KPMG

Building Cyber Security & Resilience in a Digital Africa

Publication by KPMG in Nigeria

May 2017

KPMG.com/ng

Contents

Foreword

It is no longer news that we are in the digital age. Advancement in digital technology is enabling business innovation and agility across the world.

Furthermore, the business ecosystem is rapidly evolving in response to the convergence of digital technologies. The inevitable reality is that companies are transforming and everything is connected. With the exponential growth of digital touch-points across different businesses, cyber security now directly affects the resilience of organizations, our economy and our individual safety.

Some organizations in Africa have suffered the adverse impacts of cyber security breaches at different times. There have been instances of fraudulent transactions on different online banking platforms, successful distributed denial of service (DDoS) attacks, major ransomware incidents, defacement of websites of government agencies, and identity theft, to mention a few.

Indeed, it is obvious that the African business ecosystem is not insulated from the challenges being faced by businesses across the globe. For instance, North Korea was linked to attacks on banks in 18 countries, according to a recent report from Russian cybersecurity firm - Kaspersky. Financial institutions affected included countries in the African region such as Ethiopia, Gabon, Kenya, and Nigeria.

People wrongly assume that the cyber risk only affects financial institutions. However, a better way to view this, is from the perspective of the impact on the victim. We are all connected to the internet in one way or the other; and most organisations have one internet presence (e.g. website) or the other. Several also use IT systems to run their business. These are examples of attack targets of cybercriminals and everyone is therefore exposed.

Another consideration is the value at risk. At a minimum, any organisation can be greatly damaged by reputational risk. Imagine the impact of a defaced website on your important customers. Any serious organisation regardless of its sector will be adversely affected.

It is also important to note that it is not only organisations that are exposed to cyber threats. On a personal level, we are all exposed, and, in this regard, the threat is even more exploitable.

How many of us ensure that our smartphones or tablets have antivirus software? For those that have, do we question the trustworthiness of the source? Moreover, the line between our personal and work lives is getting increasingly blurred. It follows then that businesses are yet again at risk when our personal devices or online profiles get compromised.

Interestingly, a lot of organisations focus on the cyber risk side of digital transformation. In other words, if we don't do this or that, and we have a breach, we will lose customers, it will negatively impact our brand, etc. Hence, a number of executives and directors have anxiety around adopting new technologies to gain a competitive advantage.

However, at KPMG, we also emphasise the positive aspect of this discussion, which is often overlooked. Effective cyber defense can actually enable your company harness new opportunities for revenue growth and overall business success. This is the message we focus on, and it is one that more CEOs and cyber security stakeholders should be listening to presently.

Joseph Tegbe
Partner & Head
Technology Advisory
KPMG in Nigeria
Africa Cyber Security SGI Lead

Executive summary

As digitization opens up innovative products and services with cost effective processes and enhanced customer experience, the 'incumbents' and the digital 'disruptors' must understand that the business risks will no longer be 'conventional'. The digital evolution has introduced a new dimension into the enterprise risk - the cyber risk. Unfortunately, cyber risk is not conventional, neither are the threat actors.

It all begins at the top

Countering an evolving threat landscape requires board level leadership, insight and decision making. It is imperative for investors, customers and other business stakeholders to ensure that Board and executive leadership are part of the design and implementation of a strategic and holistic approach to cyber security that will not only protect their valuable data, but also enhance enterprise agility and growth.

Government Perspectives

The evolving threat landscape and its innate dynamism continue to place demands on governments and regulators across the world to develop and implement robust frameworks, policies that can engender the capacity to effectively manage cyber risks. It is noteworthy that some African nations are beginning to take note as evidenced by cyber security policies, strategies and even bills, being pushed out. There has also been some effort towards establishing National CERTs to protect national cyber borders. However, given the dynamic nature of the threat and the increasing potential for widespread adverse impact, governments need to show more urgency in addressing this risk.

How it Affects You

With all the connected devices we carry about daily, it is obvious that our lives, economic vitality, national security amongst others, now revolve round technology. With several data breach incidents across different social media platforms, individuals need to make conscious effort to manage personal cyber risk.

Emerging Trends

A recent KPMG survey asserts that there will be over 25 billion connected devices by the year 2020. While it is important to acknowledge the advantages that IoT, blockchain and other emerging technologies promise, it is equally essential to be aware of the security challenges and risks inherent in these technologies, given that they fundamentally involve connected devices over the Internet. Also, as organizations increasingly see the need to be insured against cyber risks, the Cyber insurers need to be more sophisticated in assessing cyber risks to turn this emerging opportunity to a sustainable line of business.

Addressing the Skills Gap

Cyber security talents are becoming increasingly difficult to find in today's ever growing and dynamic technology world. Solving the growing cyber security challenges requires young skilled cyber security professionals who are proactive and willing to combat existing cyber-security threats. There is also a clear need for governments and enterprises to provide enabling environment buoyed by relevant educational curriculum to attract and groom these talents.

It all begins at the top

The Digital Business and Cyber Risk

It is no longer news that we are in the digital age; advancement in digital technology is enabling business innovation and agility across the world. The business ecosystem is rapidly evolving in response to the convergence of digital technologies. New digital companies are disrupting the market with non-conventional but innovative products, while the incumbents are also transforming their products and services to remain relevant.

Across Banking, Energy, Telecommunications, Manufacturing, Retail and Government sectors, digitization is being leveraged to improve service delivery, enhance customer experience and drive operational efficiency. Banks in Africa and other businesses are developing strategies for harnessing nimble digital technologies, unrestricted mobile access and vibrant social media to attract and retain customers.

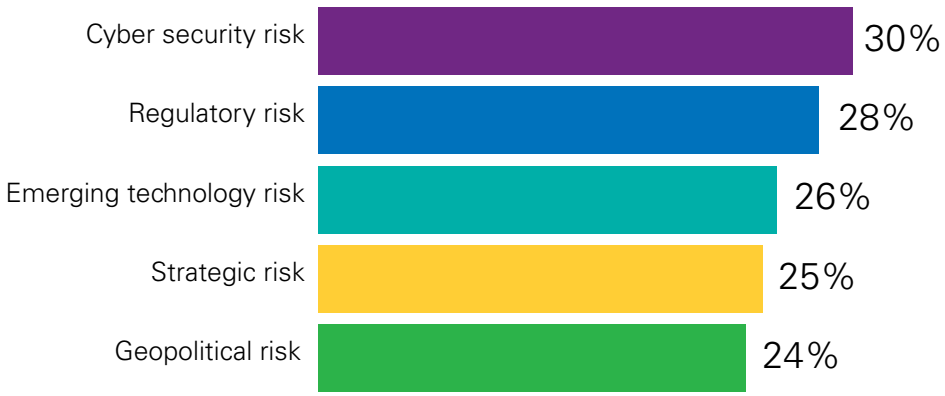
However, the digital evolution has introduced a new dimension into the enterprise risk landscape - the cyber risk. Unfortunately, cyber risk is not conventional, neither are the threat actors.

With the exponential growth of digital touchpoints, the new reality is this - Cyber Security now directly affects the resilience of organisations, our economy and our individual safety.

Global CEOs are beginning to acknowledge that the new wave of technological advancement comes with risks that cannot be ignored. Cyber security was the top risk named by Global CEOs (30 percent and up from the fifth highest ranked last year) in KPMG's 2016 Global CEO Outlook.

Organisations in Africa have also continued to face some of the cyber security challenges being faced by their counterparts in other parts of the globe. There have been instances of fraudulent transactions on different online banking platforms, successful DDoS attacks on some banks, attacks on websites of some government agencies, and identity theft. It is therefore obvious that the Africa business ecosystem is not insulated from the challenges being faced by businesses across the globe.

what risks are you most concerned about? (Top five)



Source: 2016 Global CEO Outlook, KPMG International

> The Internet has opened a new frontier in warfare: **everything is networked and anything networked can be hacked.**
>
> **- World Economic Forum Global Risk Report**

> **While organisations must view all major digital transformation initiatives through the cyber security lens, Cyber risk should not be an impediment to digital innovations but an advantage; if adequately managed.**
>
> **- KPMG**

“Every organisation should have a framework for assessing and analyzing cyber risks, and that framework should ideally be integrated into an organisations existing enterprise risk framework.”

- Malcom Marshal former KPMG Global Cyber Security Leader

“As digitization opens up innovative products & services with cost effective processes and enhanced customer experience, the ‘incumbents’ and the digital ‘disruptors’ must understand that the business risks will no longer be ‘conventional'.”

- KPMG

How prepared is your organization for a cyber attack?

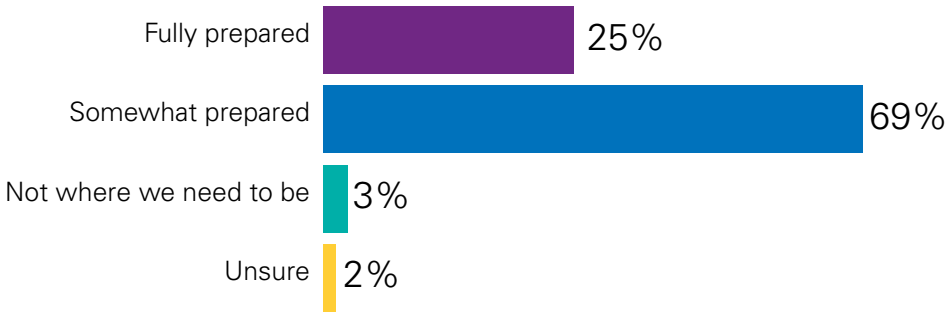
According to KPMG’s 2016 Global CEO Outlook, seventy-five percent of CEOs said they were not fully prepared for a cyber event, significantly higher than in 2015 (50 percent).

Board and executive management are increasingly aware that while they might not personally be the expert, they will be held accountable if there is a major cyber attack that disrupts business performance. They are beginning to recognize the need for senior people they trust to equip their organization to withstand potential cyber threats.

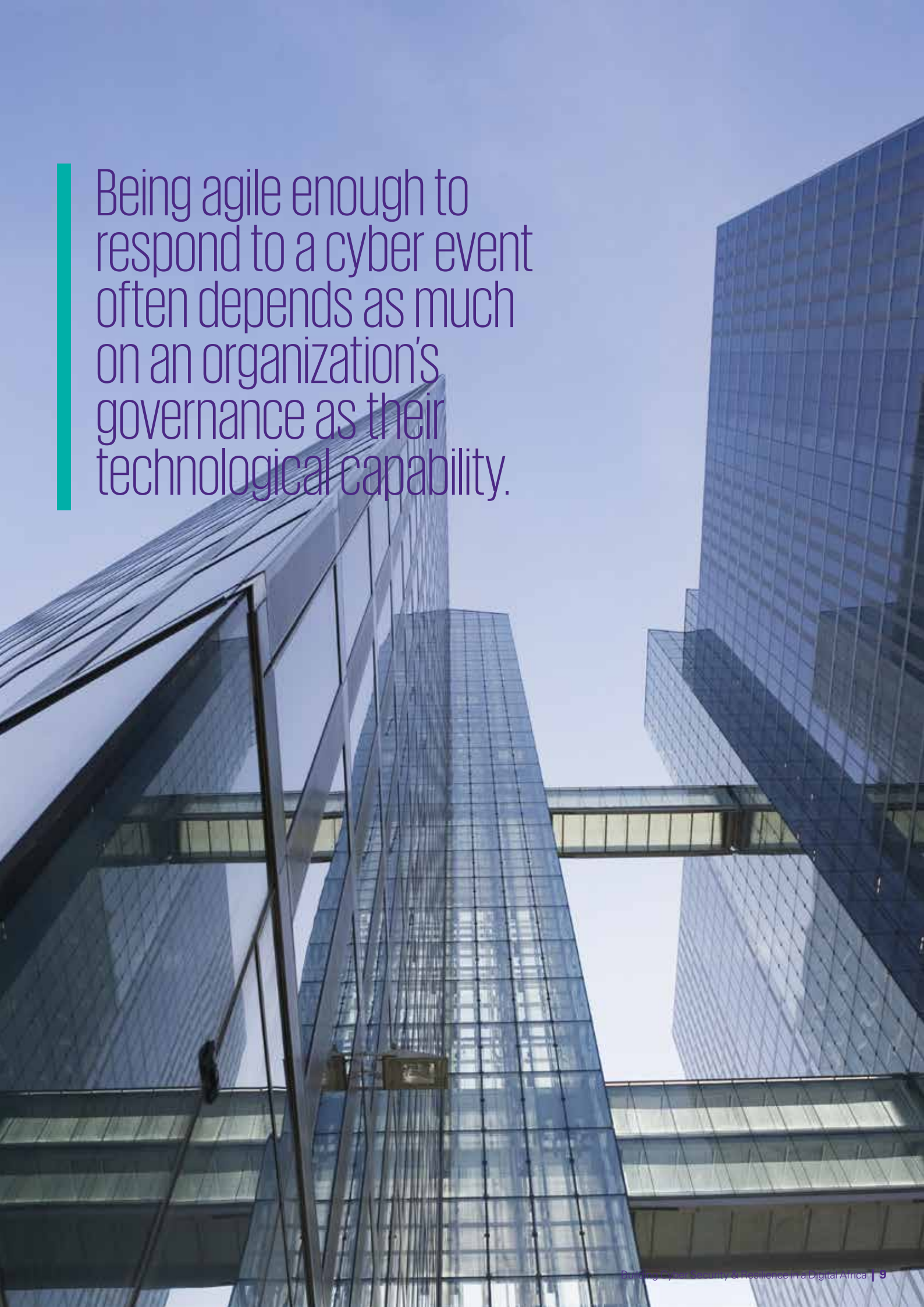
Companies will significantly improve cyber security and resilience by practicing or exercising their ability to respond to cyber events. Companies need to be agile and deal with the unexpected. Often, organizations that can deal with the unexpected in a business sense and have more effective governance are better prepared for cyber events. Being agile enough to respond to a cyber event often depends as much on an organization’s governance as their technological capability.

However, cyber security is not just a cost, it is also a revenue driver. There is a correlation between cyber security and growth/revenue. Organisations that have confidence in their cyber security capabilities are more confident to deploy new digital enabled services that drive growth.

