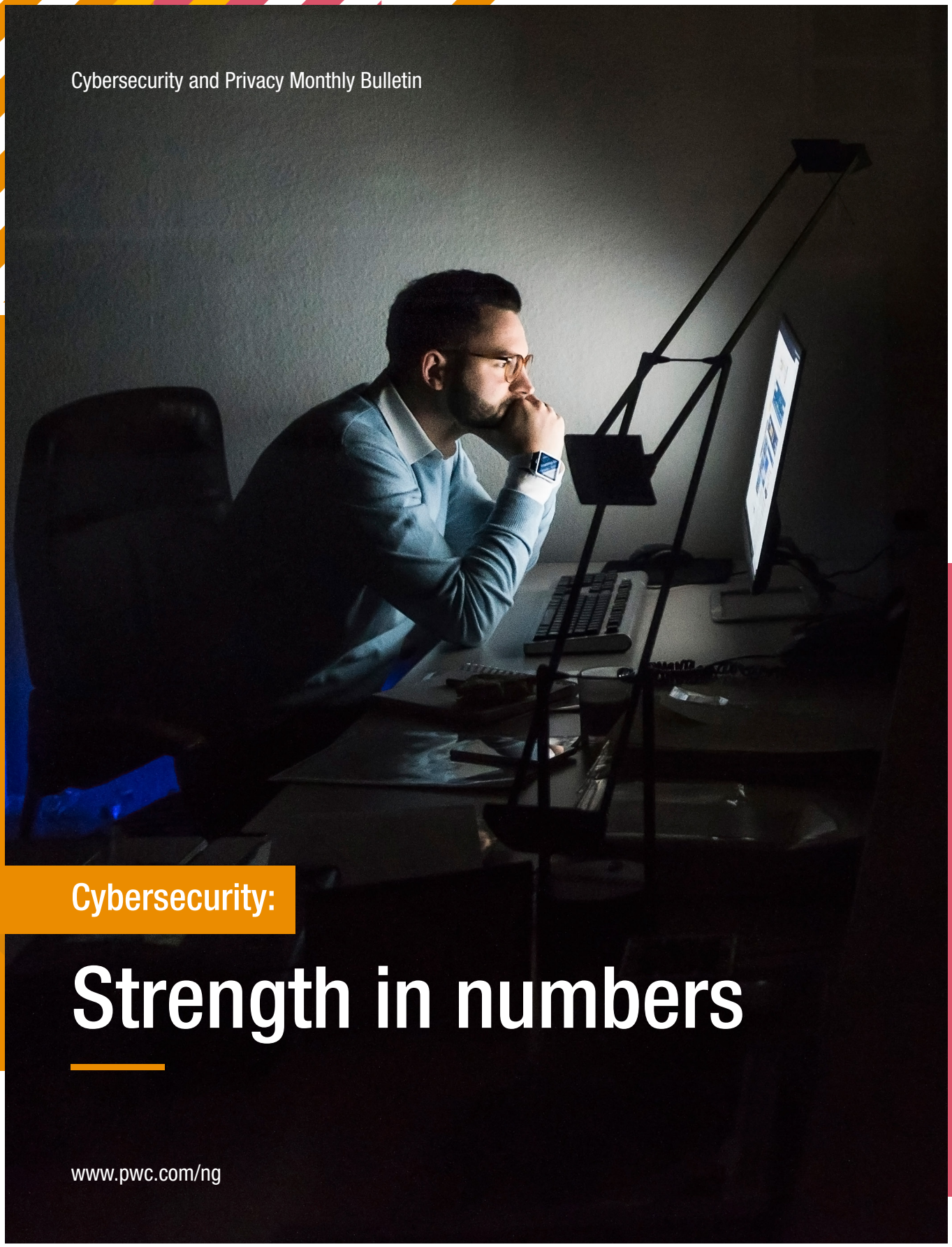
Cybersecurity and Privacy Monthly Bulletin



Cybersecurity:

Strength in numbers

www.pwc.com/ng

pwc

October, 2020

General Introduction:

Our monthly cybersecurity update focuses on critical cybersecurity developments around the world with insights on lessons learned and what your organization needs to do to improve cyber resilience and privacy.

Former Chief Security Officer Charged

In August of this year, the news appeared in several media publications, as well as the United States' Department of Justice website that a former top executive of a multinational company got charged with obstruction of justice, among other charges.

According to the complaint filed, two hackers who claimed that they had obtained a company-owned database containing personally identifying information of about 57 million people contacted him and demanded a six-figure payment in exchange for their silence. The company paid the individuals $100,000 in Bitcoin. The complaint alleges that the executive took deliberate steps to hide the breach from the Federal Trade Commission, including attempting to funnel the payment through a bug bounty program.

