Nigeria Security Intelligence Report

Theme: Cyber Security

AUGUST 2020

Insight

Our digitized world – in numbers

Over 60% of the world is online. Global internet penetration has reached new heights as 298 million people joined the online community in 2019.

Africa accounts for 27% of the total global internet users. The average internet user spends 6 hours and 43 minutes online each day. Cumulatively, it is expected that you will most likely spend 100 days online this year.

More people are worried about their privacy. 64% of global internet users showing concerned about how companies use their data.

The rate of e-commerce adoption is on the rise globally. An estimated 75% of the world's internet users aged 16 to 64 buy something online each month.

- With over 2.5 billion active users, Facebook tops the charts among the social platforms.
- 169.2 million Nigerians have mobile (phone) connections. This represents 83% penetration of the total population of 203.6 million people. Nigeria ranks at the top of the list of African countries based on the share of traffic via mobile.
- 85.49 million Nigerians have internet access (42% of the total population).

Cyber Threats

- A cyber threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber-attacks include threats like computer viruses, data breaches, and Denial of Service (DoS) attacks, etc. While many of these attacks are merely nuisances, some are quite serious, even potentially threatening to human lives.
- Cyber-attacks can cause electrical blackouts, failure of military equipment and breaches of national security secrets. They can result in the theft of valuable, sensitive data like medical records. They can disrupt phone and computer networks or paralyze systems, making data unavailable. Indeed, cyber threats may affect the functioning of life as we know it.
- The threats are growing more serious, too. Cyber security risks pervade every organisation and are not always under the direct control of IT. Business leaders are forging ahead with their digital business initiatives, and those leaders are making technology-related risk choices every day.
- As an example, on July 17, Twitter suffered an embarrassing cyber-attack. Hackers broke into a number verified accounts of popular individuals like Bill Gates, Jeff Bezos and Elon Musk, sending out tweets offering to send $2,000 worth for every $1,000 sent to an anonymous bitcoin wallet. During the short period the wallet link was shared, over $100,000 donations were made.

Search light on Nigeria's cyber-attacks

- Organisations in Nigeria suffer more cyber-attacks than any other country in Africa. According to a report by Sophos, a UK-based cyber security company, 86% of Nigerian organisations surveyed said they suffered cyber-attacks in the last 12 months; the second-highest after India.
- Importantly, the country ranked in the top five for major attacks including malware attacks, ransomware, stolen account credentials and crypto-jacking. 64% of cyber-attacks in Nigeria exploited misconfigurations on the organisation's server.
- The financial sector looses an estimated $450million to digital fraud annually, being the most IT-driven sector in Nigeria. The most pervasive crimes in the country remain electronic fraud using automated teller machine (ATM) cards and electronic banking platforms.
- Nigerian organisations suffered the most data leaks than any country surveyed in the report. 57% of Nigerian organisations claimed that their public cloud data was exposed in 2019. Meanwhile, 46% of Nigerian organisations claimed that their account credentials, the method hackers used to attack Twitter, were stolen in the last 12 months.
- These are scary threats with increasing threat levels as the internet adoption increases, including growing digitization of enterprise activities like manufacturing and payroll with the pandemic forcing more workers in the services industry to work from home, the attack surface for cyber-attacks has widened, putting more IT systems at risk.
- More local cybercriminals are doubling down on international scams such as dating scams and business email compromise schemes. In the last half of 2019, international anti-fraud efforts led to the arrest of over 100 Nigerian scammers and the disruption of over $100 million in fraudulent transactions.
- Several reports have shown Nigerian hackers participating in malicious activities on the global cyber sphere such as the $3 billion heist recently reported by the FBI that affected over 500 companies in over 50 countries including Germany, United Arab Emirates (UAE), India and Russia.

- The Australian Competition and Consumer Commission categorically list Nigerian scam as a specific type of scam in the country. “419,” synonymous to Advance Fee Fraud (the name 419 is in reference to the section of the Nigerian criminal procedure code that deals with the crime) and has been internationally recognised as a form of fraud that originates from Nigeria.