How prepared is your company for a cyber event?



Source: 2016 Global CEO Outlook, KPMG International



Being agile enough to respond to a cyber event often depends as much on an organization's governance as their technological capability.

Do you really know the enemy?

Everything is changing - the technology, the attack surface, the risks as well as the consequences. The threat vectors are expanding; the attackers are developing offensive capabilities at a much quicker rate than organisations' defensive capabilities. The days of the script kiddies are over; the "dark net" is now much more organized with diverse support functions such as ''Sales and Marketing" and "R & D".

Attackers continue to operate in ever changing networks and alliances that disseminate knowledge at high speed. There has been an increase in the complexity, novelty and persistence of cyber attacks, with varying consequences for the digital business.

According to a Symantec survey released in 2016, 430 million new malwares were discovered in 2015 alone; which is 36% higher than 2014. As the cyber threat landscape is changing so should our approach to managing cyber risk evolve.

Organisations in Africa must have a clear understanding of the motivation, intent, strategy, tactics and the tools of the attackers in order to anticipate threats and effectively prepare for, prevent, detect and respond to attacks. Bespoke correlation of technical and non-technical information is a must.

Practice shows that few organisations have understood how to distill the relevant intelligence from the myriad information feeds available in and outside their organisation. This needs to improve urgently.

The Enemy

THE INSIDER

Intentional or unintentional

Motivation: Grudge, financial gain
Business impact: Reputational damage, financial loss, regulatory censure.

COMPETITORS

Competition or rivalry

Motivation: competitive advantage
Business impact: competitive disadvantage, reputational damage, information loss

ORGANISED CRIME

Global, difficult to trace and prosecute

Motivation: financial advantage, potentially opportunistic
Business Impact: financial loss, reputational damage, theft of information

HACKERS OR HACKTIVISTS

Attention or popular causes

Motivation: dynamic and unpredictable, potentially issue motivated
Business Impact: reputational damage, operational disruption information

STATE SPONSORED

Espionage and sabotage

Motivation: political and economic advantage
Business Impact: theft of information, operational disruption, financial loss

While classic cyber security challenges have not yet been mastered, new ones are emerging on the horizon

Who is in charge?

Global news headlines confirm that cyber-attacks are not a seasonal threat or dependent on specific industry or environmental attributes, but are constant and should therefore remain forefront in every executive's thought process. In recent years, cybersecurity incidents have continued to increase in frequency and impact to enterprises. The number of breaches targeting organisations are on the rise and the sophistication of attack methodologies is evolving. Each year, breaches headline the news with the resulting business impact such as loss of customer confidence, financial loss and, in some situations, the inability of an enterprise to recover leading to eventual shut down. It is clear that security breaches are not a remote threat any longer but are now fact and as such should not be seen as an operational technological issue, rather organisations should see it as a board-level strategic business risk.

In a recent survey conducted by KPMG, nearly a third of the CEOs identified cyber security as the issue that has biggest impact on their organisation today. Operational and Compliance risks were listed as part of the top risks.

However, it is obvious that cyber security if not properly managed becomes an operational issue and/or reputational concern very fast. Hence, there is a need for the board and top management to have a proper view of the cyber risks and their responsibility. Top management must also have a clear strategy for managing cyber risks. This strategy must provide clear direction for Cyber Security Governance, Operations and Architecture.

The other question that begs for answer is – ***Do those charged with cyber security possess the capability to effectively manage this risk?***

> **Financial institutions have a tradition of protecting assets and information and continue to invest heavily as a priority. The challenge they face is to ensure the areas where they are investing will deliver the protection their customers expect, and investing in the right capability to manage the business and risk profile in a sustainable way. Those who are able to conquer these two challenges will have competitive advantage to potentially become trusted custodians of customer data for additional online identity and privacy services.**
>
> **Jeremy Anderson,**
> Global Head of Financial Services, KPMG International and Partner, KPMG in the UK

Organisations are able to

46% remediate only of legitimate alerts received[1]

44% of operations managers see more than 5000 security alerts per day[1]

22% of breached organisations lost customers[1]

29% of breached organisations lost revenue[1]

23% of breached organisations lost business opportunities[1]

1. Cisco 2017 Annual Cyber Security Report

“80%
of data breaches originate from third party[1]”

“**Countering an evolving threat landscape requires board level leadership, insight and decision making**”

“**The Center for Strategic and International Studies estimated that cybercrime alone cost the global economy US$ 445 billion in 2015.**”

[1] Combating cyber risk in the supply chain, SANS 2015

With the spate of cyber attacks on some of the biggest brands, it is obvious that Boards that choose to ignore, or downgrade the importance of cybersecurity oversight responsibility, may be doing so at their own peril.

Investors, governments, and global regulators are increasingly challenging board members to actively demonstrate diligence in the area of cyber security. Regulators expect personal information to be protected and systems to be resilient to both accidents and deliberate attacks. Value chain partners expect a trustworthy and transparent approach to risks. And customers expect that services are available and data is protected when stored or processed by leading organisations.

Customer transactions and business processes are increasingly digitalized and often cross national borders, creating new risks. But more prominently, it also induces new opportunities.

Senior management can capitalize on these opportunities while limiting unanticipated risks by establishing effective cyber risk management from the top. This includes having a comprehensive overview of your business environment, potential targets and threat actors, current state of protection and legal and regulatory requirements.

Enterprises are dealing with attacks daily and they must be prepared to deal with adversaries that are evolving and motivated to achieve their goal. In order to address the threat landscape, enterprises must have continued focus on cybersecurity risk so they can achieve resilience when an incident does occur. Security has become a board and executive level issue.

When you analyze the available statistics on the known risks posed by cyber attacks, one would expect that corporate boards and senior management would be proactively taking steps to confront these cyber risks.

However, surveys suggest that there is a disparity between the value exposed due to cyber-risks and the resources, or lack thereof, which many corporate boards have deployed to address these risks. There is a clear need for corporate boards to pay more attention and commit more resources to addressing cybersecurity risk.

Although many CEOs worry about rising cyber risks, the ownership of and responsibility for the cyber risk is less clear. While there are many “C” level owners of the risk (CISO, CFO, CEO, CRO), each of these owners have differing but related interests and unfortunately often do not integrate risk or effectively collaborate on its management. Defining clear roles and responsibilities for cyber risk is crucial.

As the interest of the board is a positive indicator for security, so is the fact that executives are actively demonstrating support for the security program. While enterprise leadership appears to be concerned with security and has taken an increased level of interest in the impact that security has on the organisation, the reporting structure for security has not matured.

The security-related gaps that exist today within the enterprise can be overcome with a shifting of focus from state-of-the-art technology to state-of-the-art mindset, where the process is continually tested and allowed to evolve and mature. The first step is recognition that cybersecurity - and its role in delivering a trusted, digital experience - is one of critical importance to the entire enterprise.

Cybersecurity professionals are asking for help from management, in the form of staffing, training, and the ability to drive a culture of cybersecurity awareness throughout the ecosystem. The future of the digital enterprise relies upon the ability of cybersecurity professionals, working in tandem with business units, executives, partners, providers and end users to create an environment of digital trust where business can flourish.

Reducing the unconstrained operational space of adversaries, and making attackers' presence known, must be top priorities for defenders. The reality is that no one can stop all attacks, or protect everything that can and should be protected. But if the focus is on closing the operational space that cybercriminals must have for their campaigns to be effective and profitable, organisations can prevent them from reaching critical systems and data without entirely evading detection.

In order to address the challenges and the diversity of threats, CEOs and executive team members must drive a cultural shift that embraces cybersecurity. This requires the concept of cybersecurity to be woven into the business model with the near-term agenda focused on closing existing cybersecurity gaps in talent, technology, organisational parity, budgets, and management.

What CEOs and Executive/ Operational Management Should Do Today

Achieving a culture of cybersecurity awareness is of utmost importance in today's technological landscape. Failure to achieve it poses a strong risk to enterprise or corporate brand value. Taking this concept further, it's about developing a culture that enables and leverages digital trust. This must weave throughout the ecosystem of partners, both business and cybersecurity, including threat information sharing, proper mutual vetting of cyber preparedness, and a mechanism for rapidly piloting and implementing new cybersecurity technologies and processes[1]. In order for enterprises to foster a culture of cybersecurity and begin to move closer to a state of digital trust, they must recognize that state-of-the-art no longer applies to technology but to an adaptive, evolutionary approach to addressing all aspects of holistic security on an ongoing basis.

Here are five questions every enterprise should be asking today[1]:

- Are we properly allocating budget towards training and the smart use of automation to improve detection and response capabilities?
- Are we measuring the success, or value, of cybersecurity efforts correctly?
- Do we have a working process for the vetting and implementation of new technologies, including behavioral analytics, automation and cognitive, for inclusion in our cybersecurity architecture?
- Are we properly ensuring parity among our business units and between us and our ecosystem partners in terms of cyber security?
- Are we properly managing our migration towards a state-of-the-art cybersecurity approach that includes embedded and holistic security throughout the enterprise and a focus on enabling digital trust between business units, partners and consumers?

"Reports show that just 21% of chief information security officers (CISOs) report to the chief executive officer (CEO) or the board, while 63% report through the chief information officer (CIO). This reporting structure is unfortunate as it positions security as a technical issue rather than a business concern[1]."

"Cyber risk and the approach for managing it need not be a stumbling block to business innovations and digital transformation"

1. ISACA State Of Cyber Security 2017

Perspectives from South Africa

In a brief interview, Kaspar Euvrard, a Senior Manager in the IT Advisory unit of our KPMG South Africa firm discussed perspectives on cyber security and cyber threats with Justin Williams, Executive Director, Information Security, MTN. Below is an excerpt from this interview.

Do you feel your executive leadership is adequately aware of the current level and business impact of cyber risks to your company?

Yes. Security currently obtains the necessary air time from the executives and board sub committees, with inputs being obtained from both internal and external sources. Security is integrated into the Enterprise Risk and Business Risk management functions which work well together.

Do you feel your employees understand their role in cyber security?

This varies across areas of the business and by country. Security awareness and training is an ongoing programme to lift the level of security awareness across the business. We aim to show employees the impact of cyber security on their personal lives in order that they can better protect themselves in both a personal and work capacity.

What do you think about the level of investment required in the private sector to increase cyber security?

The investment required in security personnel and technology is high. Current economic conditions are tough across many industries so organisations are having to dig deep to make the necessary security investments. It may take a security incident or regulatory pressure for many organisations to obtain the necessary levels of investment.

How do you feel the Government and regulators can be proactive when it comes to cyber threats?

Over-regulation can be restrictive on economic growth in many markets, however, many organisations are tempted to take shortcuts in the information security space with the view that it is easier to pay the fine than make the required investments. Sensible proactive regulation can provide the minimum requirements for information security and ensure a level playing field while improving the situation for end customers who may not know the difference between secure and insecure products and services. This needs to be finely balanced.

How can the growing cyber security skill gap be addressed?

The skills shortage in information security is a well-documented global problem that is even more of a

challenge across Africa. Resources who gain the necessarily skills become increasingly mobile and may choose to move to more mature countries.

This said, it is a growing imperative for all organisations who require security skills to be contributing towards growth of the skills pool rather than simply poaching resources from other organisations, which while solving a short term challenge drives up cost. If all organisations were investing in intern and development programmes for security skills over time we could address the challenge.

In addition to tackling this from a resource investment point of view, it is necessary to clearly define the security processes and increasingly drive automation across these.

The emerging process robotics and cognitive processing fields could provide partial solutions by leveraging the existing security resources and is something to watch over the next 2-3 years.

Justin Williams has recently been appointed to head up information security for MTN across the Group. He was previously an executive director at EY responsible for Cyber Security, having spent 19 years with the firm in various IT and information security roles. Williams also led information security at Transnet for three years, where he established the function, defined the strategy and rolled out Transnet's information security programme for the group.

Government perspectives

The world today has been largely impacted by cyber space as a result of the heavy reliance on the Internet as a part of our daily lives. Across almost every aspect of human civilization, from banking, education, commerce, communication to governments, the Internet has engendered the metamorphosis of previously adopted conventional modes of business operations, simplified business processes and provided greater coverage such that no serious business outfit can fully blossom without taking advantage of this technology.

However, with the numerous benefits the Internet has provided, there are also inadvertent consequences as it has been leveraged by criminal minds in perpetrating malicious and sinister activities, including identity theft and electronic frauds. This continuous rise in cybercrime has led to the need for effective cyber security capabilities at national levels. The cybercrime landscape in Nigeria is also changing rapidly with threat actors growing in size, scope, complexity and capability over the past few years. Recent studies show that the number of Internet users has grown from less than a million in 2003 to over 80 million in 2016[1].

In response to the dynamic landscape and growing cyber threats, certain steps have been taken by the Nigerian government to ensure the protection, security and sustainability of the nation's active presence in cyberspace. Hence, cyber security has become an issue of national priority in Nigeria and now risen to the level of being handled by the Presidency through the Office of the National Security Adviser (ONSA)[2].

In 2004, the Nigerian government developed a framework for cyber security following recommendations by the Presidential Committee on Illegal Online Activities.

In 2013, the President approved the Nigerian Cyber Crime bill.

In December 2014, the Office of the National Security Adviser developed certain frameworks including the National Cybersecurity Policy and National Cybersecurity Strategy to provide cohesive measures and strategic actions towards assuring security and protection of the country's presence in cyberspace, safeguarding critical information infrastructure, building and nurturing a trusted cyber-community[3]. These frameworks are clearly focused on the protection of critical information infrastructure and the first step towards protection of critical assets is the identification of critical information infrastructure.

In his keynote address during the 'Stakeholders forum on Identification of Critical National Information Infrastructure' in November 2016, the National Security Adviser, Major General Babagana Munguno (Rtd) explained Critical National Information Infrastructure as "those equipment essential for a nation to function, which may directly or indirectly be connected to computer networks including computer networks controlling telecommunications, power generation and transmission, finance, oil and gas, water supply, transport, health, security and defence infrastructure"[4].

A Peek into the National Cybersecurity Policy

The national security threat landscape and its innate dynamism places a demand on the development of robust frameworks and policies to engender the capacity to respond to incidents; one of such is the National Cybersecurity Policy. The National Cybersecurity Policy has identified five key cyber threats as posing significant challenges to Nigeria and inimical to national growth and security.

