ITUEvents

Regional Cybersecurity Summit for Africa

20-23 November 2023
Kampala, Uganda

itu.int/go/_RCSSA

Supported by: AfricaCERT — United Teams promoting Cybersecurity in Africa

Hosted by: UCC Uganda Communications Commission; UgCERT Computer Emergency Response Team

Organized by: ITU

REGIONAL CYBERSECURITY SUMMIT FOR AFRICA

The use of Data and Statistics in Support of Cybersecurity

Kwadwo Gyamfi Osafo-Maafo

National Communications Authority (NCA), Ghana

20-23 November 2023
Kampala, Uganda

Outline

- Defining Cybersecurity and Security
- Why information, data and statistics are important
- Cybersecurity in an Organization (perspectives)
- References and sources for framing Data, Statistics and Other Information
- Learning from Industry and ITU
- Learning from Communities and Experts
- Learning from yourselves and your organizations
- Going further with Collaboration
- Some cases of examples from Ghana or NCA

Defining Security

- Security: Is the **minimizing of risk**, vulnerabilities or threats to assets and resources. It is also the establishment and **maintenance of protective measures of controls** to ensure prevention of fraud; undesirable outcomes, undesirable activities; protection from **deliberate, natural or accidental threats**; and **protection of available**, **integrity** and **confidentiality**. Security also concerns **providing assurance of safety**, freedom from anxiety or doubt, and confidence in a state of safety. Security also concerns providing assurance of safety, freedom from anxiety or doubt, and confidence in a state of safety (Terms from Dictionary and ITU Terms Database)

X

Defining Cybersecurity

- Cybersecurity is defined as “**collection** of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies **that can be used to protect the cyber environment and organisation and User's assets**. Organisation and User's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and or stored information in the cyber environment” (X.1205 - Overview of cybersecurity)

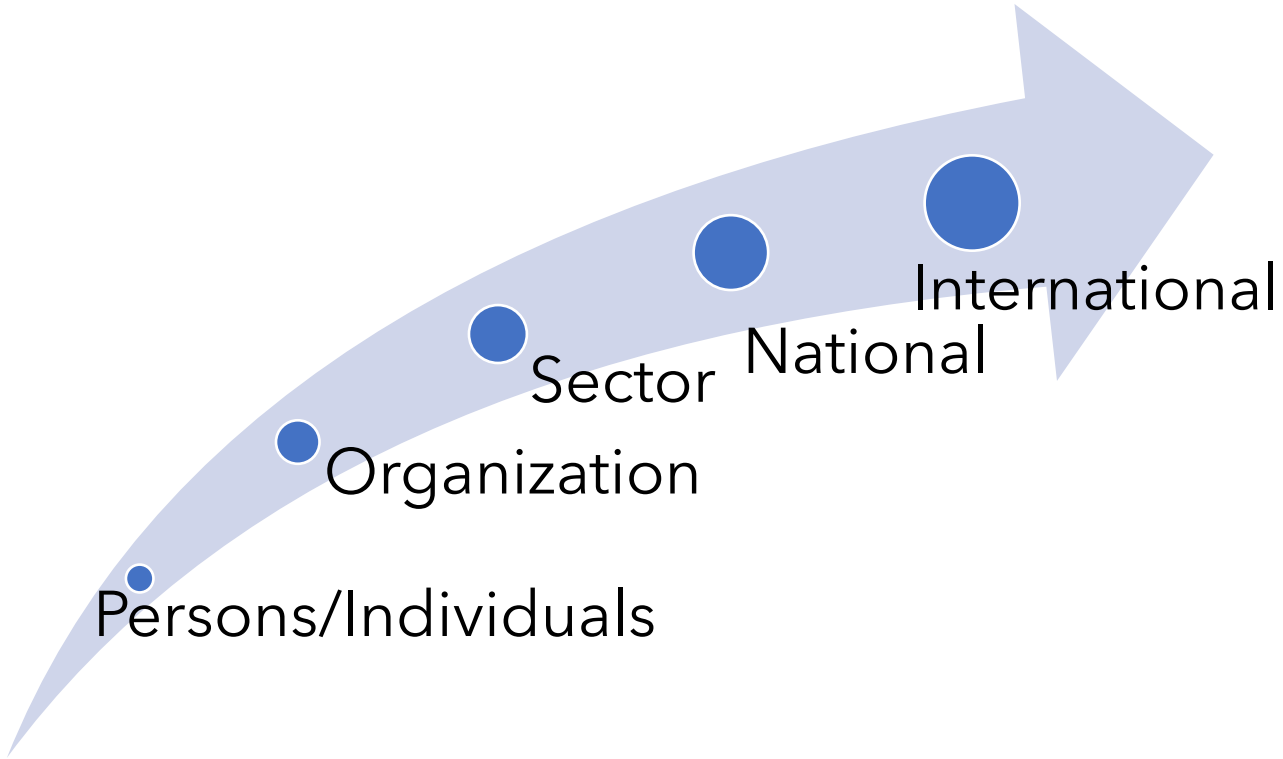
Importance of Information, Data and statistics

