2017

WEST AFRICA CYBERSECURITY INDEXING AND READINESS ASSESSMENT

A regional report on Cybersecurity ranking, readiness, vulnerabilities and mitigating measures to improve awareness.

Solutions Consulting

Acknowledgment

Over the course of the last 12 months, representatives from over 20 government agencies in Ghana, Nigeria, Liberia and Gambia, including business and professional associations, private companies, academic institutions and 350 individuals were consulted as part of a research around the readiness of public and private sectors in the West Africa sub-region to combat the growing cybersecurity risks, threats and vulnerabilities. We are grateful to all of them and their members, and to the many prominent individuals who have graciously offered guidance, advice and feedback. Their valuable feedback served as a basis for this report.

For more information, please contact cybersecurity@3tsconsulting.com

Special thanks to the following:

- Hon. Ursula Owusu-Ekuful - Minister of Communication Ghana
- Barrister Adebayo Shittu - Minister of Communication Nigeria
- Dr Frederick Norkeh - Minister of Posts and Telecommunications Liberia
- Mr. Demba Ali Jawo - Minister of Information, Communication and Technology Gambia
- ITU Cybersecurity Team
- Google Transparency Project Team
- Jeff Konadu – NITA Ghana
- Mathew Adjei- Boadu - Oasis Capital
- Yaw Benneh-Amponsah - Merson Capital
- Retired Captain Budu Koomson – Nexus Capital
- Ace Ankomah - Renowned Legal Expert
- Taiwo Adewumi –Toyota Nigeria
- Mike Okoduwa - Glo Nigeria
- Modou Joof - Frontpage International Gambia
- Basil Udotai Esq - Technology Advisor LLP Nigeria
- Margaret Donkor - Parliarment of Ghana

Table of Contents

“Ghana Election Commission website hit by Cyber-attack”
– BBC- Dec 8, 2016

“Government of Ghana website hacked”
– Graphic.com.gh - January 21, 2015

“Nigeria records 3500 Cyber attacks... lost $450 million in 2015”
– Vanguard – March 2016

“Los Angeles phishing Cyber-attack compromising 750,000 people traced to Nigeria” *– LA Times, June 26, 2017*

“Cyber-attack disrupts Liberia, slows Internet service in Liberia”
– The Guardian, Nov3, 2016

“Gambia Government Websites hacked, Jammeh asked to quit”
– Informationng.com December 12, 2016

Forward

Cyber attacks have continously evolved over the years with an escalated growth in 2017. It is against this backdrop of escalating cyber threats, that 3T Solutions Consulting launched the:

2017 West Africa Cybersecurity Indexing & Readiness Assessment: A regional report on Cybersecurity ranking, readiness, vulnerabilities and mitigating measures to improve awareness.

Technology continues to be the catalyst for growth in all aspects of individuals, communities and national development. Nations have amassed military equipment as a form of protecting their territorial integrity from known enemies. Companies have invested heavily in new services and infrastructure to gain competitive advantage over other trading partners.

However, the 21st Century enemy of a country or business competitor goes beyond the traditional norm. This enemy can be an organized individual or group of individuals creating havoc to a country's social, economic and political structures through nefarious activities in cyber space.

Not too long ago, cyber breaches was a means through which computer recreationists displayed their talents and depth of knowledge at the expense of businesses and organizations. This has escalated into a big business that is now funded by organized criminal institutions and in some instances countries.

About 3T Solutions Consulting

3T Solutions Consulting is a global Cybersecurity and Technology organization with offices in the United States, Ghana, Nigeria and India providing expert cybersecurity and innovative technology to all tiers of business and governments. Our objective is to simplify ICT and Security complexities for our stakeholders using cost-effective emerging approaches.

At the core of our operations is the promise we keep to our community to contribute in the protection, development, nurturing and growth of talents and resources through our “Community Give Back” project-based programs.

3T Solutions Consulting is focused on delivering business and technology outcomes for our clients with the lowest exposure to risks that most IT projects and management have.

Our expertise in the development of emerging and secured innovative solutions has seen us achieve the award of “Top 20 Most Promising Software Defined Solution Provider in North America in 2017” by the CIOReview board.

We look forward to continuing to add to this body of knowledge in cybersecurity, as it represents a stride in identifying areas of vulnerabilities and ensuring these are mined and improved upon. Cybersecurity is not a task for one country alone. It should be seen as a cooperation between all users of technology regardless of the boundaries they live in.

One of our recent awards:

http://sdn.cioreview.com/vendor/2017/3t_solutions_consulting

Executive Summary

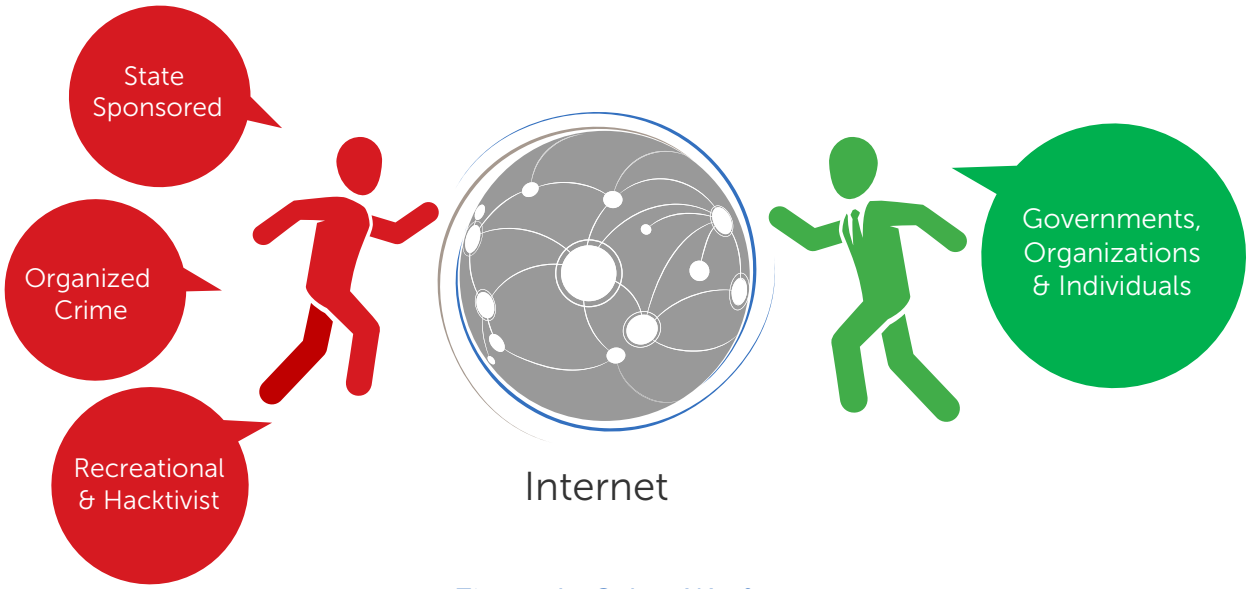


Figure 1 - Cyber Warfare

Figure 1 shows a representation of how we perceive today's cyber landscape.

The West Africa Cybersecurity Indexing and Readiness report is an aggregated index combining several indicators, with a view of creating a standard comparison of the countries involved in the report. The report looks at the scope, level of readiness and preparedness of Ghana, Nigeria, Gambia and Liberia, in their effort to combat cyber threats and intrusions into their economic, social and political structures.

The report examines:

1. **The types of cybersecurity commitments by Ghana, Nigeria, Gambia and Liberia**
2. **Success in cybersecurity policy implementation**
3. **The top cybersecurity threats in West Africa**
4. **Emerging trends with a direct impact on cybersecurity in West Africa**
5. **The imminent types of vulnerabilities these countries are susceptible to and how it affects growth and development**

Key Findings

I. Technology alone cannot address the efforts to combat cyber-threats and attacks

II. Risk management is a crucial component to addressing cybersecurity without impacting the overall operations of the organization

III. Although some industries, such as Banking and Finance have made some progress in addressing security on their infrastructure, our findings indicate most of the institutions are still very susceptible to client-side vulnerabilities

IV. Most laws in the countries involved in the study lack meaningful implementation to deter cybercriminals

V. Cybercriminals are using the path of least resistance, thus bypassing security investments that organizations have made in their infrastructure

VI. Lack of functional public emergency response team poses serious economic and national security issues

The biggest discerning factor in the report is the alacrity with which cyber criminals are able to innovate rapidly and enhance their capacity to compromise systems and evade detection.

According to a 2015 Midyear report conducted by Cisco Systems, in the first half of 2015, the hallmark of online attackers was their willingness to evolve new tools and strategies—or recycle old ones—to evade security defenses. Through tactics such as obfuscation, they can not only slip past network defenses but also carry out their exploits long before they are detected—if ever[1]

1 https://www.cisco.com/assets/global/UK/events/switchup_challenge/pdf/cisco-msr-2015.pdf

The Evolving Cyber Crime Threat Landscape

Until recently, cybersecurity has lagged behind the exponential growth of mainstream technology. The trend is however changing with countries adopting measures to track, minimize and control these nefarious activities. This report will track the trends in these countries.

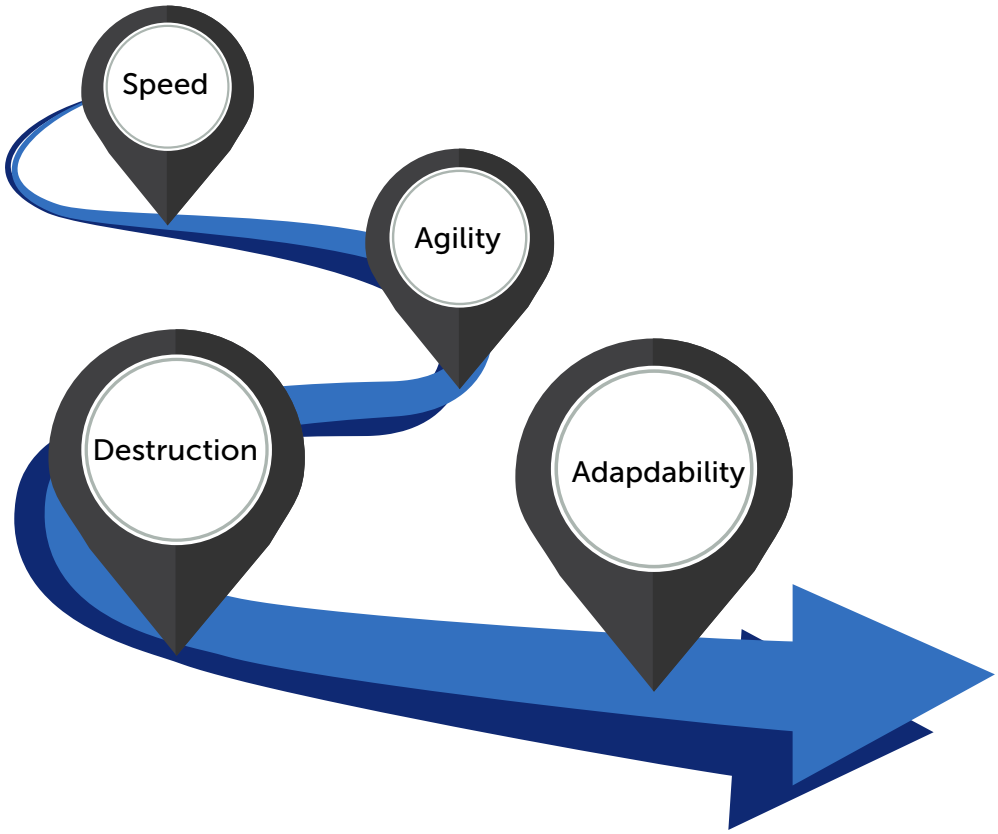


Figure 2 - Evolving Threat Landscape

The explosion of digital devices including Bring Your Own Device (BYOD) Internet of Everything (IOE) usage is almost impossible to track. Industry experts have continued to forecast an upward trend of connected devices since 2012. In as much as we have not reached the 1 trillion mark forecasted by IBM in 2012, the growth in these systems are still staggering. [1]

1 https://www.ibm.com/investor/events/investor0512/presentation/05_Smarter_Planet.pdf

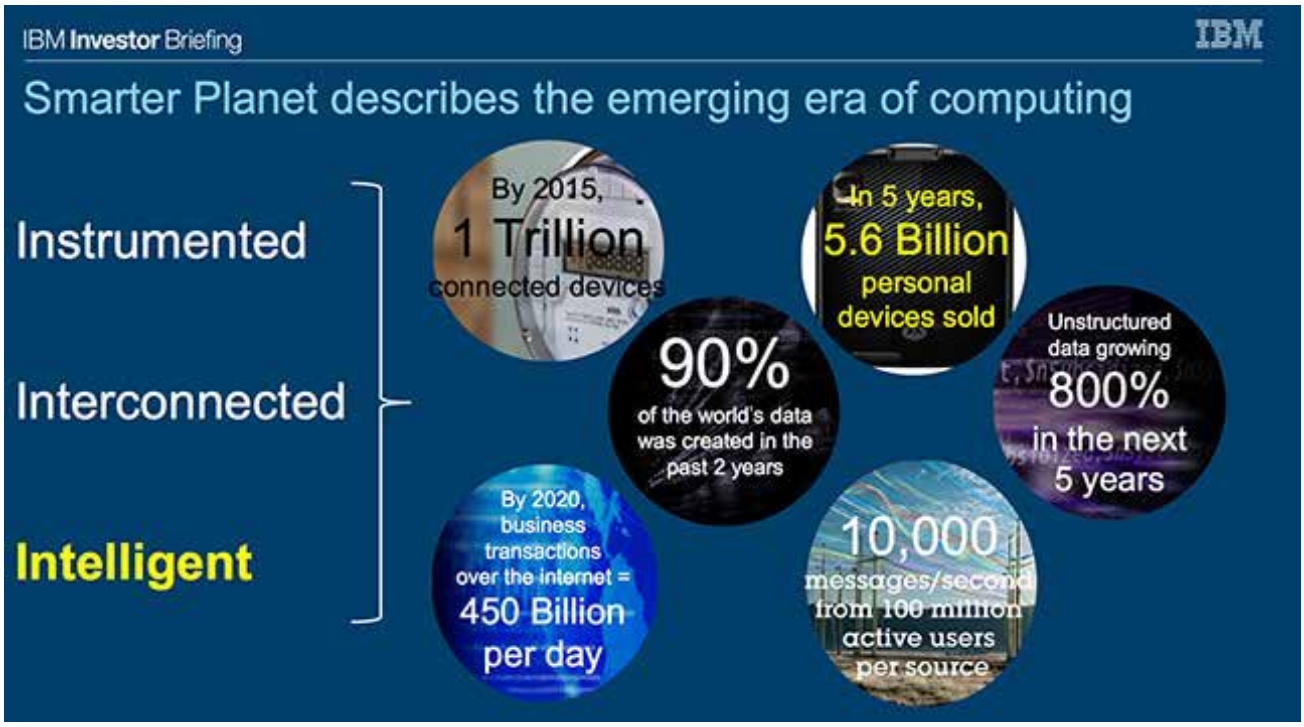


Figure 3 - Emerging Era of Computing (Credit: IBM)

The actual data showing research by world recognized technology companies put this data at a little more conservative number. The essence of this information is to juxtapose the number of connected systems from 10 years ago to 2017.

We can visualize the level of opportunities and threats that countries, organizations, users and institutions will face as more connected systems get online.

The advent of the Internet of Everything has escalated the growth of connected systems. In 3 short years, actual connected systems are estimated to reach 50 billion as shown in figure 4.

Cybercriminals are waiting to take advantage of these opportunities if the efforts at keeping these systems secured are not made deliberate and open to the public.

