Review of the CBN Cyber security Framework, its Impact on Banks and Customers

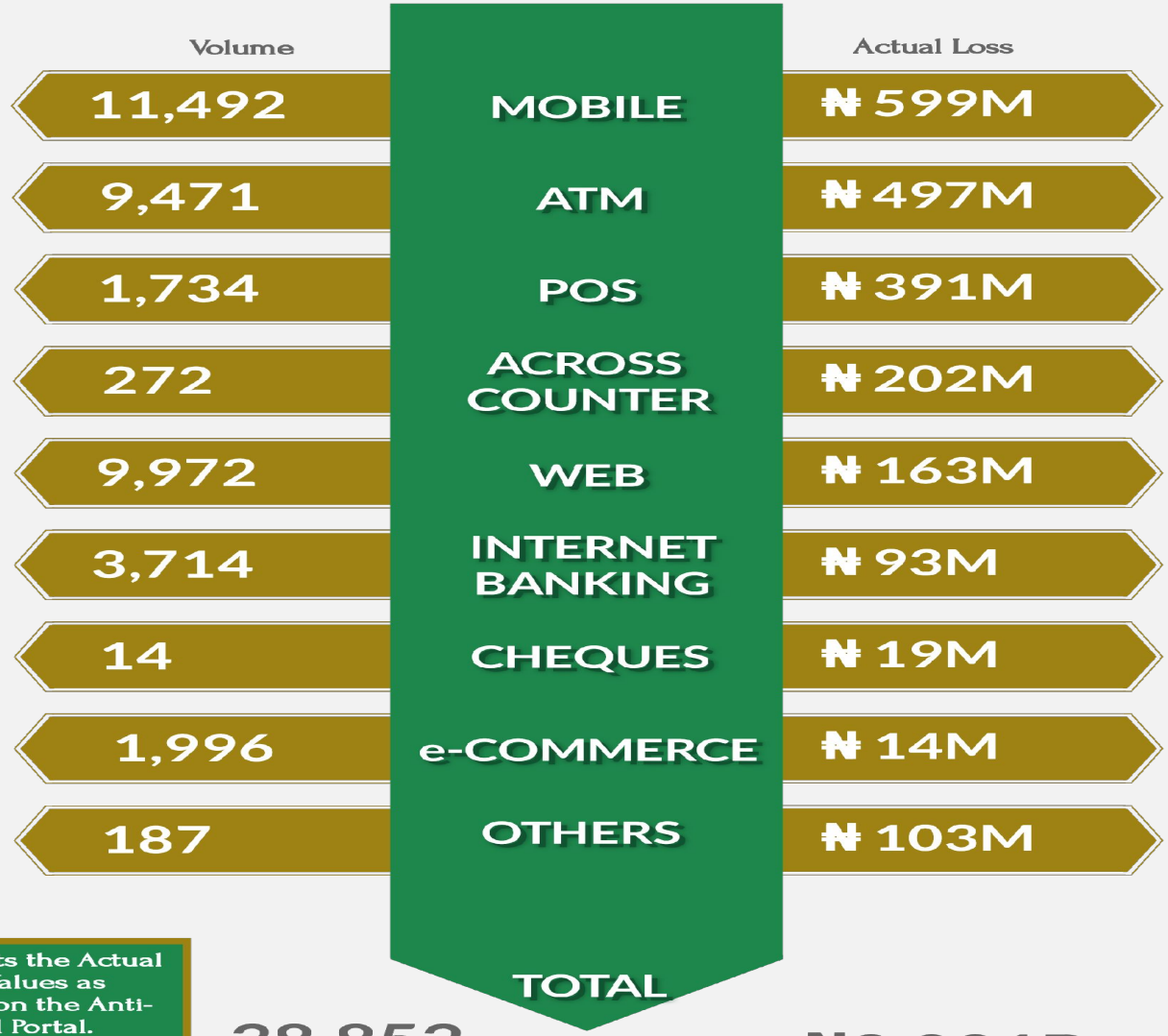
Presented
By
Sam C. Okojere
Director, Payments System Management Department
Central Bank of Nigeria

At the 2019 Annual Retreat and Conference of ACAEBIN, held from 21st to 23rd March, 2019 Park Inn by Radisson, Kuto, Abeokuta

Outline

- Data Breaches & Cyber Attacks
- Cyber Threat Actors
- CBN’s Cybersecurity Framework
- Mapping The Guidelines To Cyber Issues
- Conclusion

2018 FRAUD AT A GLANCE



This reflects the Actual Loss Values as reported on the Anti-Fraud Portal.

