Institute of Chartered Accountants of Nigeria

47th Annual Accountants Conference

Cybersecurity: What Chartered Accountants Need to Know

by

'Dipo Fatokun, B.Sc., MBA, FCA
Director, Banking and Payments System
CENTRAL BANK OF NIGERIA

Outline

- Context
- The Chartered Accountant’s Role in the Information Age
- An Overview of Cyber Risk and Cyber security
- Cyber Risk and Implications for the Accountant
- Cyber Security: Adding Value as a Chartered Accountant
- Opportunities & Challenges

Context

In the information age, ICT has made a lot of our functions more interesting, however, ICT comes with its risks that may impugn on our watch words:

Accuracy

&

Integrity

Context

- Our unique selling point as Chartered Accountants is the reliability placed on the information or any report produced by us.
- Cyber risk is that probability that the ICT systems we deployed towards efficiently managing information will be compromised thereby challenging the **Confidentiality**, **Integrity, Availability** and **Accuracy** of Information
- This risk could also heighten other risks including operational & fraud, reputational & legal , financial and business (going concern)
- It is therefore a risk to our profession, but it could be an opportunity for us to re-establish ourselves as the chief custodian of MIS and information in view of our training in managing risks and establishing controls.

The Chartered Accountant's Role in the Information Age

- The information age continues to challenge our role as accountants especially with high level of automation of business processes which hitherto forms our job description, accounting packages, analytics systems and recently artificial intelligence appear to the impacting on functions
- The information age may have refocused our roles on information risk management and controls for information system
- We are therefore central to any cybersecurity strategy and its implementation by providing assurance for the information systems that impacts on all areas of the operational and finance functions

An Overview of Cyber Risk and Cyber security

"We estimate that the **likely annual cost to the global economy** from cybercrime is more than **$400 billion**. A conservative estimate would be $375 billion in losses, while the maximum could be as much as $575 billion. Even the smallest of these figures is more than the national income of most countries and governments and companies underestimate how much risk they face from cybercrime and how quickly this risk can grow."- **-McAfee, 2014**

In Nigeria, ₦2.19 billion was lost to fraud in 2015, it was ₦2.25bn in 2015 as reported by banks

Juniper Research (2015) projected that cyber crime will cost businesses $2 trillion globally by 2019 due to the rapid digitisation of consumer lives