The two hackers have since been arrested and pleaded guilty. The complaint also alleges that the hackers successfully attacked other organizations after the attack on the company. Across the world, including in Nigeria, reporting requirements around data breaches and security incidents vary widely. Most organizations have reporting requirements that are at the intersection of federal and state laws and regulations, industry-specific regulations, and even international laws inherited through links with a sister or parent companies. It creates the potential for an uneven landscape of requirements as we look across organizations in any one country, region, or even industry.

No matter how complex the requirements may be. Leadership commitment and accountability to comply with disclosure requirements are pivotal to the success of the organization. Leadership commitment is a critical success factor for all areas of organizational security, including compliance reporting and sharing of threat information. If an organization violates compliance requirements, senior management individuals may be held responsible by authorities, beyond fines and lawsuits targeted at the corporate/legal entity.

Beyond demonstrating bare minimum compliance with regulatory requirements, there are key benefits that accrue to the entire corporate ecosystem within an industry, region, or nation when threat intelligence information is shared openly. An environment in which the circulation of threat intelligence occurs among all players fosters a more secure organization, for the following reasons:

1. Each entity "learns" from the experience that others have had, instead of only their own experience. An attack launched against one entity, once detected, can not be successfully replicated against others.

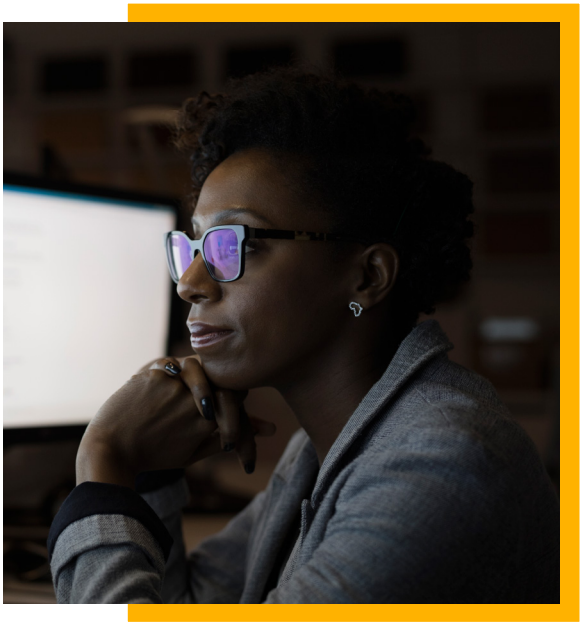
2. Each entity can reduce the time it takes to detect an incident or an attack. The earliest stages of an attack will sometimes involve activities that are very similar to normal activities or do not have the "obvious" indicators of an attack. These activities may be difficult to detect or may fall very low on the entity's priority list. But if they are already known to be part of an attack, they can be easily detected and much earlier.

3. Business impacts on time, human resources, technology, potential recovery time can significantly reduce.

All of the above, put together, help organizations improve their overall security posture, free up limited resources for other purposes, and make the industry more secure.

5 Questions for CISOs

1. Are you fully aware of all the laws and regulations you have to comply with after a data breach or a cybersecurity attack?
2. Do you have a proper process and plan for communicating with third-parties about data breaches, including regulators, law enforcement, and the general public?
3. Are relevant personnel aware of their roles and responsibilities in the execution of this plan?
4. Is your team a cross-functional team that can effectively manage the disclosures and responses?
5. Do you share threat intelligence information with other organizations in the country, your region, or your industry?



How PwC Nigeria Cybersecurity help businesses to create value:

PwC Nigeria Cybersecurity and Privacy practice consist of dedicated professionals with significant business and technical experience that help you address your most complex business imperatives. We are leveraging the power of our global network to provide organizations with profound and timely expertise on evolving cybersecurity and privacy challenges. We don't just protect business value. We create it – using cybersecurity and privacy as a tool to transform businesses.

Our services include:

- CISO and Data Protection Officer as a Service (Virtual CISO)
- Cyber Resilience and Cyber Risk Management
- VMaaS, Cyber Penetration Testing and Application Security
- Compliance Management & Third Party Security Assessment
- Data Privacy Program Implementation
- Data Protection / Privacy Compliance Audits
- Training and Awareness
- Cyber Risk Quantification

ONE ON ONE WITH TOYIN

What made you decide to join PwC?

"Desire to be part of a global brand, work with bright professionals and an opportunity to gain experience from various industry sectors."

How has working in PwC been like so far? Please share your journey so far as a cybersecurity professional in PwC

Working with PwC has helped me build and develop myself professionally. I particularly love the work culture/ethics. As a cybersecurity professional in PwC, I am opportuned to work with amazing people, leverage resources across the global network and be a part of teams that add value to clients.