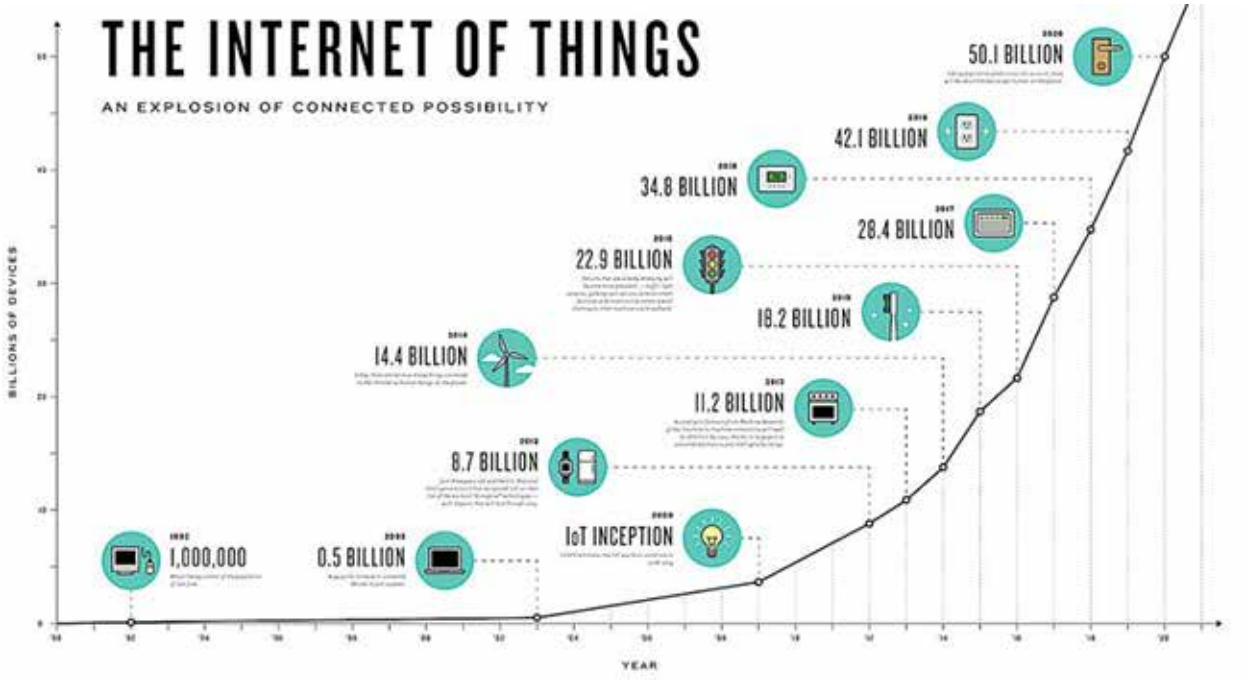


Figure 4 - The Internet of Things (Credit: The techladder.com)

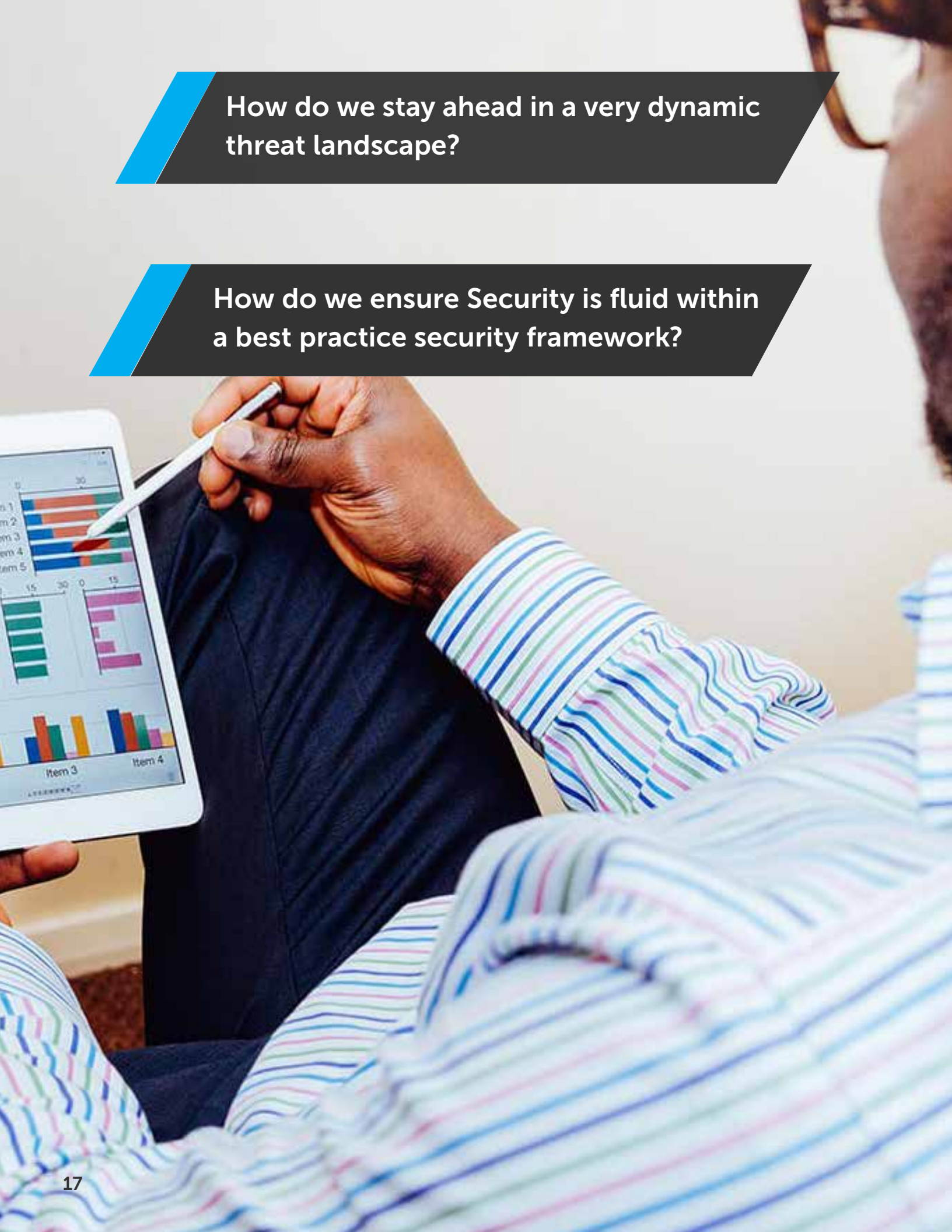
Without a deliberate effort to combat the nefarious cyber activities, the social, economic and political structures can be at a heightened risk.

This calls for an awareness in the development of well thought out and measurable strategies to combat cybersecurity threats. In this manner, dynamic response to new threats from cyber criminal activities can be properly evaluated and dealt with.

Public training and awareness is one of the most important first defense mechanisms needed to combat and curtail the menace of cyber attacks. We hope to use this report to generate awareness that will result in the development of consistent countermeasures to combat the existential threats we face as a society.

How do we stay ahead in a very dynamic threat landscape?

How do we ensure Security is fluid within a best practice security framework?



Methodology

3T Solutions Consulting in partnership with global cybersecurity Institutions in the United States and West Africa developed this report for 2017. This is to continue the trend of bringing cybersecurity awareness to the fore-front in the national, corporate and individual planning and discussions of the countries included in the study.

This report is intended to help speed the effort to make the West African sub-region a hub for fighting cyber crime on the African continent.

The methodology used to prepare this report is based on the following:

1. Responses to data collated by the ITU on cybersecurity readiness for Ghana, Nigeria, Gambia and Liberia.
2. Monitoring and assessments of some private and public infrastructure in Ghana, Nigeria, Gambia and Liberia.
3. Cybersecurity threats and vulnerability assessment using industry vulnerability assessment tools.
4. Regional Data from public Service Providers (SP) and Managed Security Service Providers (MSPP).
5. Interviews and surveys with public and private leaders of business and governmental institutions in Ghana, Nigeria, Gambia and Liberia.

While the report recognizes the need to address physical security and cyber terrorism, we did not include findings or recommendations relating to them.

Cybersecurity is not an effort to be left to the individual countries alone. It should be thought of as a culture and a way of life. Partnership have to be established among nations to counter the activities of nefarious cyber attacks in order to create a world-wide culture of cybersecurity consciousness.

Our research questionnaires to leaders of private and public institutions and agencies was very perceptive in its findings.

One common trend in the analysis of the feedback was the reluctance to share information about data breaches for fear of creating a negative perception about their organizations. Sharing cyber threat information is a key component for formulating countermeasures to common threats and risks.
We therefore encourage public and private institutions to share information regarding breaches with their reporting agencies.

Research Team

Kojo Degraft
Joel Amao
Dayo Abiodun

Contributors

Joe Abellard
Luis Cardona
Adebola Osundahunsi
Souley Diaby
Tejeswara Tammineni
Yomi Olaogun
Ebenezer Acquah
William Darkwah

Introduction

We live in a connected world made smaller each day by the exponential growth of technology. Individuals, companies and countries rely on cyberspace for everything from cell phone card recharge transactions to business partnership arrangements or the movement of military forces from one country to the other.

In West Africa, this trend is on an upward mobility. According to Ericsson Mobility report for sub-Saharan African, 2016, there are currently 720 million mobile subscriptions. This figure is set to increase to over 1billion by 2022.[1]

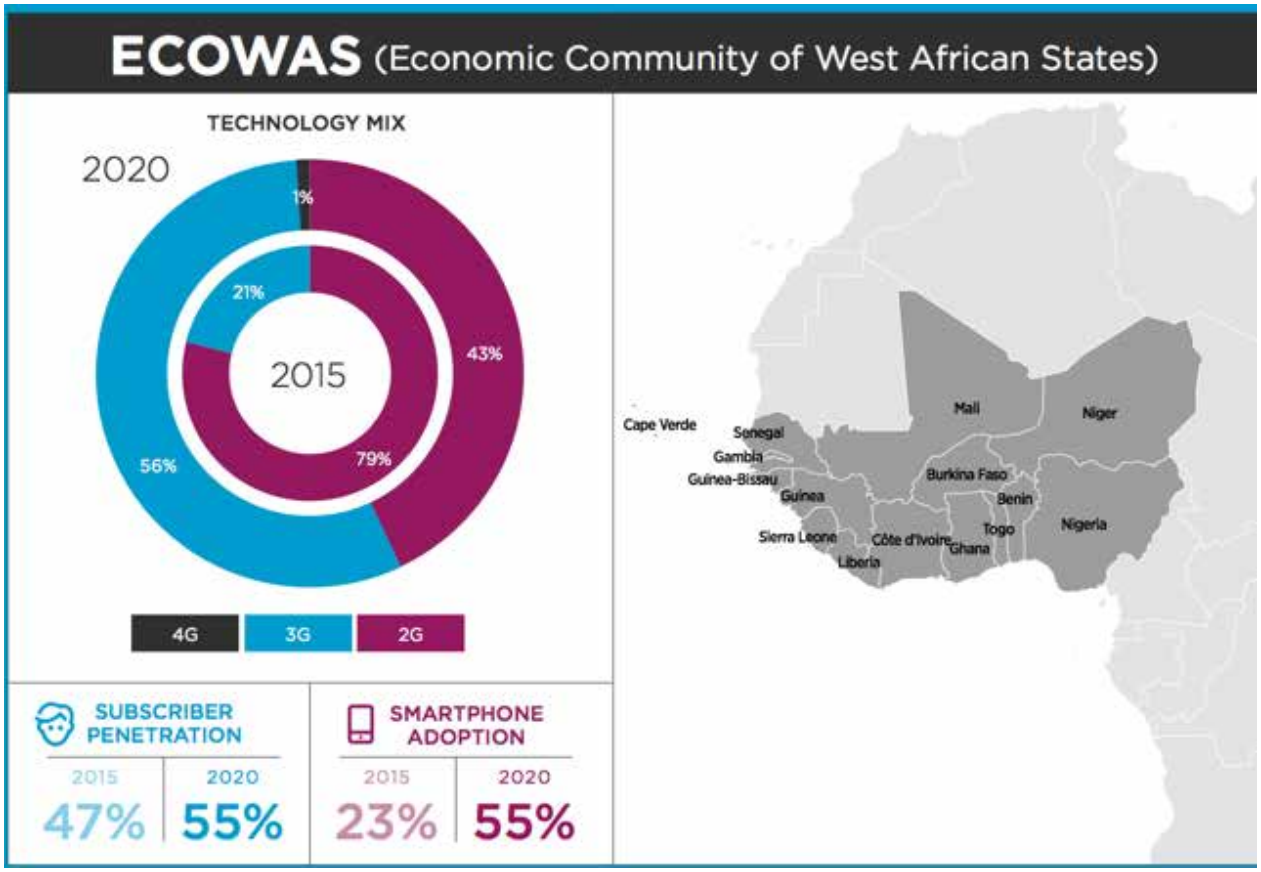


Figure 5 - Wireless Penetration - Credit- GSMA Intelligence- The mobile economy 2016

1 https://www.ericsson.com/assets/local/mobility-report/documents/2016/ericsson-mobility-report-november-2016-rssa.pdf

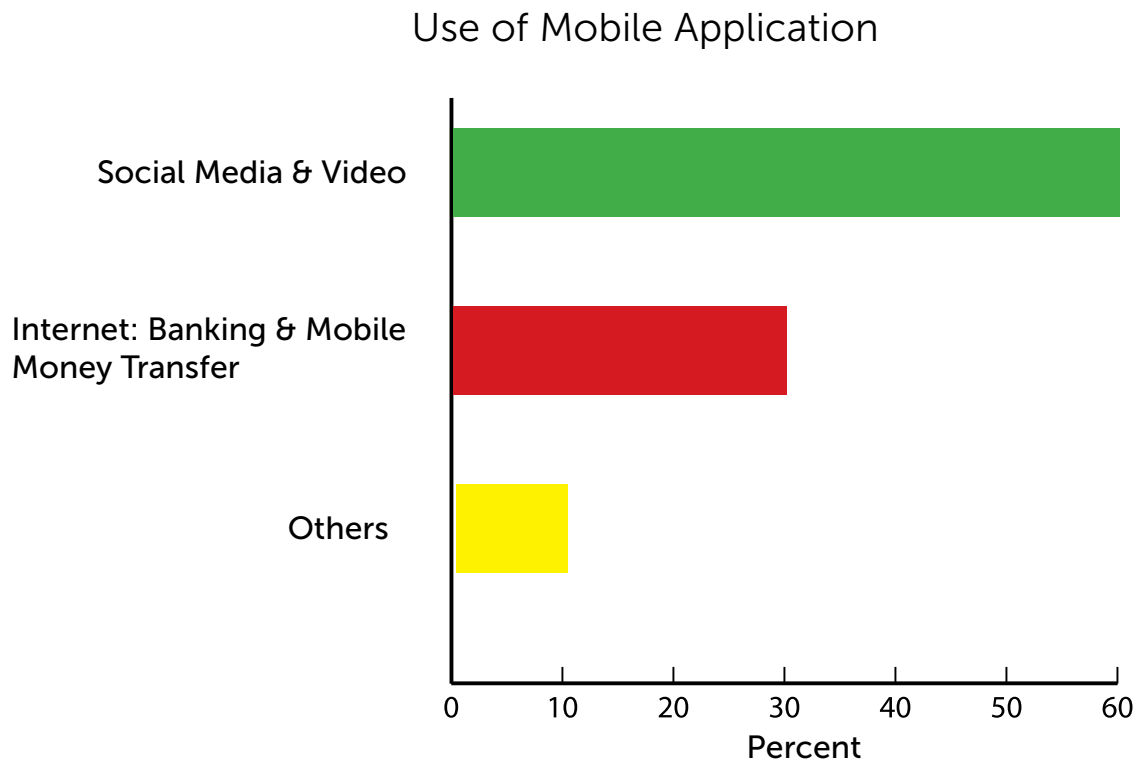


Figure 6 - Use of mobile Application Trend

As shown in figure 6, the fastest growing use of mobile applications in Nigeria is video streaming and social interactions (60%), followed by Internet banking and mobile money transfer.[1]

This is a similar trend in Ghana, Liberia and Gambia. These cyber activities leaves a lot of vulnerable systems especially where users are ignorant of the threat vectors they face in the use of their connected systems.

1 https://www.mediaupdate.co.za/marketing

The Cyber-Security Experts Association of Nigeria (CSEAN) has warned that with the level of vulnerability of the country to cyber attacks, financial institutions bear the highest risk and exposure. According to the president of the Association, Remi Afon, corporate organizations and government establishments have failed to prepare against obvious dangers of cyber threats posed by increasing sophistication in cyber crookery.

“Cyber attacks were becoming more sophisticated, stressing the need to build resilient cyber defense mechanism for the country” said Afon.[1]

“Cyber attacks were becoming more sophisticated, stressing the need to build resilient cyber defense mechanism for the country”

The West African Cybersecurity Indexing and Readiness report, 2017, is born out of the need for a cooperative partnership between private-public sectors and international organization to drive the issue of cybersecurity to the forefront of national agendas of the countries surveyed.

The Cybersecurity Indexing looks at the level of commitment in five areas using ITU’s Global Cybersecurity Index (GCI) framework . The five areas are; legal measures, technical measures, organizational measures, capacity building and international cooperation.