> "With over 56 million Nigerians on the internet daily, digital technologies and the internet have become the backbone of the Nigerian economy."
>
> **- Fmr. Chairman, EFCC, Ibrahim Lamorde**

> "Activities of hackers and cyber criminals in recent times have threatened government presence, economic activities and security of Nigerians and vital infrastructure connected to the internet."
>
> **- National Security Adviser (NSA), Maj-Gen. Babagana Munguno (rtd)**

1. Key Note Address For Stakeholders Forum On Identification Of Critical National Information Infrastructure by the National Security Adviser, General Babagana Munguno (Rtd) on 24 November 2016
2. International Journal of Cyber Criminology Vol 9 Issue 1 (National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis by Oluwafemi Osho & Agada D. Onoja)
3. National Cyber Security Strategy
4. https://cert.gov.ng/publications/nsas-key-note-in-the-cnii-forum

“The estimated annual cost of cybercrime to Nigeria is 0.08 percent of the country’s Gross Domestic Products (GDP), which represents about

₦127 billion

–- National Security Adviser (NSA), Maj-Gen. Babagana Munguno (rtd)”

Over 90 million internet subscribers in Nigeria in November 2016

- Nigerian Communication Commission

Identification and assessment of these threats is fundamental to the establishment of effective policies and they include:

Cybercrime: This encompasses all forms of cyber assisted criminal activity such as cyber stalking, cyber bullying, identity theft, computer-aided forgery, email scams, virus dissemination and malware attacks[1].

Cyber-espionage: This is synonymous to modern day spying and it involves the use of computer networks to gain unauthorized access to confidential information, typically held by a government or an organisation.

Cyber conflict: Cyber conflict is the use of computers and associated technologies to disrupt the activities or information network of a state or organization for strategic or military purposes[2].

Cyber-terrorism: This is the convergence of terrorism and cyberspace, and it means unlawful attacks and threats of attack against computers, networks, and the information stored therein to intimidate or coerce a government or its people in furtherance of political or social objectives[3].

Child online abuse & exploitation: This involves all forms of activities which take advantage of the timid nature of children by preys over the internet.

Hence, there is a need to protect the National cyberspace and foster harmonious, sustainable and integrated readiness and coordination capacities towards mitigating the nation’s risk exposure in cyberspace.

What purpose does the Cybersecurity Policy intend to fulfil?

The cybersecurity roadmap consists of several objectives some of which have taken root, while others are yet to be accomplished, ranging from the establishment of legal frameworks around the cybersecurity ecosystem to increasing the cybersecurity awareness level among the citizenry. Some of the objectives are listed below:

- To develop security and control mechanisms for ensuring the protection and safety of Nigeria’s national critical information infrastructure.
- To develop a centralized national emergency readiness and incident management coordination capability.
- To develop a national mechanism for the establishment of a National Cybersecurity Coordination Center (NCCC) to serve as the focal point for cybersecurity incident monitoring and response and coordinate and regulate Sectoral Computer Emergency Response Team (S-CERT).
- To promote and engage cybersecurity innovations through research and development in partnership with industry and academic institutions.
- To develop a framework for inter-agency collaboration on combating cybercrime and cybersecurity.
- To develop a coordinated national awareness strategy, capacity building, and structured cybersecurity professional cadres across all national constituents[4].

1. International Journal of Cyber Criminology Vol 9 Issue 1 (National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis by Oluwafemi Osho & Agada D. Onoja)
2. https://www.rand.org/topics/cyber-warfare.html
3. Symantec, 2003. Cyberterrorism? by Sarah Gordon, Senior Research Fellow Symantec Security Response
4. National Cybersecurity Policy

Although, the development of this Policy is a huge step in the right direction, the Policy is expected to be an active living document, as a purposeful and operational cyber security policy would engender the realization of reduced successful cyber incidents on a national level and would provide the country with the direction towards prevention of such attacks and to swiftly address them in the event of their occurrence.

National Cyber Security Strategy

As a framework for facilitating the implementation of initiatives in the Cybersecurity Policy, the Cybersecurity Strategy document outlines the actions government and other players alike will take to lessen the risks and secure the gains of Nigeria's continuous dependence on cyberspace, by recognizing three key approaches to a successful national cybersecurity program:

- public private sector partnership;
- multi-stakeholders engagement; and
- international cooperation.

Certain strategies to be adopted in implementing measures in the Cybersecurity policy are as follows:

1. The development and implementation of appropriate legal framework, with initiatives that will allow for the identification and prosecution of cybercrimes that impact Nigeria regardless of whether they originate within Nigeria or are launched from outside of the country.

2. Establishment of a National Incidents Management Strategy which facilitates the commissioning of a National Computer Emergency Response Team (CERT) and introduces the roadmap for implementing detective, preventive and response capabilities to deal with cybercrime activities.

3. The strategy for protecting critical information infrastructures including shared responsibility between government and owner operators of critical infrastructure.

4. The development of information security assurance and monitoring plan, which includes a new national mechanism on cybersecurity assurance, adoption of fit for purpose standards for Governance, Risk and Control, Core Assurance Capabilities, National Enterprise Architecture Framework.

5. The introduction of a sustainable strategy to develop, maintain and ensure Nigerians are informed and equipped to deal with cybersecurity events by establishing a mechanism for Cybersecurity Skill and Manpower Development initiatives

6. The strategy for protecting Nigerian Children from Online Child Exploitation and Sexual Abuse includes initiatives, such as the national awareness programmes through multi-stakeholder engagement, and international cooperation in the countermeasures.

7. Adoption of a framework for a public and private partnership in developing a cohesive response to mitigating cyber-risk[1].

Cybercrime Act

In response to the various requests and demands from concerned stakeholders in both the ICT and legal sectors, the Cybercrime (Prevention, Prohibition etc.) Act was signed into law on May 15, 2015. The Cybercrime (Prohibition, Prevention, etc) Act, 2015 provides a legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria[2].

The cybercrime act details over thirty (30) cyber related offences as well as associated penalties. These offences include cyber terrorism, identity theft and impersonation, electronic cards related frauds, failure to report cyber threats, cyberstalking amongst others, with several punitive measures including fines and/or jail terms.

One wonders the extent to which private and public entities are aware of the content of this act especially the obligatory and protective requirements, as well as Nigerian citizens who are frequent users of cyber space. For instance, the cybercrime act requires that "any person or institution, who operates a computer system or a network, whether public or private, must immediately inform the National Computer Emergency Response Team (CERT) Coordination Center of any attacks, intrusions and other disruptions liable to hinder the functioning of another computer system or network, so that the National CERT can take the necessary measures to tackle the issues"- Section 21 Subsection (1).

The Act further goes to state that "Any person or institution who fails to report any such incident to the National CERT within 7 days of its occurrence, commits an offence and

1. National Cybersecurity Strategy
2. Cybercrime (Prevention, Prohibition etc.) Act

> **In line with fostering the growth and development of cyber security response mechanisms and intelligence gathering across sectors within the country, KPMG Nigeria is flagging off a cyber security incident reporting portal ('cybersec iReport') that provides a medium for anonymous reporting of cyber security incidents in both private and public organisations.**

shall be liable to denial of internet services. Such persons or institution shall in addition, pay a mandatory fine of NGN2,000,000.00 into the National Cyber Security Fund" – Section 21 Subsection (3).

While the issue of reporting cyber security incidents is very critical to ensuring adequate preventive measures are implemented across different sectors on a national scale, it is also important to ensure that appropriate capabilities, response mechanisms and associated policies are developed and enforced locally within private and public institutions. Furthermore, organisations that submit such reports need sufficient assurance that sensitive details in such reports such as IP addresses, attack vectors and extent of damage are kept confidential by the National CERT.

In addition to cyber offences and penalties, the Cybercrime Act also focuses on duties of financial institutions regarding records retention and protection of data.

Implementation and Enforcement Strategies

Although the National Cybersecurity Policy and Strategy outline several requirements and initiatives for dealing with cybercrime and protecting critical information infrastructure, it does appear that these initiatives have either not been properly prioritized for implementation or they have been inadequately implemented.

Frameworks and capabilities that ensure adequate incident and emergency response are critical and must be properly established in order to deal with cybersecurity incidents, as the issue is no longer 'if' but 'when' these incidents do occur.
For example, in order to ensure adequate response to security incidents, the National Cybersecurity policy highlights the need for information sharing to be facilitated by Sector-based Computer Emergency Response Teams (CERT).

However, there is currently no known policy that enforces the reporting of cyber-attacks within institutions of the Nigerian economy, neither is there a known database or repository of information on cyber related attacks or detected indicators of compromise across sectors in the Nigerian economy, particularly the financial services which has been a known target by cyber criminals.

In line with fostering the growth and development of cyber security response mechanisms and intelligence gathering across sectors within the country, KPMG Nigeria is flagging off a cyber security incident reporting portal ('cybersec iReport') that provides a medium for anonymous reporting of cyber security incidents in both private and public organisations.

E-governance initiatives

Developments in Information and Communication Technology (ICT) have also impacted the process of governance in the world today, such that governments have adopted e-governance technologies in service delivery and to manage the affairs of government for the benefits of citizens. E-Governance is the application of the internet, web and telecommunications services in the administration of public services.

Many government organisations have since adopted this technology, which is aimed at enhancing government operations to ensure greater efficiency, effectiveness, transparency and accountability.

In Nigeria, a number of projects which are focused on employing ICT initiatives in connecting communities, vital agencies, institutions of Government and educational

institutions at all levels have been pursued by the government.

Some components of e-governance have already been implemented in Nigeria as the government seeks to utilise e-government in providing services to citizens, businesses and foreign nationals. For example, under the health, education, transportation, finance and agriculture sectors, a number of e-governance initiatives are evident. Citizens can obtain relevant information on the National Health Insurance Scheme (NHIS), perform tax payment registration, register businesses, and so on, while foreigners can process immigration requirements. In addition, some other state governments in Nigeria have launched official state websites so as to provide relevant information to citizens on ongoing and proposed projects, project fees and timelines, as well to enable them participate in the decision-making process of government.

Another aspect is the adoption of social media which is being used to a large extent by government agencies in providing information on government activities and receiving feedback from the public.

Despite the opportunities e-governance offers, it also introduces new challenges. One of the key factors affecting the implementation and success of e-government in a country is the ICT literacy level among the citizens. Although with the rise in adoption of mobile devices among the citizenry, it appears that Nigeria is making progress in the area of Internet penetration, but a lot still needs to be done.

While there is much hype about ICT among the younger generation, overall the awareness among the citizens about ICTs is low, and as such it limits the extent of appreciation and adoption of e-government services.

Similarly, the utilisation of social media as part of e-governance is not without certain challenges, hence, the government must be well-prepared to deal with these challenges and scenarios that could potentially come up. This implies having comprehensive risk management systems, clear escalation procedures and strict behavior guidelines for social media communities.

Furthermore, the risks associated with the adoption of e-government services also bring to bear the question: **Can the government protect itself from hackers?**

In the recent past, there have been attacks on several websites owned by the Nigerian government, including that of the Nigeria Security and Civil Defence Corps (NSCDC)[1] and Independent National Electoral Commission (INEC)[2]. Recent reports reveal that according to the Nigerian Information Technology Development Agency (NITDA), out of the 2,175 Nigerian websites hacked in 2015, 585 were government owned. This underscores the need for government to take very important steps to curb this growing threat, and one of the ways to deal with this is for government to treat cyber security as a critical national issue.

Cyber security should be embedded into the ICT procurement approach, to ensure that adequate security standards are adhered to in the development of web applications, as web service developers and providers are mostly focused on functionality and delivery and less on security.

In addition, given the investment and efforts of private sector establishments in combatting cyber crime, government should consider harnessing some of this expertise and experience through collaboration. If done properly, collaboration can bring in fresh ideas and approaches to providing more secure platforms.

> **A total of 585 government-owned websites were among the 2,175 Nigeria websites hacked in 2015**
>
> **- Dr Isa Pantami (DG, NITDA)**

> **Nigerian banks, others lose billions to North Korean cyber attackers**
>
> **- Kaspersky**

1. http://theeagleonline.com.ng/recruitment-fraudsters-hack-nscdcs-website/
2. http://www.premiumtimesng.com/news/top-news/179539-inec-website-hacked.html

Perspectives from Ghana

Key Developments

National Cyber Security Policy & Strategy

The policy was established to assist the country in the fight against cybercrime.

The Bill was passed in 2016 and brings stakeholders from the public and private sectors, industry, civil society, and the international community together to work towards a more secure cyber space for Ghana.

Security Governance Initiative (SGI)

In February 2016, The United States and Ghana signed the Security Governance Initiative (SGI) Joint Country Action Plan agreement which provides a comprehensive roadmap to improve Ghana's capacity to address security threats with regard to cyber security, maritime security, border surveillance and control.

An amount of US$ 65 million has been dedicated to the initiative in its initial year and includes five other African countries; namely, Nigeria, Niger, Mali, Kenya and Tunisia

National Cyber Security Council

In March 2017, the Government of Ghana, through the Minister of Communications, Mrs Ursula Owusu-Ekuful, disclosed its plans to establish a National Cyber Security Council to address the surge of cybercrime in Ghana. The initiative is geared towards building a more comprehensive cyber security governance structure with the inclusion of key public and private sector stakeholders.

The National Cyber Security Council will be an independent body made up of public and private parties who will advise Cabinet on digital security.

NITA CERT

The National Information Technology Agency (NITA) has established a Computer Emergency Response Team (CERT) to provide education and awareness programs and manage cyber security incidents that occurred in Ghana's cyber space.

More capacity building and awareness creation activities are set to begin in 2017 under the Security Governance Initiative (SGI).

National Data Centre

The National Data Centre was opened to private businesses in Ghana in January 2016. The facility, classified as a tier three data centre, was built by the Government of Ghana to enhance the efficient delivery of government's services and promote use by the private sector to deseminate local content in a secure environment.

The Centre also provides businesses with the opportunity to rent space to co-locate their computer systems. The primary data centre is located in Accra with a backup site in Kumasi. It is currently managed by NITA along with partners such as Huawei and Alcatel.