Kindly share your personal cybersecurity Journey

I joined PwC and worked with the IT operations team. Amongst others, my responsibility was to support the management of the ISMS (Information Security Management System). This birthed my interest in Cybersecurity. Currently, I lead teams in supporting clients with the implementation of IT Standards and Compliance Management engagements.

Please share your previous experiences before PwC?

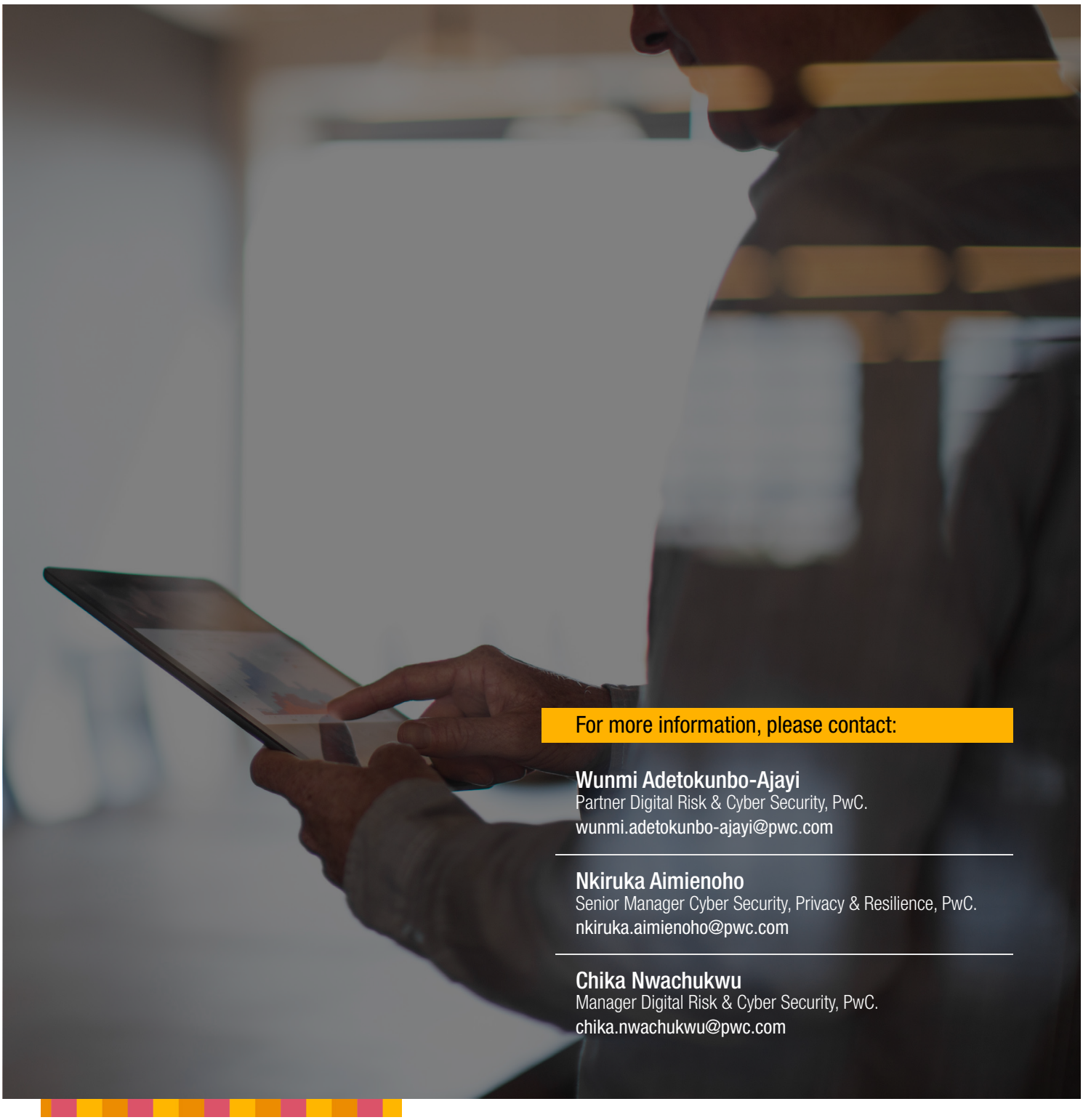
Started my career as a network engineer with an Internet Service Provider before joining PwC. Part of my functions included the configuration and deployment of internet modems for client; particularly organisations in the financial services and energy sector.

How is the cyber security team keeping up the rise of new technologies, techniques and strategies in the cyberspace?

We have access to resources and forums across the PwC global network. We have daily sessions where cyber issues and trending threats are discussed.We are encouraged to attend webinars and join InfoSec and cybersecurity associations and groups. The firm sponsors professional certifications.

Any fun facts about yourself and your job?

The people I work with make the job fun.



For more information, please contact:

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

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

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

pwc