1 http://www.biztechafrica.com/article/cyber-attacks-nigerian-banks-imminent-warns-group/12380/

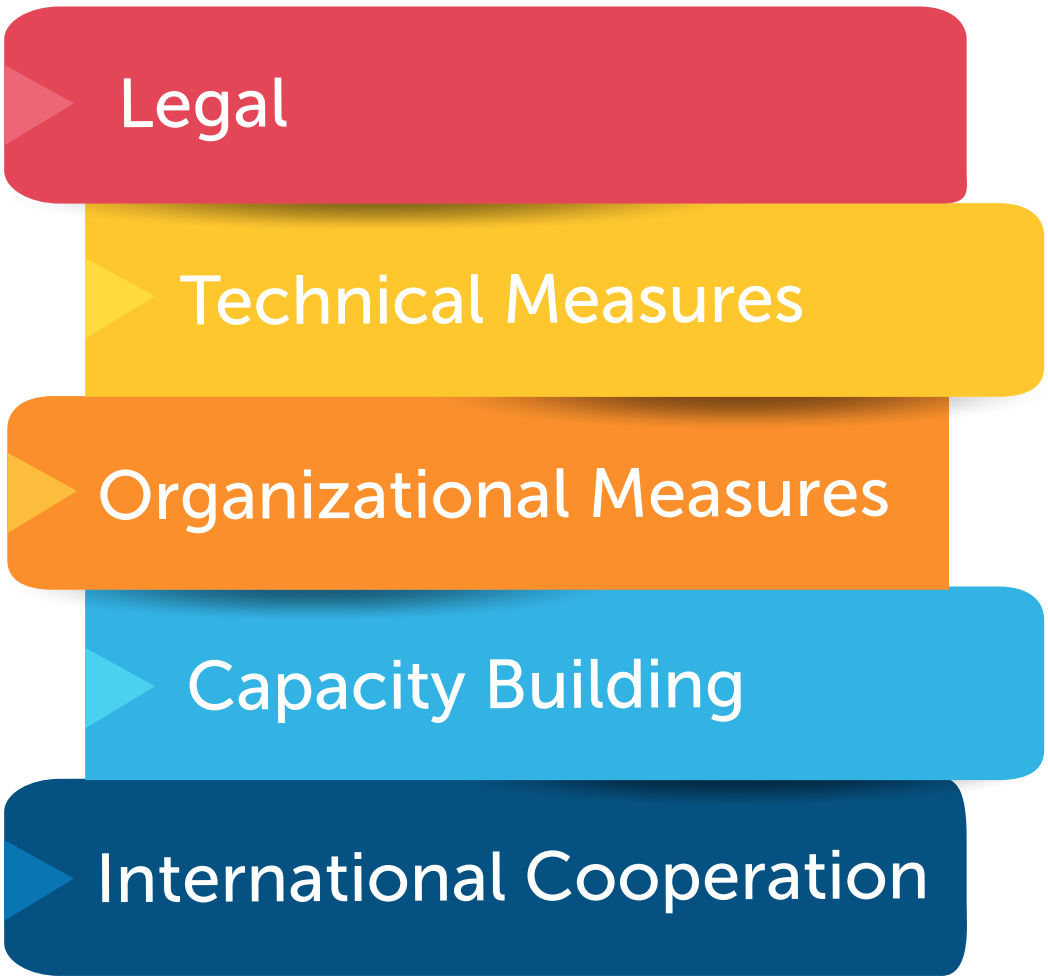


Figure 7 - ITU Measuring Index

The result is a country-level index on cybersecurity readiness and the existence of national structures in place to implement and promote cybersecurity awareness.

Information was collected on laws, regulations, Computer Emergency Response Teams (CERT)s and Computer Incidence Response Teams (CIRTs), policies, national strategies, standards, certifications, professional training, awareness raising, and cooperative partnerships. The aim of the cybersecurity Indexing is to provide a snapshot of where countries rank in their cybersecurity engagement at the national level.

The visions as seen by 3T Solutions Consulting together with international institutions such as the ITU is to promote cybersecurity awareness and the important role governments have to play in integrating appropriate mechanisms to both support and promote this crucial discipline in West Africa. Safeguarding the integrity of cyberspace must involve the development of cybersecurity practices and strategies.

The information below examines the countries involved and the trends towards connected systems. With the proliferation of smart phones, Internet of Everything etc. we can safely assume the number of connected systems will increase. Following that, the countries should expect an increase in cybercriminal attacks and activities.

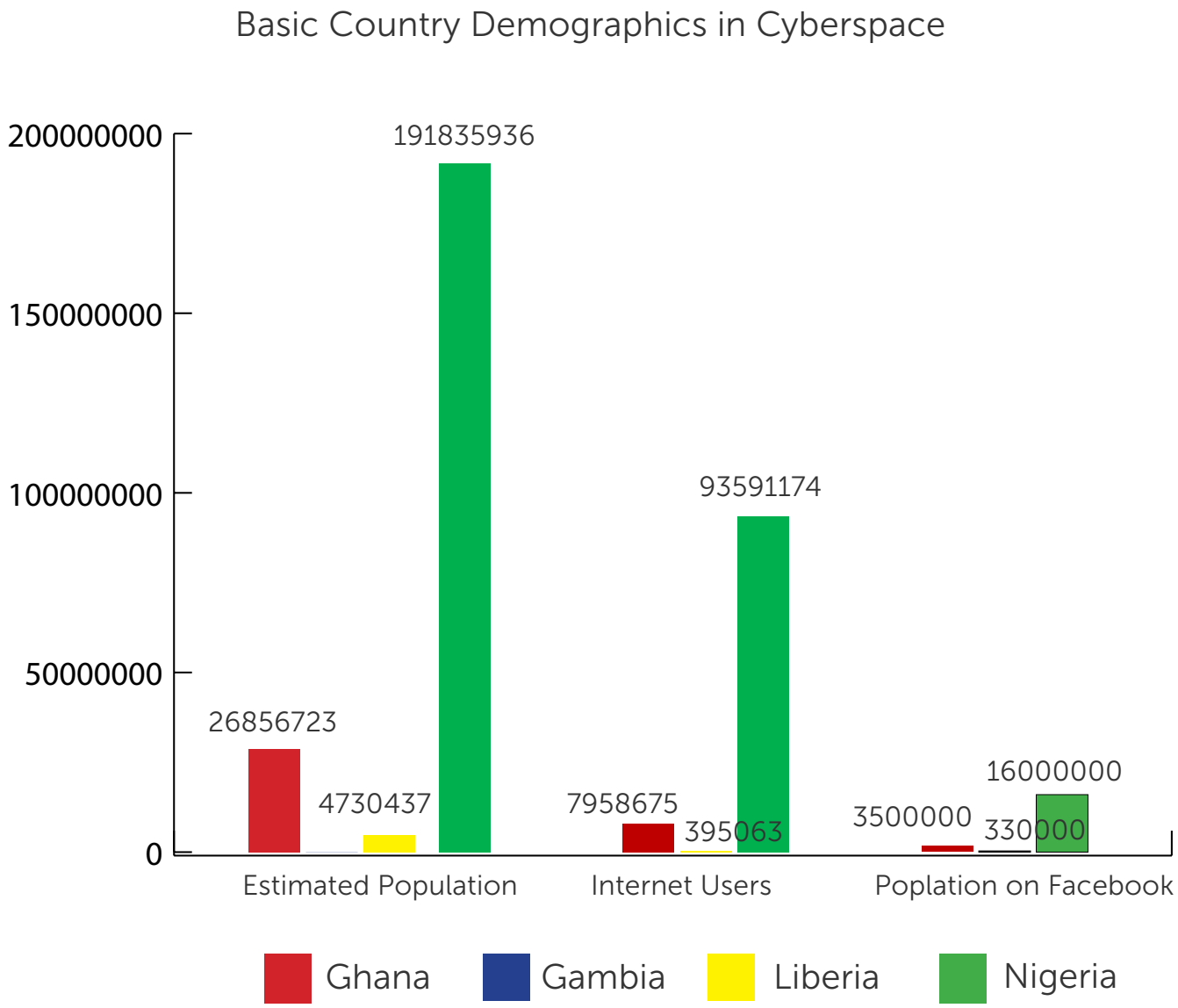


Figure 8 -Country Demographics in Cyberspace

Figure 8 shows:

- Estimated Population
- Estimated Internet users
- Estimated Facebook users

Country Ranking

Figure 9 shows Ghana, Nigeria, Gambia and Liberia ranking in relation to the global mark in terms of readiness to tackle cybersecurity. This shows the level of effort and commitment by the government in these countries towards combating nefarious cyber activities. The index is based on a mathematical formula used by the ITU, Global Cybersecurity Index & Cyberwellness Profiles.[1]

It has to be noted here that the ranking does not examine the vulnerabilities. The index is graded from 0.000 to 0.999. The higher spectrum indicates a higher readiness in response to nefarious cyber activities.

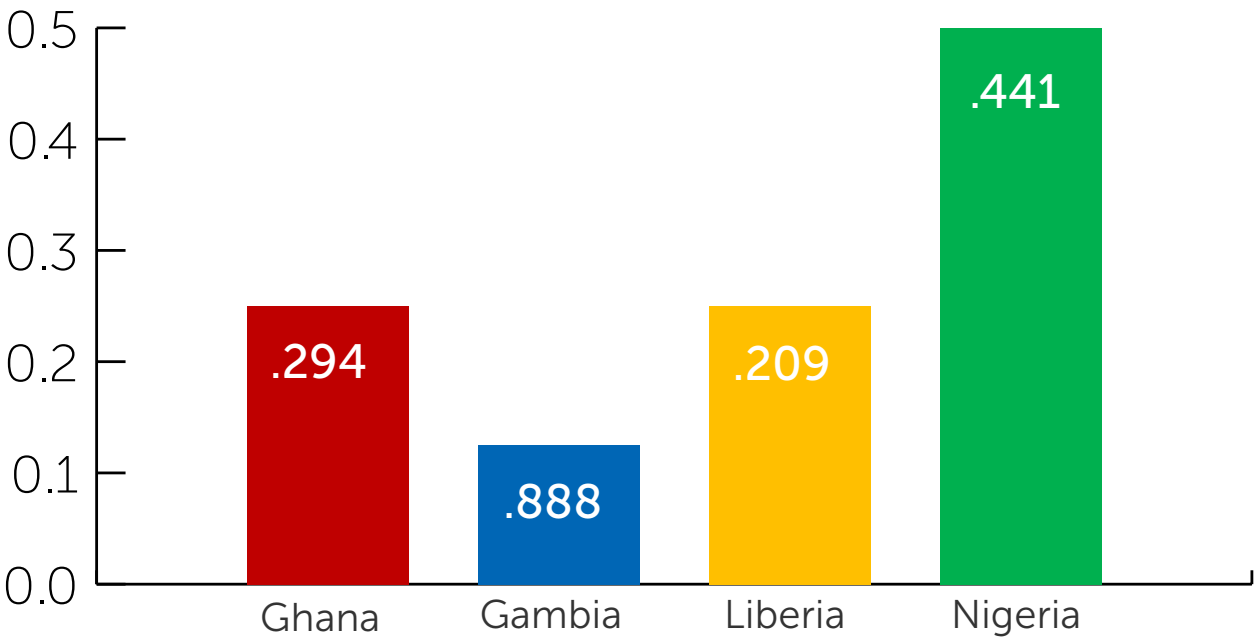


Figure 9: Country Rank by Index based on score from ITU

1 http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx

Legal

The lack of cohesive legislative and regulatory frameworks regarding cybersecurity in West African compounds the threat of creeping cybercrimes. In spite of the growth in technology adoption and Internet penetration, the development and enforcement of cybersecurity legislation among the four participating countries in our research has been relatively stagnant.

According to the ITU, Legislation is a critical measure for providing a harmonized framework for entities to align themselves to a common regulatory basis, whether on the matter of prohibition of specified criminal conduct or minimum regulatory requirements. A legislative framework sets the minimum standards of behavior across the board, applicable to all, and on which further Cybersecurity capabilities can be built.[1]

> **Ultimately, the goal is to enable all countries in the region to have adequate legislation in place in order to achieve a higher level of legal and policy interoperability.**

1 https://www.itu.int/en/ITU-D/Cyber-Security/Documents/GCI_Conceptual_Framework.pdf

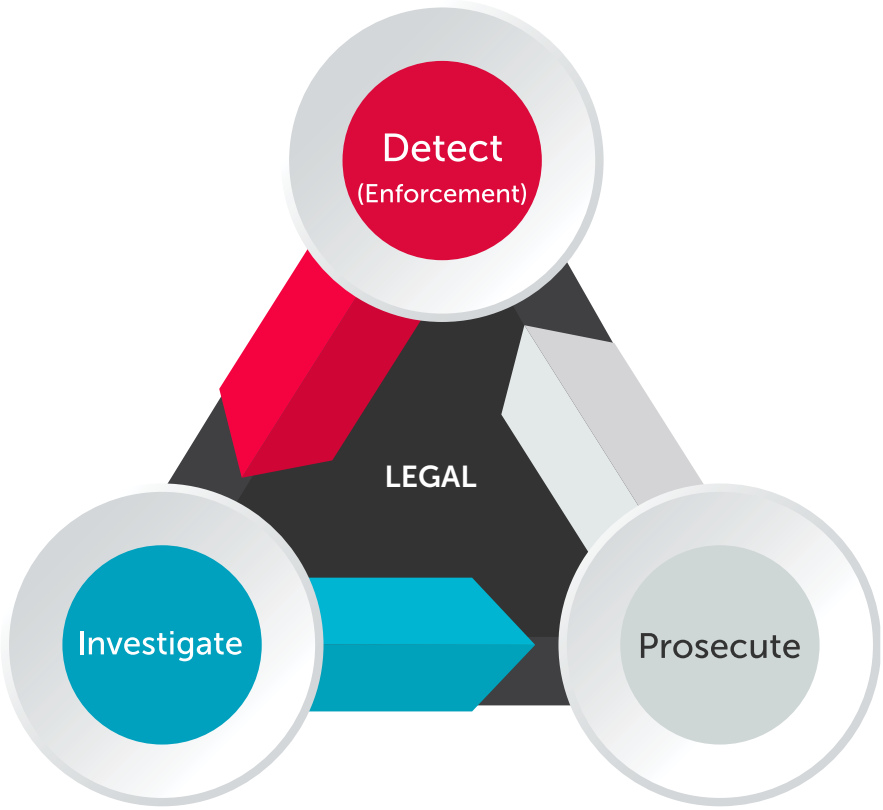


Figure 10 - Legal infrastructure

Figure 10 shows a framework for an effective legal framework infrastructure

In West Africa, Ghana's legal infrastructure was able to put in place legal structures to combat cyber-criminal activities. Ghana is currently a signatory member of the Council of Europe (COE) Convention on Cyber crime.

Liberia legal system almost seems nonexistent. However, Liberia passed 2 Supplementary Acts on February 16, 2010 which was named the Electronic Transactions and Data Protection and Directive on Cyber crime counter the threats and risks of cyber attacks.[1]

1 Liberia Annual Report. 2013/2014. Liberia Telecommunications Authority- Page 33

Nigeria passed the Cybercrimes Act 2015 that deals specifically with cyber crime, in May 2015.

Gambia established the Information and Communications Act 2009 with substantive criminal law provisions.

We asked over 300 respondents from the four countries in our research, to rate the effectiveness of existing cybersecurity laws, in context to regional efforts to combat cybercrimes.

Do you think existing laws on Cybersecurity is effective in tackling cyber crime?