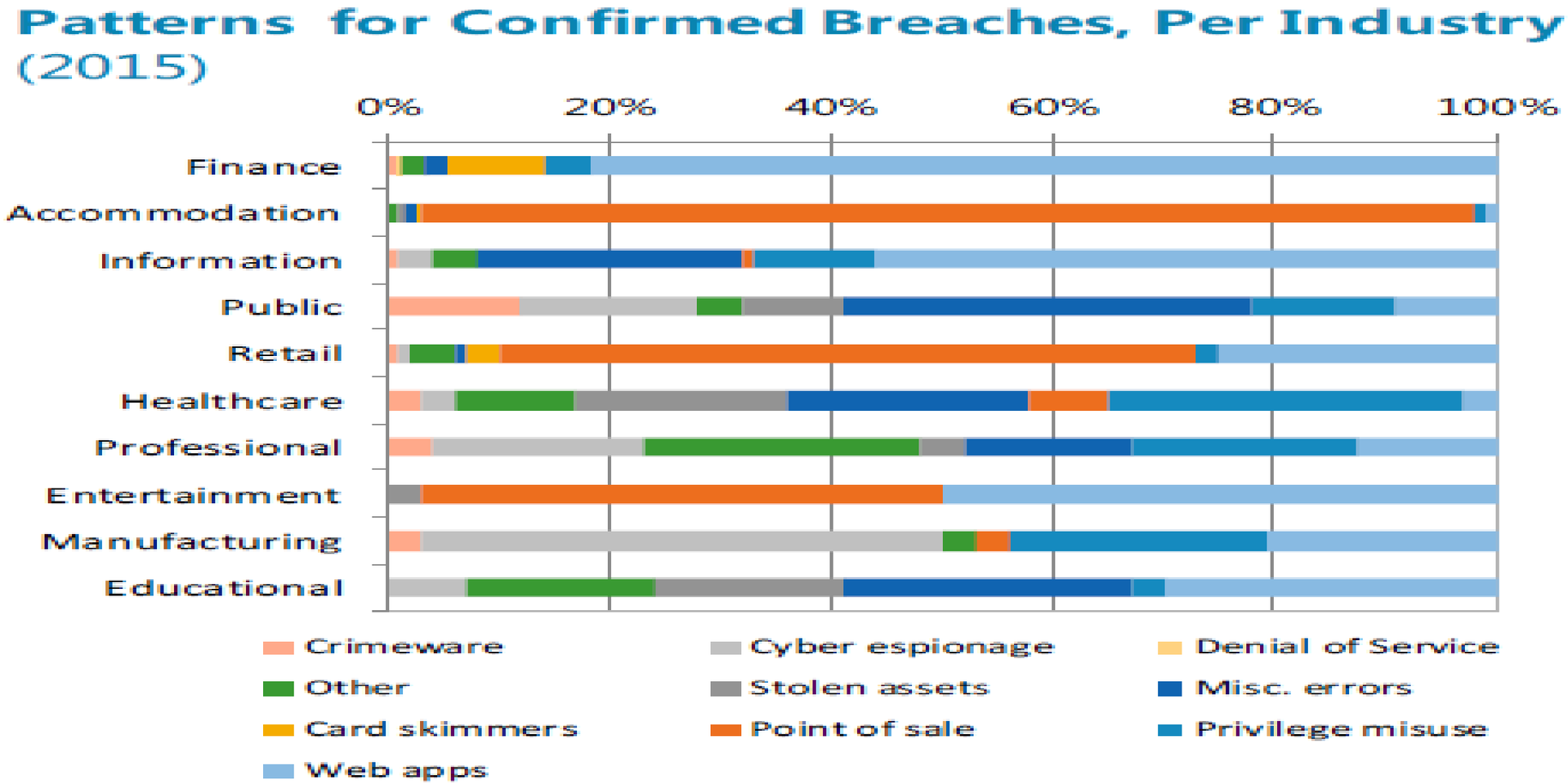
CyberRisks: Threat and Vectors

- Social Engineering, Phishing, Spear-Phishing, Pharming
- Malware, Ransomware
- (Distributed)Denial of Service (DDOS)
- Advanced Persistent Threat
- SQL Injections
- XSS Scripting
- Trojan Horses and Backdoors
- Wireless Networks Attacks

Accountants should have some understanding of these threats and ask questions on how their institutions are protected from these

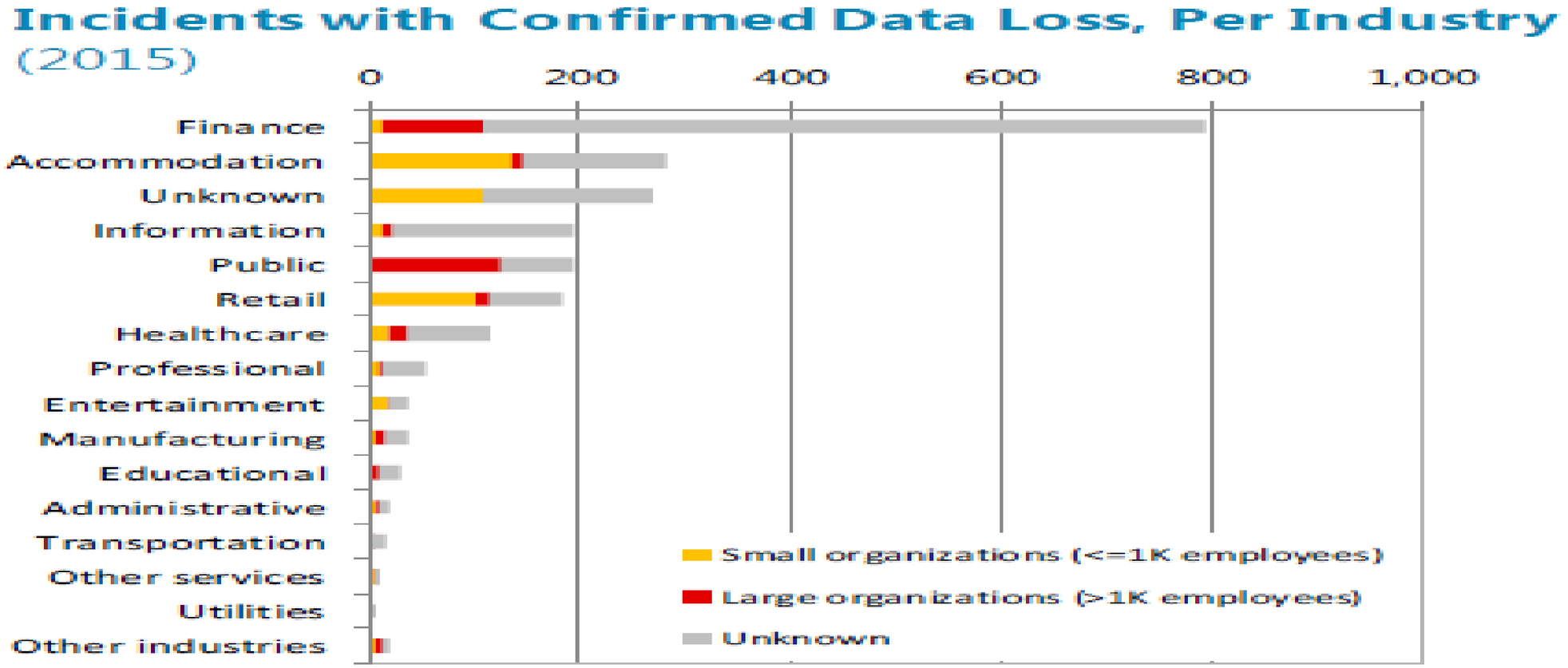
See : https://www.slideshare.net/patelripal99/tools-and-methods-used-in-cybercrime

