www.pwc.com/ng

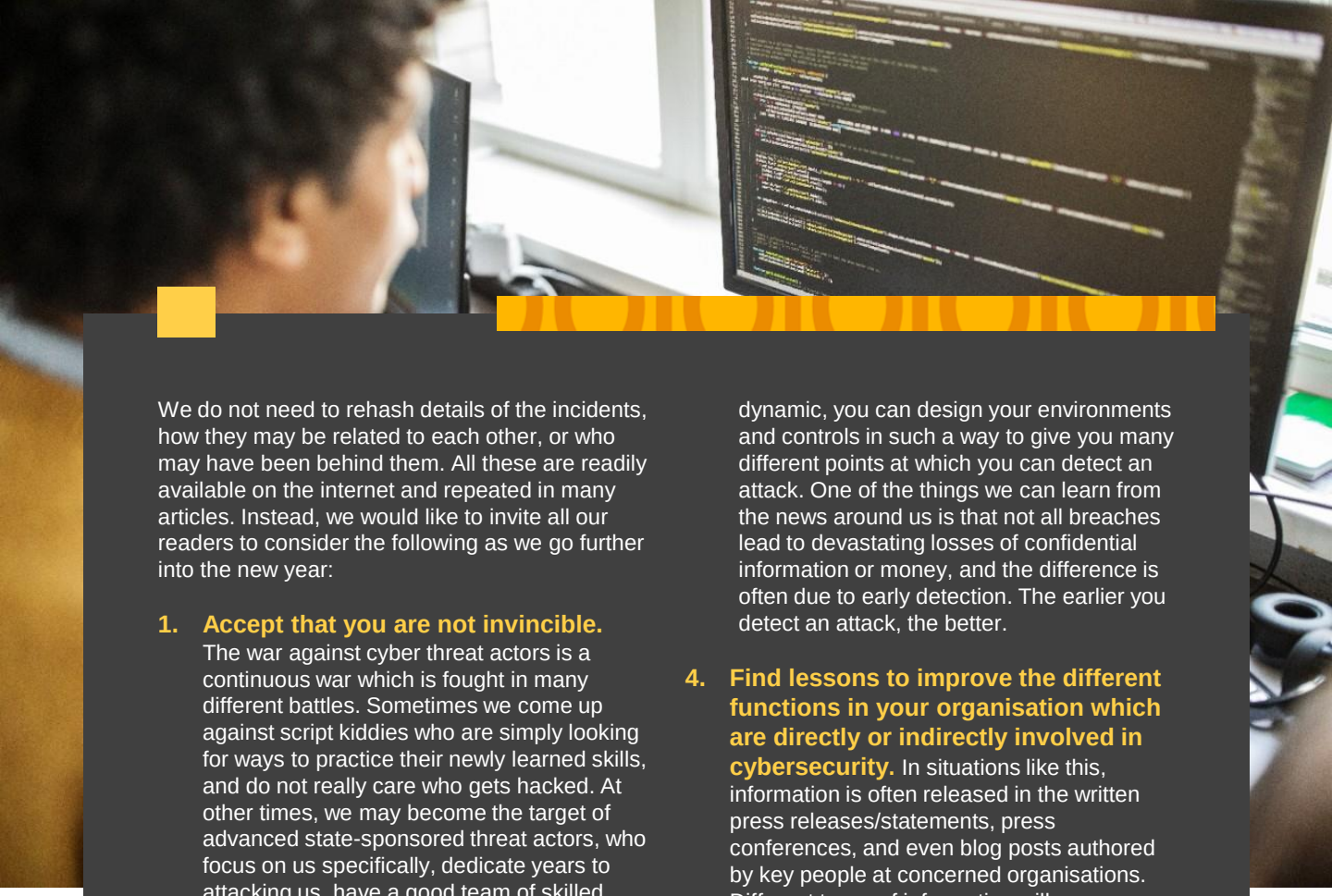
Learning from 2020 and looking forward

Cybersecurity and Privacy Monthly Bulletin

2020 was a momentous and tumultuous year for cybersecurity. The usual issues and threats normally expected were multiplied and exacerbated due to the global pandemic. Perhaps the most significant breaches of the year came at the end, with multiple large entities compromised by threat actors. Some of these compromises led to one of the most advanced supply chain attacks we have seen so far.