Sources:
1. www.nca.org.gh/regulatory-framework/legislations/
2. www.moc.gov.gh/sites/default/files/.../Electronic%20Communications%20Act-775.pd.

Looking Ahead

For Ghana to stay ahead of the threat curve, there is the need to continually invest in research, implement and comply with relevant cyber security laws and regulations, build capacity in the subject matter and cultivate a vibrant IT security ecosystem within our unique environment.

1. **Implement & Enforce Relevant Cyber Security Regulations:** This could be achieved through the enforcement of privacy and cyber security laws and through investments made in cybercrime investigation and defense.

2. **Harden Security of IT Infrastructure and Platforms:** Public and private institutions need to harden (i.e. improve security controls on) their IT infrastructure and platform to enhance the resilience of their key systems to combat information security threats.

3. **Build Capabilities in IT Security:** IT practitioners and consultants need to enhance their competencies in IT security. This will ensure that there is greater adoption of essential security practices among IT professionals to manage IT security risks.

4. **Cultivate Vibrant IT Security Ecosystem:** Ghana needs to establish local research on IT security issues. Such research will enable the government agencies, universities and IT security hubs etc. to develop a vibrant IT security ecosystem which will strengthen Ghana's ability to protect its IT infrastructure and platforms.

Perspectives from Kenya

KPMG East Africa's Technology Advisory team led by Gerald Kasimu, Partner and Head of IT Advisory interviewed Dr. Katherine Getao, ICT Secretary, Ministry of ICT, State Department of Broadcasting and Telecommunications at her office, Nairobi Kenya.

Below is the excerpt of this interview.

Cyber security is a real threat across the world and increasingly so in Africa. What is the current state of cyber security in the Kenyan government? Especially given recent cases of cyber-crime that are reported in the local dailies?

There is no government exempt from cyber attacks, even the governments of the most technologically-advanced countries! Governments everywhere are a target and no one can claim to be capable of fully protecting themselves from all the threats emerging in the cyber space. Cyber criminals are looking for information, financial gain, to advance a specific agenda or for opportunities to embarrass a government.

A critical component of cybersecurity is the level of governance in place and therefore the effectiveness of processes for making diplomatic, operational and technical decisions necessary to achieve Cybersecurity. For example, I represent Kenya in the UN's Group of Governmental Experts on Cybersecurity which focuses on state-to-state conflict. The group looks at capacity building, emerging threats and risks at a global level and how these threats can be minimised across states. State-to-state conflict is perceived to be the most dangerous form of cyber risk and this is because states have the resources necessary to do the most harm.

There are four African countries represented in the current UN group session of 2016/17: Botswana; Egypt; Senegal and Kenya. In the previous session of 2014/15, Kenya received a special mention alongside Pakistan and UK for its contribution.

How does a country get to participate in the UN's Cybersecurity Group? Is it by appointment or election? And how do we benefit as Kenya and Africa?

Participation in the UN's Cybersecurity Group is by appointment by the UN Secretary General. The previous session included the following African countries: Egypt, Ghana and Kenya. Kenya is one of the eight countries globally, that was reappointed to the current session.

Although Africa is not considered high risk with regards to state-to-state conflict, research shows that there are many countries which are in the process of developing technology for cyber war. Africa needs to be prepared, because we could be involved in cyber conflict either directly or through being used as a proxy.

It is therefore important for Kenya to participate in the global conversation on cybersecurity as we are a relatively technologically-advanced African nation with good telecommunications infrastructure. One tangible risk is that this infrastructure could be used to

Dr. Katherine W. Getao serves the Government of Kenya as the ICT Secretary, the strategic head of ICT in Kenya. In 2014 and 2015 she was an active member of the United Nations Group of Governmental Experts in the field of security in the context of information and communication technology.

Dr. Katherine Getao was appointed the ICT Secretary in charge of the eGovernment Directorate in August 2010. The eGovernment Directorate was the strategic advisor on ICT issues to the Government of Kenya and manages the ICT operations of the government.

wage war by proxy thus opening Kenya to the risk of reprisal attacks.

Being part of international cybersecurity processes helps Kenya to be knowledgeable about emerging risks and threats and to identify ways in which to mitigate cyber threats. While Governance is recognized as an important element of cyber security there is a tendency to under-prioritize it in favour of building technical capacity.

The Kenyan government is taking Cybersecurity governance seriously and and has formed the necessary leadership structures to take charge of our security.

What are African countries governments doing with regards to Cyber security?

The African Union has recognized the importance of cyber security threats and has published an 'African Union Convention on Cyber Security and Personal Data Protection'. The convention is about two or three years old and a few countries have already ratified it.

The slow pace of ratification may be due to the need for each country to assess the Convention's legal, technical and economic impact in context. Kenya has thriving ICT innovation and a strong ICT private sector and we carefully assess all international instruments to ensure that they will have a positive impact on business and innovation in the country.

The East Africa community has a programme on Cybercrime. The Northern Corridor Infrastructure Programme, involving Kenya, Rwanda, South Sudan and Uganda as members, and a number of other Eastern African countries as observers, also has a strong interest in Cybersecurity, with Rwanda perhaps taking the lead as they have developed a state of the art Cybersecurity Centre.

Which government agency is in-charge of cybersecurity in Kenya?

Security in Kenya is governed by the National Security Advisory Committee (NSAC) which is chaired by His Excellency the President of Kenya. Since 2015 NSAC has had a Cybersecurity Subcommittee. The Subcommittee was initially chaired by the Ministry of ICT, but has more recently been chaired by the Ministry of Interior and Coordination of National Government. Therefore, as you can see, Cybersecurity is governed by the top echelon of Government in Kenya.

Operationally, the Cybercrime function sits in the Ministry of Interior and Coordination of National Government, which makes a lot of sense since this is a coordinating Ministry and cybercrime is multi-faceted and multisectoral, and it also hosts the various internal security organs such as the police and intelligence services. However, you should note that the Ministry of Interior works closely with the Ministry of ICT and the Department of Defence in the fulfilment of this function.

In 2014, His Excellency the President of Kenya, Hon. Uhuru Kenyatta, launched the National Cyber Security Strategy. The strategy is drawn from the National Cybersecurity Master Plan which covers all the strategic, tactical and operational issues necessary to maintain cybersecurity.

At the operational level Kenya's National Computer Incident Response Team – Coordination Centre (National KE-CIRT/CC) based at the Communications Authority monitors the national gateways and infrastructure, while a smaller CIRT based at the ICT Authority focuses on the public sector infrastructure and systems.

Speaking of private sector, how does the government interact with the private sector on cyber security matters?

It is a tenet of the values of Kenya as enshrined in Article 10 of the Constitution of Kenya 2010 that the public sector must involve all relevant stakeholders in its policy and decision-making. I also note that, as is the case across the world, most of Kenya's ICT infrastructure and systems are owned and operated by the private sector. Kenya is also a strong proponent of public - private partnerships, and indeed the TEAMS submarine optical fibre cable which connects Kenya to the Middle East was built through such a partnership. Lastly, Kenya connects its National and County Governments through a web of wide area networks, which used private sector infrastructure in part.

Thus, it makes sense for the Government to collaborate closely with the private sector because it is

consistent with our national values, our obligation to protect both private and public critical infrastructure, our strategic interest to forge partnerships between the public sector and the private sector and our determination to achieve end-to-end security on a multi-protocol, multi-channel wide area network which uses both public and private infrastructure.

We work together with the private sector in a number of ways including:

a. We often include private sector representatives on our task forces when drafting laws, regulations or policies. We always include the private sector in the stakeholder consultations for such guiding documents;

b. We procure nearly all our ICT infrastructure, goods and services from the private sector and we work closely with them in to successfully implement projects and to maintain infrastructure, applications and services;

c. The latest draft of the ICT Policy which shall shortly be published has as one of its five guiding principles "Private sector first." This exemplifies the determination of the Government of Kenya to create jobs and build wealth by supporting a strong private sector.

d. We enhance Kenya internet security through KE-CIRT/CC which is under the Communication Authority of Kenya. The team behind KE-CIRT/CC is a collaboration between the Government and private sector industry associations representing keys sectors such as telecommunications, internet service providers and banking and financial services.

e. The private sector also independently prepares a number of cybersecurity reports as well as commentaries, social media blogs and visits to relevant Government organs to discuss specific issues. The Government carefully considers all inputs from the private sector and indeed H.E. the President holds a regular round table meeting with the Private Sector during which each Ministry considers and responds to all issues raised.

By collaborating with the private sector the Government ensures that it has the best resources available to monitor and detect cyber security threats. Even the most recent cyber security incidents in government were in areas of known vulnerability.

Are there regulations in place on data protection and privacy?

There is a Data Protection Act that has been in process for several years. The first draft was conceptualized at a time when Kenya was positioning itself as a Business Process Outsourcing (BPO) destination. Since then Kenya, alongside our East African partner countries, has continued to gain knowledge and skills and mature in the development and use of ICTs and we currently have an enhanced understanding of data protection requirements in the light of emerging initiatives such as the One Network Area (seamless mobile telecommunications between Kenya, Rwanda and Uganda.) I think that the new draft is much more coherent with our current context and will be more robust towards future regional developments in ICT.

In 2015 Kenya drafted a Critical Infrastructure Protection legislation to provide the necessary protection to the

"Ethics is also the key towards having a selfless government working for the interests of its people. Without ethics, good governance will continue to be a challenge and a moving target."

roads, bridges, energy infrastructure and telecommunications network that have become so necessary to our social and economic life. This bill is also in process sponsored by the Ministry of Interior. Another important bill that is in process sponsored by the same Ministry is the Cyber and Computer Crimes Bill. The Access to Information Bill defines the extent of information access mandated by Article 35 of the Constitution of Kenya 2010. These four pieces of legislation, taken together provide the backbone of data protection and privacy legislation.

Beyond this, the Ministry of ICT is in the process of developing an information security policy for the public sector to standardize information security policy and practices across government organs. The policy will be open for adoption by the private sector, and indeed those transacting with Government will be expected to follow the same rules.

Does the Ministry of Interior and Coordination of National Government have the critical mass and man power to implement these acts?

As mentioned before, the Ministry of Interior and Coordination of National Government is appropriate because it is a coordinating ministry which helps many ministries to work seamlessly together to achieve our national goals.

It is also the ministry that hosts internal security organs. Through the Cybersecurity subcommittee of NSAC and other internal operational processes, the Ministry works closely with other ministries which have aspects of the technical and operational skill necessary to complete the picture including, of course, the Ministry of ICT, the Department of Defence and the Ministry of Foreign Affairs. I am not by any means claiming that there is no room for improvement in our governance and operations, but I believe that we have made a good start and we are going in the right direction.

What are your final comments?

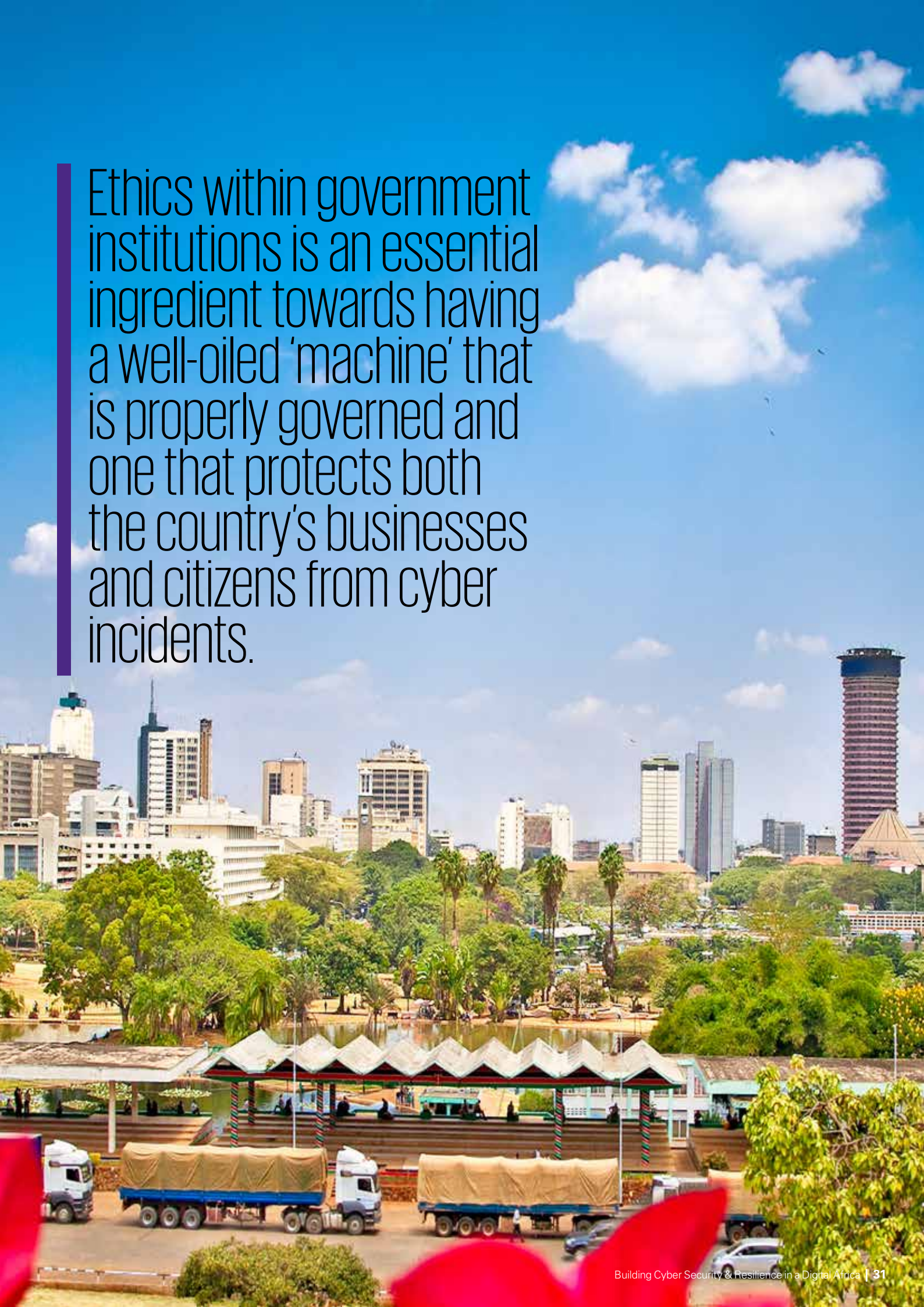
Governments are continuously building capacity in the areas of cyber security. Hackers can no longer feel comfortable as they know they can and will be caught for cyber related crimes. However, a lack of effective governance, or entrenched informal ways of doing business. What I would call the matatu ideology (*matatu – an informal public transport system shrouded by lack of structure and discipline) can severely impact effective achievement of cybersecurity - even when there are strong technical incident response arrangements.