Threats and Vectors



Source: Verizon. IMF staff illustration.

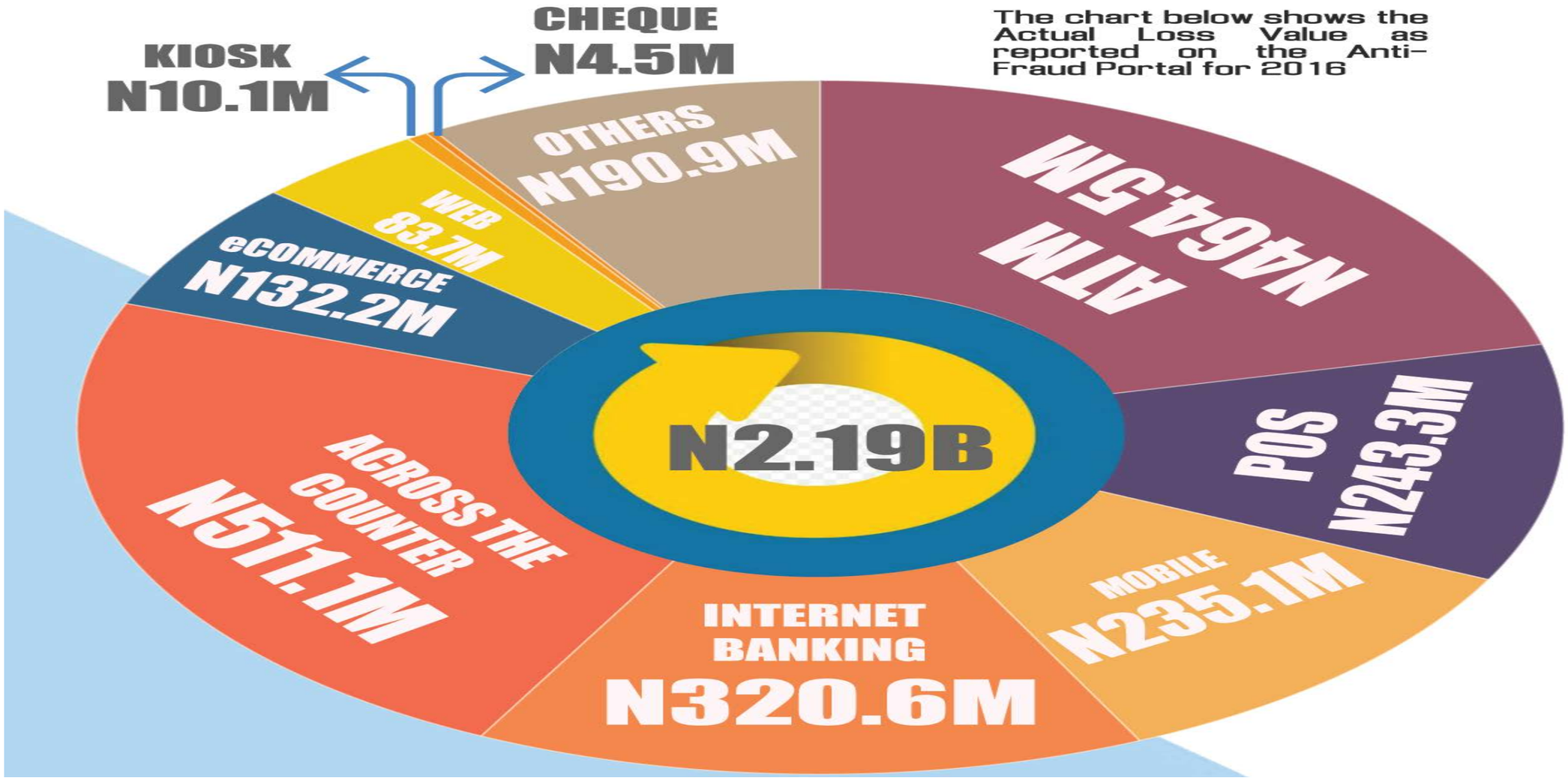
Threats and Vectors



Source: Verizon. IMF staff illustration.

IMF Working Paper WP/17/185

Threats and Vectors: Frauds by Channels as Reported by Nigerian Banks in 2016



Source: Fraud Landscape in Nigeria, NIBSS, 3rd Edition

Threats and Vectors as it applies to payments processes

S/N	Payment Process	Attacks
1.	Customer/Channels (Instruction)	• Session hijack • Compromised details • Pharming • Phishing • SQL Injection • DDOS
2.	Authentication	• MITM • Insider Abuse • Data Breaches
3.	Authorization	• Insider abuse (e.g. Limits) • DDOS