Figures may not add up due to approximation

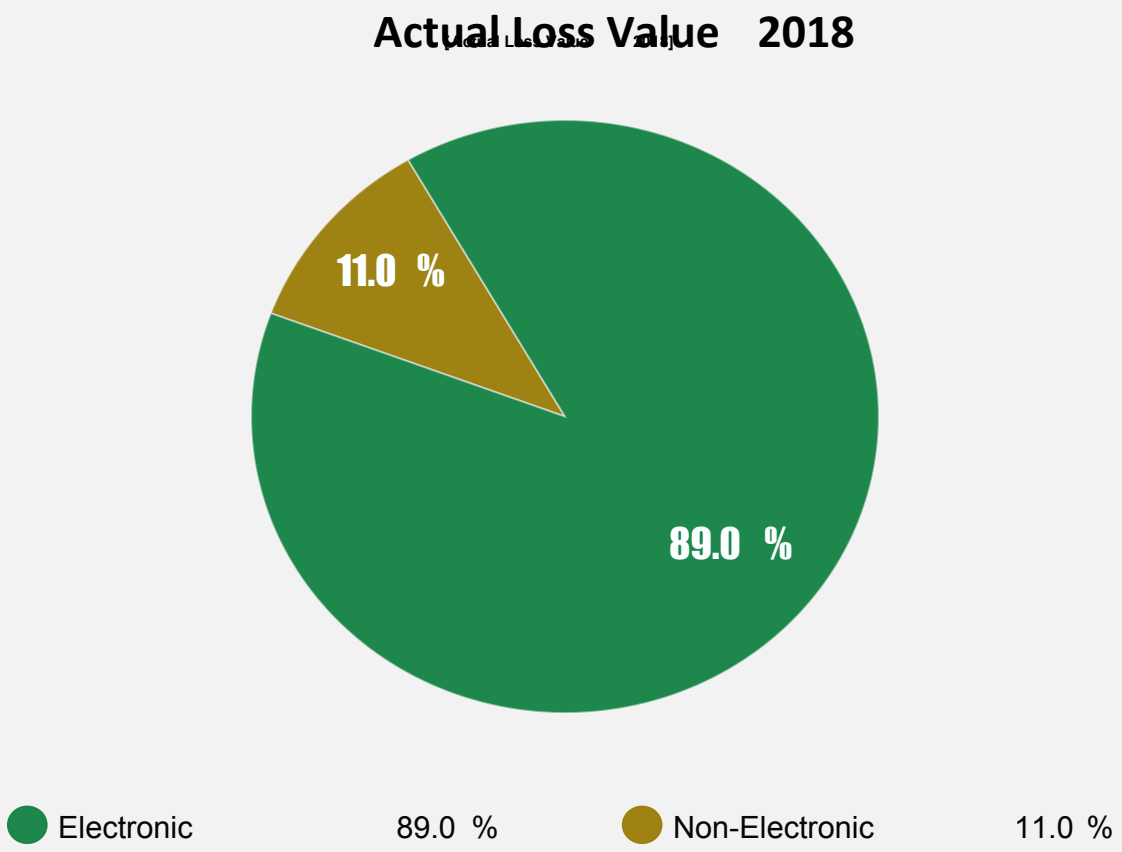
Year	Fraud Volume	Attempted Fraud Value (₦)	Actual Loss Value (₦)
2018	38,852	9,047,449,391.29	2,081,090,699.56
2017	25,043	4,034,258,639.07	1,631,680,256.85