The news seemed to creep into the headlines and gradually gained momentum without warning. There was a new development almost every day, yet many unknowns. Articles, blog posts, and think pieces appeared everywhere, some of which included statements that could not be verified. Tech giants and federal law enforcement worked together to get to the root of the cyber incidents that occurred.

January 2021



We do not need to rehash details of the incidents, how they may be related to each other, or who may have been behind them. All these are readily available on the internet and repeated in many articles. Instead, we would like to invite all our readers to consider the following as we go further into the new year:

1. **Accept that you are not invincible.** The war against cyber threat actors is a continuous war which is fought in many different battles. Sometimes we come up against script kiddies who are simply looking for ways to practice their newly learned skills, and do not really care who gets hacked. At other times, we may become the target of advanced state-sponsored threat actors, who focus on us specifically, dedicate years to attacking us, have a good team of skilled attackers, and have millions at their disposal. Some of these attackers study the technologies we use at a very deep level, discover zero-day vulnerabilities, and are not bothered with ethical responsible disclosure. Like it is often said, it's not if you are breached, but when.

2. **Consider that breaches are not necessarily evidence of poor cyber hygiene.** Some of the organisations which were breached were organisations who are leaders in cybersecurity, and offer a large range of security products and services. But following from point 1 above, attacks will sometimes be well-resourced and highly targeted. If we think about the fact that our technical security solutions are made of millions of lines of code, any one of which could give rise to a vulnerability, sometimes it may happen that our best efforts may not protect us from the specific threat actors we are up against at a particular point in time. So the focus should be on building and fortifying resilience.

3. **Strengthen and test your detective capabilities.** While you may have a lot of strong preventive controls, they are never 100% guaranteed to protect you, and attackers will always seek ways to bypass them. Even though attacks may be highly dynamic, you can design your environments and controls in such a way to give you many different points at which you can detect an attack. One of the things we can learn from the news around us is that not all breaches lead to devastating losses of confidential information or money, and the difference is often due to early detection. The earlier you detect an attack, the better.

4. **Find lessons to improve the different functions in your organisation which are directly or indirectly involved in cybersecurity.** In situations like this, information is often released in the written press releases/statements, press conferences, and even blog posts authored by key people at concerned organisations. Different types of information will serve different stakeholders within your information security function and the wider organisation. Information such as indicators of compromise, if released, might be useful to your technical security teams. Press releases, press conferences, and so on can provide positive or negative lessons for teams charged with corporate communications. Reactions of customers and regulators may also serve as learning points for teams handling compliance and legal services. This proactive strategy will be one of the most important steps organizations take this year.

5. **Find ways to level the playing field with attackers by building resilience now.** With the increase in double extortion (which involves the exfiltration and leakage of sensitive data from targeted networks, in addition to a ransomware attack), the use of artificial intelligence by criminals to further automate attacks, and remote work becoming a permanent aspect of business operations. How ready are you for the imminent threats? Consider having a tried-and-tested plan that can address prevalent threats. Check out the threat outlook for the year highlighted in our 2021 digital trust insights to aid the process of building resilience for any scenario.

Questions for security leaders?

01	Do you actively draw lessons and technical resources from publicised breaches?
02	Do your teams know how to incorporate those lessons into their work to improve security and incident response?
03	Do you proactively hunt for threats in your environment, instead of only reacting to alerts?

How PwC Nigeria's Cybersecurity and Privacy practice helps businesses to create value:

At PwC we help you build resilience so that you can confidently adapt and grow. We bring the right capabilities and experience to aid the delivery of your objectives. Our team of dedicated professionals have significant business and technical experience to help you address your most complex imperatives. We leverage the power of our global network to provide organizations with deeper, broader and timely expertise on evolving cybersecurity and privacy challenges.

Our services include:

- CISO as a Service
- Cyber Transformation
- Cyber Risk Management and Quantification
- Technical Assessments - Cyber Penetration Testing and Application Security
- Security Standards Compliance Management
- Third Party Security Assessments
- Privacy Maturity Assessments and Compliance
- Training and Awareness (Digital Risk & Cybersecurity Academy)

For more information, please contact:

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

Nkiruka Aimienoho
Associate Director Cyber Security, Privacy & Resilience, PwC.
nkiruka.aimienoho@pwc.com

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