- **Efficiency and Effectiveness**: You must know your assets (including knowledge, facts)
- **Process Management**: Knowing what went in (inputs), how things worked (processing), and outputs
- **Framing**: Understanding how things went, are going, or will go
- **Support Decision Making**: Providing direction and confidence in decision (and chance to review and optimize)
- **Communication**: Telling or understanding your journey or story
- Scientific and logical

Concepts and Types of Information or Data

- Qualitative through Quantitative
- Lead and lag Indicators (inputs through outputs)
- Small Data and Big Data
- Simple (single values) to complex (flows, processes, technologies such as ML/AI)
- People, processes and technologies
- Primary, secondary and other sources
- Confidence and uncertainty (fuzzy arithmetic)
- Unstructured, Semi-structured structured data
- Files to Databases

Cybersecurity in an Organization
Levels of Security



ITU-T SG 17 Structure (Working Parties and Study Questions)

WP 1	WP 2	WP 3	WP 4	WP 5
Security strategy and coordination **Q1, Q15**	**5G, IoT and ITS security** **Q2, Q6, Q13**	**Cybersecurity and management** Q3, Q4	**Service and application security** **Q7, Q8, Q14**	**Fundamental security technologies** Q10, Q11
Q1/17 Security standardization strategy and coordination	Q2/17 Security architecture and network security	Q3/17 Telecommunication information security management and security services	Q7/17 Secure application services	Q10/17 Identity management and telebiometrics architecture and mechanisms
Q15/17 Security for/by emerging technologies including quantum-based security	Q6/17 Security for telecommunication services and Internet of Things	Q4/17 Cybersecurity and countering spam	Q8/17 Cloud computing and Big data infrastructure security	Q11/17 Generic technologies (such as Directory, PKI, Formal languages, Object Identifiers) to support secure applications
	Q13/17 Intelligent transport system (ITS) security		Q14/17 Distributed Ledger Technology (DLT) security	

ITU-T SG 17 Security Resources and Products

Recommendations (ITU-T Recommendations under SG-17)

E series: Overall network operation, telephone service, service operation and human factors

F series: Non-telephone telecommunication services

X series: Data networks, open system communications and security

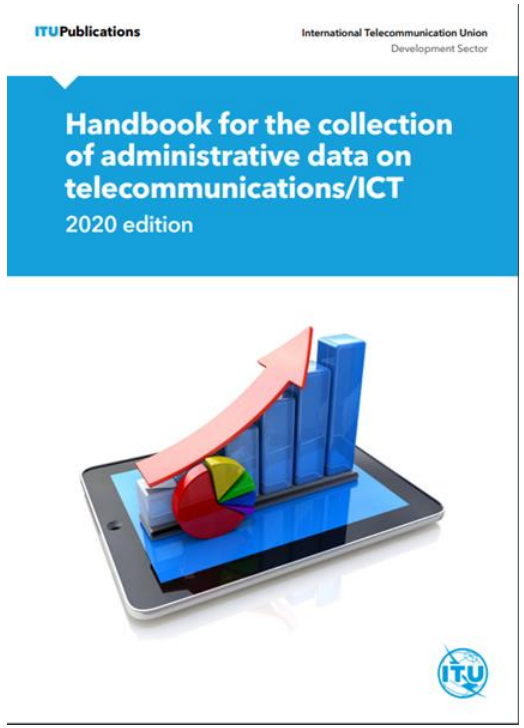
Z series: Languages and general software aspects for telecommunication systems

ITU-T Security Manual (Introduction to Security work of ITU-T, response to global cybersecurity challenges with international standards and recommendations)

Technical Reports, guidance documents and outreach initiatives.