- The word ‘Nigerian’ is on lists of email spam trigger words for 2020. It is considered a spam word and should be avoided because it sounds shady or unethical. This means that a legitimate email could get filtered as spam or blocked if it contains the word ‘Nigerian’. Words hardly get red-flagged by email providers unless associated with scam overtime.

Nigerians predict that cybercrime will increase

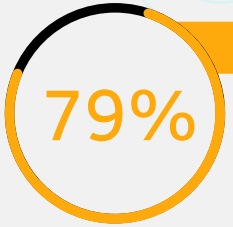
- The activities of cybercriminals have caused huge financial loss and psychological trauma, including depression and self-harm to their victims. In the US, one victim of romance fraud committed suicide after losing millions of dollars, while in the UK, another victim attempted suicide after falling victim of such fraud.

- Nigeria has been recognised as one of the dens of internet fraudsters and cybercriminals because law enforcement agencies of the victims’ country like the US FBI, Action Fraud and NCA in the UK, etc. were able to trace the origin of some of these scams to the country.

- The Nigerian government has often disavowed cyber criminality in various forms. In 2019 for instance, the EFCC shut down a training school for internet fraudsters in Lagos, with both proprietor and students arrested.

- The office of the National Security Adviser developed a common framework that aggregates Nigeria’s collective response towards addressing the challenges in tackling cyber security in its ‘National Security Policy’. The NSP outlines the actions that the government and other stakeholders will take to mitigate the risks and secure the gains of our continuous dependence on the cyberspace.

- However, much is still left to be desired as far as Nigerians are concerned. Academy Halogen recently asked to ascertain the risks exposure of the citizens to cybercrime. The following is the feedback from that survey:

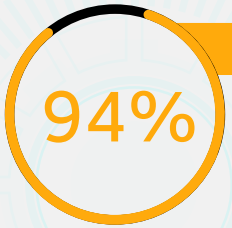


79% Nigerians believe that cybercrimes will increase in the country.

- Their fears are connected with the information relating to cyber criminality they are exposed to on a regular basis.

OUR RECOMMENDATION

- Government and other stakeholders must allay these fears with practical solutions; otherwise the online economy will suffer in Nigeria.



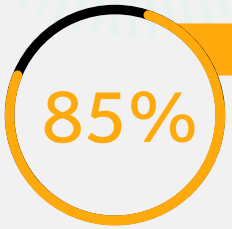
For most Nigerians (94%), internet fraud is the major activity that constitutes cybercrime.

The other close threats are computer hacking (**90%**) and computer viruses (**88%**).

o In other words, people are now generally more apprehensive when using their personal or organisation's laptop or desktops to access the internet.

OUR RECOMMENDATION

o While expecting more reassurance from the government, it is expedient for everyone to take personal responsibility for their safety online. Talk to experts if you are not sure how secured your system is.

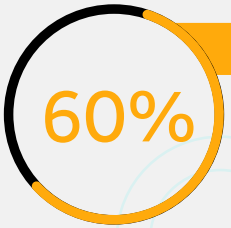


85% Nigerians are aware of and/or have experienced more than two (2) cybercrime incidents in 2020.

o This is a frightening statistics considering that the year is just half way gone. It means that the threats of cybercrimes are now pervasive and widespread.

OUR RECOMMENDATION

o There is a need to equip everyone with the right knowledge on how to overcome the scourge. You must closely guard your personal information online.

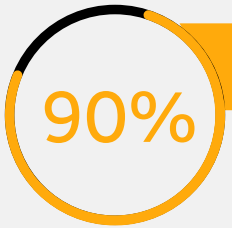


60% Nigerians consider themselves less secured regarding their engagement with the cyberspace.

o This realisation will affect how people interact online and invariably affect the expected economic activities from that sector of the economy.

