Cybersecurity: What Chartered Accountants Need to Know

David Isiavwe, PhD
President, Information Security Society of Africa-Nigeria

At the 47th Annual Accountants Conference
News...

- US accuses Russia of hacking into computers to favour a presidential candidate
- UK parliamentarians point to Russia as attackers of their systems
• Berlin confirms an attack on her political power-house.
• Cyber-attack on Malta’s election from Russia
• Kenya is boiling now because the opposition believes the voting system is compromised.
• Sony is on its knees after an attack allegedly by North Korea
News...

- Nigeria is on the world map of cybercrime
- World’s Top 5 Cybercrime Hotspots
- 3rd in global internet crimes behind UK and US
- Owns 27% of $2B cybercrime losses in Africa
- Loses about N127bn yearly to cybercrime
News...

• Businesses are suffering
• Companies are dying
• ‘Defenders’ are being attacked too
• Big consulting firms have their fair share

David Isiavwe, PhD
The Top Emerging Technologies and Innovation

- Fintech
  - The use of technology for financial services away from traditional financial market. Using technology for deposit mobilization, credit and financing.

- Cryptocurrency
  - Digital currency that can be generated and validated without central bank or government. Peer-to-peer payment system using cryptography.
  - Bitcoin, ether, Litecoin, Swiscoin

- Blockchain & Distributed Ledger
  - This is a public ledger for keeping transactions done with cryptocurrency.
  - The ledger is distributed such that transaction integrity check is always carried out.

David Isiavwe, PhD
The Top Emerging Technologies and Innovation

• Artificial Intelligence & Robotics
  • This is the attempt to make intellectual abilities from machines. The ability to learn just about anything, the ability to reason, the ability to use language and the ability to formulate original ideas.
  • Some robots and behavioural tools are using AI including for analytical review and advise.

• Internet of Things (Everything)
  • The network of day-to-day physical devices like vehicles, household appliances and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data.
  • This is also being extended to human beings with nanosensors embedded in human body to collect and exchange data
The Top Emerging Technologies and Innovation

- **Big Data & Analytics**
  - This is the analysis of large dataset from various sources for patterns and correlations.
  - It enhances decision making, provides insight and discovery, and supports and optimizes processes.
  - It is journey from REACTIVE to PREDICTIVE to PRESCRIPTIVE

- **Cloud Computing**
  - A shift from physical servers and self-hosted IT services to remote and shared resources. All as a service (AaaS).
  - Infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).

David Isiavwe, PhD
The Top Emerging Technologies and Innovation

- Virtualization
- Autonomous Car
- Drones
- Virtual Reality
- Augmented Reality
- 3D Printing

David Isiavwe, PhD
Convenience Vs Security

- Our Convenience is inversely proportional to Security
- Equilibrium is hard to find in reality
- Android Phones and Blackberry
The Cyber Threats Landscape....

- **Phishing and Smishing**
  - Obtaining private and confidential data through disguised and infected email (phishing) or SMS (smishing)

- **Social Engineering**
  - Psychological manipulation of victim into performing actions or disclosing confidential information

- **Botnet**
  - A collection of bots that may range from dozens to millions of ‘zombie’ computers that co-operate together and are essentially used to increase the impact of offences

David Isiawwe, PhD
The Cyber Threats Landscape....

- **Ransomware**
  - Malware designed to intimidate or force victims to pay a ransom, typically by encrypting victims’ files.

- **Distributed Denial of Service**
  - DDoS attacks aim to disrupt websites and network systems from operating normally and preventing legitimate users from accessing them. DDoS actors use collection of co-operating ‘zombie’ computers (botnets) to flood target websites or network system with data requests.

- **Insider Abuse**
  - The misuse and abuse of the privileges granted to legitimate users. This is an internal attack.

David Isiavwe, PhD
The Cyber Threats Landscape....

- **Identity Farms**
  - This is identity theft and storage for sale.