ITU-T Technical Report on successful use of security standards (examples of ITU-T recommendations used to protect networks, people, data and critical infrastructure, offering guidance of particular value to security practitioners in developing countries)

Points of Reference (Standards and Guidelines for Data)



- **ITU-D Handbook for Collection of Administrative Data**

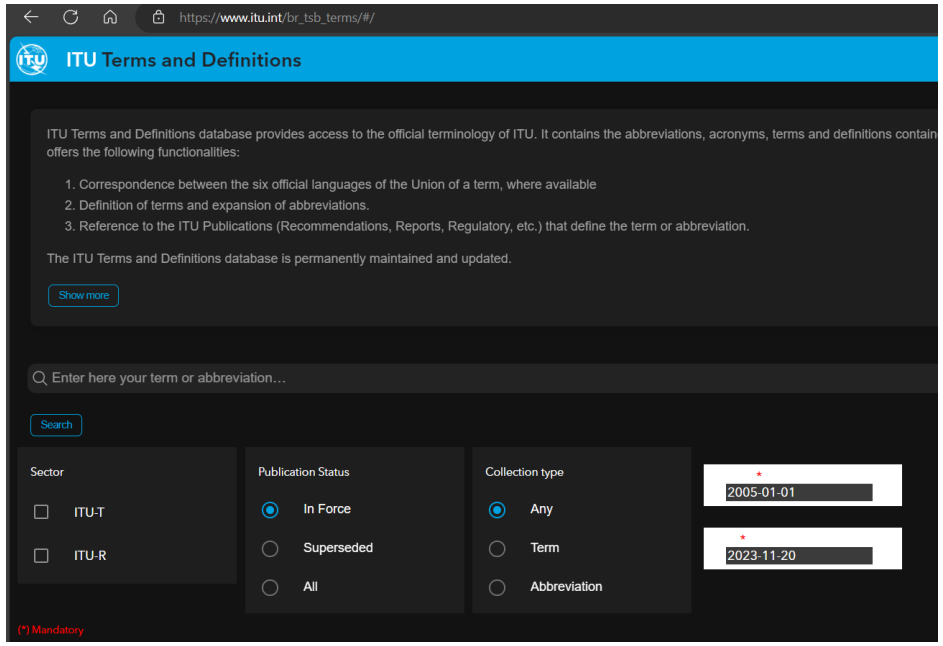
Indicators

- Fixed Networks (subscriptions, types)
- Mobile cellular networks (subscriptions, types of technology, porting)
- Internet (international bandwidth)
- Bundles
- Traffic
- Employment, Revenue and Investment
- Broadcasting indicators
- Quality of Service indicators

Source: ITU Publications https://www.itu.int/publications

Points of Reference (Definitions and Terms)