Ethics within government institutions is an essential ingredient towards having a well-oiled 'machine' that is properly governed and one that protects both the country's businesses and citizens from cyber incidents.

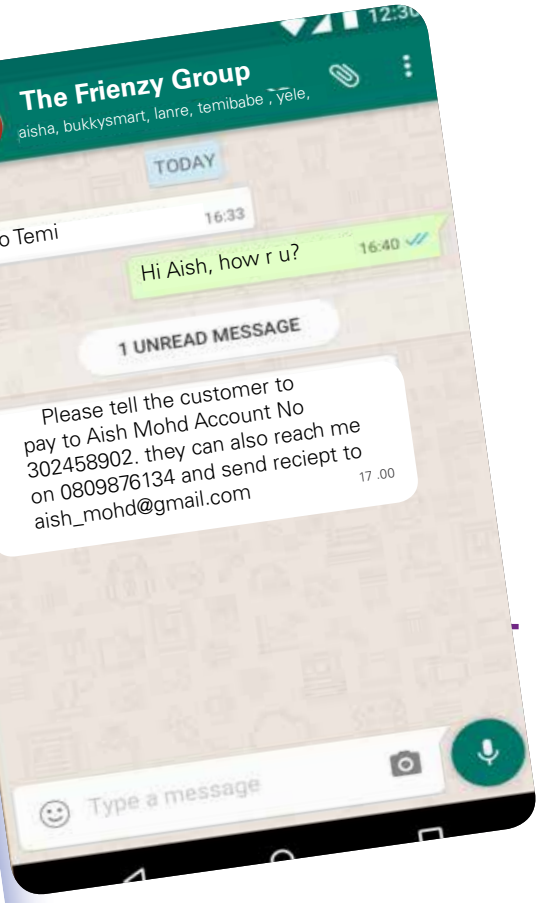
Ethics is also the key towards having a selfless government working for the interests of its people. Without ethics, good governance will continue to be a challenge and a moving target.

Ethics is primarily based on the values held by individuals and the society as a whole, it does not come entirely from Government. The Ministry of ICT continues to work closely with professional associations and others to ensure that ICT in Kenya is founded on ethical beliefs and practices, and to support the work of agencies that ensure that Kenyan children approach digital technology with the right values from inception.

Ethics within government institutions is an essential ingredient towards having a well-oiled 'machine' that is properly governed and one that protects both the country's businesses and citizens from cyber incidents.

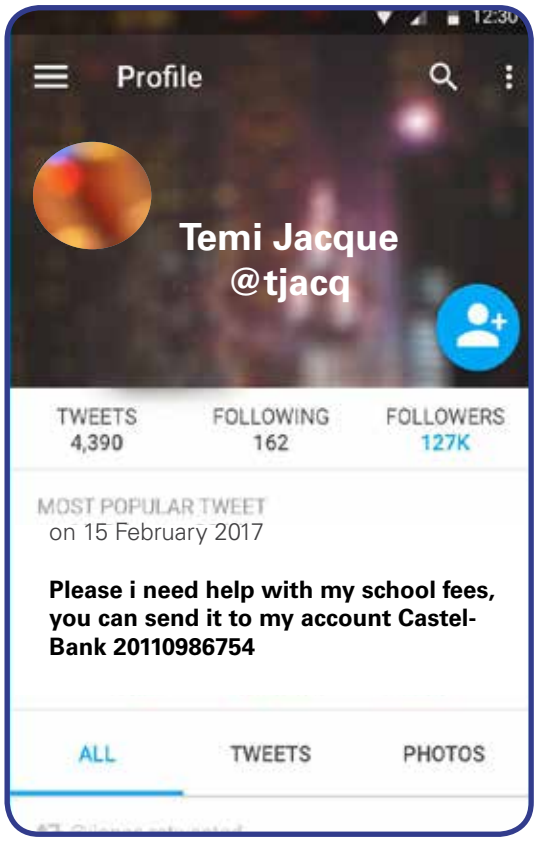


How it affects you


The Frienzy Group
aisha, bukkysmart, lanre, temibabe, Yele,
TODAY
o Temi
16:33
Hi Aish, how r u?
16:40
1 UNREAD MESSAGE
Please tell the customer to pay to Aish Mohd Account No 302458902. they can also reach me on 0809876134 and send reciept to aish_mohd@gmail.com
17 .00
Type a message


Instagram
Temi Jacque
55s
76 likes
Temi Jacque my kids at their school at lekki penisular, the best school ever and most expensive.


89% 22:51
Temi Jacque
Added Me
Add Friends
My Contacts


Profile
Temi Jacque
@tjacq
TWEETS
4,390
FOLLOWING
162
FOLLOWERS
127K
MOST POPULAR TWEET
on 15 February 2017
Please i need help with my school fees, you can send it to my account Castel-Bank 20110986754
ALL
TWEETS
PHOTOS

The US Department of Health and Human Services

Records breached:
5 million names and Social Security numbers
Year: 2016
Why was it big: It was done by breaking into the office and stealing a personal computer containing the records.

Yahoo

Records breached:
500 million accounts which include names, email addresses, telephone numbers, dates of birth , hashed passwords
Year: 2016
Why was it big: In December 2016, Yahoo also announced a breach which occurred in 2013, where about 1billion accounts were hacked.

LinkedIn

Records breached:
167 million accounts which include usernames, passwords, emails
Year: 2016
Why was it big: It had previously reported a data breach in 2012 when 6.5 million encrypted passwords were posted on a Russian site.

DropBox

Records breached:
68 million user accounts which include email addresses and passwords
Year: 2016
Why was it big:
It had previously reported a data breach in 2012 where user email addresses and passwords were leaked.

Turkish Hospitals

Records breached:
10 million records of patients' sensitive personal and medical information
Year: 2016
Why was it big: The hack was in retaliation against the hacking of 2 American hospitals

Federal Bureau of Investigation, Department of Homeland Security

Records breached:
30,000 records of FBI & Department of Homeland Security
Year: 2016
Why was it big: It was done by hacking into a Justice Department email and then posing as a new employee who needed help navigating the web portal.

Ashley Madison

Records breached:
37 million accounts which include passwords and other personal information
Year: 2015
Why was it big: Attackers posted personal information of customers seeking extramarital affairs with other married persons which led to embarrassments and suicides.

Premera Blue Cross

Records breached:
11.2 million accounts
Year: 2015
Why was it big: A broad range of customer data may have been exposed, ranging from medical records and bank account information to Social Security numbers and dates of birth

News Flash

Hacking Team

Records breached:
1 million records - 400GB of files including zero day exploits, source code, list of customers and emails
Year: 2015
Why was it big: Full list of customers including governments, banks and intelligence agencies who bought attacking tools from Hacking Team and how much it was bought was leaked.

Slack

Records breached:
500,000 email addresses and other personal account data (phone number, skype ID, etc)
Year: 2015
Why was it big: Slack is a popular online collaboration platform with which businesses work on critical projects where security is a must.

Experian/ T-Mobile

Records breached:
15 million user accounts
Year: 2015
Why was it big: T-Mobile uses Experian to process credit applications. This type of incident exploits trust that businesses have amongst themselves and how customers are affected by lapses of companies they do not deal with directly.

Sources:
1. http://www.crn.com/slide-shows/security/300083246/the-10-biggest-data-breaches-of-2016.htm
2. http://www.crn.com/slide-shows/security/300079193/the-10-biggest-data-breaches-of-2015.htm

How it affects you

With all the connected devices we carry about daily, the world has indeed gone digital. Our lives, economic vitality, national security amongst others, now revolve round technology.

This high and inevitable dependence on technology ushers in a whole new set of threats, to individuals, businesses and the society at large. Computers and networks are being misused at a growing rate by cybercriminals and users. Now, more than ever, we need a stable, safe and resilient cyberspace.

Mobile Devices

In the past two decades, we have seen technological advances in mobile devices from personal data assistants (PDAs) to smartphones such as iPhone 7, Samsung Gear and Google Pixel[1]. As Smartphones have become more technologically advanced, intuitive and cheaper, leading to phenomenal increase in consumer adoption. Sensitive information such as contact details, business information, social media accounts, pictures and videos are stored on smartphones.

Apps are rapidly becoming the primary channel for engaging with customers and employees. People expect the apps they installed to be secure and to respect and protect their privacy. But many organizations struggle to get a grip on their apps' security and privacy postures, whether apps are built by third parties, developed in-house, or purchased off-the-shelf.

Mobile devices are hyperconnected hubs on which information is stored, communicated and made accessible to end-users. Many users operate and connect to a multitude of unknown and untrusted networks and peripherals. Being able to trust the device as being a secure platform 'out there in the world' is very critical.

Given that mobile device users do not actively demand for security on mobile devices, coupled with user preferences for storing personal information such as contact details, pictures, social media accounts and other documents on these devices due to convenience, cyber criminals have found mobile devices to be very attractive for perpetrating malicious acts.

These threats can be broadly classified into web-based threats and application-based threats[2].

Web-Based Threats are threats that affect smartphones and mobile devices due to the fact they are always connected to the internet. Users visiting harmful websites could unknowingly infect their devices with malwares propagated via these sites. In addition, there are advanced phishing scams that target mobile devices. This involves using texts and malicious links via social media to trick victims into providing sensitive information.

Application-Based Threats are threats that utilize malicious apps to gain sensitive information. These apps are available via app stores like Google Play Store and Apple Store. Ignorant users are tricked into downloading malicious apps which appear to be useful but are designed for malicious purposes. For instance, Palo Alto Networks reported the Xcode Ghost malware which was responsible for infection of several popular apps on Apple's App Store in September 2015. Similarly, in 2016, Google Play Store was found to host more than 400 malicious apps which turned phones into eavesdropping devices.

Social Media Age

Social media is the future of communication; a countless collection of internet based tools and platforms that increase and enhance information sharing[3]. This new form of media makes the transfer/sharing of text, photos, audio, video and other personal and business information increasingly common among internet users.

Some platforms have created online communities where people share as much or as little personal information as they wish with other members. Such platforms are Twitter, Facebook, LinkedIn and Instagram. The result is an immense amount of information that can be shared, searched, promoted, disputed, and created easily.

Indeed, thanks to social networking, the way we interact with friends, family and associates have been greatly enriched. However, we are also exposed to significant risks depending on the sensitivity of the information we put online.

Let's face it, we put a lot of sensitive information on social media platforms such as our next itinerary or pictures and schools of our children; circle of friends; employment details; and so on. These information can be harvested by attackers and used for the wrong reasons.

[1] Official (ISC)2 Guide to the CISSP CBK - Fourth Edition By Adam Gordon
[2] https://usa.kaspersky.com/internet-security-center/threats/mobile
[3] www.iiste.org/Journals/index.php/DCS/article/download/25900/26425

Social Engineering Attacks

Social engineering, in a cybersecurity context, refers to manipulative acts performed by hackers to get people to give up confidential information, or perform actions that may compromise their computer system. It usually depends on the attackers' ability to manipulate the victim using various tactics

> **"This is to notify you that your account has been placed on hold pending additional electronic verification. To avoid account suspension, follow the instruction below."**

> **"Please click here to update your BVN number"**

These are some of the common attack methods users fall victim to. Ultimately, no matter what technical measures have been taken, the effectiveness of these attack method highly depends on the behaviour of individuals.

Types of Attacks Targeted at Individuals

Phishing: This is the most common form of social engineering attack. It involves the use of baits such as well-crafted emails sometimes with attachments containing malicious payload. Examples are emails claiming to come from real banks asking people to update their bank details.

Smishing: This attack is similar to phishing scams but is text based or SMS based. It involves the attacker promising the prospective victim prizes or gifts by calling a number or clicking a link. For example, an attacker could send a message stating that there is an issue with the victim's Bank Verification Number (BVN) registration and it would be corrected by calling a number.

Spear Phishing: This is a type of phishing attack that focuses on a particular individual or organisation. The attacker uses personal information obtained online such as social media accounts in order to gain the trust of the individuals or organisations. Often times, the aim is to lead the victim to a malicious website.

One of Singapore's largest banks was also the target of such a phishing scam in 2014. A phishing website built to resemble the bank's original website was detected by the bank. At first glance, it was impossible to tell them apart.The rest, as they say, is history.

Baiting: This involves requesting for sensitive information or login credentials in exchange for information such as music, movies and documents. Another form of baiting attack is uploading malware-infected software/applications on a site where someone would likely download it.