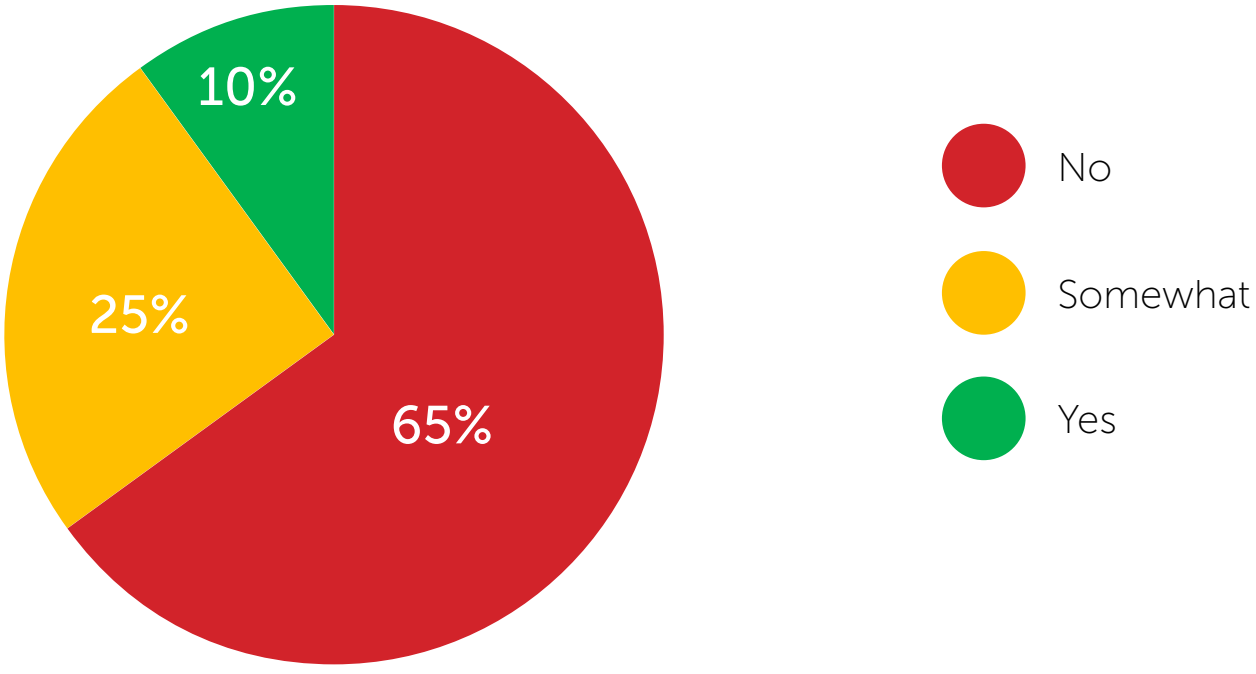


Figure 11 - Survey result on existing Legal readiness

As shown in Figure 11, more than 80% of respondents felt existing cyber laws are not sufficient or need additional improvements to deter and combat cyber crime.

It is worth noting that other countries in West Africa (such as Senegal) are signing up to the Council of Europe's (COE) Convention on Cyber crime. The Convention was drafted by the Council of Europe (COE) in France.
In addition to COE Member states, Canada, Japan, South Africa, and the United States participated in the negotiation of the Convention as observers.[1]

The Convention seeks to pursue a common criminal policy aimed at the protection of society against cyber crime through legislation and international co-operation.The Convention on Cyber crime has the following tenets which had an initial signatory of 55 countries, in and outside of Europe. The articles of the treaty sought to set a framework for activities detrimental to national development. This is a framework which guides signatories in their attempt to develop substantive laws on cyber crime.

1 http://static.cs.brown.edu/courses/csci1800/sources/lec16/Vatis.pdf

Substantive criminal law under the Budapest Convention on Cybercrime

Article 2	Illegal access to a computer system
Article 3	Illegal interception of non-public transmissions to, from or within a computer system
Article 4	Data interference
Article 5	System interference
Article 6	Misuse of devices
Article 7	Computer-related forgery
Article 8	Computer-related fraud
Article 9	Offences related to child pornography
Article 10	Offences related to infringement of copyright and related rights
Article 11	Attempt, aiding or abetting
Article 12	Corporate liability

Council of Europe/Project Cybercrime@Octopus page 3

These provisions alone or in combination, still cover most of what constitutes cyber crime, fifteen years after adoption of the Convention. This is primarily attributed to the technology agnostic manner of the provisions. Guidance Notes adopted by the Cyber crime Convention Committee show how different provisions can be applied to address botnets, distributed denial of service attacks and other cyber-attack vectors.[1]

1 http://www.coe.int/en/web/cyber crime/guidance-notes

Country Rating using ITU index

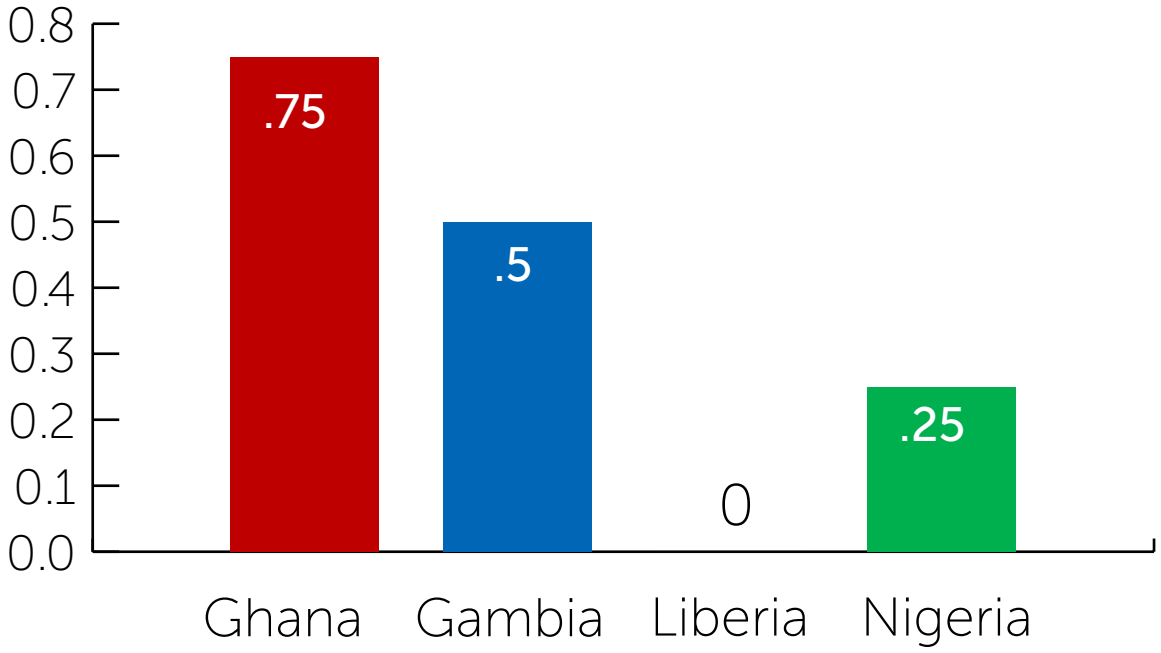


Figure 12 - Country Ranking - Legal

Figure 12 shows the ranking of countries in relation to Legal Frameworks. Ghana ranked highest in its efforts. It should be noted that a score of zero does not indicate non-existence of legal framework.

Technical Measure

Implementing a defense-in-depth strategy requires adequate technical measures to protect technology infrastructure and data against all offensive actions like intrusion, disruption, theft or intentional manipulation of data. Technology is an important line of defense against cyber threats and attacks.

A strong cyber defense that is increasingly resilient to cyber intrusion and better anticipate risk is paramount to the success and growth of the participating countries in our research.

To achieve this level of success, government, businesses and the research & prevention community must partner to constantly review the effectiveness of existing technical measures, in contrast to the evolving arsenals in the hands of cyber criminals.

> Having a functional national Cyber-Security Emergency or Incident Response Team (CSERT and CSIRT) that is available to critical sectors of the country such as the financial sector, is a right first step to developing technical measures.

According to ITU, Technical measures can be measured based on the existence and number of technical institutions and frameworks dealing with cybersecurity endorsed or created by the nation state.[1]

At the national level, Ghana has charged Cert-GH, the National Information Technology Agency under the Ministry of Communication to develop and provide safeguards to cybersecurity.

1 http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx

NG-Cert has the same responsibility in Nigeria.

Gambia is in the process of completing its certification in concert with ITU-IMPACT modalities.

A functional national Cyber-Security Incident Response Team (CSIRT) or Cyber-Security Emergency Response Team (CSERT) should constitute a diverse team of security experts whose main focus is to respond to Cybersecurity incidents, provides necessary services to key sectors of the economy, such as financial sector and support organization that provides critical infrastructure services, to quickly recover from security breaches. In addition, the CSERT or CSIRT will work with Internet Service Providers (ISPs) to identify IP addresses affected by malware, or are part of infected networks called Botnet.

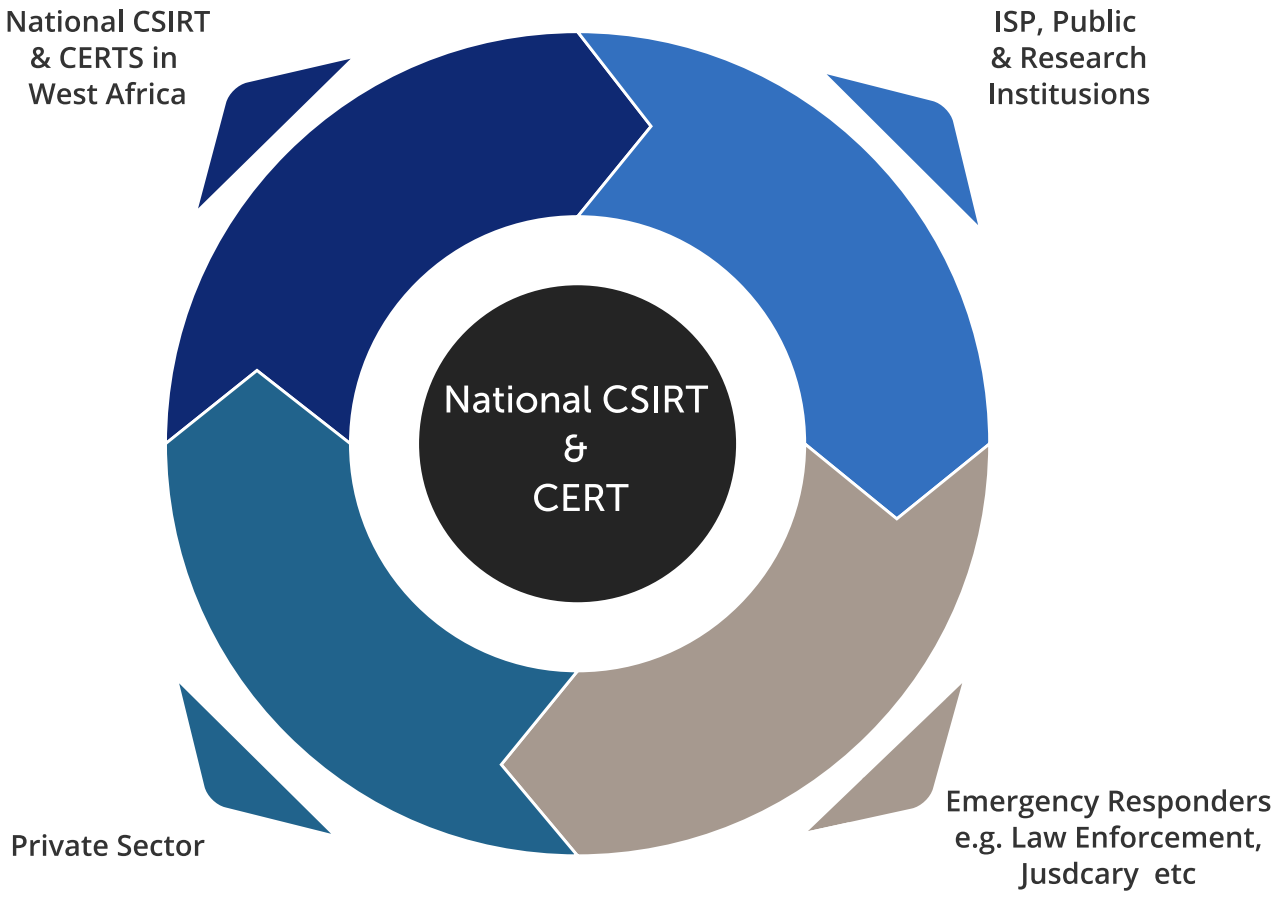


Figure 13- CSIRT and CERT

Are you aware of a national Cyber-Security Incidence Response Team (CSIRT) or Cyber-Security Emergency Response Team (CSERT) that provides emergency and incidence response to private and public sectors in your country or region ?

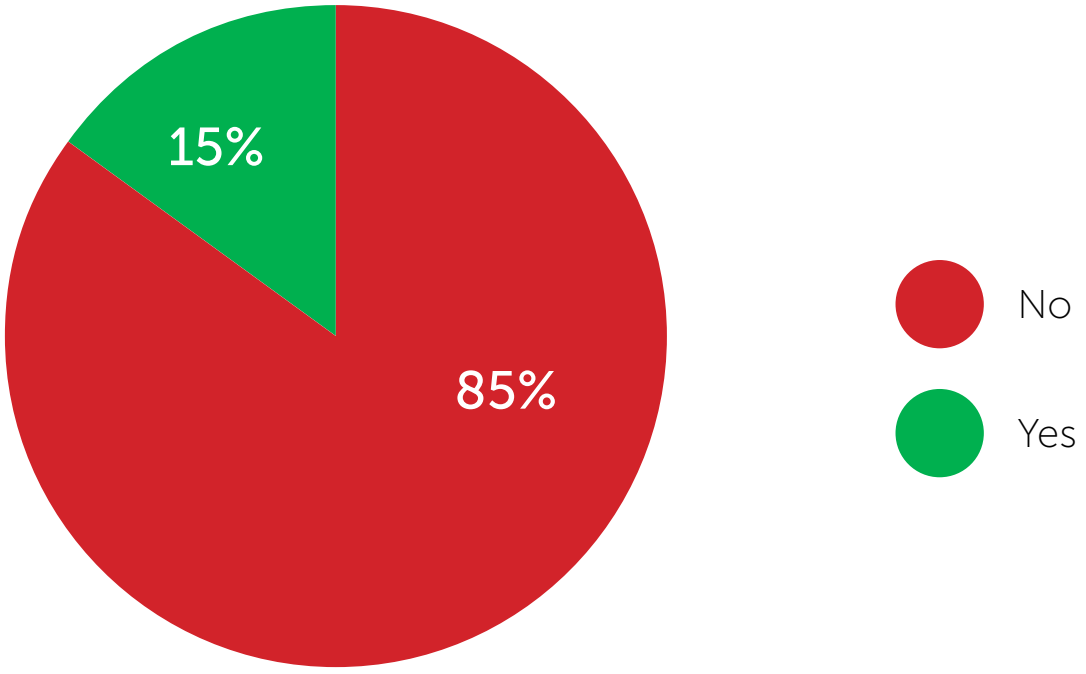


Figure 14 - Survey Results on Technical Measure

85% of those surveyed or interviewed were not aware of a functional national CSIRT or CERT that can respond to cyber threats in their country. This finding shows how unprepared the countries are in responding to national cybersecurity incidents and illustrates that perhaps efforts to provide a functional CSIRT and CERT need to be stepped up.

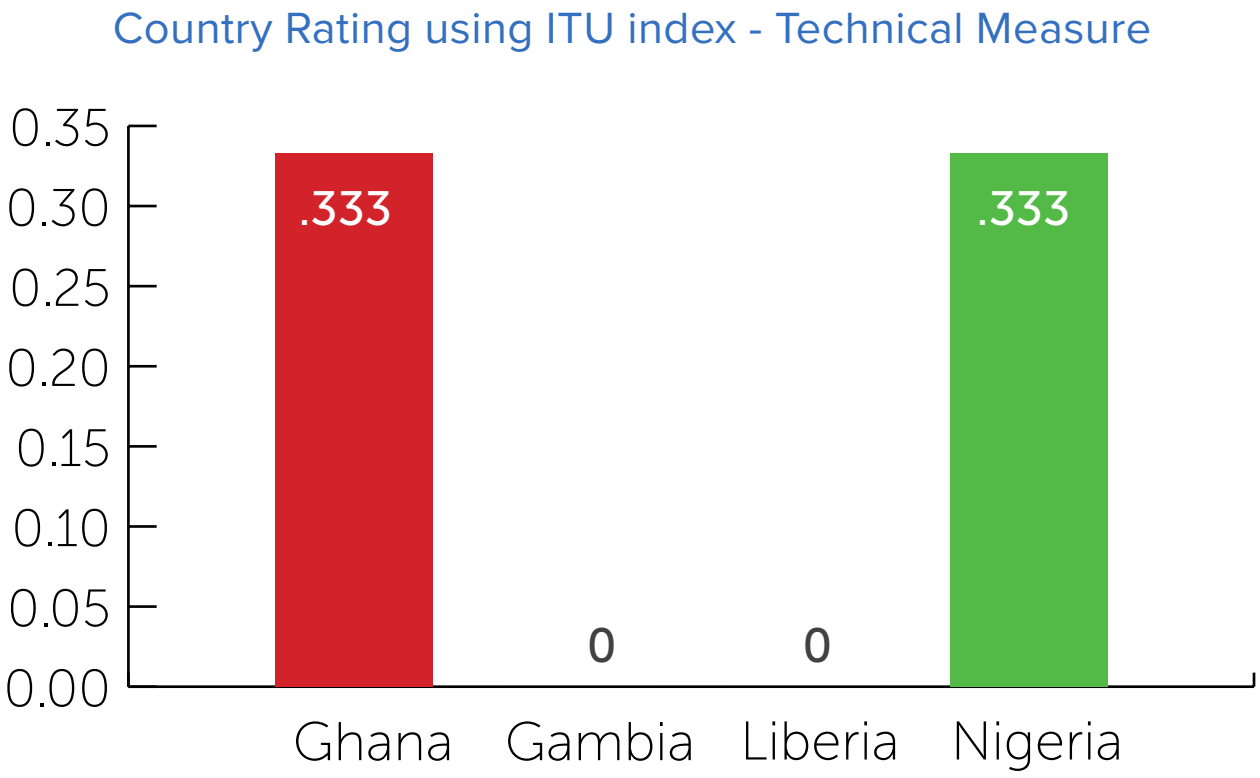


Figure 15 - Country Ranking on Technical Measure

Figure 15 shows the ranking of countries in relation to Technical Measures. Nigeria and Ghana both ranked highest in its efforts.