- ITU Terms and Definitions

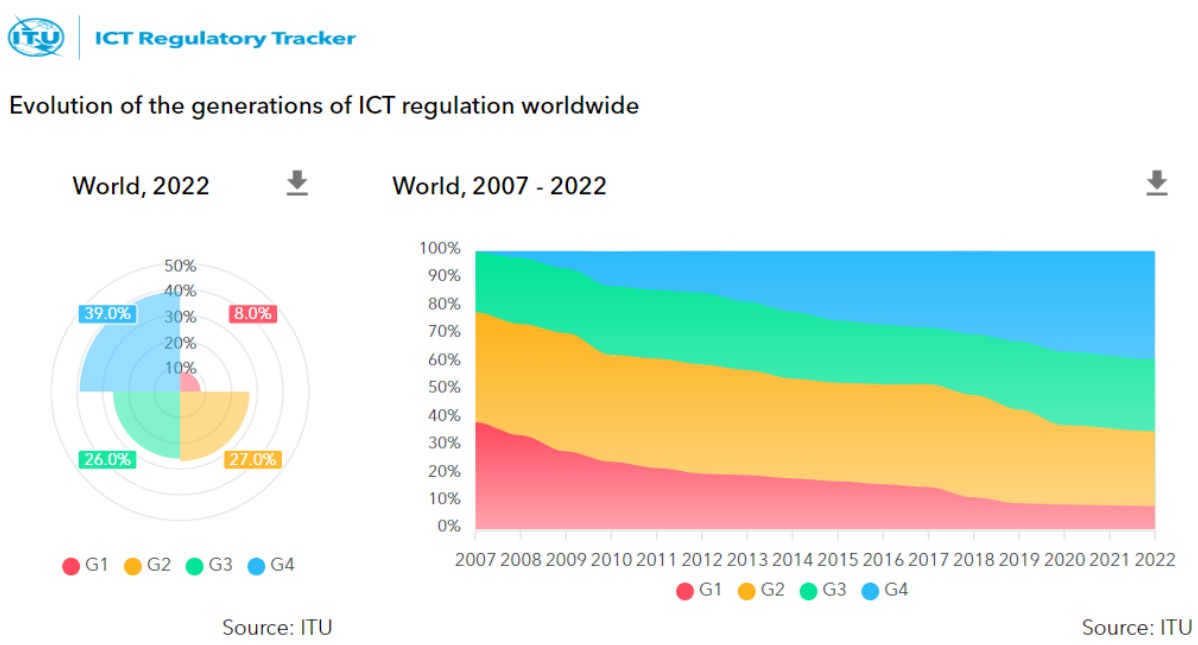


ector			Text	Date	Source	
	Security	term	The term 'security' is used in the sense of minimizing the vulnerabilities of assets and resources. An asset is	11/17/2021	Recommendation ITU-T E.800 (09/2008)	In force
	security	term	Condition that results from the establishment and maintenance of protective measures that ensure a state	6/6/2023	Recommendation ITU-T Y.4602 (03/2023)	In force
	Data security	term	Security preservation of integrity and availability of data.	11/17/2021	Recommendation ITU-T E.800 (09/2008)	
	Cybersecurity	term	The protection of data and systems in networks that are connected to the Internet.	11/17/2021	Recommendation ITU-T E.800 (09/2008)	In force
	security	term	The ability to prevent fraud as well as the protection of information availability, integrity and confidentiality.	5/11/2012	Recommendation ITU-T Q.1741.7 (11/2011)	In force
	security level	term	Security specification of the system which defines effectiveness of risk protection.	5/27/2011	Recommendation ITU-T Y.2740 (01/2011)	In force
	physical security	term	The measures used to provide physical protection of resources against deliberate and accidental threats.	1/1/2009	Recommendation ITU-T X.800 (03/1991)	In force