14%

of Internet users in Nigeria suffer one form of cyber-attacks or the other

Dr. Isa Pantami, (DG, NITDA)

> **"Palo Alto Networks reported the Xcode Ghost malware which was responsible for infection of several popular apps on Apple's App Store in September 2015. Similarly, Google Play was found, in 2016, to host more than 400 malicious apps which turned phones into eavesdropping devices."**

Tips on staying secure online

Emerging trends

Internet of Things

Smart meters

2015
313 m

2020
> 1 bn

Home and city

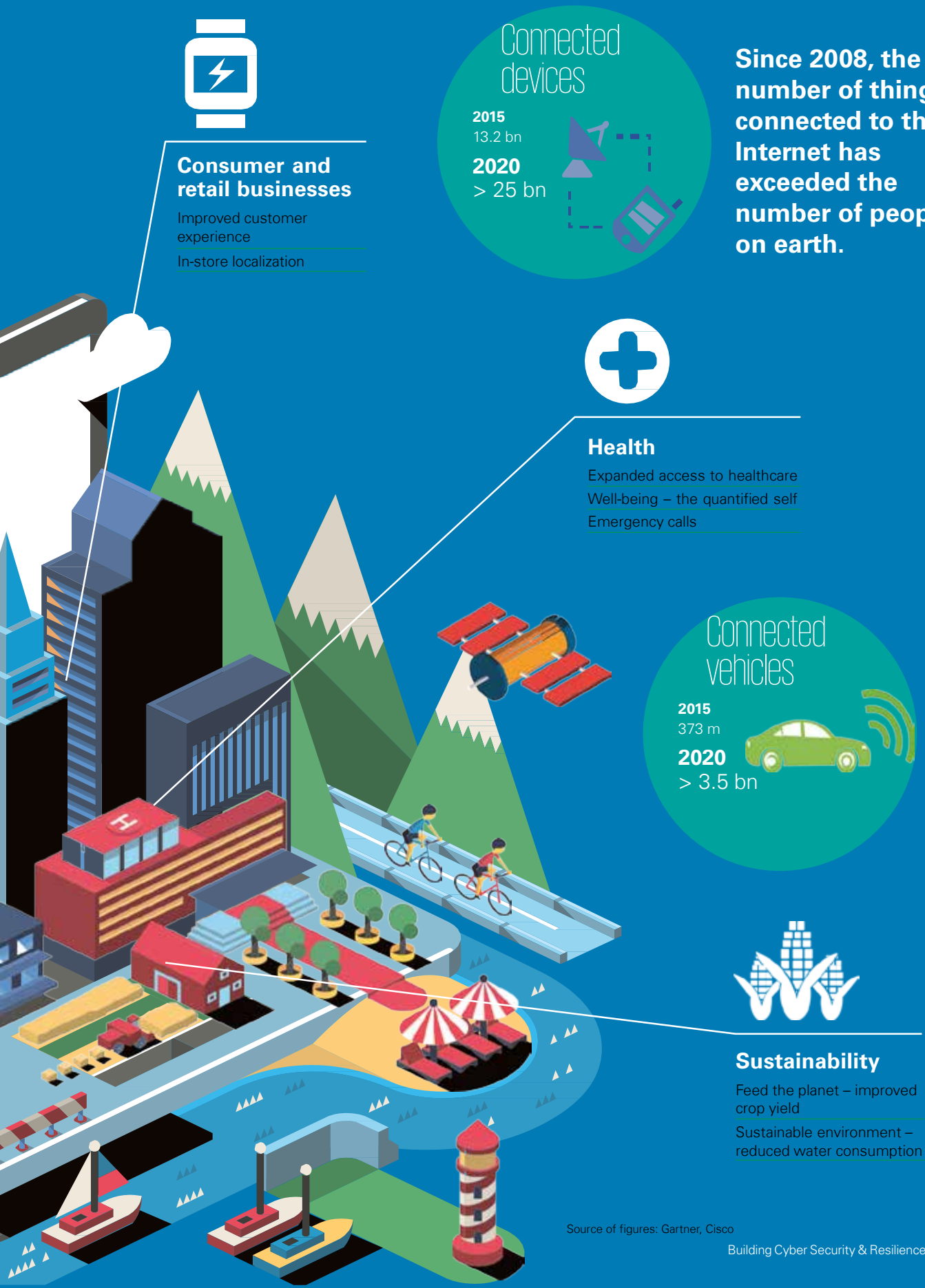
- Smart meters – efficient use of energy
- Home automation
- Smart management of city infrastructure
- Surveillance
- Water supply
- Sewage disposal

Transportation

- Connected vehicles
- Self-driving cars
- Smart infrastructure
- Public transportation
- Aviation
- Sea faring

Manufacturing and operations (Industry 4.0, IoT)

- Industrial controls
- Health and safety management
- Supply chain optimization (RFID)



Consumer and retail businesses

Improved customer experience

In-store localization

Connected devices

2015
13.2 bn

2020
> 25 bn

Since 2008, the number of things connected to the Internet has exceeded the number of people on earth.

Health

Expanded access to healthcare

Well-being – the quantified self

Emergency calls

Connected vehicles

2015
373 m

2020
> 3.5 bn

Sustainability

Feed the planet – improved crop yield

Sustainable environment – reduced water consumption

Source of figures: Gartner, Cisco

“Traffic System implemented in Tyler, Texas, was reported to have reduced traffic delays by 22%.”

Worldwide IoT market will grow to $7.1 trillion by 2020, compared to $1.9 trillion in 2013.

- IDC

By 2018, the spending on IoT security is expected to reach

$547 billion

– Gartner

Internet of Things (IoT)

In Nigeria today, one of the controls implemented at various intersections on our roads is the traffic light system - to prevent accidents and control the movement of vehicles. This method of managing and controlling traffic on the road is not efficient as Programmable Logic Circuits at the heart of this system are preset (with specific values) to determine when vehicles are to Stop, Ready or Move (Go).

Imagine, a traffic system that dynamically controls traffic based on live feeds gotten from integrated cameras and sensors. Surely, this would control traffic more efficiently, get people off the road safely and faster to their various destination. This traffic system is driven by the IoT technology. Already, smart traffic control systems exist in developed countries around the world – for instance, an Intelligent Traffic System implemented in Tyler, Texas, was reported to have reduced traffic delays by 22%[1]. Going by this statistics, leveraging on the technology that IoT provides in the area of transportation will help reduce the traffic challenges in urbanized cities in Nigeria such as Lagos.

So, what is Internet of Things (IoT)? Basically, this is a network of physical “things” embedded with sensors and connected to the Internet. With IoT technology, devices are able to communicate and share data between one another without manual intervention. Also, the technology enables physical objects to be sensed and controlled remotely across networks, creating opportunities for more direct integration between the physical world and computers.

Opportunities

The opportunities to be derived from the adoption of IoT are enormous.

Some areas of application of this technology are in Health, Home and City, Transportation, Manufacturing, Consumer and Retail Businesses, etc.

For each of these areas, embracing the IoT technology means that more devices will be connected to the internet. A study conducted by KPMG revealed that in 2015, there were 13.2 billion connected devices, a figure that is expected to exceed 25 billion by the year 2020. This increase in the number of connected devices will translate to more market revenue for the manufacturers and service providers of the connected devices, as well as companies operating in the telecommunication industry such as Internet Service Providers.

In homes and cities, IoT technologies can be leveraged to achieve production and deployment of smart meters – necessary to drive efficient use of energy. Other areas of application are in home automation, smart management of city infrastructure, security surveillance, water supply, and sewage disposal.

In transportation, application of IoT can be utilized in achieving connected vehicles, self-driving cars, smart infrastructure, public transportation, aviation and sea faring. Also, the application of IoT can enable the establishment of a smart car park.

In manufacturing and operations, the IoT technology can be leveraged in Industrial Controls, Health and Safety Management, Supply Chain optimization (using RFID and GIS technology), etc. For consumer and retail businesses, this technology can assist to improve efficiency in in-store localization and improved customer experience.

---

1. http://fortune.com/2015/08/20/smart-traffic-signals/

Threats

One of the biggest challenges confronting the technology industry today is security. While it is important to acknowledge the advantages that IoT promises, it is equally essential to be aware of the security challenges and risks inherent in this technology, given that it fundamentally involves connected devices over the internet. Many cyber attacks have been successful on IoT and many are still occurring as of this moment. The more connected our world becomes, the higher the potential of attacks – this is a concern that security researchers have continued to express.

IoT, like any other technology innovation has widened the attack surface. The reason for this is obvious – some of the connected devices have weak security protections while others are poorly configured.

Recently, A French based hosting company, OVH suffered a record high 1.1 Tbps Distributed Denial of service (DDoS) attack, an attack that was made possible by hackers using Command & Control servers to hijack weakly configured connected IoT devices[1].

The security threat to an improperly implemented home automation system could lead to unauthorised access and operations in the home or apartment by cyber criminals.

Cyber security researchers at the University of Michigan, USA were able to compromise a home automation system – giving them access to the security PIN code to gain access into the home[2].

Given the security threat that IoT poses, many organisations around the world are now thinking more clearly about how they might improve IoT security. Bridget Karlin, Managing Director, Internet of Things Group Intel was quoted as saying "At Intel, we believe that integrating security into the platform and into the silicon is critical to helping drive IoT's adoption and scalability. Integrating security at the onset is key to establishing trust for IoT solutions".

In conclusion, while adopting IoT technology in areas such as transportation, health, manufacturing, home and cities would assist to improve the ease of doing business, deliver better traffic management, introduce comfort in homes and improved efficiency in company operations. Emphasis must be put in ensuring that connected devices are properly configured and the security risks associated with implementing the devices are identified and appropriate measures to mitigate them are in place. Effective IoT security will only lead to increased adoption of this technology – which is what we all want.

By 2020, more than 25% of identified attacks in enterprises will involve IoT

– Gartner

By 2018, 66% of networks will have had an IoT security breach

- IDC

$445 billion is the estimated cost of cybercrimes globally each year. The IoT is expected to increase this figure

– McAfee

1. https://arstechnica.com/security/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/)
2. http://ns.umich.edu/new/multimedia/videos/23748-hacking-into-homes-smart-home-security-flaws-found-in-popular-system

Cyber Risk Insurance

Cyber insurance is a broad range of insurance products designed to protect businesses from operational risks affecting confidentiality, integrity and availability of information assets. Cyber insurance products can include coverage for various risks including data breach, cyber extortion, identity theft, disclosure of sensitive information, business interruption, network security, and breach notification and remediation.

Globally, the cyber insurance market is booming. There are several indicators that shows it will be the biggest market for insurance organisations in the coming years. However, insurance organisations in Nigeria need to be more sophisticated in assessing cyber risks to turn this emerging opportunity to a sustainable line of business and create products and policies leveraging this business opportunity.

Insurers willing to take advantage of this line of business will need to consider three key areas:

1. **Security assessment and Monitoring:**

   In order for insurers to quantify the risk they will be underwriting, they will need to develop the capability to conduct security assessments on their customers in a way that provides visibility and helps them better understand the controls the customers have in place to mitigate cyber risks and therefore the likelihood of such risk crystallizing. The outcome of these assessments will spur customers seeking to transfer or mitigate cyber risk through insurance to make considerable investments in security solutions other than the traditional access controls, threat detection and threat protection solutions currently in place. These investments would ultimately boost security control measures on customer's valued assets.

   Businesses then need to assess the costs of the security solutions to determine which security solution provides reasonable security benefits at acceptable costs and performance for their organisation. While the cost to benefit assessment is important, businesses need to understand that the impact of a cyber attack is unquantifiable and may lead to total business value erosion.

2. **Data Management and Analytics:**

   Given the speed at which the threats – and therefore the required levels of protection – change within the cyber arena, insurers will need to become much better and much faster at managing and analyzing their data in order to better inform their pricing and risk models.

   Armed with detailed information taken from their security assessments, insurers could, for example, combine such with actual claims information to more precisely quantify how much protection each security method or tool provides.

3. **Product Development and Innovation**

   What is clear about the future of the cyber insurance market is that product innovation will be key. Major Nigerian insurance industry operators are seeking to explore cyber insurance in the financial services industry which is the major target of cyber attacks in Nigeria and have started developing policies and creating products to this effect.

   The Nigerian Insurance Industry is currently faced with the daunting challenge of quantifying cyber risk due to the lack of actuarial data. They compensate by relying on qualitative assessments of applicants' risk management procedures and risk culture.

   This in turn has restricted the growth of cyber risk insurance in Nigeria. While insurers may still be struggling to understand the market, evidence suggests that the purchasers of cyber policies are no better informed. Generally speaking, few organisations truly understand what their cyber policies cover and in what circumstances. Many organisations still believe that their general property and liability policies will provide them with protection from cyber risk damages.

In conclusion, insurers will play a key role in helping companies secure their most valuable data and information by demanding implementation of effective cyber security controls. Furthermore, insurers will provide a degree of loss protection to organisations impacted by cyber attacks. However, insurers will need to work hard to achieve the level of expertise and sophistication needed to offer competitive services that the market demands.

Global cyber insurance market is expected to generate $14billion by 2022

– Security Week

Cloud Security

The increased adoption of cloud computing in emerging African markets is no secret as organisations are seeking avenues to lower operational costs.

Cloud security is termed as the policies and controls designed to protect information data, applications and infrastructure associated with cloud computing use.

Most Nigerian businesses are wary of cloud adoption as they are burdened with concerns of data security, sovereignty, legal and regulatory compliance, internet broadband downtime amongst other adoption issues.

However, this appears to be greatly compensated by the cost savings and apparent transfer of cyber risk to the cloud service provider.

In recent times, several Nigerian companies have started migrating from the traditional on premise infrastructure to cloud services such as Microsoft Office 365 email platform. Several companies are also becoming bolder to host more of their critical servers and applications in the cloud. These companies need to conduct comprehensive cloud maturity assessments which will help with providing a clear roadmap towards fully integrating cloud and hybrid IT.

The questions, after satisfying regulatory and legal requirements, will be:

- Are original equipment manufacturers (OEMs) and system integrators capable of providing adequate cloud security?
- Do we have skilled cloud security practitioners in-house to adequately evaluate our risk?
- Are there matured SLA's with cloud computing vendors amongst others?

Technology companies like IBM and Oracle have developed various technologies and they have been encouraging customers to adopt their cloud computing and cloud security offerings. Popular cloud security models saddle customers with the responsibility of securing provisioned virtual machines and managing other security configurations (identity and access management, network and dynamic firewall configuration, data security and network traffic protection) using custom tools provided by OEMs.

In closing, cloud computing adoption in Nigeria is on a rapid increase. However, it is worthy to emphasize that technology companies need to do more to encourage customers who adopt cloud computing by providing assurance on data security and allaying other fears customers may have.

$11.8 billion

estimated to be the global cloud security market by 2022

– Transparency Market Research

27.8%

of the worldwide enterprise applications market will be SaaS-based by 2018, raising revenue to $50.8 billion, from 22.6 billion in 2013.

