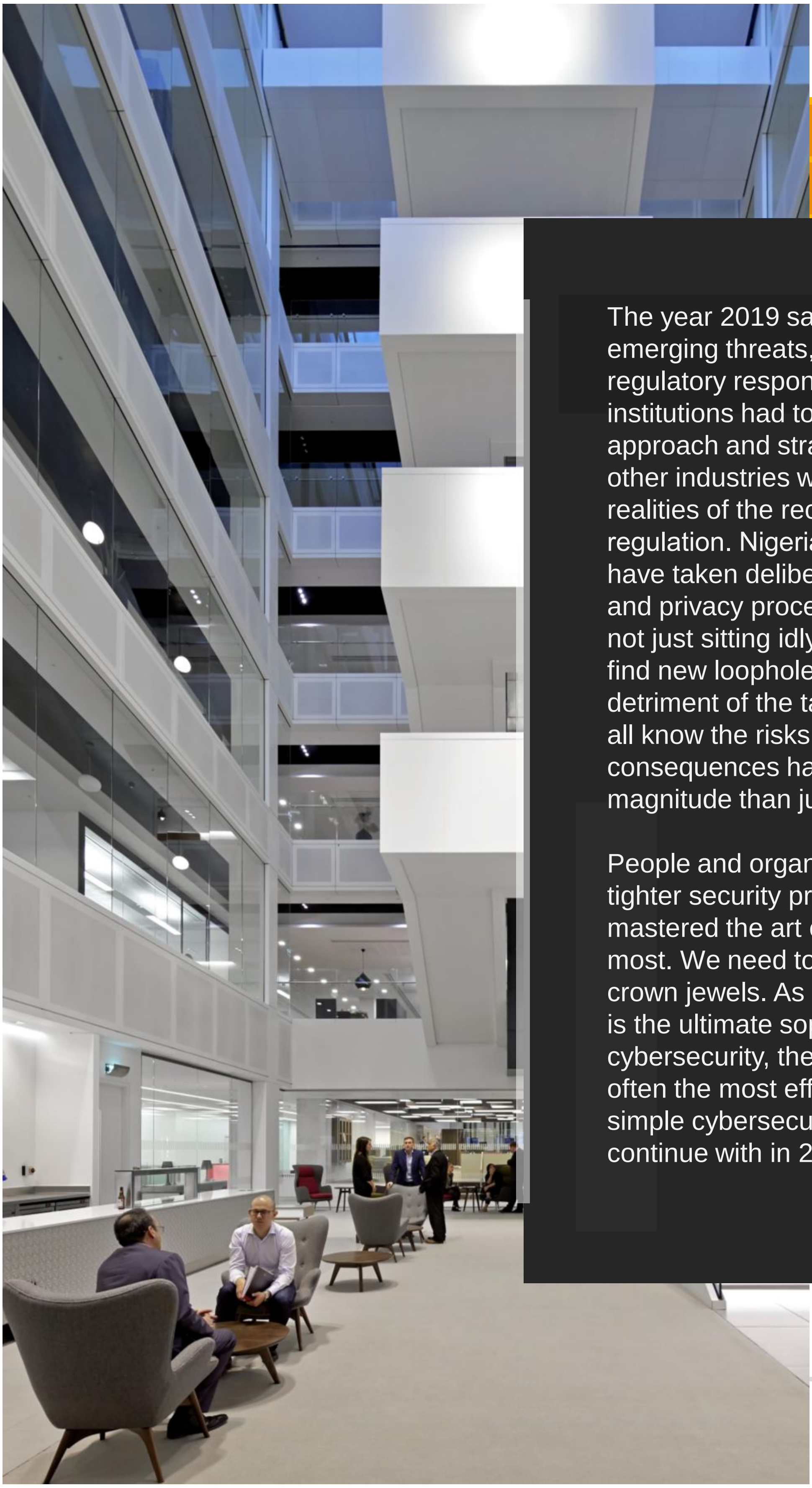
Cyber Actionable Insights Series 2020
Issue 1

Cybersecurity & Privacy in Nigeria:

Simple steps in the right direction

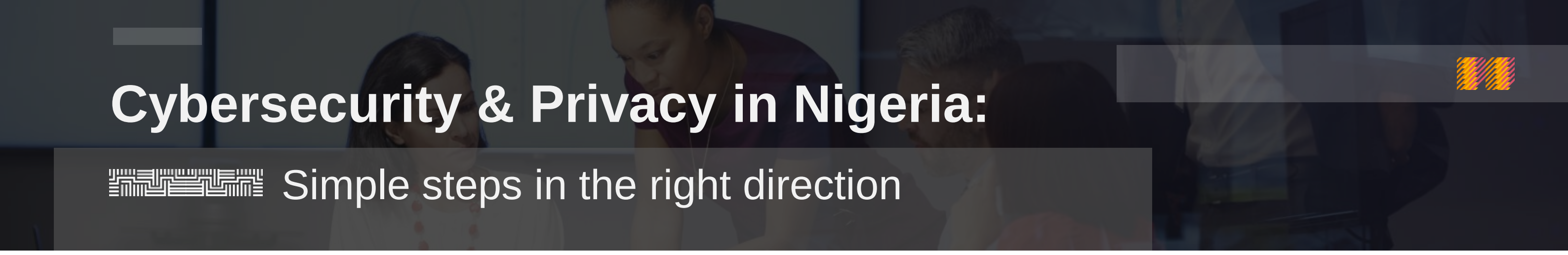
January 2020

www.pwc.com/ng



The year 2019 saw a mix of new attacks, emerging threats, and some corresponding regulatory responses. Many financial institutions had to re-think their cybersecurity approach and strategy, while organizations in other industries were faced with the hard realities of the recent data protection regulation. Nigeria’s regulatory organizations have taken deliberate steps to build security and privacy processes, but the attackers are not just sitting idly either. They continually find new loopholes and flaws to exploit, to the detriment of the targeted organizations. We all know the risks; they are not new, but the consequences have a significantly higher magnitude than just a few years ago.

People and organizations need to adopt tighter security practices, as attackers have mastered the art of hitting where it hurts the most. We need to ensure we protect our crown jewels. As the saying goes, simplicity is the ultimate sophistication. Even in cybersecurity, the simplest practices are often the most effective. Here are a few simple cybersecurity practices to adopt or continue with in 2020.



Cybersecurity & Privacy in Nigeria:

Simple steps in the right direction

1 Use strong authentication

In 2020, we need to embrace the use of strong authentication techniques. This means

- use stronger and longer passwords or passphrases. A simple example would be *“B0rg3rs m4ke me ve5y Happy!.* Studies have shown that it takes attackers significantly more time and effort to break long random passphrases than it would take them to crack passwords that can be easily associated to individuals.
- use biometric authentication if available. Specific and unique characteristics of a person can be used to restrict access to confidential information. Methods of biometric authentication include, fingerprints, retina scans, facial recognition, analysis of a person’s physique.
- in addition to the above, incorporate multi-factor authentication wherever possible. Even on our personal devices and accounts, having more than one form of authentication provides a strong line of defense. For instance, using a password and a soft/hard token increases the difficulty of exploitation by attackers.

2 Use email and social media with care

Generally, we think of enterprises as having a network boundary. However, the wide range of interactions which the employees of an organisation have with third parties means that data and information is often flowing inward in an organisation from a variety of sources.

Several social engineering campaigns often take advantage of email and social media platforms to deliver disguised malicious content, which are designed to provoke a sense of fear, urgency, worry, or otherwise play on our emotions. Our use of email and social media opens us up to the whole world, therefore we should be as guarded as we would be if we had extremely valuable assets on us in public spaces. As general rules:

- If something looks too good to be true, it probably is. There are no free things on the internet anymore.
- If an email or post from a known sender looks suspicious, verify its origin through a separate means of communication, e.g. a phone call.
- Do not open an email and/or its attachments or click links within it if you do not recognize the sender or the attachments.
- Hover your mouse over suspicious email addresses/links and check internet headers to know their true source and/or identity.
- If you think you may have been compromised, contact your IT team immediately. A few seconds can make a big difference when trying to contain a breach.

3 Install updates

Updates are often created and released by equipment or software manufacturers in response to security weaknesses. These weaknesses may be identified by the manufacturers themselves, or by third parties. However, updates are often considered optional by users, and sometimes by corporations. Individual users especially lament about the cost of internet data bundles required to download and install updates on computers and mobile devices, and often choose to skip it altogether.

Installing updates is one of the most effective ways to prevent several types of attacks, and it requires no technical knowledge. Updates will often patch vulnerabilities that are exploited by most low-skilled and medium-skilled hackers, giving users protection from most of the attacks which may come their way.

4 Stay cyber aware and informed

Just as technology is evolving, cyber-criminals are getting more creative and innovative in their approach. Therefore, it is of utmost importance that we keep abreast of developing information about cyber security, new attack techniques and best practices for staying digitally safe.

Because the internet has made us all interconnected, one person’s compromise could lead to other people getting affected. In the same way, one person’s compromise could help us learn and be more secure. Remember, an organisation is as strong as its weakest link.

5 Comply with applicable laws and regulations

Greater amounts of data continue to be generated, analysed, and used for a variety of purposes. But with a lot of use comes the potential for data to be misused, and data owners and subjects are becoming increasingly worried about the potentially damaging uses to which their data is being put.