Organizational Measure

The government in collaboration with private sectors should be responsible for driving cybersecurity standards development, as well as establishing and meeting security baselines for critical and non-critical information and government systems.

Organizational measures are systematic procedures and processes used in the implementation and operations of national Cybersecurity agenda. Once the legal, technical measures and the supporting objectives have been set by a country, a consistent infrastructure should be completed to guide, manage and evaluate those actions.

> Without an effective organizational measures to guide the strategy, it will be difficult to measure and rank its effectiveness.

Technology advancement has been unstoppable and in most cases, changing very rapidly in the last three decades.

In the countries surveyed, Gambia and Liberia's, organizational procedures and processes have lagged behind in developing organization measures to counter cyber threats.

In 2015, Gambia made its first attempt at putting in place a Cybersecurity strategy. In Gambia's Request for Expressions of Interest, it recognizes the importance of constructing the institutions and building the capacity necessary for law enforcement to address the issues of Cybersecurity/ cyber crime/ evidential issues/ privacy and cyber-contracts.[1]

1 http://www.projects.worldbank.org

In our interview, we asked corporate leaders in the countries the following;

Do you think a documented national policy and procedure for tackling cybersecurity will be beneficial to your organization's readiness to tackle global cybersecurity challenges?

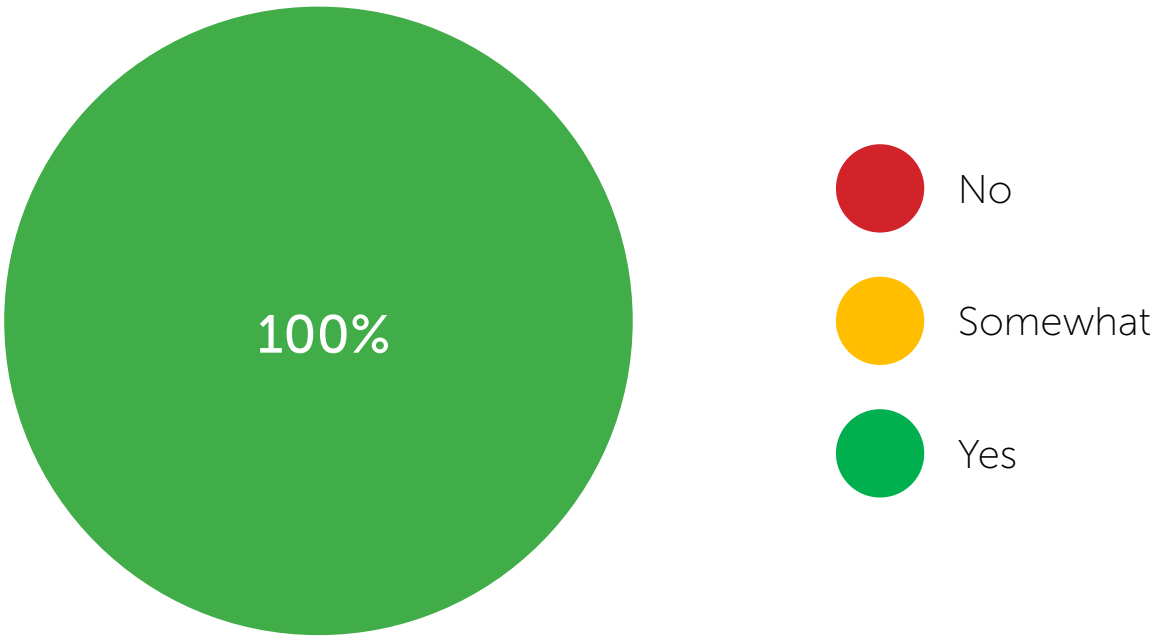


Figure 16 - Survey result on Organizational Measure

100% of those interviewed agreed that a documented national policy and procedure will help them be better organized and informed, to tackle cyber threats within their organization. This reaffirms the importance of systematic processes and procedure as a pillar of an effective national cybersecurity strategy.

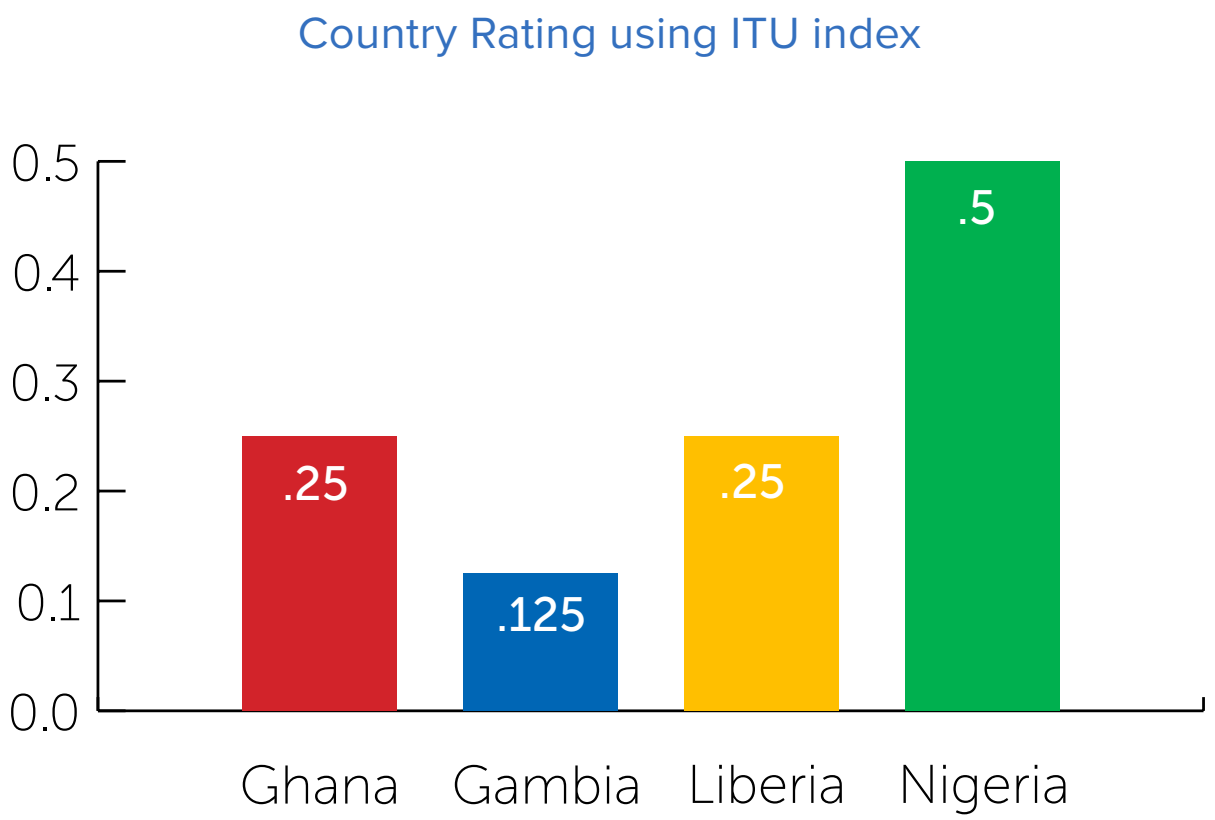


Figure 17 - Country Ranking- Organization Measure

Figure 17 shows the ranking of countries in relation to the Organizational Measures. Nigeria ranked highest in its efforts.

Capacity Building

Capacity building examines the level of professionals identified, educated and trained in cybersecurity and related computer education. The availability of qualified personnel with knowledge about cybersecurity policies and strategies can set the platform to develop the organization's skills and support structure needed to counter cyber threats.

We have to look at capacity building from the perspective and alignment of the other pillars used in the measurement of the readiness of the countries involved to counter activities of cyber threats.

There are international organizations, such as the ITU, ISO and COE among others that have standards in aiding and developing capacities to help countries fight cyber crime

Professional skill development is also a component of capacity building in the effort to counter cyber criminal activities. Institutions for training in Ghana, such as the Kwame Nkrumah University of Science and Technology have an Information Systems department charged with training and developing skills with computer knowledge. Almost all the university systems in Ghana and Nigeria have computer Science as part of their training programs. This is indicated also by numbers of certified professionals in each of the research countries. Gambia until 1999 did not have any higher institute of learning. (University).[1]

This potentially is one of the reasons for the low score. Most of the students who went overseas for advance education preferred to stay out of the country after their training.

1 http://africauniversities.org/gambia-2/

How many cyber security professionals do you have in your workforce?

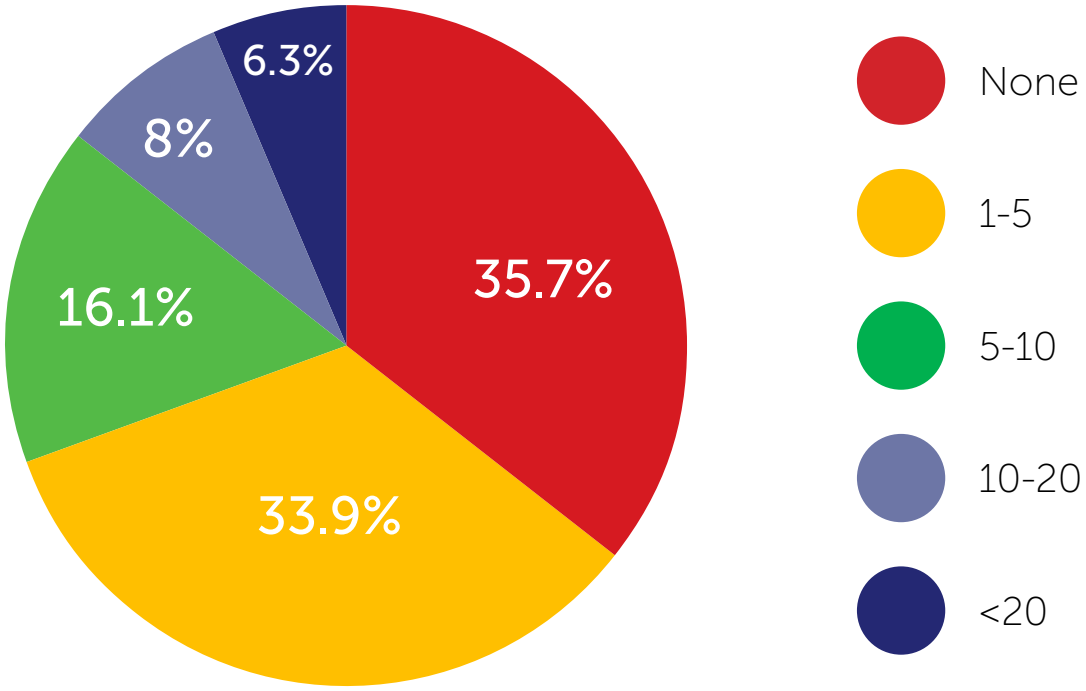


Figure 18 -Survey result on Capacity Building

Majority of those surveyed had zero or less than six cybersecurity professionals as shown in figure 18. Universities and other higher institutions need to do more to train the next generation of workforce dedicated to the discipline of cybersecurity.

Country Rating using ITU index

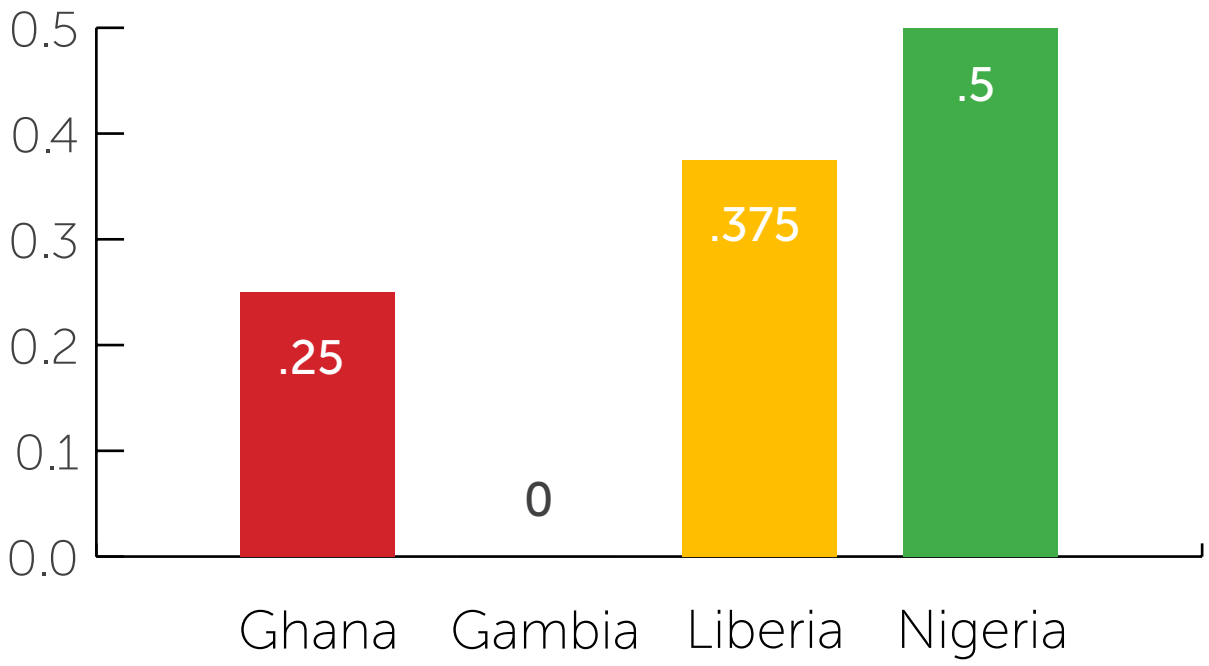


Figure 19 -Country Ranking - Capacity Building

Figure 19 shows the Capacity Building rankings of the countries involved in the survey

Cooperation

Efforts to develop and create awareness on the impact of cybersecurity within the West African region should not be carried out in isolation

Cooperation is the process of building alliances with and between institutions, both public and private and with other countries or global agencies, with the objective of countering cyber threats. With external cooperative alliances, Cybersecurity initiatives and capabilities can be consistent in the effort to defend, apprehend and prosecute cyber criminals across different national boundaries.

Through such collaborative processes, the regional members can launch aggressive and comprehensive mitigation strategies through joint investigations and operational partnerships with law enforcement partners, private industry, and academia.

Externally, the countries in the sub-region should have a cooperative effort in partnering for common cybersecurity objectives, risks and assessments. Beyond West Africa, the African Union organized a convention on Cybersecurity and Personal Data Protection. The preamble of the treaty established the legal framework for Cybersecurity and Personal Data Protection as a commitment for all member states. The treaty has been signed by 7 countries as at January 29, 2016.[1]

1 https://www.au.int/web/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

Ghana in March 2017, hosted a convention in collaboration with the Council of Europe and the European Union to set up a framework for cybersecurity response to the growing threats to nation development.[1]

When asked about the level of cooperation outside of the national borders, more than 70 percent of the correspondents agrees or somewhat agrees with the need to build mutually beneficial alliances outside their country, in order to combat cyber crime as shown by our survey result in figure 20.

Do you think your country or the region should work with other international bodies to address cyber threats?

