ie/organisations/know-your-obligations/data-protection-design-and-default accessed 24 Feb. 2023

Data Protection Commission (DPC) Ireland, 'Data Protection Impact Assessments', available at: www.dataprotection.ie/organisations/know-your-obligations/data-protection-impact-assessments

Data Protection Commission (DPC) Ireland, 'Guidance Note: A Practical Guide to Personal Data Breach Notifications under the GDPR', (DPC, October 2019) https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Data%20Breach%20Notification_Practical%20Guidance_Oct19.pdf accessed 4 November 2022.

Guardian Nigeria, 'Ransomware hits 71% of Nigerian Organisations', 4 May 2022, https://guardian.ng/technology/ransomware-hits-71-of-nigerian-organisations/ accessed 4 November 2022.

GVZH, 'Data Protection Implications of a Bring Your Own Device Policy', 18 Oct. 2019, https://gvzh.mt/insights/data-protection-implications-bring-your-own-device-policy/ accessed 1 November 2022.

Imperva, 'Phishing attacks', n.d., https://www.imperva.com/learn/application-security/phishing-attack-scam/ accessed 4 November 2022.

Information Commissioner's Office (ICO), 'Step 5: Identify and assess risks', https://ico.org.uk/for-organisations/childrens-code-hub/sample-data-protection-impact-assessment-online-retail/step-5-identify-and-assess-risks/ accessed 3 November 2022.

Irene, M (2021), 'Nigerian employers and employee monitoring', PressReader, 14 June, available at: www.pressreader.com/nigeria/business-a-m/20210614/282029035175985 (accessed 1 November 2022).

Mantelero, A and G Vaciago (2017), 'Legal Aspects of Information Science, Data Science and Big Data', in M Dehmer and F Emmert-Streib (Eds.), *Frontiers in Data Science,* CRC Press (Boca Raton, Florida).

McLellan ML, Sherer JA, and Fedeles ER (2015), 'Wherever You Go, There You Are (with Your Mobile Device): Privacy Risks and Legal Complexities Associated with International Bring Your Own Device Programs', *Richmond Journal of Law and Technology*, Vol. 21, 1.

NL Times, 'Dutch employee fired by U.S. firm for shutting off webcam awarded €75,000 in court', 9 Oct. 2022, https://nltimes.nl/2022/10/09/dutch-employee-fired-us-firm-shutting-webcam-awarded-eu75000-court accessed 4 November 2022.

Oxford University News Science Blog, 'FBI follows Oxford academics' guide to beat Zoom bombers', 24 April 2020, https://www.ox.ac.uk/news/science-blog/fbi-follows-oxford-academics-guide-beat-zoom-bombers accessed 24 February 2023.

PortSwigger, 'Remote working during coronavirus pandemic leads to rise in cyber attacks, say security professionals', (PortSwigger, 2020) https://portswigger.net/daily-swig/remote-working-during-coronavirus-pandemic-leads-to-rise-in-cyber-attacks-say-security-professionals accessed 24 February 2023.

Pressreader, 'Nigerian employers and employee monitoring', 14 June 2021, www.pressreader.com/nigeria/business-a-m/20210614/282029035175985 accessed 1 November 2022.

Rai, S, P Chukwuma and R Cozart (2016), *Security and Auditing of Smart Devices: Managing Proliferation of Confidential Data on Corporate and BYOD Devices,* Auerbach Publications (Boca Raton, Florida).

Samsung, 'Maximizing Mobile Value', White Paper, Samsung Business, available at: https://samsung.com/us/business/short-form/maximizing-mobile-value-2022/ accessed 11 September 2022).

Sophos (2021), 'BYOD Security: The Importance of Mobile Device Management (MDM)', retrieved from: www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophos-byod-security-factsheet-en.pdf

Sophos, 'State of Ransomware in Retail 2022 report', retrieved from https://www.sophos.com/en-us/whitepaper/state-of-ransomware-in-retail accessed 4 November 2023.

Technavio, Bring your own device (BYOD) market by end-user and geography - Forecast and analysis 2022-2026 retrieved from https://www.technavio.com/talk-to-us?report=IRTNTR74271&type=sample&rfs=epd&src=report&utm_source=prnewswire&utm_medium=pressrelease+&utm_campaign=t42dtcs_rfs1_wk41_2022_007&utm_content=IRTNTR74271 accessed 1 November 2022.

TechTarget, 'BYOD (bring your own device)', (TechTarget, 2023) https://www.techtarget.com/whatis/definition/BYOD-bring-your-own-device accessed 24 February 2023.

Tessian, 'Understand the mistakes that compromise your company's security', retrieved from: www.tessian.com/research/the-psychology-of-human-error/

The Daily Swig (2020), 'Remote working during coronavirus pandemic leads to rise in cyberattacks, say security professionals, 14 July; VMware (2020) *Carbon Black Global Threat Report June 2020 – Extended Enterprise under Threat*, available at: https://www.carbonblack.com/resources/global-threat-reportextended-enterprise-under-attack-index/ accessed 23 February 2023.