OUR RECOMMENDATION

o Instead of being terrified by cyber threats, people should rather find means to protect themselves and organisations through knowledge and technology.



Social media (90%) is the main reason why Nigerians use the internet – with making online purchases (75%) and e-Banking (70%) closely following. Education (60%) is now a major factor as people continue to embrace virtual learning due to the effect of the pandemic lockdown.

OUR RECOMMENDATION

o Since these are essential activities, it is expedient for users to learn how to protect themselves online.

How Nigeria can tackle cybercrime

- Nigeria should identify its most critical infrastructures, identify vulnerabilities in them and analyse the typical risks to each of these systems. An example of a critical infrastructure includes systems hosting classified national security information amongst others. A long-term detailed plan that will guide investments in securing our infrastructure should be devised.

- Nigeria will also do well to plan across the five core pillars that were used by the International Telecommunication Union (ITU) – legal, technical, organisational, capacity building and cooperation. An example is the NG-CERT (Computer Emergency Response Team), which should work towards proactively monitoring and taking measures to mitigate threats on networks within the country.

- An equally significant measure is that Ministries, Departments and Agencies (MDAs) of government should link all their databases. This will help achieve 'data harmonisation', which will, in turn, assist cyber forensic/assurance specialists overcome the cyber security challenges in Nigeria. A data harmonisation approach could save cost by channelling defence resources to a single pane of glass.

- The nation should work towards developing capacity for cyber security. A massive investment in training initiatives for students and workers, wide-scale Federal Government and private sector scholarships for students with interests in cyber security and the inculcation of cyber security in our school curriculum are all good ways to start. The country needs to win the future and it can be won by educating the present.

- A National Cyber Command Centre could be built that will be the go-to centre for cyber security in the country and will facilitate cyber intelligence integration for all government parastatals and private institutions.

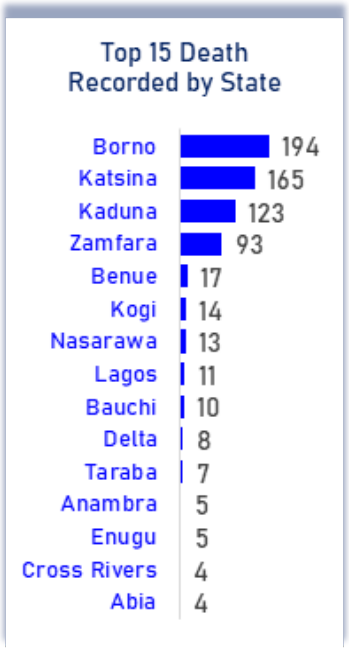
- Collaboration among stakeholders and cyber-intelligence sharing is key to having a united front against cyber terrorism. It will be difficult to estimate the level of damage a successful catastrophic cyber-attack may cause on Nigeria's fragile economy. It is recommended that the country stay prepared while still being relatively safe than looking for escape routes when caught unawares.

- Nigerians must collectively come together to condemn, criminalise, denounce and discourage cybercrime. As part of government efforts to curb cybercrime, there is a need for societal reorientation. The government should engage influential figures in community, religious leaders, traditional leaders and scholars to sensitise the public against youth participation in cybercrime.