4.	Settlement	• DDOS • Ransomware
5.	Payment	• Chargeback

CyberSecurity Implications for the Accountant

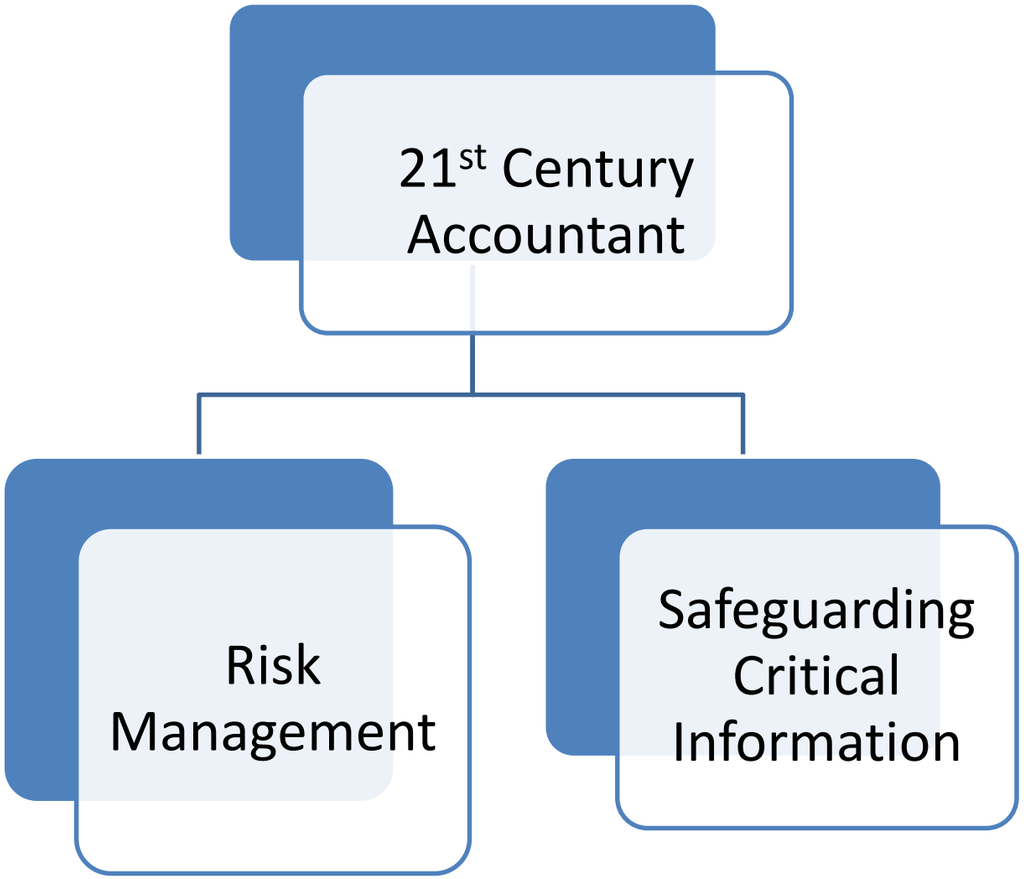
- Traditionally, Accountants are placed to enforce controls in any form of payments or disbursement of funds by any organisation
- From the preceding charts, the cyber-criminals are majorly after the money
- In the ensuing cyber environment, Accountants must re-tool to ensure that we are able to continue to safeguard assets
- We must therefore understand the dynamics of the electronic payments processes and advise on proper implementation of electronic payments and controls in our various organisations