Times of Malta, 'HSBC fined €5,000 for monitoring employee's bank account', 15 August, available at: https://timesofmalta.com/articles/view/hsbc-fined-5000-for-monitoring-employees-bank-account.728921 accessed 4 November 2022.

T-Mobile for Business, The T-Mobile for Business 2020 Workplace Mobility Report, 2020, https://www.t-mobile.com/content/dam/tfb/pdf/T-Mobile-for-Business-2020-Workplace-Mobility-Report.pdf?icid=TFB_TMO_P_TFBFTRWRKS_7LCBNVDVYBXY27WF321599 accessed 1 November 2022.

VMware, Carbon Black Global Threat Report June 2020 – Extended Enterprise under Threat, 2020, https://www.carbonblack.com/resources/global-threat-reportextended-enterprise-under-attack-index/ accessed 4 November 2022.

Wired, 'BYOD, CYOD, COPE, COBO — What Do They Really Mean?', www.wired.com/brandlab/2018/06/byod-cyod-cope-cobo-really-mean/ accessed 2 November 2022.

Yonhap News Agency, 'S. Korea probes cyberattack on digital currency exchange', 3 July 2017, https://en.yna.co.kr/view/AEN20170703010400320 accessed 1 November 2022.

Zippia, '26 surprising BYOD statistics [2022]: BYOD trends in the workplace', Zippia.com, 17 October 2022, https://www.zippia.com/advice/byod-statistics/ accessed 2 November 2022.

Laws, regulations and guidelines

1999 Constitution of the Federal Republic of Nigeria

Credit Reporting Act of 2017.

Cybercrimes (Prohibition and Prevention) Act 2015

European Data Protection Supervisor (EDPS) (2022), 'Guidelines on the protection of personal data in mobile devices used by European institutions (Mobile devices guidelines)', available at: https://edps.europa.eu/sites/default/files/publication/15-12-17_mobile_devices_en.pdf (accessed 2 November 2022).

Freedom of Information Act 2011

NDPR Implementation Framework 2020

Nigerian Data Protection Regulation (NDPR) 2019

Regulation (EU) 2019/881 of the European Parliament and of the EU Council of 17 April 2019 (Cybersecurity Act) on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013.

Further reading

Abdulrauf, LA (2021), 'Giving "teeth" to the African Union towards advancing compliance with data privacy norms', Information and Communications Technology Law, Vol. 30 87–89.

Australian Government (2019), 'Part 3: Responding to data breaches — four key steps', Office of the Australian Information Commissioner, available at: www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-3-responding-to-data-breaches-four-key-steps

Bispham, M et al. (2021), 'Cybersecurity in Working from Home: An Exploratory Study', available at: SSRN 3897380 (accessed 4 November 2022).

Cavelty, MD (2010), 'Cyber-security', in The Routledge Handbook of New Security Studies, Routledge, p.4.

CyberlinkASP (2014), 'Consider Desktops in the Cloud for BYOD, available at: www.cyberlinkasp.com/insights/consider-desktops-cloud-byod/ (accessed 2 November 2022).

Fruhlinger, J (2022), 'What is Phishing? How This Cyber-attack Works and How to Prevent It', 13 April, CSO, available at: www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-preventit.html (accessed 2 November 2022).

Hakak, S et al. (2020), 'Have you been a victim of COVID-19-related cyber incidents? Survey, taxonomy, and mitigation strategies', IEEE Access, Vol. 8, 124134.

Informer, 'A CISO's Guide to Attack Surface Expansion in 2023', (Informer, 12 January 2023) https://informer.io/resources/attack-surface-expansion accessed 24 February,2022.

IT Governance (2022), 'List of Data Breaches and Cyber Attacks in August 2022 – 97 Million Records Breached', Itgovernance.co.uk, blog, 1 September, available at: www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-august-2022-97-million-records-breached accessed 2 November 2022

KMicro (2019), 'How to Implement a BYOD Policy Your Employees Will Actually Follow', available at: https://kmicro.com/how-to-implement-a-byod-policy-employees-will-follow/ accessed 3 November 2022.

Lewis Silkin (no date), Bring Your Own Device, 3, available at: www.lewissilkin.com/api/download/downloadattachment?id=8e57d419-b986-4353-b813-91f6eef3e41e (accessed 2 November 2022).

Mantelero, A et al. (2020), 'The common EU approach to personal data and cybersecurity regulation', International Journal of Law and Information Technology, Vol. 28, 297.

Ottis, R and Lorents, P (2010), *'Cyberspace: Definition and implications'*, Academic Conferences International Limited, available at https://www.proquest.com/docview/869617247/fulltextPDF/1794 1F23CCD04FBAPQ/1

Veeam (2022a), 2022 Data Protection Trends Report, available at: https://www.veeam.com/wp-data-protection-trends-report.html (accessed 18 September 2022).

Veeam (2022b), 'Real-World Statistics on Downtime and Data Loss in 2022', available at: www.veeam.com/blog/data-loss-2022.html (accessed 18 September 2022).

Weil, T and S Murugesan (2020), 'IT risk and resilience – Cybersecurity response to COVID-19', IT Professional, Vol. 22, 4.