Fraud Landscape in Nigeria NIBSS Report 2018

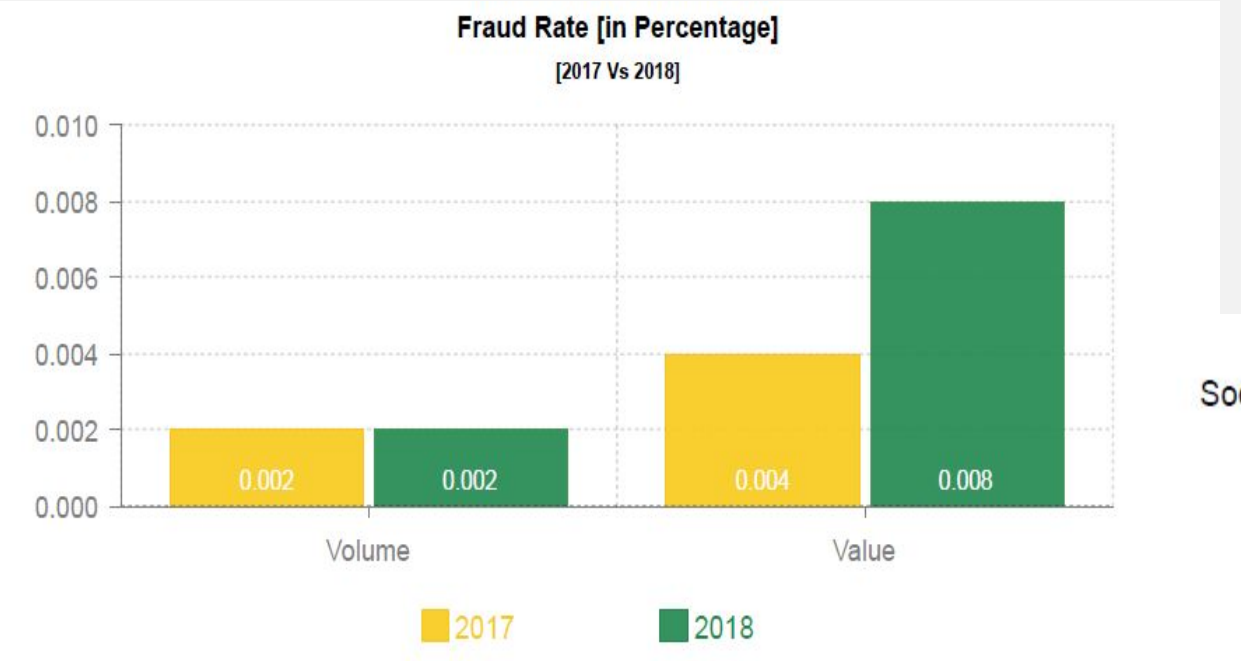
eFraud, a Major Source of Risks

₦143,236,895.90
Attempted Fraud

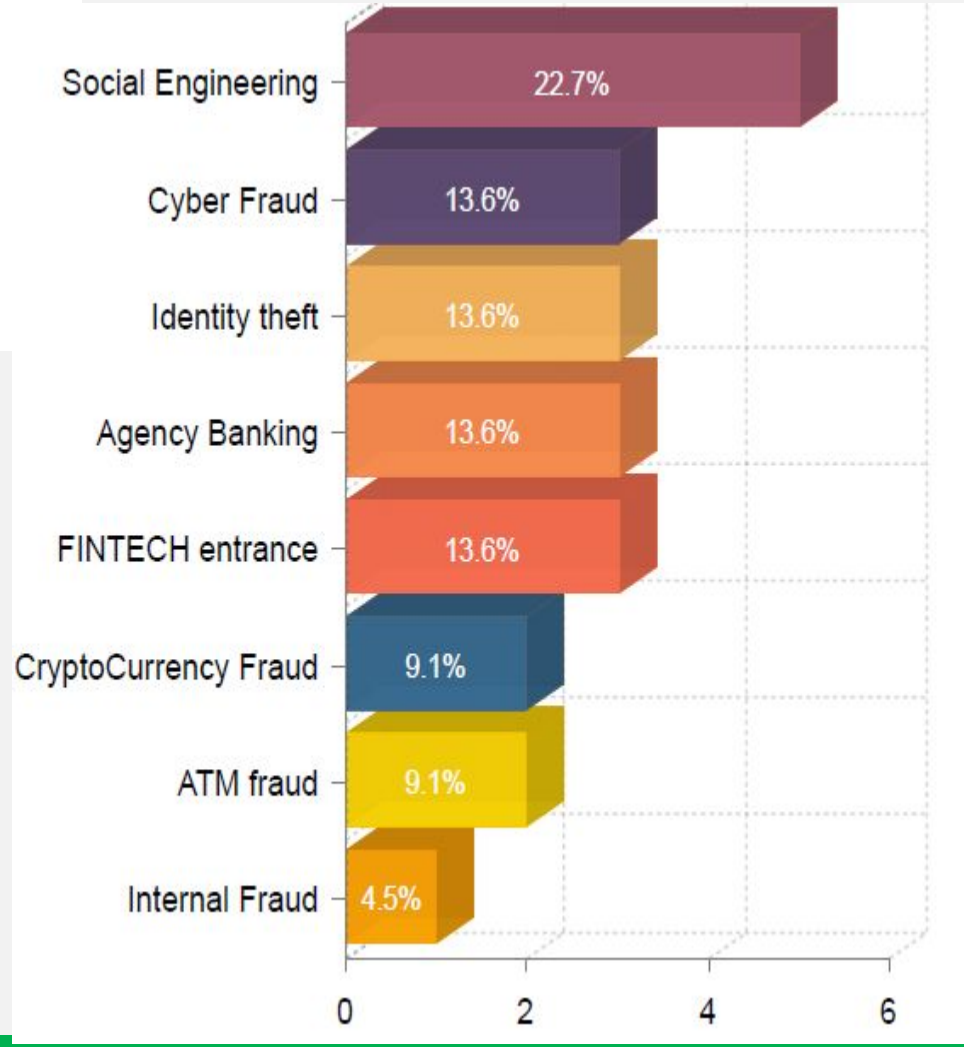
₦120,978,048.50
Actual Loss Fraud



Fraud Landscape in Nigeria NIBSS Report 2018



Current threats

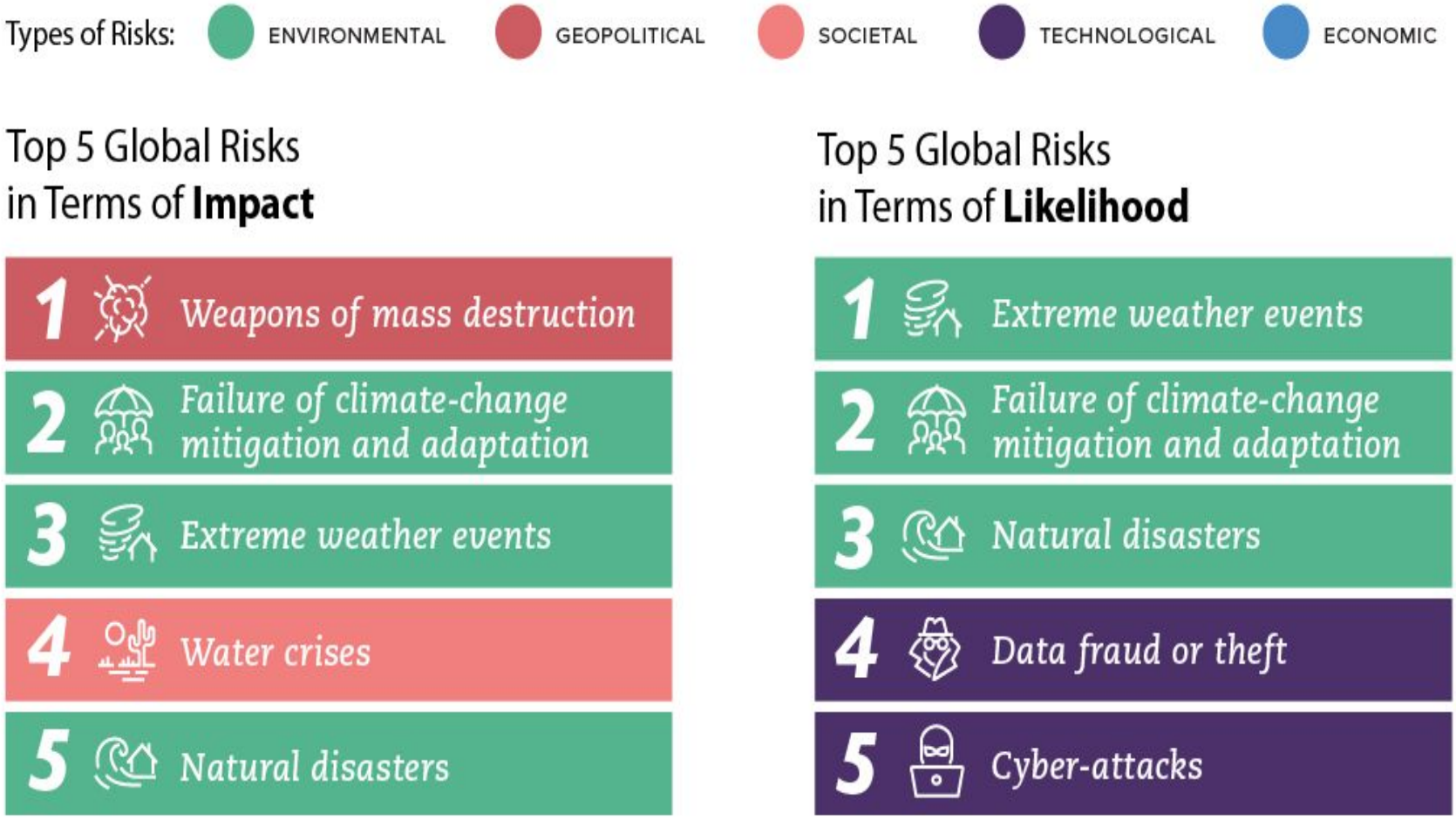


Evolving Cyber threats

≡

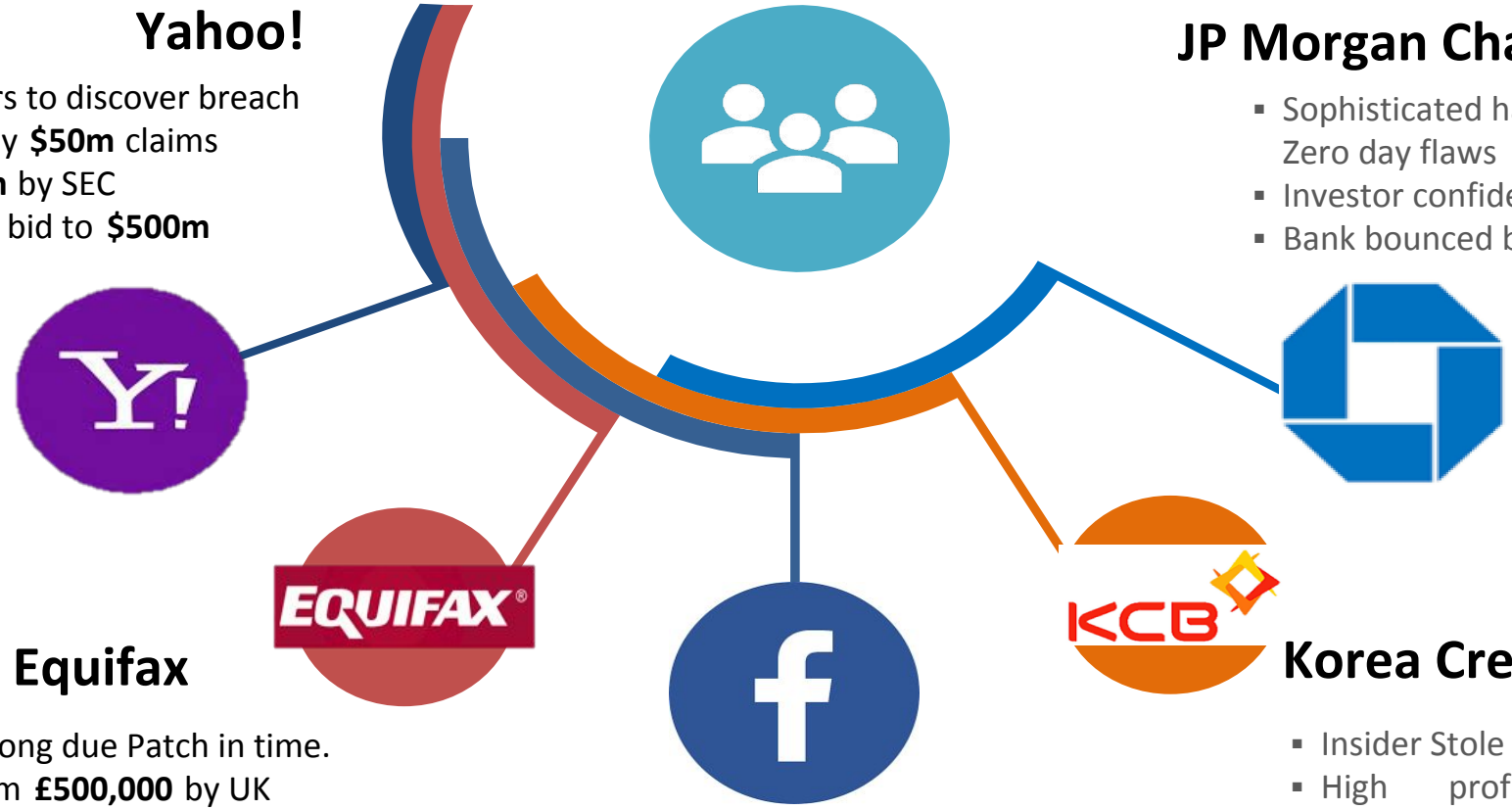
Increasing Fraud?

THE GLOBAL RISK OUTLOOK FOR 2019



https://www.weforum.org/reports/the-global-risks-report-2019

A Closer Look at Some Cases



Yahoo!

- Took 3 years to discover breach
- Made to pay **$50m** claims
- Fined **$35m** by SEC
- Verizon cut bid to **$500m**

JP Morgan Chase

- Sophisticated hackers exploited Zero day flaws
- Investor confidence shaken
- Bank bounced back stronger

Equifax

- Did not apply long due Patch in time.
- Fined maximum **£500,000** by UK
- Investors cut stakes in company

Facebook

- New implemented feature led to vulnerability
- Fined by various countries incl. UK

Korea Credit Bureau

- Insider Stole and sold Data
- High profile resignations amidst Lawsuits

Other Cyber Attacks

Police Uncover Billionaire Fraudsters Cloning Websites of Major World Banks from Lagos (18th Oct, 2018)