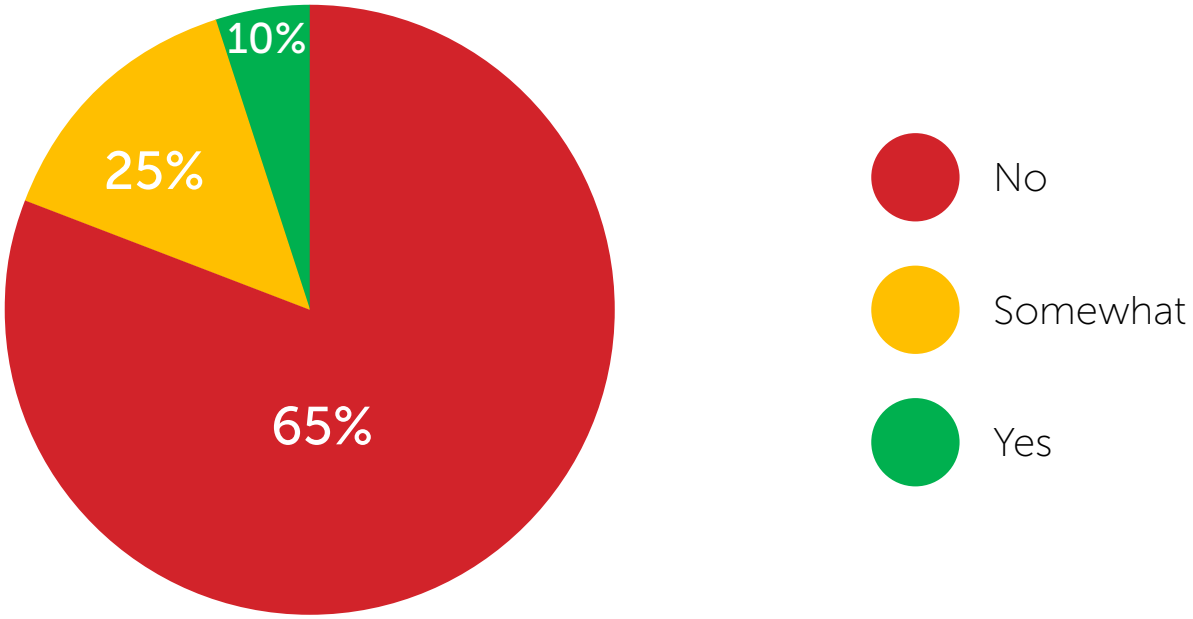


Figure 20 - Survey result on Alliance and Cooperation

1 http://www.graphic.com.gh/news/general-news/ghana-to-set-up-national-cyber-security-council.html

Country Rating using ITU index

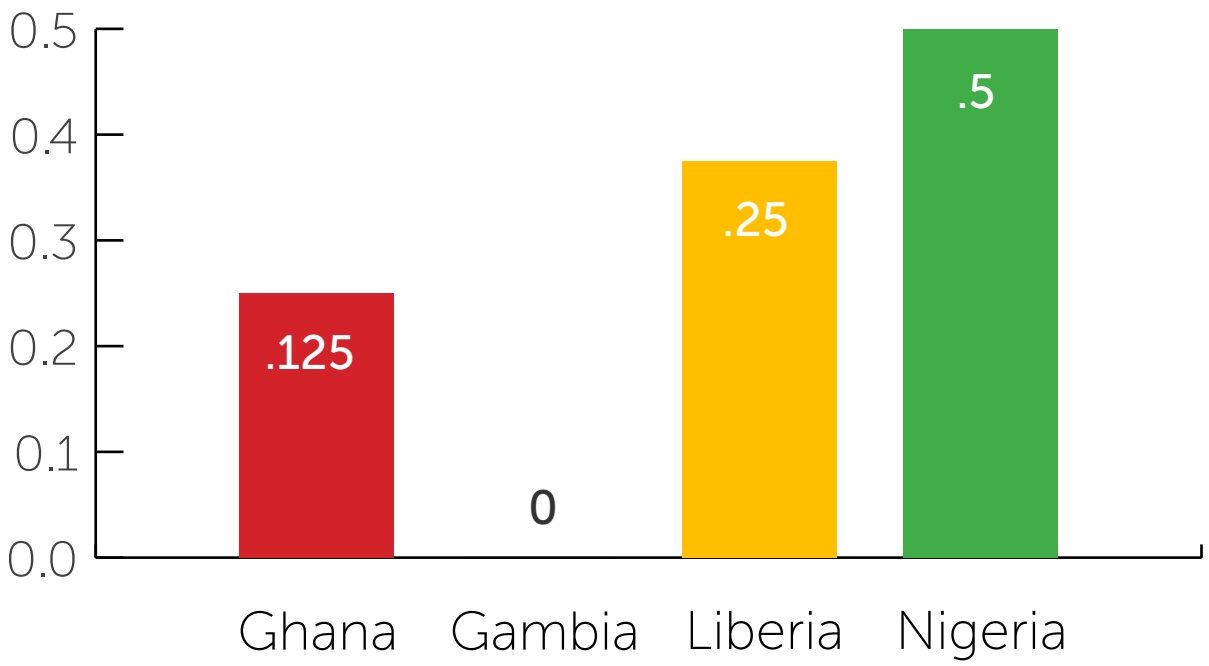


Figure 21 - Country ranking - Alliance and Cooperation

Cyber-Threat Result Analysis

This section looks at the most common cyber-attack vectors we encountered in the course of our research. We used one or a combination of the following methods to probe the security readiness of 20 public and private organizations in the region.

1. Vulnerability Analysis and Risk Assessment
2. Security Architectural Review
3. Social Engineering Assessment
4. Security Configuration Assessment
5. Security Interviews with SMEs supporting the organizations.
6. Review of data from global security providers.

70 percent of private and public organizations polled in the survey and analysis in the countries involved had little to no idea about the reality of cybercrime.

During one of our workshop with a top financial institution, several employees were deliberately sent phishing information as part of a test case to assess the readiness of the institution and its employees to the threat vectors of cyberattacks. Almost 90 percent of the respondents on the email succumbed to the attack.

At one of the government institutions in the survey, security policy was not thought of in their normal operations. The use of shared password and other poor security practices such as the use of telnet and unattended computer systems, placed the end user data at risk of being breached.

Although there are many types of attack vectors used by cybercriminals, our report is limited to the top three predominant types seen in our assessments of public and private organizations that participated in the research.

Client-Side Vulnerabilities Attacks

Client-based attacks are unpredictable thus they pose a significant challenge to public and private organization in West Africa. The adoption of cloud based services such as office365 has elevated the browser to the new gateway between organization's network and the Internet. With increasing global trends where cyber criminals exploit client-side vulnerabilities, we expect an increase in browser based attacks within the region.

A Web browser is a software application that allows users to view and interact with content on a web page, such as text, graphics, video, music, games, or other materials.[1]

Browsers like all applications on connected systems, are coded. Without appropriate security patches applied, web browsers are vulnerable to attacks or exploits.

1 en.wikipedia.org/wiki/Web_browser

Even a fully updated web browser can still be susceptible to attacks or exploits if the browser plug-ins and other required components are not updated. Plugins are bits of upgrades added to browsers to make them view and present some web applications better.

It is important to remember that plug-ins are not automatically patched when the browser is patched.[1]

Typically, browser-based attacks originate from bad websites. However, due to poor security coding of web applications or vulnerabilities in the software supporting web sites, attackers have recently been successful in compromising large numbers of trusted web sites to deliver malicious payloads to unsuspecting visitors.

Figure 22 shows the browser distribution of the participating organizations in our research.

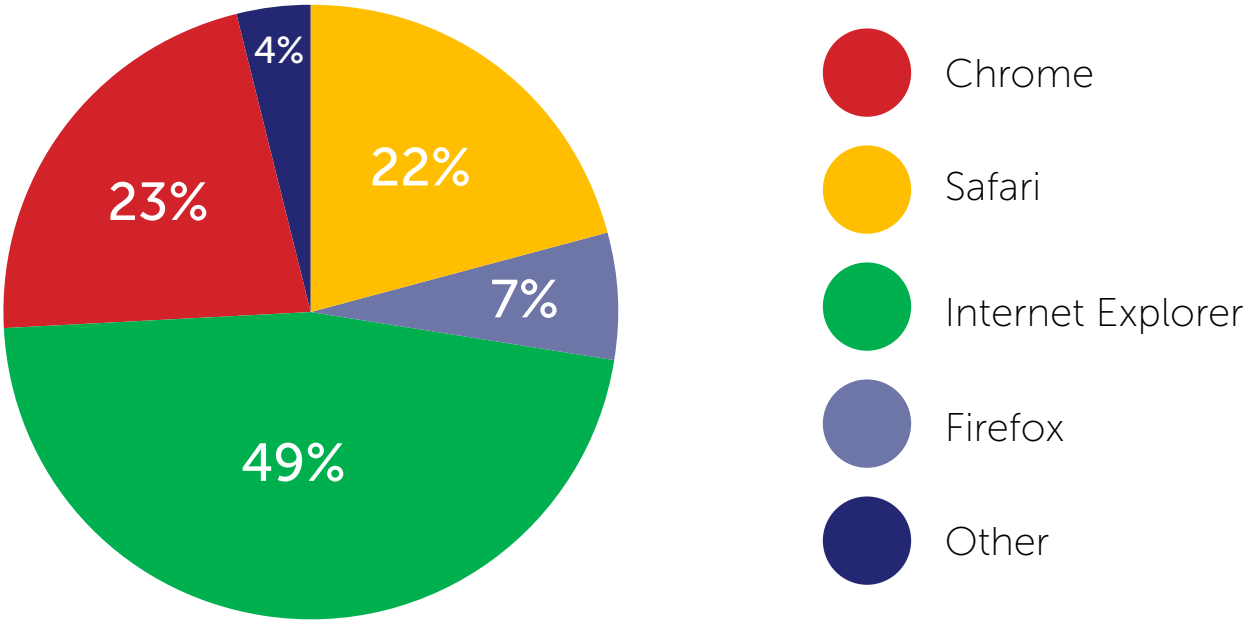


Figure 22 -Browser Distribution

1 https://www.pvamu.edu/Include/ITS/Vol3Issue2.pdf

In our assessments, we found 56% of browsers in use were outdated. Several critical OS security updates were also found to be outdated at more than 80% of the organizations. A screenshot from one of our results is shown below;

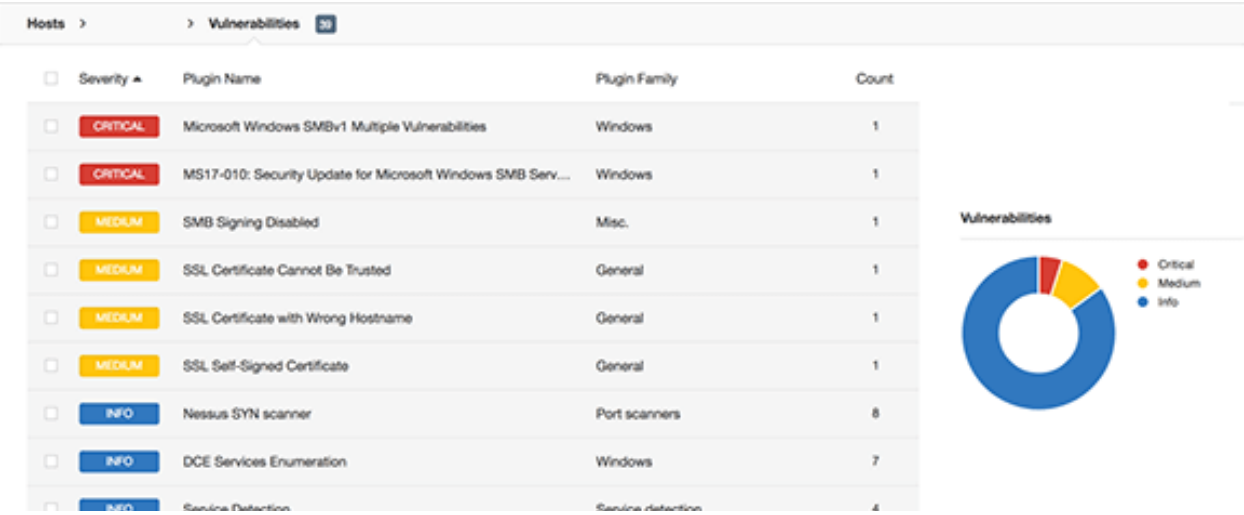


Figure 23 -Vulnerability Assesment

We observed that most of the security operation teams were more focused on protecting network perimeters. Very little attention was placed on client-side vulnerabilities, discounting the fact that most intruders that gain access to an end-user, often also gain access to company sensitive data or could use the end-user's device as back-door to infiltrate further into the organization.

Trends from Google Transparency[1], a database that tracks and categorizes by Autonomous System (AS), weekly activities of networks that hosts malware sites. The findings shows recent upticks in number of malicious or compromised sites that are being hosted in some AS within the region.

1 Google Transparency Report

The Following Charts shows the percentage of malware distribution based on the estimate of the ratio of sites on the AS that Google has recently scanned.

AS 37282 – MainOne Nigeria.

Figure 24 - AS 37282

AS 37170 - University of Lagos (UNILAG), Nigeria

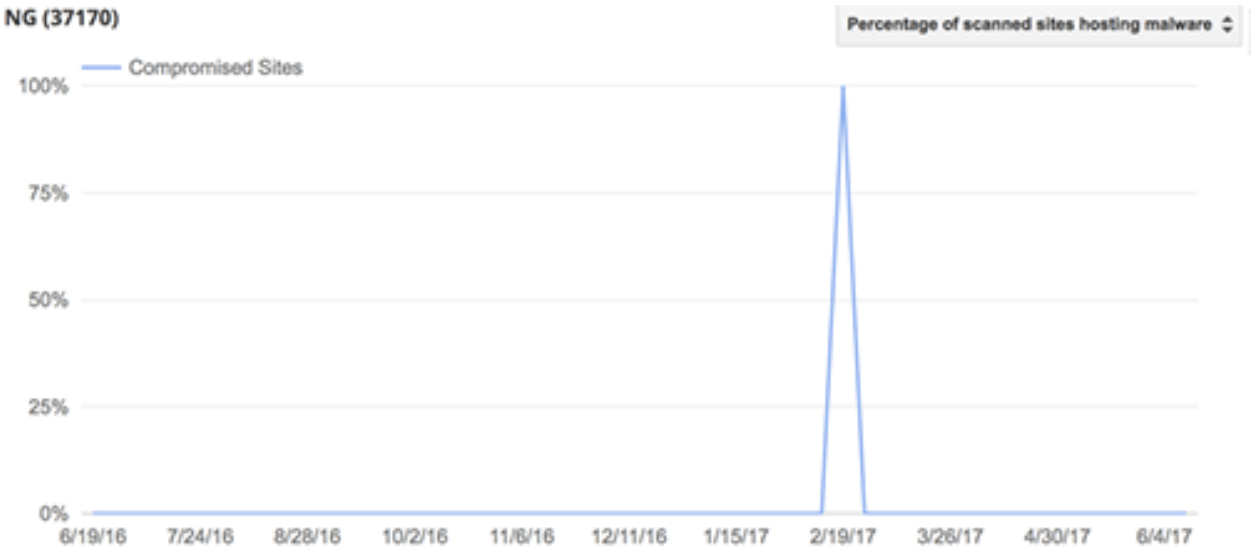


Figure 25 - AS 37170

AS 36900 - Engineering Systems and Services Ltd, Ghana

Figure 26 - AS 36900

AS 37309 QCell Gambia.

Figure 27 - AS 37309

Social Engineering

Social engineering attack vectors such as Phishing are deceptive attacks where cybercriminals impersonate an official or legitimate source by using spoofed emails and/or fake web pages impersonating as trusted sources, in an attempt to steal sensitive information from end-users.

In the case of fake emails, they are typically perceived by the end-users as legitimate emails. Unlike other attacks, phishing does not directly target the systems, instead it targets the end-users that uses these systems. Phishing has become one of the most effective attack vector, since It takes one careless employee to take down an entire organization.

With the proliferation of do-it-yourself phishing kits, the attack is becoming very difficult to detect, as attackers are almost able to create domain as real and close to the target user's service domain. The methodology of this attack is to get the user to think they are signing onto legitimate services. Once their critical information is collected, the results can be very damaging to the user or the institution.

In our simulated phishing campaign conducted, we used simulated phishing emails that attempted to originate from the human resources department. The actual domain name of the email was slightly modified. In one organization, 90 percent of the respondents clicked on the simulated phishing link. 60 percent entered their user credentials.

Key metrics tracked during our Phishing campaign included:

1. Number of users that opened the email.
2. Numbers of users who clicked on a link within the email
3. Number of users who entered their credentials on the phishing site.