- **Backdoor Architecture**
  - A deliberate act by software developers to design own access to the system without the knowledge of the users.

- **Cybercrime Franchise in-a-box**
  - This is the automation, organization and established network of cybercrime. It allows cybercrime to be perpetrated by even non-technical attackers by click of mouse.
The Cyber Threats Landscape....

- **Keylogger**
  - A piece of surveillance that records everything that is entered on a keypad or keyboard, usually targeting passwords, PIN codes, instant messages, emails and other sensitive information.

- **Skimming Devices**
  - A device affixed on the ATM card reader to secretly swipe card information from unsuspecting customers.

- **Website Defacement**
  - This attack changes the visual appearance and contents of a website or a webpage.

- **SQL Injections**
  - SQLi is a technique often used to attack data-driven applications authored using Structured Query Language (SQL). This is done by including portions of SQL statements in an entry field so that the website will pass a newly formed rogue SQL command to the database (e.g. to update customer account balance).

David Isiavwe, PhD
The Cyber Threats Landscape....

• **Data Leakage**
  - This is the access and movement of confidential and critical business information during internal or external attacks.

• **Advanced Persistent Threat**
  - This is a network attack in which the unauthorized agent gains access to the network and stays there undetected for a long period of time.

• **Darkweb**

David Isiavwe, PhD
The Cyber Threats Landscape....

- Cybercrime as-a-Service
- Cyber Espionage
- Cyber Terrorism

David Isiavwe, PhD
The Cyber Threats Actors….

- Cybercriminals
- Nation States
- Cyber Activists

David Isiavwe, PhD
New Concerns for Chartered Accountants….

How can you provide assurance on financial statement?
New Concerns for Chartered Accountants….

- How reliable is this data/information?
- How confidential?
- What is ‘going-concern’?
New Concerns for Chartered Accountants….

- How relevant are chartered accountants in the scheme of things?
Countermeasures....

- Sustained investment in Cybersecurity
- Executive participation and commitment in Cybersecurity projects and initiatives
- Cyber Risk should rank with strategic risk in Enterprise Risk Management
- Innovative Cybersecurity awareness and education
- Capacity Building on Cybersecurity for IT professionals and Allies.
- Institutionalization of International cooperation on Cybersecurity
- Chartered Accountants should be Cybersecurity Agents

David Isiavwe, PhD
For Chief Information Security Officer (CISO) ....As Business Enabler

- Strategy
  - Business Aligned Strategy
- Strategic Organizational Framework
  - Executive Management Forum
- Tactical Organizational Framework
  - Middle Management forum
- Direct Communication
  - Establish direct relationship with stakeholders
- Automation
  - Automate Controls
- Pain Areas
  - Understand pain areas, provide solutions
- User Buy-in
  - Enable users to follow policies and controls

David Isiavwe, PhD
For Chief Information Security Officer (CISO) .... Doing Simple Right Things

- Inventory of all assets
- Effective incident management
- New business/products clearance
- Business enabling security
- Budget, resources, skill
- Data-centric online/offline

- Root cause and corrective action
- Policy deployment automation
- Clear visibility of all traffic
- Vendor/partner connectivity
- External interfaces visibility

David Isiavwe, PhD
For Personal Safety Online….

- Make your password complex by using a combination of numbers, symbols, and letters (uppercase and lowercase)
- Change your passwords regularly (every 30 to 60 days) or when you perceive compromise
- Do NOT give your usernames, passwords or other computer/website access codes to anyone
- Do NOT emails, links or attachments from strangers
- Do NOT allow installation of any software or connection of any hardware to your device without good understanding of its use and purpose.
- Always make electronic and physical back-ups or copies of your important documents
- Ensure your devices/systems have updated anti-virus
Cyber War or Nuclear War

Which one will be deployed for the next WORLD WAR?

Ease of deployment
Cost
Impact
Thank you