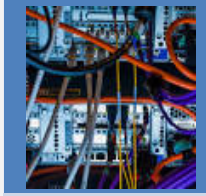
..the fraudsters were found to have stolen huge sums using cloned websites of the CBN, United Bank for Africa (UBA), Union Bank, IMF etc.

http://www.newsmakersng.com/police-uncover-billionaire-fraudsters-cloning-websites-of-major-world-banks-from-lagos-scammers-target-wells-fargo-cbn-imf-uba-others/

India's Cosmos Bank loses $13.5M in Cyber Attack (14th August, 2018)

Cyber criminals hacked the systems of India's Cosmos Bank and siphoned off nearly 944 million rupees ($13.5 million) through simultaneous withdrawals across 28 countries.

https://www.reuters.com/article/cyber-heist-india/india-cosmos-bank-loses-135-mln-in-cyber-attack-idUSL4N1V551G



North Korea Hackers Tried to Take $1.1 Billion in Bank Attacks (8th October 2018)

A North Korean hacking group has tried to steal at least $1.1 billion in a series of attacks on global banks over the past four years, according to cybersecurity firm FireEye Inc.

https://www.bloomberg.com/news/articles/2018-10-08/north-korea-hackers-broke-into-banks-tried-to-take-1-1-billion

Bank Servers Hacked to Trick ATMs into Spitting Out Millions in Cash (3rd October 2018)

The US-CERT has released a joint technical alert warning about a new ATM scheme being used by the prolific **North Korean** APT hacking group known as Hidden Cobra.

https://thehackernews.com/2018/10/bank-atm-hacking.html

Google+ is Shutting Down After Vulnerability Exposed 500,000 Users' Data (8th October 2018)

Google is going to shut down its social media network Google+ a massive data breach that exposed the private data of hundreds of thousands of Google Plus users to third-party developers.

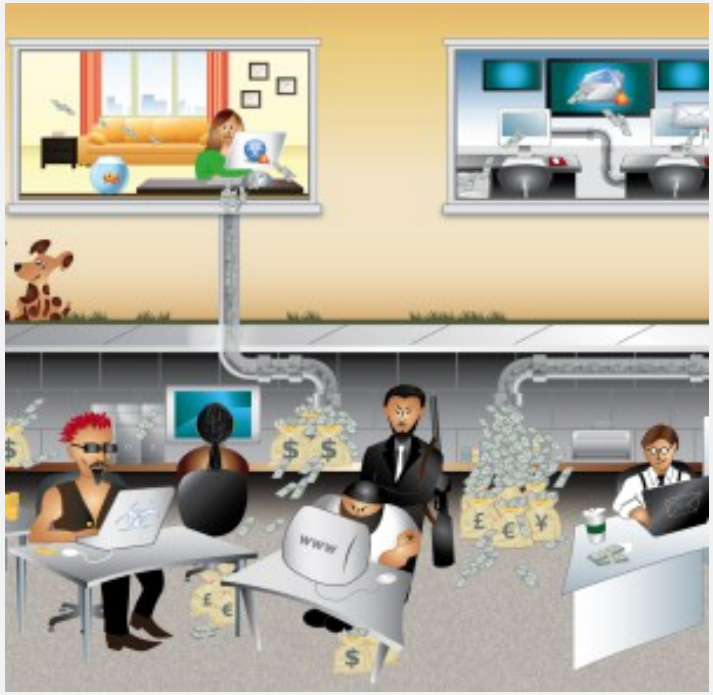
https://thehackernews.com/2018/10/google-plus-shutdown.html

WannaCry Cyber attack cost UK NHS £92m (11th October, 2018)

A devastating global cyber attack that crippled computers in hospitals across the UK has cost the NHS £92m, a report from the Department of Health has found.

https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/

Trends Driving Cybercrime Globally



- Increased Technology Adoption
- Lower Risk of Detection
- Easy access to Cybercrime Tools (Cybercrime-as-a-Service, CyaaS?)
- Advent of the **'Dark Web'** (Organized Underground Financial Fraud Community)