CyberSecurity Implications for the Accountant

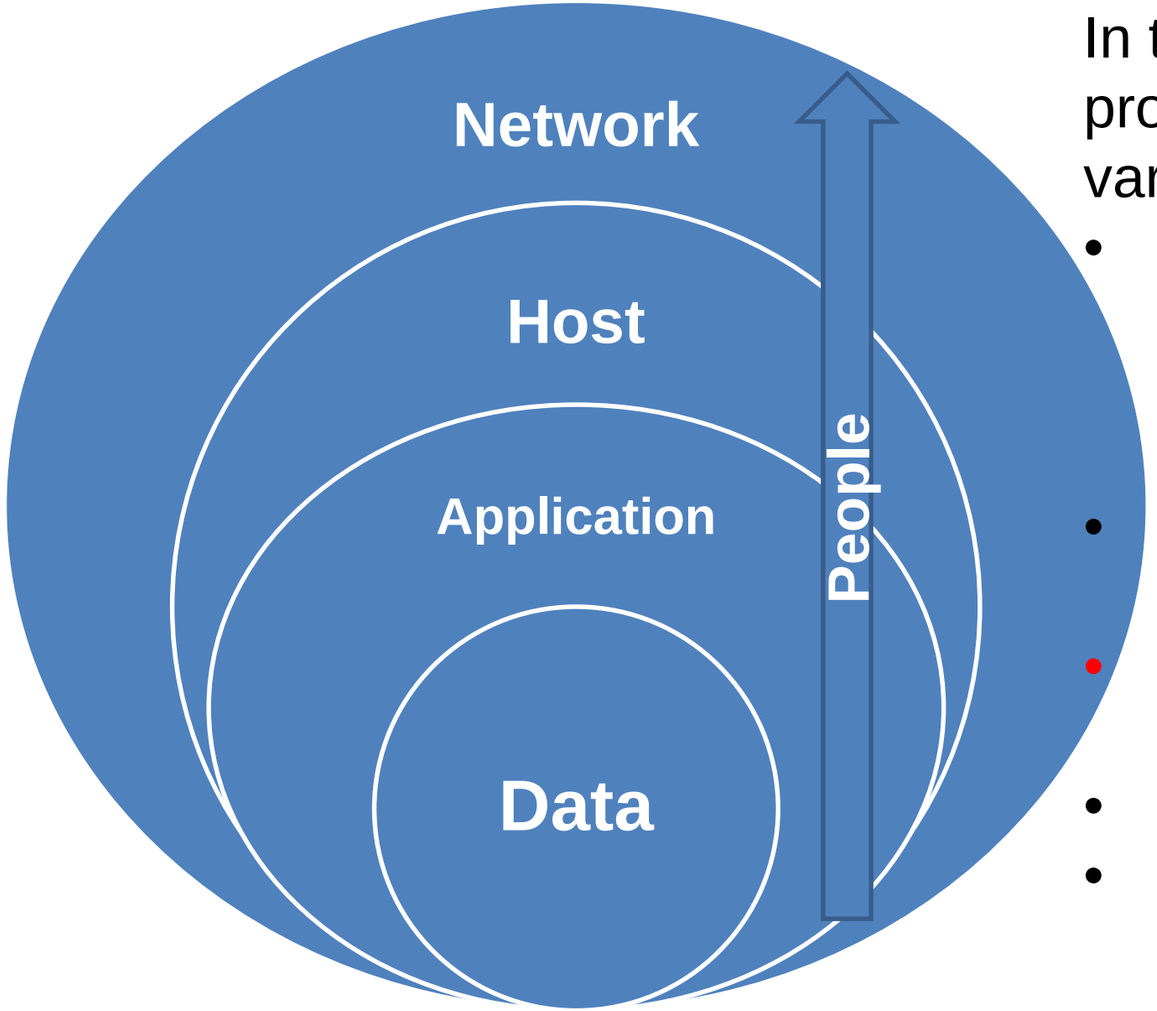
- Understanding of system controls and its implementation is now essential
- Accountants should be able to evaluate cyber risk introduced by third parties
- Time tested controls remains valid e.g. staff rotation, staff profiling, etc, because top three sources of attack remain:
  - Unauthorised access by insiders
  - Employees abuse of internet privileges
  - Viruses
- Internal/External Audit should scope ICT Audit, System Scanning and Penetration testing