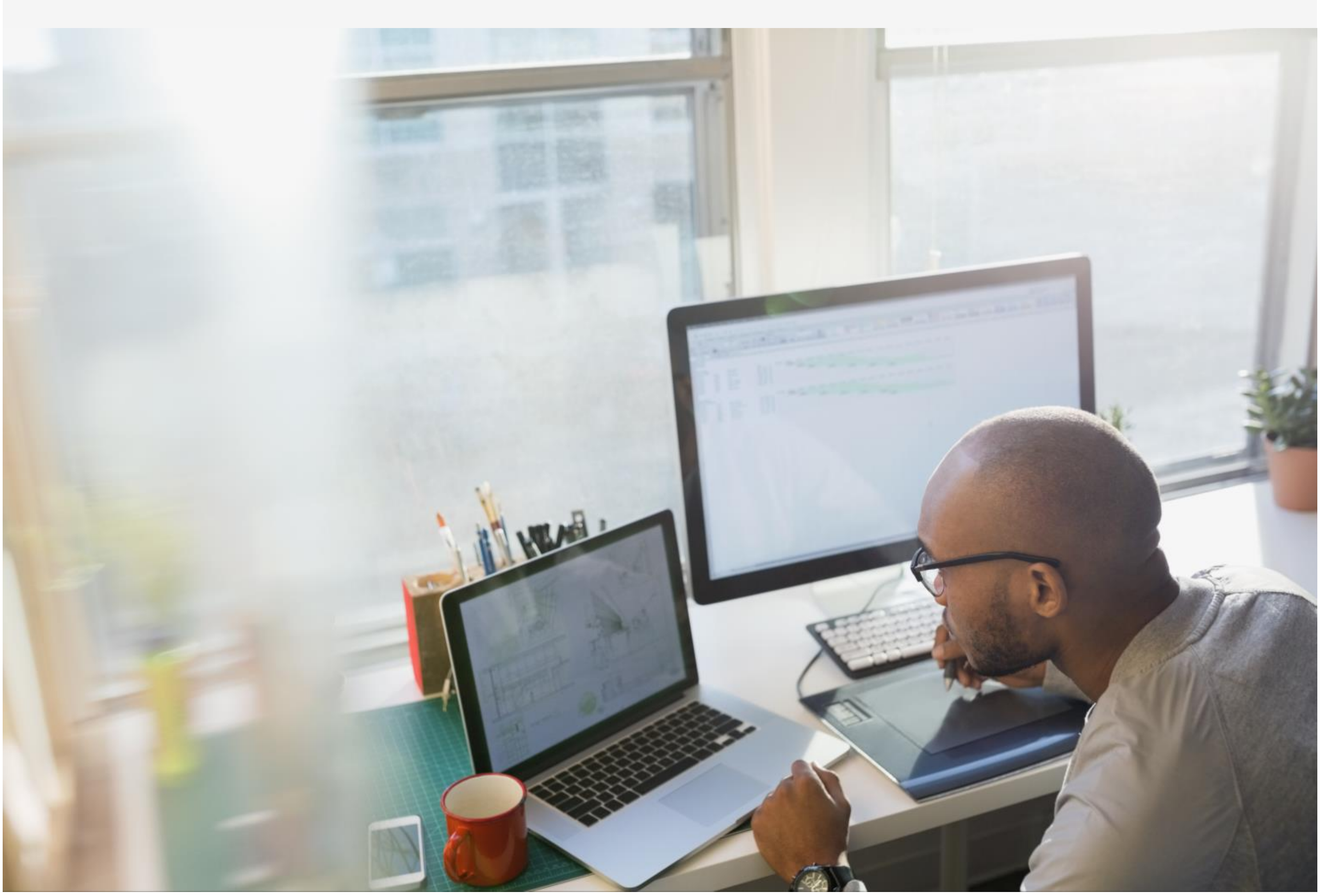
Consequently, in recent years, there has been a proliferation of data privacy and data protection-related laws and regulations all over the world, including in Nigeria (with the NITDA Data Protection Regulation).

No matter the country, industry, regulation or law in question, a few general, similar and important themes emerge when we study them, which are important to adhere to. Some of these are listed below:

- When you collect personal information, ensure you are collecting only what you absolutely need, and nothing more.
- When you collect personal information from people, ensure you tell them exactly why you need the information, and obtain their consent for that use.
- If you must use the information for a different purpose than what was agreed initially, you have to obtain consent again.
- Your data subjects have a right to get their data erased. Subject to certain limitations, if they request this, you must erase the data you have on them.
- You have a responsibility to apply effective information security mechanisms to the information to prevent unauthorised access.

Specific requirements, implementation mechanisms, and penalties vary between regions and industries, so ensure that you are very familiar with the requirements that apply to you.

The pitfalls of cybersecurity can be subtle and easy to miss, but also easy to pay attention to. We must ensure we stay mindful of the seemingly insignificant mistakes that can cost us so much. Basic cybersecurity hygiene will never go out of fashion and will always be our responsibility. As the year unfolds, let us make new cyber-aware resolutions to adopt these simple things. We would be grateful we did by the end of the year.



Wunmi Adetokunbo-Ajayi
Partner Digital Risk & Cyber Security, PwC.
wunmi.Adetokunbo-ajayi@pwc.com

Nkiruka Aimienoho
Senior Manager Cybersecurity, Privacy & Resilience, PwC.
nkiruka.aimienoho@pwc.com

Chika Nwachukwu
Manager Digital Risk & Cyber Security, PwC.
chika.nwachukwu@pwc.com

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We’re a network of firms in 158 countries with more than 250,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more by visiting us at www.pwc.com/ng