Source: ITU Terms and Definitoins - https://www.itu.int/br_tsb_terms/#/

Learning from the Industry and ITU

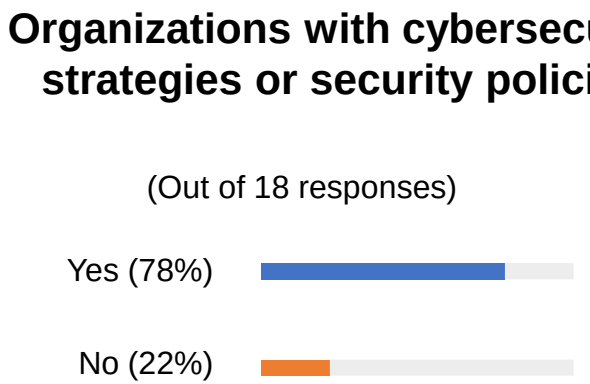
- ITU Regulatory Tracker



- ITU Global Cyber Security Index

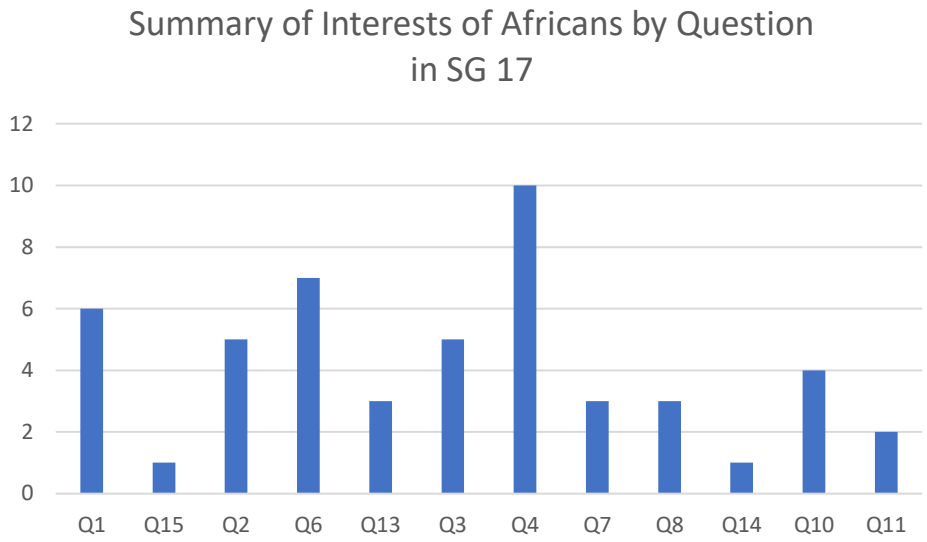
Learning from the Industry and ITU

- ITU-T SG 17 Survey on X.1060 Results



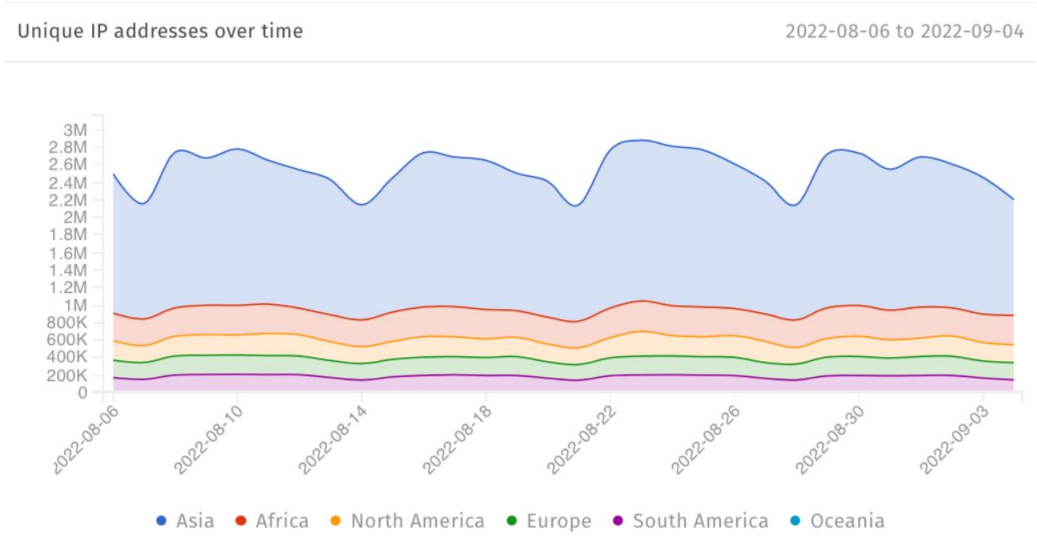
TD218

- ITU-T SG 17 Survey of Interests

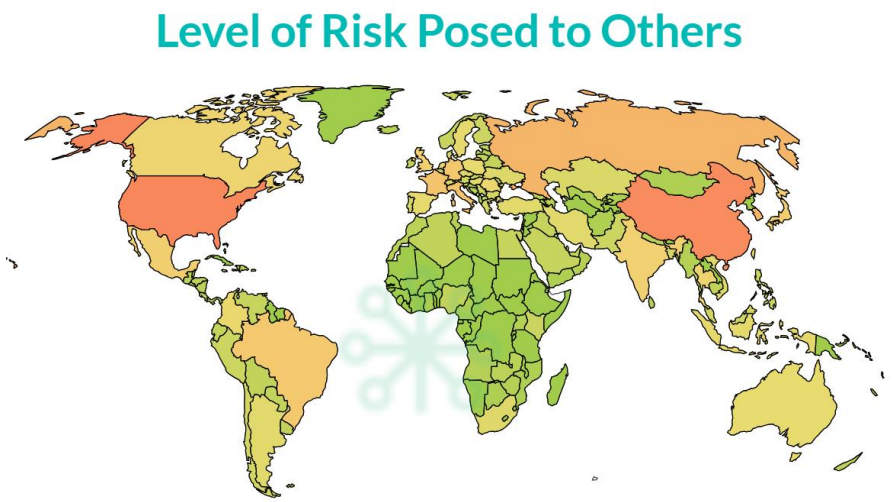


Data and Statistics from Communities and Experts (some examples)