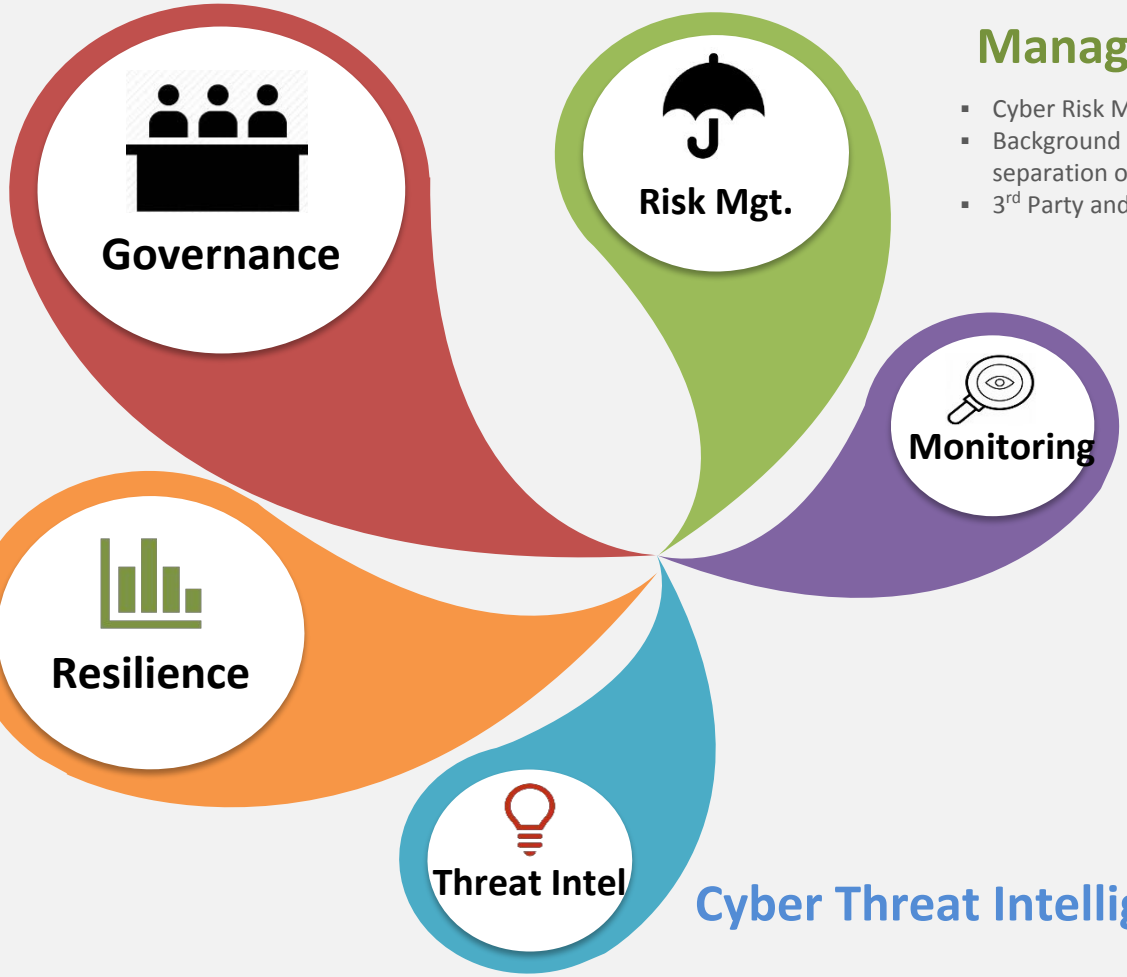
CBN Cybersecurity Framework Main Areas

Cybersecurity Governance and Oversight

- Regular Board review of Cyber risks
- Appointment of CISO
- Establish Info-sec Steering Committee

Cyber Risk Management Program

- Cyber Risk Mgt. part of Enterprise Risk Mgt.
- Background checks, Privileged access Mgt., separation of duties etc.
- 3rd Party and Insider Risk Mgt.



Cyber Resilience Assessment & Operational Resilience

- Determine "current" cybersecurity status
- Document gaps and communicate to the Board
- Develop roadmap to address gaps
- Report self-assessment to CBN bi-annually (February, August)
- Know your environment

Monitoring, Metrics & Reporting

- 24/7 Monitoring via SOC
- Establish metrics and monitoring process
- Report to CBN all cyber incidents whether successful or not immediately after such incident was identified.

Cyber Threat Intelligence

- Establish Cyber Threat Intelligence (CTI) program
- Tactical and Strategic Threat Intelligence

More Framework Highlights

Appendix 3.

- Identify IT security administrators, security guards, etc. and conduct background check on such employees
- Ensure access is least privilege and on need-to-know basis
- Ensure Insider and Vendor/3rd Party risks are regularly assessed as part of the Enterprise Risk Mgt. framework.
- Know your environment (Asset management)
- Establish controls to prevent unauthorized modification or removal of its authorized software/applications while preventing the installation of unauthorized software/applications on its network.

More Framework Highlights

Appendix 4.