– IDC

“The Bitcoin Market Potential Index **by the London School of Economics ranked Nigeria 5th out of 178 countries likely to adopt the Bitcoin cryptocurrency**”

Innovative business built on a blockchain will be worth $10 billion by 2022

– Gartner

Bitcoin transactions in Nigeria have been hovering at over $1 million weekly since the beginning of 2017

– LocalBitcoins

Blockchain

Many disruptive technologies are continuously permeating the technological space, blockchain being one of these. Blockchain - a peer-to-peer oriented technology that underpins the development of various cryptocurrencies (notably Bitcoin, Litecoin and Ethereum amongst others) has drawn the attention of business leaders, bankers, consultants, scientists, developers and other stakeholders since its announcement in late 2008.

Whilst blockchain or distributed ledger technology is still in its early stages of adoption in Nigeria, Bitcoin and other digital currencies have been in use globally since the late 2000s. The Bitcoin Market Potential Index by the London School of Economics (a composite of 39 variables such as technology penetration, remittances, financial crises etc.) ranked Nigeria 5th out of 178 countries likely to adopt the Bitcoin cryptocurrency (a digital asset and payment system that relies on the blockchain technology)[1].

Although, many people might at one time or another have heard about blockchain, only a few people actually understand the role it plays in enabling the many cryptocurrencies that exist today.

The following scenario will attempt to explain in simple terms, the concept of blockchain.

Imagine that Alice needs to make payment to Bob using a cryptocurrency. When Alice sends the payment to Bob and Bob receives it, Alice (if she has malicious intention) could decide to send the same payment to Mark since it is digitally owned - Needless to mention that a common practice in digital space is the ability to copy or reuse a digital resource. If this was possible, it means that Alice can send (spend) this same amount to as many people and for as long as she wants without exhausting her money. This is not desirable in any payment system as it violates the basic rule of performing transaction - which is to prevent "double-spending". The prevention of the double-spending in digital currency such as Bitcoin is what blockchain helps to achieve. This is accomplished by adding every block of successful transaction to previously processed blocks - such that a transaction that has been processed and completed cannot be reversed, modified or revoked. This essentially is what guarantees security, prevents double-spending and establishes trust in a decentralized system

Opportunities

The security that blockchain provides and its ability to enable a tamper-proof system for managing digital credentials and reputation has extended its application beyond cryptocurrencies. The blockchain technology is being leveraged in areas such as Currency Creation, Payment Infrastructure, Digital Assets, Anti-Counterfeiting, Identity, Verifiable Data, Electronic voting and voter authentication, Smart Contracts amongst others to create value and disrupt traditional practice. Looking at Currency creation for example, blockchain has been leveraged to develop Bitcoin, Litecoin and over 700 other cryptocurrencies.

Bitcoin and other cryptocurrencies enable secure payment transactions irrespective of the location of the sender or receiver. Bitcoin transactions offer cost effective transaction charges when compared to the fees charged by traditional players. This provides an opportunity for both end-users and Bitcoin or cryptocurrency Exchanges due to the increasing market potential. For example in 2015, the size of annual remittances to Nigeria was estimated at $21 billion. By the end of 2016, the remittances recorded had risen to $35 billion[2].

1. http://blogs.lse.ac.uk/businessreview/2016/05/12/most-countries-in-the-10-most-likely-to-adopt-bitcoin-are-in-the-developing-world/
2. http://thenationonlineng.net/nigerias-diaspora-remittances-hit-35b/

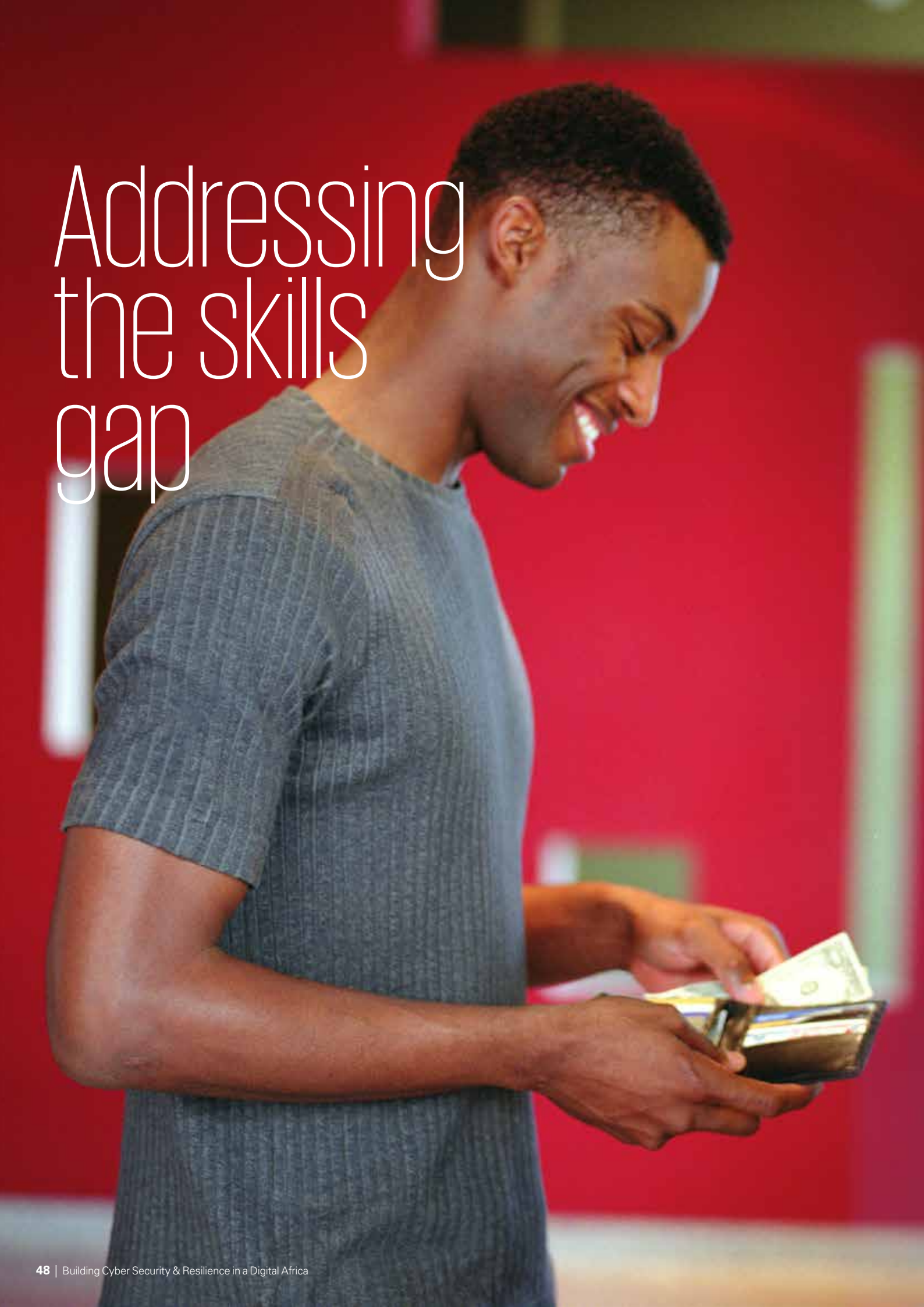
Given the cost effectiveness of transactions done through Bitcoin, This is one area that would likely experience a paradigm shift in the option that people choose to conduct their transaction – hence opportunities for potential players.

Another factor that would drive people towards adopting Bitcoin - an offshoot of the blockchain technology as their preferred method of transaction is the challenge of accessing Foreign Exchange in Nigeria. Already, there are entities that offer services that allow people to carry out transactions and make payments using Bitcoin Debit cards. CryptoPay and SpectroCoin are two examples.

While blockchain guarantees some level of security – bearing in mind that there is no such thing as absolute security, there have been reported cyber attacks on companies providing blockchain and cryptocurrency services. DAO and Bitfinex are two examples of companies that have been hacked – leading to the theft of Customers' Bitcoin. Because the security of Bitcoin is also dependent on the owner's private key, owners of Bitcoin are advised to keep their private key secure.

In conclusion, Bitcoins are vulnerable to theft if not properly secured although the technology that underpins it guarantees security. While blockchain provides a technology that establishes trust in a decentralised system, which amongst other things has led to the development of digital currencies such as Bitcoin, there are challenges impeding its adoption and this is not peculiar to Nigeria alone. These challenges include uncertainty around regulatory acceptance, cyber security concerns, the inherent anonymity and high capital outlay required at the initial stages.

Addressing the skills gap



A recent survey by Information System Audit and Control Assocation (ISACA) indicates that the global shortage of cyber security professionals would hit 2 million by 2019[1].

This is owing to the surge of demand for cybersecurity professionals in today's industry.

Another survey indicates that the rate of cybersecurity job growth is three times more than that of non-cybersecurity job growth within the same information technology industry[2].

One major challenge currently facing organisations today is the dynamic nature of threats as technology continues to act as a double-edged sword by opening up new criminal opportunities using its recent breakthroughs. Existing threat actors are constantly developing and improving their attack techniques to stay relevant in the cyber threat landscape.

Technology has been the touchstone of development in major economies of the world. Acquiring advanced technologies helped boot-strap economies of countries like China and India out of recessions at different points in their history. It is believed that poor technological capability remains one of the major constraints to Africa's efforts to achieve its vision of sustainable development.

One major solution to this would be developing policies to suit our peculiar environment and identifying critical innovation barriers to address and enable Africa achieve increased productivity and structural transformation of its economies. Technology-based businesses and solutions offer an opportunity for innovation and creation of powerful new disruptive business models yet to be seen in its relatively untapped market.

Capture young talents

As the global pool of entrepreneurs now boasts of young billionaires, it is clear that the teenage heart beats faster for business more than ever. Reason suggests that there is no better time to start a business than when brimful of youthful vigor, given the youthful exuberance and high risk appetite typically exhibited by the younger generation.

There is a constant influx of young technology entrepreneurs looking to launch new businesses and possibly collaborate with the government and communities to support their ideas. Consequently, it has become essential for African governments to foster an enabling environment to nourish this growing innovation eco-system. Supporting and partnering with entrepreneurial hubs would go a long way in unveiling a lot of young individuals who could then pitch their startups on a platform and network with potential investors.

There is still a market for startups in the cyber security space. This should be encouraged, especially among the youth in Africa.

Information and Commuincation Technology (ICT) Education Curriculum Updates in Nigeria

Quality improvement in IT education is driven by a relevant and functional ICT curriculum[3]. Prevailing issues such as job creation and poverty reduction can only be solved through a revised ICT curriculum. The mode of delivery of knowledge is currently not influenced optimally by ICT, though with the development of a National Policy on ICT in Education, Nigeria has predictably taken a step in the right direction. The National Policy on ICT Education is aimed at promoting ICT across all levels of the educational

"A recent survey by ISACA indicates that the global shortage of cyber security professionals would hit 2 million by 2019"

"Another survey indicates that the rate of cybersecurity job growth is three times more than that of non-cybersecurity job growth within the same information technology industry."

1. ISACA - 2016 Cyber Security Skills Gap
2. Burning Glass Job Market Intelligence: Cyber Security Jobs 2015
3. IT Deployment as a tool for rapid Transformation of Education & Capacity Building, 2011

Another survey shows that about 53% of organisations experience delays as long as 6 months to find qualified security candidates

As of 2015, ISACA boasts of 2000 resident members in Nigeria which indicates a low certification level amongst industry professionals

system. Key initiatives highlighted in the policy include the development of a National Standards for IT Education document which specifies requirements for the establishment of an IT curriculum governing teaching, learning and assessment at all levels of the Nigerian Education System, development of an e-curriculum portal for effective management of senior secondary school education curriculum and a student-PC ownership scheme aimed at enabling students of Nigerian Universities own brand new computers at subsidized costs.

Special Intervention Training Programs

The Nigerian Educational Research and Development Council (NERDC) is charged with a mandate to develop a curriculum with emphasis on creative thinking, entrepreneurial skills, and positive social and cultural values. Some of the most important developments in education have happened since the launch of the Internet. Students have become well versed in the use of smartphones, text messaging and using the Internet thus changing the mode of learning to include electronic media.

The Federal Government of Nigeria in its role to enhance access to qualitative education initiated an e-learning initiative to cut across all the Ministries, Departments and Agencies in the country. A committee was set up to steer this initiative in 2010 by the Federal Ministry of Education.

In addition, it is expected that the introduction of the Computer Studies/ ICT curricula as a compulsory subject will facilitate the speedy integration and implementation of Information Technology in the government's plans on capacity building and educational reform.

The Federal Government of Nigeria also plans to establish two super hubs in Abuja and Lagos as well as six regional hubs in the respective geo-political zones to facilitate practical skill acquisition amongst its citizens in the technology workspace encompassing cybersecurity, software innovations and so on.

Addressing the skills gap in Cybersecurity

Solving the growing cybersecurity challenges requires young skilled security professionals who are proactive and willing to combat existing cyber-security threats.

As the rate of cybersecurity incidents continues to escalate, the magnitude of related brand, reputation, and fiscal impact is driving organisations to address this risk. Executive leadership teams are demonstrating cybersecurity resiliency support by taking a more active role in enforcing policy, mandating security awareness training, supporting budgetary increases for cybersecurity-related technology and training, and modeling the way by adopting leading cybersecurity practices[1].

Although enterprises continue to increase spending and effort on cybersecurity, respondents constituting majorly cybersecurity managers and practitioners in a global survey conducted by ISACA and RSA Conference between November and December 2015, indicate that they struggle to fill positions with highly skilled workers[1].

Another survey shows that about 53% of organisations experience delays as long as 6 months to find qualified security candidates[1].

Relevant cyber security talent is becoming increasingly difficult to find

1. ISACA's State Of Cyber Security: Implications for 2015

in today's ever growing cyber security field[1]. Recent reporting from the Center for Strategic and International Studies states that the shortage in cybersecurity skills does direct and measurable damage to organisations operating in today's interconnected world[1].

Companies look favorably on cyber security professionals who are passionate and have taken the initiative to develop a deeper understanding of the ever-growing cybersecurity landscape.

Furthermore, high-value skills are in critically short supply, creating an employment environment in which enterprises experience difficulty filling positions. Practical skill competency and certification attainment are the key attributes that hiring managers consider when making cyber security position hiring decisions.

Therefore, an appropriate hiring strategy that emphasizes performance based certifications that require practical applicant cyber security skills is key to successfully filling open positions.