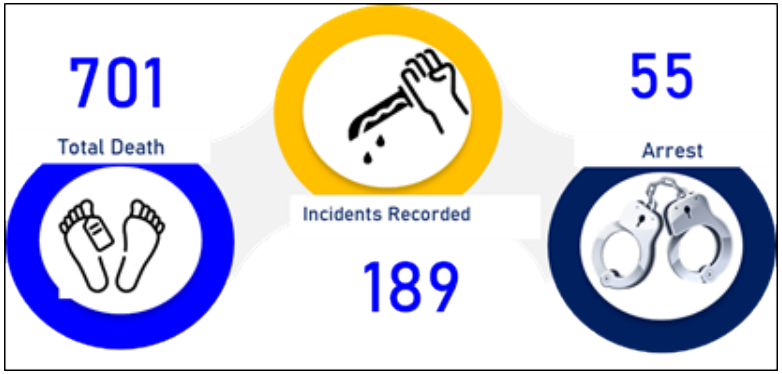
National Security Profile

-JULY 2020

See the latest data and analytics from **http://halogenintel.com.ng/.**

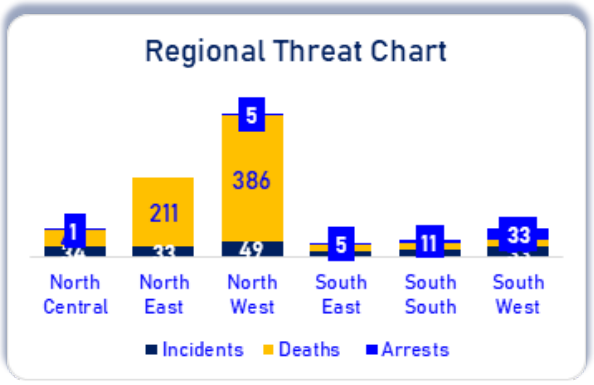


- Highest death was recorded in Borno.
- Katsina overtook Zamfara and Kaduna in Banditry reported deaths and attacks in July 2020.



- Death Recorded reduced by 41% against last month
- Approximately 4 deaths were recorded per crime in July 2020

Threats	Incidents	Deaths	Arrests
Terrorism	22	357	
Banditry	38	152	
Herdsmen Attack	7	62	
Safety Accident	10	30	2
Murder	24	25	7
Political/Civill Unrest	8	21	
Community Crises	3	20	
Kidnap	42	20	4
Cultism	4	8	
Armed Robbery	9	4	25
Child Abuse	5	1	7
Others	10	1	5
Drug Crime	1		
Theft	3		5
Fraud	3		
Grand Total	**189**	**701**	**55**



- There were 50% more banditry related activities than Terrorism in July 2020.
- Death from Terrorist related activities comprises half of the total deaths.
- Banditry and Terrorism has the highest death to crime ratio.

Regional Outlook

North West

- Armed banditry claimed the life of 61 persons and led to the abduction of 62 persons. In turn, troops killed about 75 bandits in different operations in Katsina, Zamfara and Sokoto.
- An estimated 40 bandits were reportedly killed when federal troops attacked bandits' camps in Kwiambana forest in Zamfara.

North East

- 38 soldiers of the Nigeria Army Special Forces were killed after a deadly ambush by suspected Boko Haram members in an ambush between Limanti and Bulabulin villages not far from Damboa.
- An estimated 30 soldiers were killed and hundreds others injured during separate attacks by Boko Haram insurgents in Borno State. The terrorist also killed eight soldiers in an attack on a military convoy near Kumulla village, roughly 40 kilometres (25 miles) southwest of regional capital Maiduguri.

North Central

- Armed bandits abducted 30 persons and killed two vigilantes in Nasarawa LGA of Nasarawa State.
- Two personnel of the Benue Livestock Guards were reportedly ambushed and killed by suspected armed herdsmen in Tombo Council Ward, close to Ayilamo in Logo LGA.
- The Defence troops of Operation Whirl Stroke have rescued an estimated 34 kidnapped victims, apprehended suspected kidnappers and recovered cache of arms and ammunition in Benue state.
- An estimated 16 persons have been feared kidnapped in fresh bandit attacks in in Magani and Tungan-Bako communities of Rafi LGA in Niger state.