- Cybersecurity Awareness
- Ensure secure system configuration using security baselines, SOPs, system configuration change management etc.
- Data Loss Prevention
  a. Develop Data Loss Prevention Strategy to discover, monitor, and protect confidential business and customer data/information at endpoints, storage, network, and other digital stores, whether online or offline.
  b. The strategy should provide mechanism that classifies data and monitors how data is stored and used.

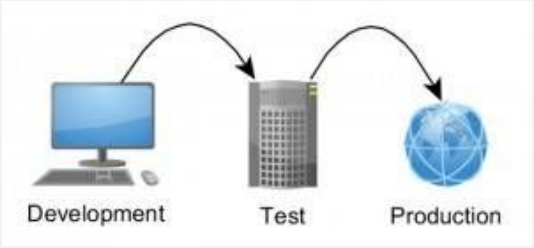
More Framework Highlights

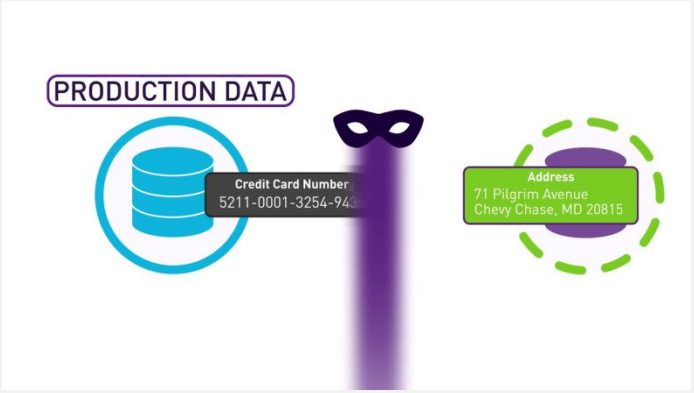
- Continuous Security Monitoring
  (24/7 SOC, in-house or outsourced)

- Incident Response
  DR/BC Plans shall be created and regularly tested
  Overall Incident Response Strategy (all stakeholders)
  Establish Cyber Incident Response Team
  Establish Communication plan etc.

- Vulnerability Management
  Periodic Vulnerability Assessment
  Prompt application of patches and other fixes.

More Framework Highlights





- System Lifecycle Management

  e. Separate the Production/Live environment from the Development and Testing environment(s).

  f. Sanitize sensitive data in the Development and Testing environments by implementing a **Data Masking** solution to mask bank's and customers' sensitive information for the purpose of Development, System and User Acceptance Tests.

  g. Establish a procedure for the maintenance of on-site and remote organizational assets to prevent unauthorized access.

  h. Adopt **Cryptographic controls** such as public key infrastructure, hashing and encryption to guard confidential and sensitive information against unauthorized access.

Common Cyber Issues vs Cyber Framework

Cyber Issues	Cyber Framework Provisions
…took 3 Years to Detect	Monitoring 24/7 via SOC
…failed to apply patch in time	Regular Vulnerability assessment and prompt implementation of patches
…New feature implementation introduced Vulnerability	System configuration lifecycle and vulnerability assessment
…Insider stole data	Data Loss Prevention

Opportunities and Impacts

Opportunities

1. Board support for Cybersecurity being now a compliance issue
2. More budgetary provision for Cyber program
3. Cybersecurity can now be treated as an ongoing program instead of a project
4. Integration of Cybersecurity into the business goals of banks and PSPs
5. Aggregation of previously silo security efforts with the CISO as focal point with singular responsibility

Impacts

1. Cybersecurity will take center stage among staff with management's commitment and cyber being a compliance issue
2. More security and less losses due to cyber crime
3. Overall rise in financial system security as entities rise above the benchmark enforced by CBN

Cybersecurity Disclosure Act of 2019

House Dem introduced bill requiring public firms to disclose cybersecurity expertise in leadership. Publicly traded companies are to disclose to investors whether any members of their board of directors have cybersecurity expertise amid growing cyberattacks

- The bill comes at a time when "cyberattacks and data breaches are becoming more frequent and sophisticated," according to a US press release accompanying the rollout of the bill.

A study extract from Identity Theft Resource Center found that there was a 126 percent rise of data breaches that exposed records containing personally identifiable information. This rise took place across all industries, from 197.6 million in 2017 to 446.5 million in 2018.

- The Cybersecurity Disclosure Act will give the public information about which companies are likely to have better protections and cyberdefense strategies.

Conclusion

The CBN Cybersecurity Framework and Guidelines for Deposit Money Banks (DMBs) and Payment Services Providers (PSPs) is a product of long research and wide consultations.

Yet it is a living document.

The Central Bank remains open to suggestions on any areas of improvements towards safe-guarding the Nigerian Financial System against the adverse impacts of Cybercrimes.


Thank
you