Cyber Security: Adding Value as a Chartered Accountant:

- In the face of this new challenge, the Accountant's value can be seen from two perspectives:



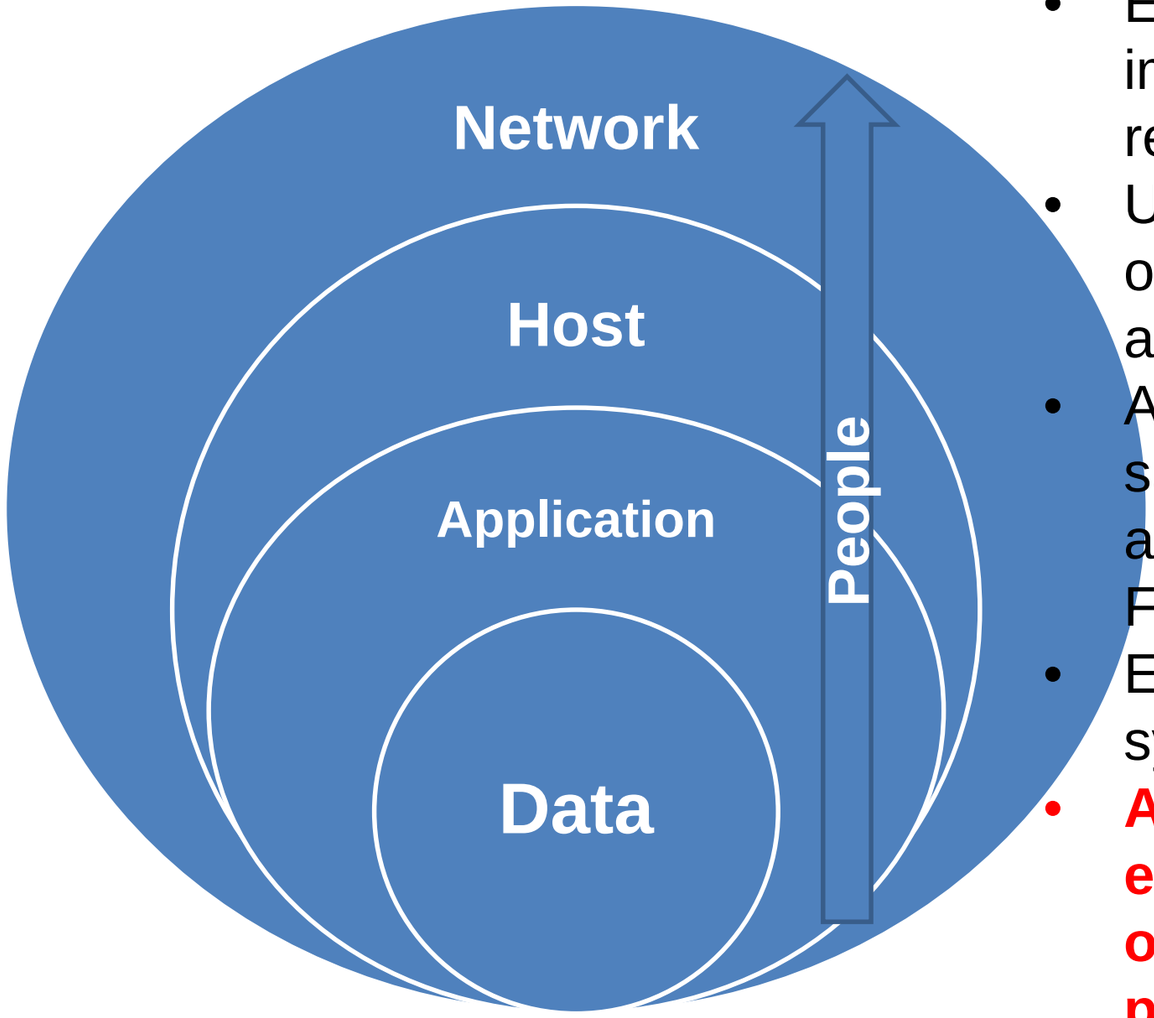
Cyber Security: Adding Value as a Chartered Accountant: Cyber Security Best Practice