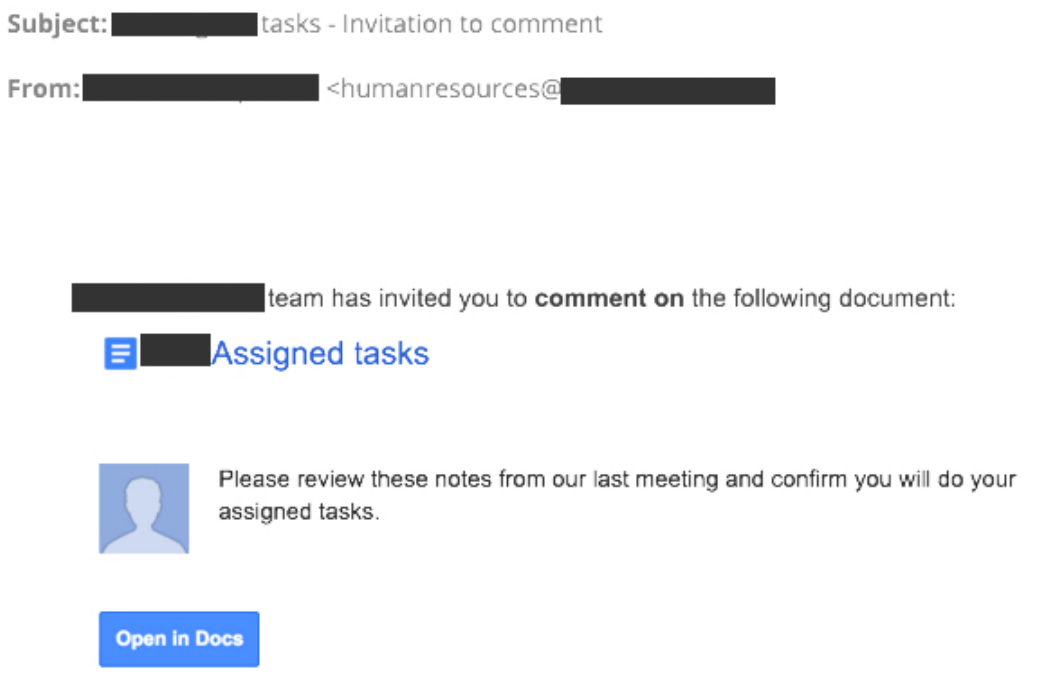


Figure 28 - Phising Email used in one of the campaigns

User Results to Simulated Phishing Email

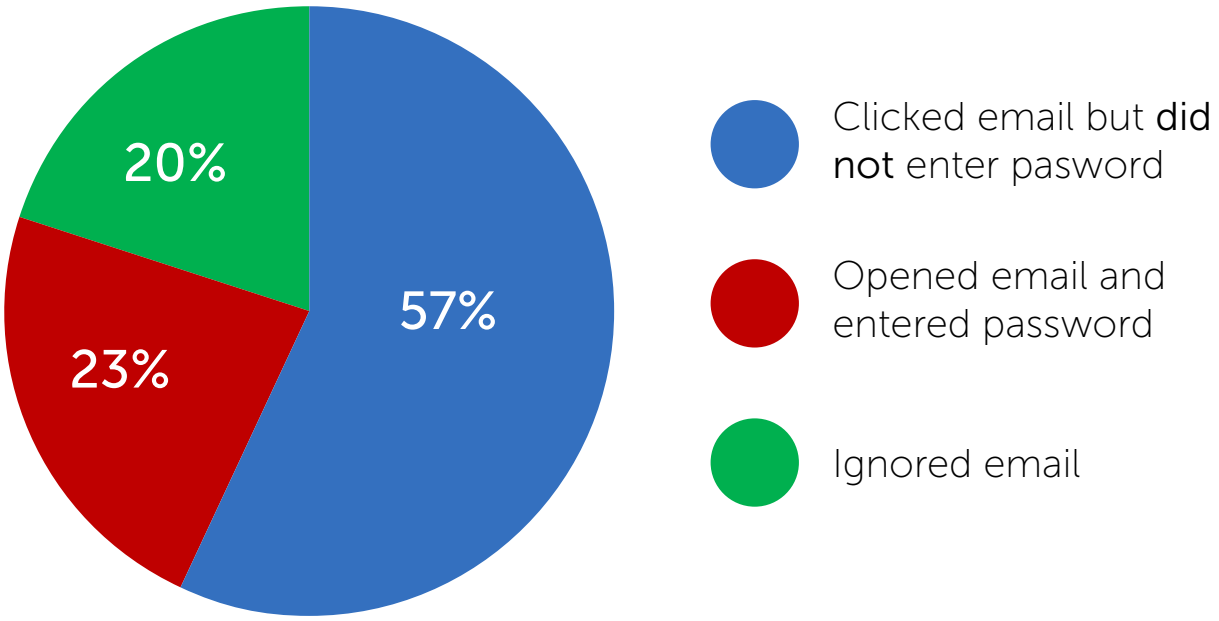


Figure 29 -Phising Assessment Result

Only 10 percent of the organizations in the research, used some form of Multi-Factor Authentication (MFA).

Mobile Device Vunerabilities

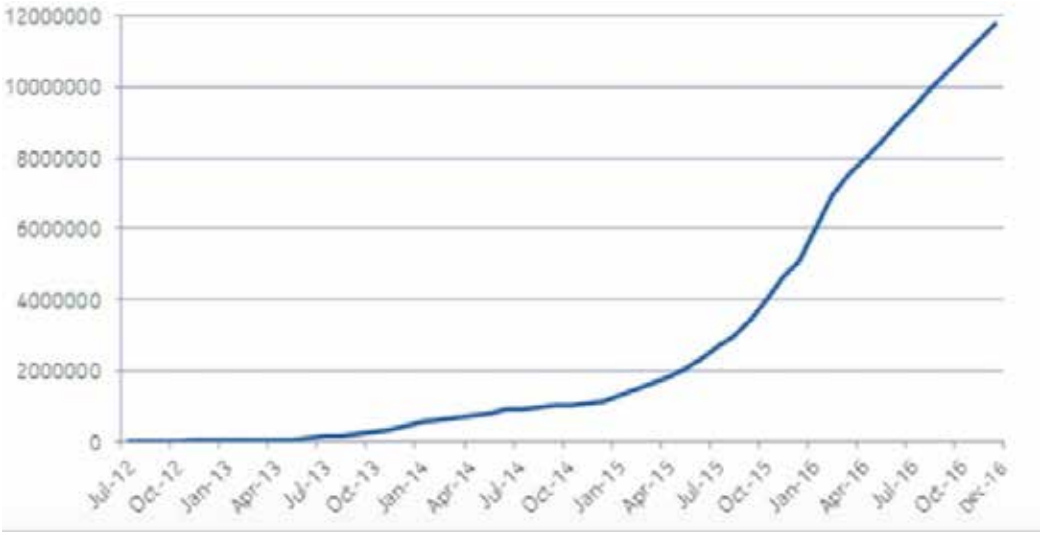
The rise in the use of mobile devices is a major factor changing the security threat landscape in West Africa. Millions of consumers are already using mobile devices to conduct banking and other daily activities such as social media.

With increasing computing power in smart phones, mobile smart phones are set to become the preferred method of business and personal computing in West Africa.

Mobile devices are increasingly being connected to corporate Wi-Fi networks as individuals become more reliant on them to conduct daily activities. Such actions increase the attack surface in the organization, as more cyber-criminals target mobile devices.

According to a 2016 Threat Intelligence Report by Nokia, there has been a surge of 400% in smartphone malware attacks in 2016. The report further stated that the second half of 2016 saw these malware attacks rise by 83%.[1]

> A very staggering number that can have negative socio-economic impact in West Africa.



1 2016 - Nokia Threat Intelligence Report

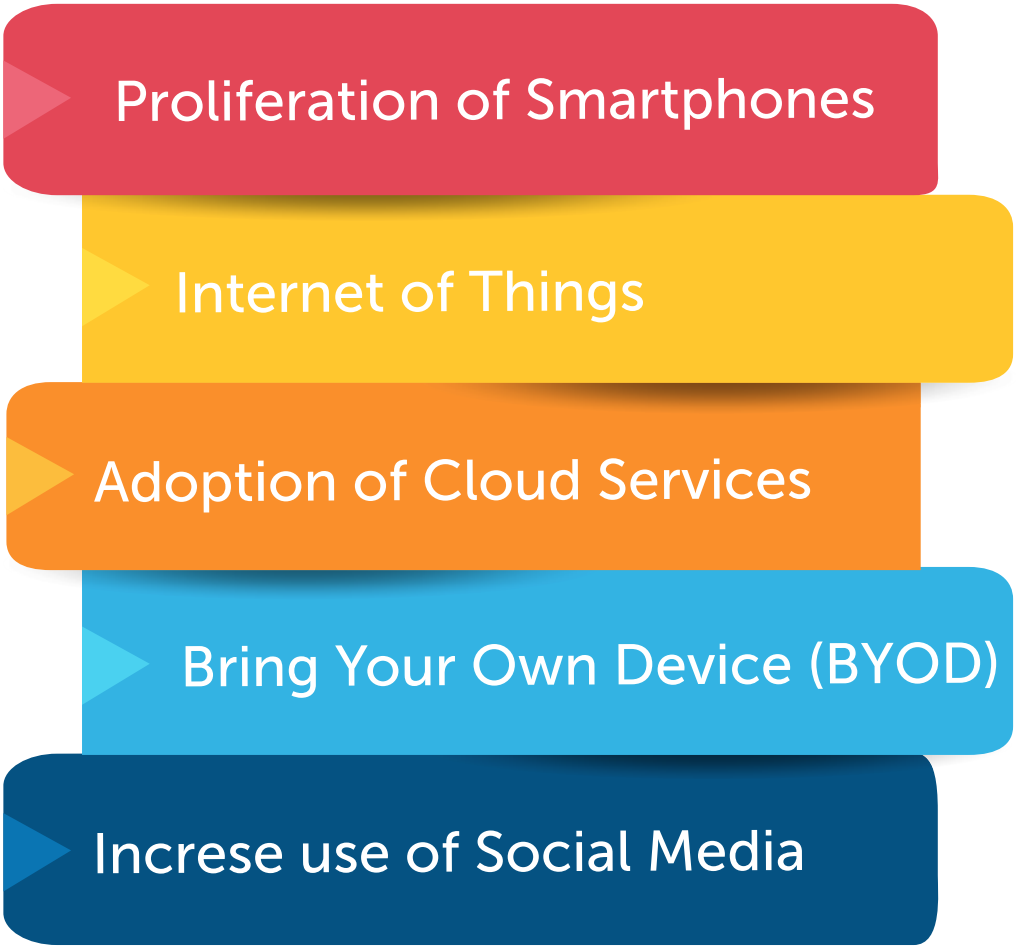


Figure 30 - Trends Impacting Security in W.Africa

West Africa is a sub-region on an upward swing towards economic, political and social growth. Almost all the countries have had democratic elections and peaceful transition to political change. According to WorldoMeters, a global organization dedicated to tracking changes in global demographics, West Africa is home to over 371,839,034 million people with a median age of just 19.5 years, one the youngest population in any part of the world. the world.[1]

The explosion of technology coupled with the growth of the Internet and electronic accessibility of daily activities leaves a large swath of the population with systems that are potentially vulnerable. With this growing population and access to connected systems however comes new risks and vulnerabilities that could undermine progress. Prime among these is the global rise of cyber-crime.

1 http://www.worldometers.info/world-population/western-africa-population/

1. Proliferation of smart phones

A report by GSMA Intelligence indicates mobile Internet adoption in Africa continues to grow rapidly; the number of mobile Internet subscribers tripled in the last five years to 300 million by the end of 2015, with an additional 250 million expected by 2020.[1]

The more access is available, the larger the pool of vulnerable systems. According to available figure for 2017, the number of smart phones in Nigeria is 28,381,000.[2]

The Ghana National Communication Authority's mobile voice and mobile data market share trends for December 2015 also reported the number of mobile data subscribers rose from about 17.73 million to 18.03 million, an access rate of 65.74 percent.[3]

Liberia had a record 395,063 people with access to the Internet in 2016.[4]

Gambia has 373865 Internet users as of March 2017.[5]

Globally, smart phones are an increasingly attractive target for cyber criminals who are investing in more sophisticated attacks that are effective at stealing personal data or extorting money from victims. As access to smart phones become cheaper the vulnerability vectors also increase.

---

1 The Mobile Economy Africa 2016, GSMA Page 5

2 http://resources.newzoo.com

3 http://www.theafricareport.com/West-Africa/ghana-mobile-phone-penetration-soars-to-128.html

4 http://www.internetlivestats.com/internet-users/liberia/

5 http://www.internetworldstats.com/africa.htm#gm

Do you think the proliferation of smart phones and mobile devices puts your company security at risk?

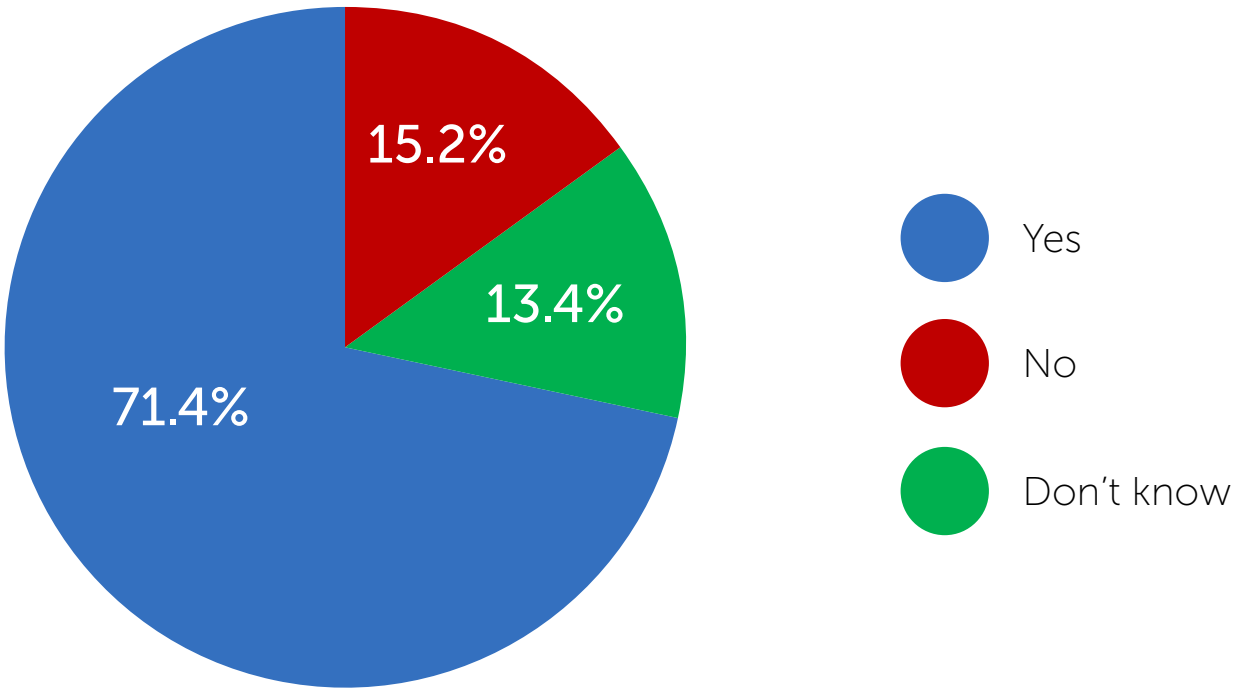


Figure 31 - Proliferation of smart phone - survey results

More than 70 percent of participants in our research felt the proliferation of smart phones and mobile devices puts their company or organization at risk.

2. Internet of Things

Internet of Things is enabling systems to be connected at an incredible pace. With the availability of IP addresses for most consumer and industrial products, new spheres of vulnerable systems are opening up. Most of these devices are insecure with inherent difficulties in updating their firmware and codes. “Smart everything” is opening up opportunities for cybercriminals to continue the trend of criminally affecting these systems. We expect IOT devices to increase in Africa alongside with global projection.

2010, IBM: “A world of 1 trillion connected devices” by 2015.
2011, Ericsson’s CEO Hans Vestberg: “50 billion connected devices” by 2020.
2013, Cisco: “50 billion things will be connected to the Internet by 2020.”
2013, ABI Research report: “30 billion” by 2020.
2013, Morgan Stanley report: “75 billion devices connected to the IoT” by 2020.
2014, an Intel infographic: “31 billion devices connected to Internet” by 2020.
2014, ABI Research updated report: “41 billion active wireless connected devices” by 2020.
2015, Gartner Research: “4.9 billion connected things in use in 2015 … and will reach 20.8 billion by 2020.”

Figure 32-global projection of IOT devices – credit: rcrwireless.com

3. Proliferation of Cloud Services

Cloud solutions offer businesses in West Africa opportunities which were hitherto only available to big corporations. Several "X as a Service" solutions have enabled small and large organizations access to telecommunications and network infrastructure solutions easily. This trend comes with its inherent opportunities for cyber criminals. Microsoft is the latest technology company to fully announce a cloud infrastructure solution in Africa.