Certifications, which can be garnered in less time than a formal degree, have become a prevailing consideration when filling an open cyber security position. Certifications such as CISSP, OSCP and CEH are definitely a must have in filling the experience and skills gap within the cybersecurity industry.

As of 2015, ISACA boasts of 2000 resident members in Nigeria which indicates a low certification level amongst industry professionals[2]. While certifications and degrees are an important factor in filling cybersecurity positions, hiring managers also look at practical experience garnered in similar positions before making their decisions. It is easy to list the number of certifications and degrees earned, but companies are looking to hire people who can come up with solutions to problems on the job and not individuals who can just answer questions on a certification exam.

In conclusion, possessing academic knowledge and certifications are clearly important distinctions to stand out in an applicant pool, but the real differentiators are hands-on experience in the field, which goes beyond that gained from the classroom.

1. State of Cyber Security 2017: Current Trends in Workforce Development
2. http://www.nigeriacommunicationsweek.com.ng/e-guest/nigeria-cyberspace-neglected-unprotected-territory-onifade

KPMG Cyber Capabilities

An Overview

The constantly evolving threat landscape means that cyber risk is an everyday business consideration, in the same way that threats in the real world have always been. However, cyber security is not a quick technical fix nor is it a matter solely for the IT department.

KPMG Cyber Security team assists organisations in transforming their security, privacy and continuity controls into business-enabling platforms while maintaining the confidentiality, integrity and availability of critical business functions. The KPMG Cyber approach strategically aligns with our clients' business priorities and compliance needs

The KPMG Cyber Approach

The KPMG Cyber approach is designed to be simple, effective and most importantly, aligned with the business needs of our clients.

Our services are segmented and supported by specialised teams, providing our clients with the right resources for any particular cyber-related need. Below is a breakdown of service offerings and our approach to cyber security:

Prepare	Protect	Detect & Respond	Integrate
Helping clients understand and improve their current state of preparedness against cyber-attacks, including services such as;	**Helping clients design and implement their cyber defense infrastructure, including services such as;**	**Helping clients maintain visibility of their cyber weaknesses and respond to cyber-attacks, including services such as;**	**Helping clients embed cyber security into culture and decision making of the organisation including services such as;**
• Cyber Readiness Assessment • Cyber Strategy and Transformation • Cyber Governance and Resilience • Data Governance and Privacy • Emerging Technology Risk Management • Threat Modeling • Cyber Defense Architecture Design	• Identity and Access Governance • Cloud Service and Cloud Provider Assessments • Vulnerability Management • Secure Application Development Services • Data Leakage Prevention Services • Critical Infrastructure Services • Secure SDLC	• Cyber Operations and Incident Response • Vulnerability and Penetration Testing • Platform and Network Security Assessments • Threat Detection and Intelligence Services • Cyber Asset Inventory Services • Post Breach Investigation	• Cyber Security Awareness • Cyber Incident Simulation • Red Team / Blue team Exercises • Cyber in the Boardroom Services

Cyber Assurance Services incl. ISO, ISAE, PKI/NIST, etc.

The KPMG Difference

THE KPMG DIFFERENCE

Having worked with major organisations from across various industries in Africa and across the globe including financial services, telecommunications, energy and natural resources, consumer markets and the public sector, KPMG's cyber team can help your organisation be cyber resilient with the end-to-end management of cyber security threats.

We can help your organisation prevent, detect and respond to cyber threats.

GLOBAL, LOCAL

KPMG is a global network of member firms with over 174,000 professionals in 155 countries with over 2,700 security practitioners globally, giving member firms the ability to orchestrate and deliver to consistently high standards worldwide. KPMG's regional practices can service your local needs from information security strategy and change programs, to low level technical assessments, forensic investigations, incident response, training and ISO certification.

INDEPENDENT

Our recommendations and technical strategies are objective and based solely on what is fit and appropriate for your business.

TRUSTED

KPMG member firms have a long list of certifications and permits to work on.

- Information Security
- Business Continuity and IT Disaster Recovery Assessments and Implementation
- Data Privacy Assessments and Implementation

AWARD WINNING

KPMG International has been named a Leader in the Forrester Research Inc. Report. The Forrester Wave™ Information Security Consulting Services, Q1 2016.

To learn more about how we can help your organisation be cyber resilient, please contact us *(see back page for contact list)*.

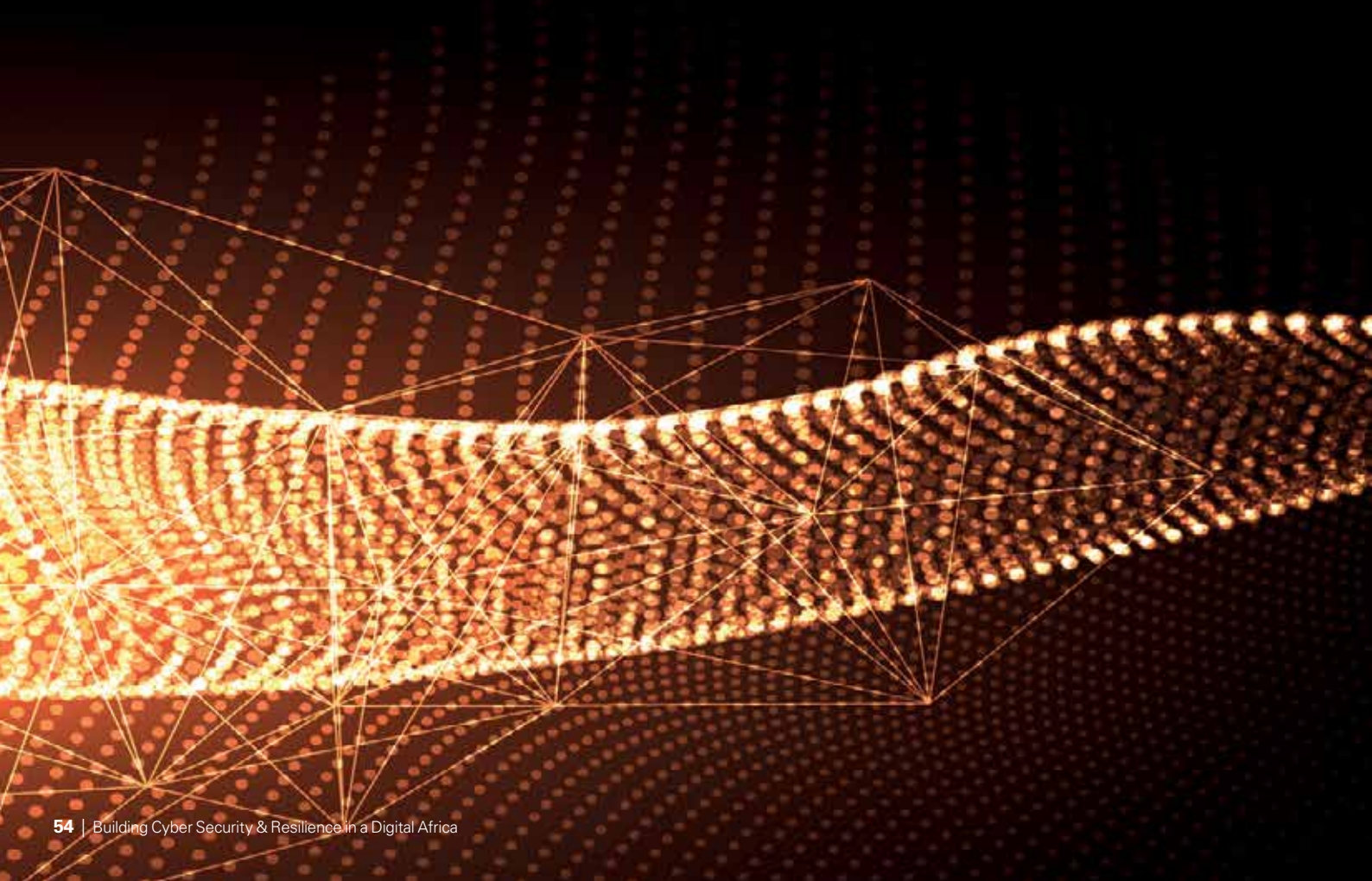
Acknowledgements

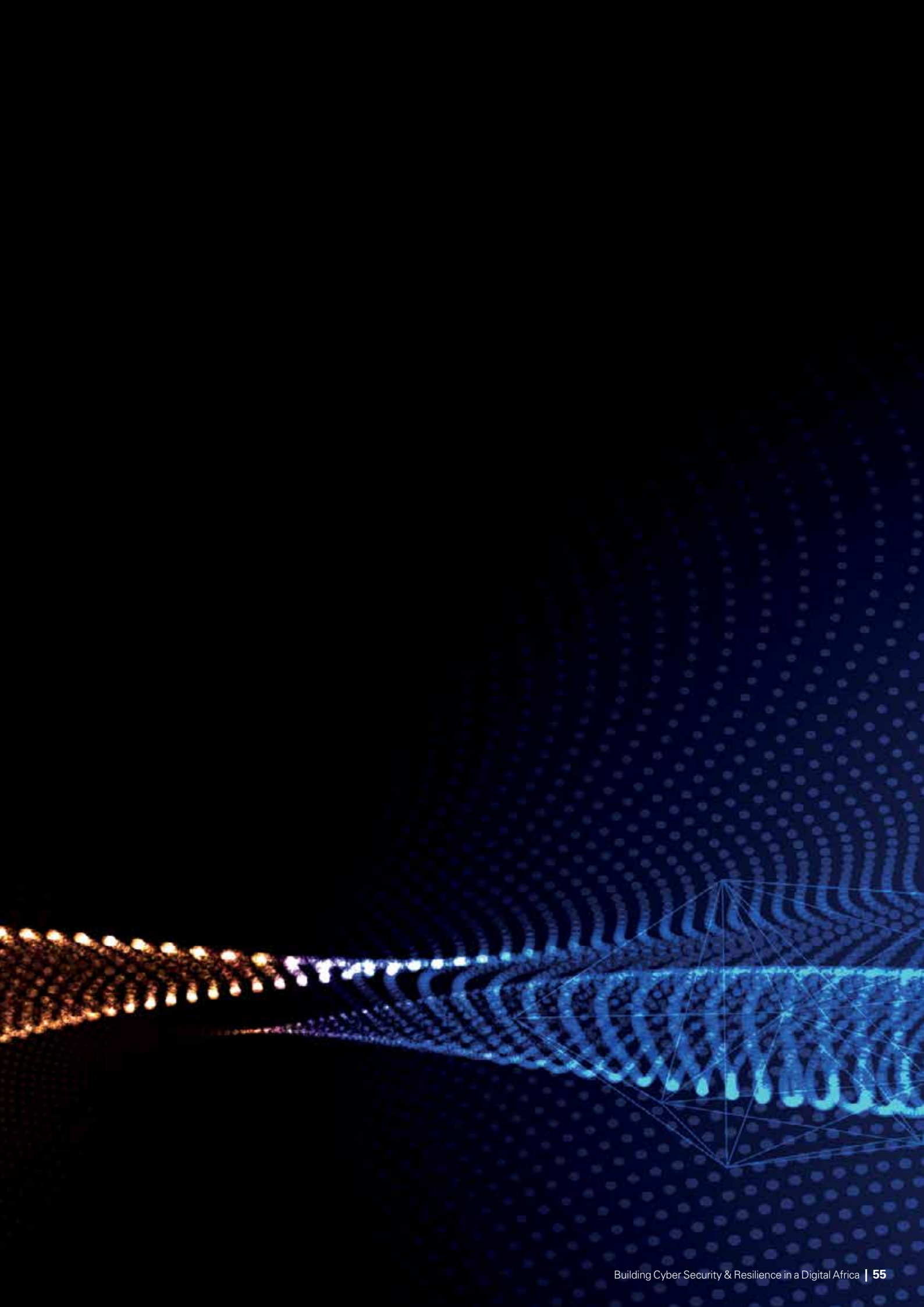
Research team:

John Anyanwu
Samuel Asiyanbola
Olaniyi Otolorin
Francis Acquaah
Olaoluwa Agbaje
Busayo Abayomi-Olomolaiye
Lanre Akomolafe
Mosimilolu Odusanya
Timilehin Lawal
Ahmed Obadun

Brand and design team:

Adanma Matthews
Omowunmi Martins





Contacts

Joseph Tegbe
Partner & Head
Technology Advisory
KPMG in Nigeria
Africa Cyber Security SGI Lead
M: +234 803 402 0989
E: joseph.tegbe@ng.kpmg.com

Sipho Ndaba
Partner & Head
Technology Advisory
KPMG in South Africa
M: +278 245 14297
E: sipho.ndaba@kpmg.co.za

John Anyanwu
Associate Director
Technology Advisory
KPMG in Nigeria
M: +234 803 975 4061
E: john.anyanwu@ng.kpmg.com

Samuel Aluko
Senior Manager
Information Technology Advisory
KPMG in Ghana
M: +233 560 223 555
E: samuelaluko@kpmg.com

Gerald Kasimu
Partner & Head
Information Technology Advisory
KPMG in Kenya
M: +254 202 806 000
E: gkasimu@kpmg.co.ke

Boye Ademola
Partner
Technology Advisory
KPMG in Nigeria
M: +234 803 402 0983
E: boye.ademola@ng.kpmg.com

Antony Nzamu
Associate Director
Information Technology Advisory
KPMG in Kenya
M: +254 709 576 247
E: anzamu@kpmg.co.ke

Samuel Asiyanbola
Manager
Technology Advisory
KPMG in Nigeria
M: +234 806 042 7195
E: samuel.asiyanbola@ng.kpmg.com

Andrew Akoto
Partner & Head
Risk Consulting
KPMG in Ghana
M: +233 302 766 307
E: aakoto@kpmg.com

Nancy Mosa
Partner
Information Technology Advisory
KPMG in Kenya
M: +254 709 576133
E: nmosa@kpmg.co.ke

Kaspar Euvrard
Senior Manager
Information Technology Advisory
KPMG in South Africa
M: +278 257 63588
E: kaspar.euvrard@kpmg.co.za

KPMG.com/ng

Follow us on:
kpmg.com/ng/socialmedia

Printed in Nigeria.

Publication name: Building Cyber Security & Resilience in a Digital Africa

Publication date: May 2017