In the implementation of electronic payments processes, among other IT implementations, in our various organisations, the Accountant must :

- Understand how data is processed and stored and ensure that proper **access controls** are built around it. e.g. need-to-know, need-to-access, need to update basis
- Ensure that application provides audit trail and time stamp of every transaction and/or actions
- **Test the application to ensure that necessary risk controls are put in place.**
- Avoid usage of pirated applications
- Ensure regular updates and application of patches

Cyber Security: Adding Value as a Chartered Accountant: Cyber Security Best Practice



- Ensure non-usage of default passwords and implement two-factor authentication for all payment related applications
- Understand the roles of any third party involved in the operations of your systems and controls around their activities
- Appreciate the access points and networks supporting all applications and ensure that appropriate controls are implemented e.g. encryption, Firewalls, etc.
- Ensure that data, application, hosting and networks systems initiates deviation alerts to control officers
- **Advocate documentation of IT Security Policy and ensure compliance to it by the ICT officers/consultants through ICT audits, penetration testing and remediation of weaknesses**

CyberSecurity: Challenges for the Chartered Accountant

Rapid innovation in the ICT space such as:

- Internet of Things (IoT)
- Cloud computing and Outsourcing
- Artificial Intelligence
- Blockchain

- Artificial Intelligence(AI) may put a lot of the accounting function at risk, however we should be involved in designing and implementing such technology to ensure that appropriate controls are embedded .
- In the era of Bring-Your-Own-Device and Bring-Your-Own-Network, ensuring compliance with system controls have become more challenging

CyberSecurity: Opportunities

- Cyber Risk Management Advisory Services
- ICT Audit- ACAs are getting Certified in Information System Audit
- Collaboration with ICT experts to design and develop fraud management tools for corporate and individual
- Cyber Fraud Analytics and Advisory
- Cyber Security Awareness for SMEs -Periodic training on Cyber Awareness and prevention of Cyber attacks
- Accountants should be involved in the process of design, adoption and implementation of ICT innovation to ensure that, we remain relevant while also preserving the assets of our organisation by ensuring adequacy of system controls in their advent

Cyber Security: Adding Value as a Chartered Accountant: Resources for ACAs

- Control Objectives for Information and Related Technology (COBIT) on isaca.org
- There are some resources also on the CIMA website: https://www.cgma.org/resources/tools/cgma-cybersecurity-tool.html and AICPA website- http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPACybersecurityInitiative.aspx
- Chartered Accountant should also be familiar with the following resources from the CBN website on security of e-payments:
  - Circular for Implementation of Two Factor Authentication for Internal Banking Processes
  - Guidelines on Operations of Electronic Payments Channels
  - Circular on the Review of NIP and other E-Payments Options with similar features
  - Circular on Industry Fraud Desk
- Cybercrime (Prohibition, Prevention, etc) Act 2015

In Conclusion…

The CBN’s approach to cybercrime within the financial services industry is informed by the need for collaboration. The Bank established the Nigeria electronic Fraud Forum (NeFF), a broad based platform for financial institutions, consultants and service providers, law enforcement agencies, and the Judiciary to collaborate to manage cybercrime risks within the financial services industry.

In Conclusion…

Further to the establishment of NeFF, we had established the Industry Fraud Desk as an industry coordinating point towards forestalling frauds within the industry while a full-fledged centre for managing cybercrime risks within the banking and payments system landscape is in the making.

The Bank Verification Number (BVN) which was implemented in 2013 has also greatly helped to forestall identity theft within the banking industry

In Conclusion…

- Tackling cybercrime is not a competitive issue. Rather it is a collaborative one. No organization is self-sufficient in provisioning its ICT infrastructure. This suggests that a single organization cannot by itself mitigate cyber risks without engaging other stakeholders ranging from vendors, telcos, clients, etc.
- Accountants must therefore be in the vanguard of collaborative efforts to share knowledge and collaboratively tackle the menace before it drives us out of business
- Similarly, awareness and education of employees within an organisation cannot be overemphasized as a first line of defence against cybercrime

Thank you