4. Bring Your Own Device(BYOD)

This trend is expected to increase as different forms of telecommunication becomes available to employees and employers in West Africa. Employees are using smart devices to continue work activities at home, on the road and several other places. In most cases, the access media are not properly secured. This leaves a big vulnerability gaps for cyber criminals to take advantage of.

5. Increase use of social media

In 2014, 100 million people were using Facebook each month across Africa, over 80% via mobile. That figure has now jumped to over 120 million in 2015. [1]

- 220,000 Facebook users on June/2016,
- 3,500,000 Facebook subscribers for June/2016
- 330,000 Facebook subscribers on June/2016
- 6,000,000 Facebook users on June/2016.

1 http://www.cnn.com/2016/01/13/africa/africa-social-media-consumption/index.html

Top Cyber Security Threats in West Africa by Industry

Top 3 verticals with the most exposure to cyber crime activities

Banking & Financial Institutions

Available information from all four countries put the Banking and Finance sector as the most vulnerable to cyber attacks.

> "Nigeria looses N127b annually to Cyber Crime."[1]

1 http://dailypost.ng/2017/03/08/nigeria-losses-n127b-annually-cyber-crime-buhari%E2%80%8E/

"Brussels-based SWIFT, a cooperative owned by more than 11,000 global financial institutions with connection in over 200 countries financial institutions warned in early 2016, financial institutions should take additional internal and external measures to close gaps in their security. Unknown hackers breached the computer systems of Bangladesh Bank and in early February attempted to steal $951 million from its account at the Federal Reserve Bank of New York, which it uses for international settlements. Some attempted transfers were blocked, but $81 million was transferred to accounts in the Philippines in one of the largest cyber heists in history."[1]

"In the year 2015, the Information Security Society of Nigeria (ISSAN) revealed that 25% of the cybercrimes in Nigeria are unresolved and that 7.5% of the world's hackers are Nigerians."[2]

"From the information that we have from the Central Bank, potential money loss if all the fraudulent transactions had gone through will be about seventy million cedis... The hack into emails and take hold of correspondences and instructs banks to transact businesses on their behalf...We also have issues of ATM fraud, where cards are cloned."[3]

- Phillip Owiredu Chief Executive Director of CAL Bank

1 www.swift.com

2 http://dailypost.ng/2017/03/08/nigeria-losses-n127b-annually-cyber-crime

3 http://citifmonline.com/2016/05/21/bog-banks-tighten-security-against-fraud/

Do you know of a company or institution that has been at the end of an infrastructure breach in the last 12 months?

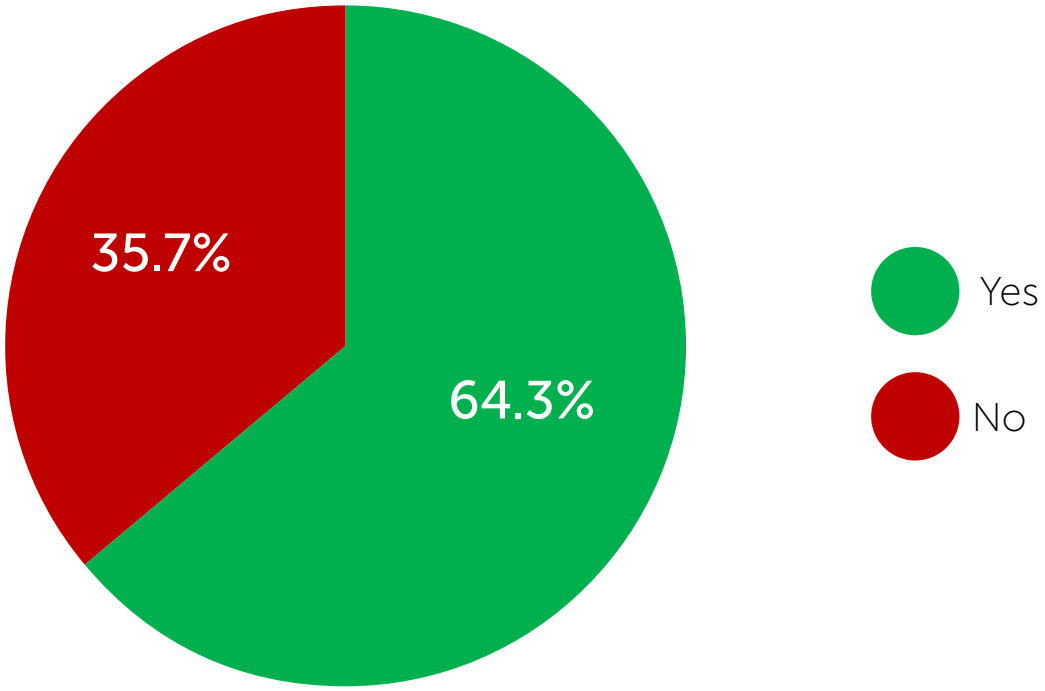


Figure 33 - Survey results for Banks and Finacial institutions

More than 60% of those surveyed within the Banking and financial institutions have been victims or have known victims of cyber crime in the last 12 months.

Government

All 4 countries had one attack trend in common. The hacking of electoral systems and government websites.

> "Hack attacks cut Internet access in Liberia."[1]

> "The official website of Gambia's Government House has been shut down by suspected hackers after disputed electoral results."[2]

> "Hackers Paralyzed Computers at Gambia's U.N Perm Mission."[3]

> "Hackers have targeted the website of Ghana's electoral commission as votes are counted after tightly contested elections."[4]

> "The majority of the Ghanaian government's websites, including its main site, have been hacked and are currently offline."[5]

1 http://www.bbc.com/news/technology-37859678
2 http://www.informationng.com/2016/12/gambian-governments-website-hacked.htm
3 http://thegambiaecho.com/
4 http://www.bbc.com/news/world-africa-38247987
5 http://www.bbc.com/news/world-africa-

Has your company conducted a cybersecurity vulnerability assessment in the last 12 months ?

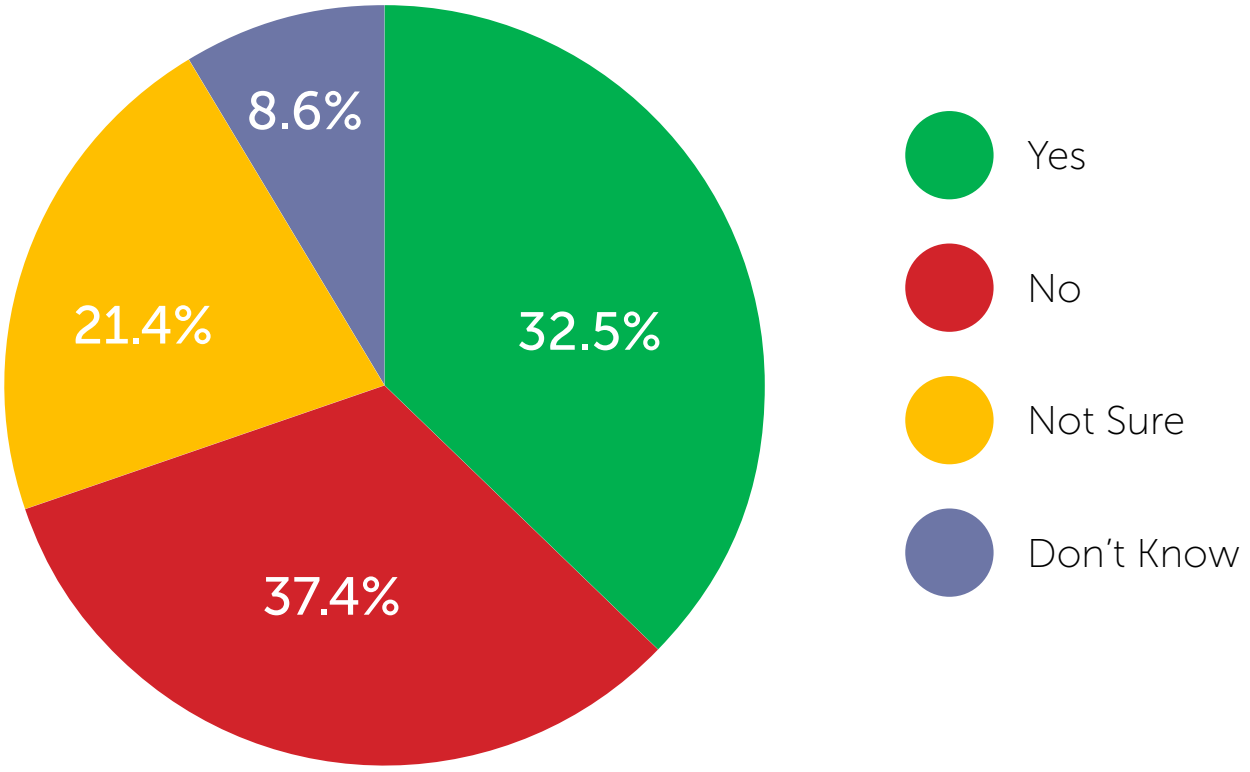


Figure 34 Vulnerabilities Assesment

More than 60 percent of those surveyed in the public sector had not conducted vulnerability assessments in the last 12 months

The level of responses to cyber threat were at different levels in each country. Public officials interviewed in all the countries agreed more state intervention was needed in combating the threats in cyber-space.

Telecommunications/MNOs

Network bypass theft and other incidents of cyber intrusion continue to plague the Telecommunication industry in all four countries, even as they look forward to invest in new technologies to boost their security and infrastructure.

> Responses from telecommunications companies when asked if they have specific budget set aside for cybersecurity, showed that more than half had no budget set aside for security.

Do you have specific budget set aside for cyber security planning and incidents?

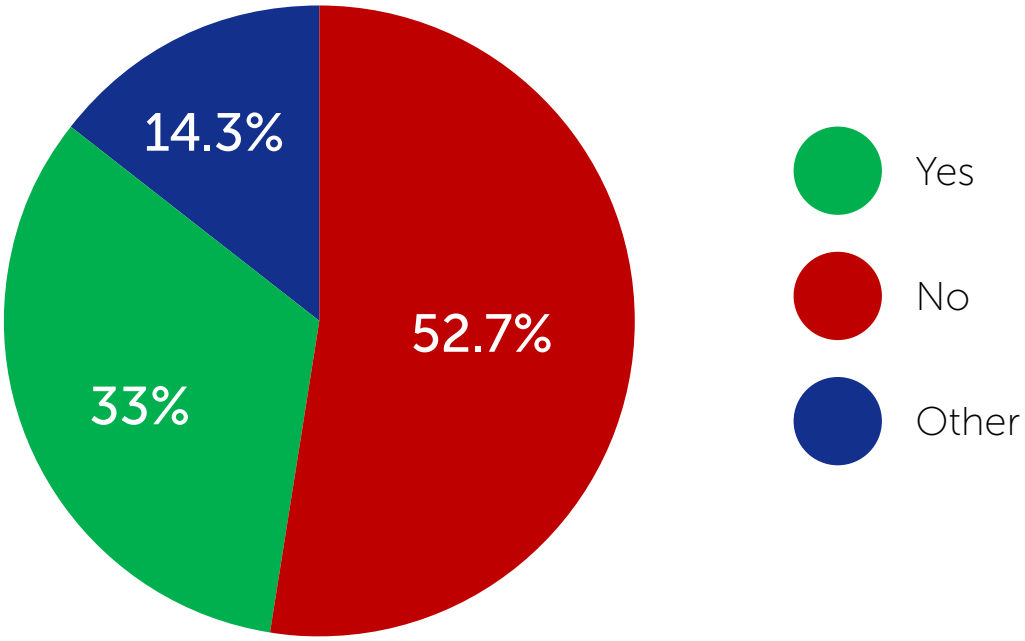


Figure 35- Telecoms and MNO survey results

Some of the respondents interviewed, acknowledge the “sim-card swap” as an issue. This is an attack vector is expected to rise. It involves cyber criminals hacking the user phones and stealing data embedded on the cards. The data is used in mobile money transfers. Analysis of this type of breach indicates that insider information is part of this attack vector.

Telecommunication operators surveyed also believed they were losing revenue of about 20% due to illegal system access. This network breach is known as SIM Box fraud.

100% of responses indicated awareness of available hacking tools for accessing their network to compromise mobile money transactions.

Best Practice for Developing a National CyberSecurity Strategy

The threat of cyber attacks within countries in West Africa will not be curbed without specific and targeted efforts by the countries in the sub-region. These efforts should have cooperation as part of the framework to be successful. As most organizations and individuals who have been victims of criminal cyber activity can attest, this is a very expensive cost to their organizations or individuals. Unlike other criminal activities, cyber attacks do not reside in a particular boundary, hence the difficulty in creating normal rules for them.

With the acceleration of technology, countries and global organizations as well as individuals are going to be more connected than ever. The vulnerabilities that comes with these developments will therefore increase.

Efforts in fighting against cyber issues should be a continuing offensive approach. Equally in this effort should be a good defensive approach by the countries.

From our research and feedback, Ghana and Nigeria already have some actions, strategies and frameworks to thwart the scourge of negative cyber activities. The Government cannot do it alone. Businesses are responsible for protecting customers' personal data. Individuals need to practice good cyber practices to keep personal devices and data safe. If we each do our part to use our systems and devices responsibly, then collectively we can help to protect West Africa's cyber infrastructure.

We put forth a regional framework to complement the already established efforts for the countries to aid in the fight against organized cyber-criminal activities.

DEVELOP A RESILIENT NATIONAL INFRASTRUCTURE

- Protect the national fundamental services
- Respond positively and strongly to cybersecurity threats
- Improve governance and legal framework by making it explicit to the entire citizenry
- Secure government, public and community network infrastructure
- Drive cyber security from the top down with governmental and industry leadership support
- Establish a layered approach for sharing real time public-private cyber threat information through cyber threat sharing centers
- Update already established frameworks on cybersecurity threats through cooperation with international cybersecurity Agencies
- Support small and big businesses access to cybersecurity Readiness and Assessment report at least annually
- Conduct cybersecurity Readiness Assessment for Public and Private organizations.

CREATE A SAFE CYBER SPACE FOR THE COUNTRY

- Create an offense and defense effort to combat cyber crime
- Develop and promote country as a trusted hub for technology innovation
- Promote responsible use of technology
- Boost education in cyber security training to develop skilled manpower to support national efforts against cyber crime

NURTURE A VIBRANT CYBER SECURITY ECOSYSTEM

- Create a national cyber security certification to develop a professional Cyber-Security workforce
- Establish or develop existing facilities into specialized areas to develop local talent to create a specialized local response towards cyber security
- Collaborate with academia, for profit and non-profit cyber security institutions to develop innovative ideas and capabilities

BUILD STRONG INTERNATIONAL PARTNERSHIPS

- Sign on with international organizations dedicated to countering cyber threats and cyber-crime
- Facilitate international cyber security capacity development initiatives
- Participate in global and regional discussions on cyber security practices, policies, legislation, cyber security deterrence and cyber-crime cooperation.

With a young population that is rapidly adopting new technologies, West Africa is fast reaching an Internet explosion usage. The current cyber threat landscape in West Africa shows users are being impacted both by threats that are trending globally as well as some that more specific to the sub region. Some of the efforts to combat Cyber threats have been outlined in the Best Practice for Developing National Cybersecurity Partnership section of this report.

The entire sub-region and its industries are highly vulnerable to negative cyber activities. Even though the attack vectors have been escalating, they are not up to the level of what is happening in developed countries.

Cybercriminals are starting to wake up to the fact that West Africa is a gold field with wide open systems.

Ewu risk

Moving Cybersecurity from an era of Vulnerability Remediation to Risk Management

EWU Risk Management

- Construction
- Healthcare
- IT
- Mining
- Banking & Finance
- Oil & Gas

See more at **myewu.com**

3T Solutions Consulting

To find out more about 3T Solutions Consulting visit:
http://www.3tsconsulting.com

GLOBAL HQ

USA: FLORIDA
13194 US HWY 301 S.
STE 316 RIVERVIEW, FL
33578
+1.800.310.1433 Ext 1001
+1.813-778-5619
info@3tsconsulting.com

EMEAR HQ

GHANA: ACCRA
2 AKO ADJEI STREET
EAST LEGON, ACCRA
+233-244-986-966
+1.800.310.1433 Ext 1001
info@3tsconsulting.com

WEST AFRICA

NIGERIA: LAGOS
6B, BENDEL CLOSE OFF
BISHOP ABOYADE COLE
VICTORIA ISLAND,
LAGOS 101241
+234-813-537-9704
+234-802-840-4873
info@3tsconsulting.com

ASIA PACIFIC

INDIA: HYDERABAD
PLOT NO: 121, NO: 101
SRI DINESH RESIDENCY
ROAD NO: 6
BALAJI NAGAR,
NIZAMPET 500090
+91-4040078027
info@3tsconsulting.com