South South

- The Nigeria Security and Civil Defence Corps (NSCDC), Delta State Command impounded three trucks loaded with stolen crude oil and arrested over 11 suspects in Rivers state. A naval drone discovered an illegal refining site with 300,000 litres of diesel and a large wooden boat containing 314 barrels of crude oil in Cawthorne channel, Port Harcourt.
- Shell Petroleum Development Company Limited (SPDC), with over 600,000 barrels daily output, recorded 39 oil spill cases in the second quarter (April – June) of 2020. This indicated a drop of 61.5 per cent when compared to 63 cases recorded in the corresponding period of 2019. 15 cases were recorded in March 2020, all of which were attributed to mainly pipeline vandalism and oil theft.
- Pirates attacked BW Offshore's Sendje Berge FPSO and kidnapped nine crewmembers.
- Seven persons died after an explosion at the 'Oil Mining Lease 40' operated by the Nigerian Petroleum Development Company (NPDC).The incident happened at Gbetiokun in Delta State where the facility belonging to its subsidiary is located.

South East

- In Anambra, 10 communities in Awka North LGA reported the destruction of their farmlands by herdsmen.
- In Ebonyi, two separate incidents leading to the death of 4 people and the abduction of 5 others were recorded. This is a resurgence of long standing communal clashes over land. The incidents occurred at the boundary between Ekoli Edda in Afikpo South L.G.A of Ebonyi state and Biase LGA of Cross River state.
- Crisis ensued between Nguji Ojiegbe Onunwakpu and Ndiegede, both in Igbeagu autonomous community in Izzi LGA of Ebonyi State. Investigation revealed that the boundary disputes started in 2012, but was later put off by the state government.

South West

- Calm was restored to residents of Ejigbo, Isheri Oshun and Ijegun areas of Lagos after the Police from Ejigbo subdued some teenage robbers terrorizing people in the area. The suspects were arrested at Elemu Bridge in Bucknor Estate area of Ejigbo.
- The Oyo State Police Command arrested some suspects in connection with serial killings in Akinyele community in Ibadan. Two people were murdered within the space of 4 days in their homes in a somewhat similar fashion with one with his abdomen ripped open and his intestines exposed. The Chairman, Ejigbo LGA of Osun State imposed a dusk-to-dawn curfew on Ejigbo following the killings.
- Police operatives attached to the Special Tactical Squad have arrested a 7-man syndicate that specialize in robbing commercial banks. The criminal gang had attacked and robbed three commercial banks in Ondo and Ekiti between 2019 and 2020, killed innocent citizens including six (6) policemen and carted away several millions of naira. The most recent incident carried out is the robbery of a commercial bank in Ile-Oluji, Ondo State on 7th February, 2020 where four (4) policemen were killed.
- The leader of a notorious gang, One Million Boys, who was on the wanted list of the Oyo State Police Command, has been killed in Ibadan after a reported gun duel between him and a rival gang. Until his death, at Olomi area of Ibadan, Biola Ebila was leader of the violent gang.
- One person was allegedly killed after two factional members of the National Union of Road Transport Workers (NURTW) clashed over ticket fee collection at Idumota, Lagos Island. The hoodlums ("Kunle Poly" boys and another union called Okoro) used dangerous weapons on each other, leading to the death of one person, while many others sustained injuries. Traders close to the park were attacked and their goods destroyed.

About Us

Halogen Group is a premium, digital-enabled and integrated security group that provides end to end security risk solutions to enterprises as well as individual consumers.

Our single minded purpose is to enable SAFETY in today's open and continuously volatile world, for you, your family, your assets, both physical and virtual, and your business.

At Halogen Group, we are committed to enabling you safely pursue the ACHIEVEMENT of your goals and purposes. We do this by creating security risk solutions that help you forestall and mitigate threat.

ABOUT US: ACADEMY HALOGEN:
A learning institution that demonstrably shapes enterprise security risk management in the digital space via education, policy and thought leadership

WHAT WE DO:
·School of Security Studies
·School of Security Management
·School of Security Technology
·Thought Leadership








Halogenlimited | HalogenNg | @Halogensecurity

Head Office:
19B, Mobolaji Bank Anthony Way, Ikeja, Lagos.

Call:
+234 1-3429012,
+234 1-3429021
+234 8081602646,
+234 700HALOGEN

Email:
info@halogen-group.com

ACADEMY HALOGEN

HALOGEN GROUP