- Shadowserver.org



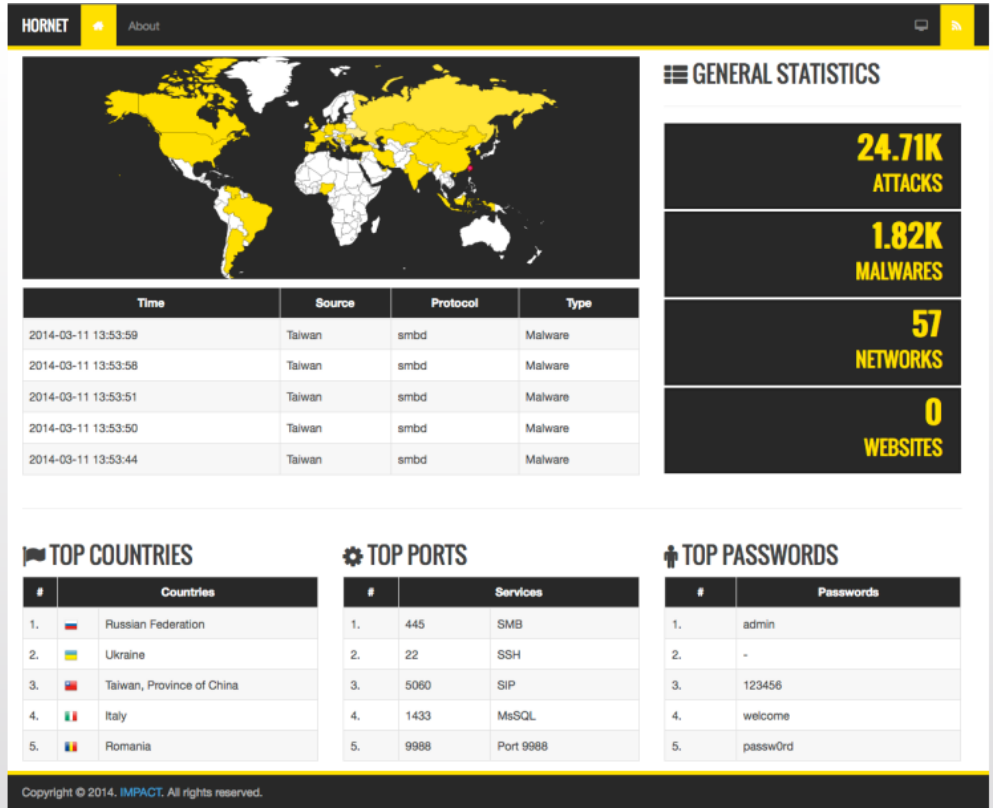
- Cybergreen.net



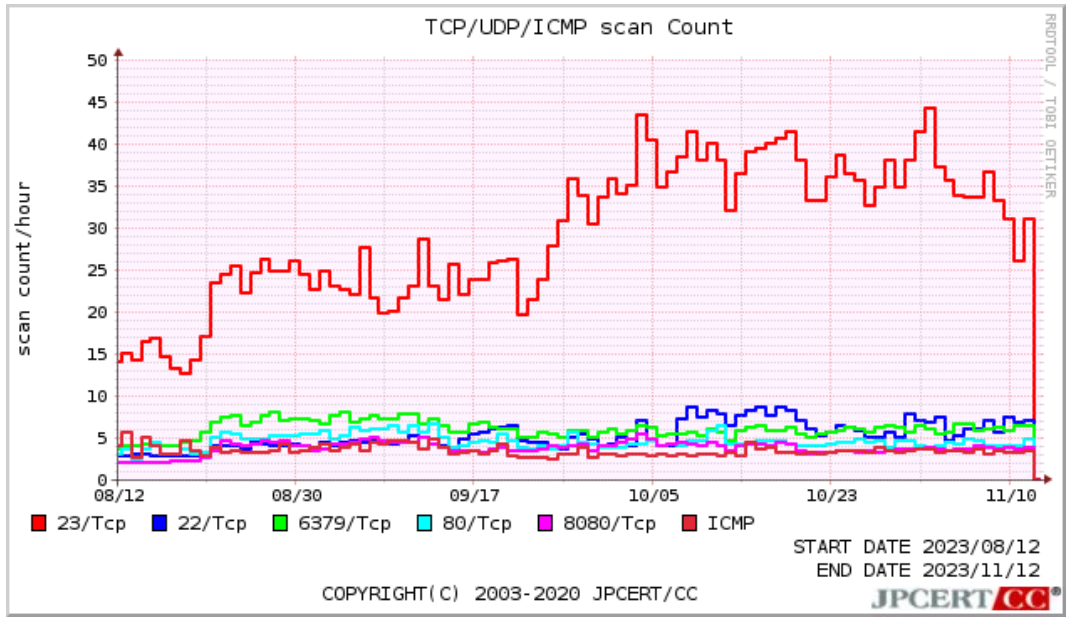
https://stats.cybergreen.net/

Data and Statistics from Communities and Experts (some examples)

- ITU-IMPACT Hornet - Honeypot Research Network



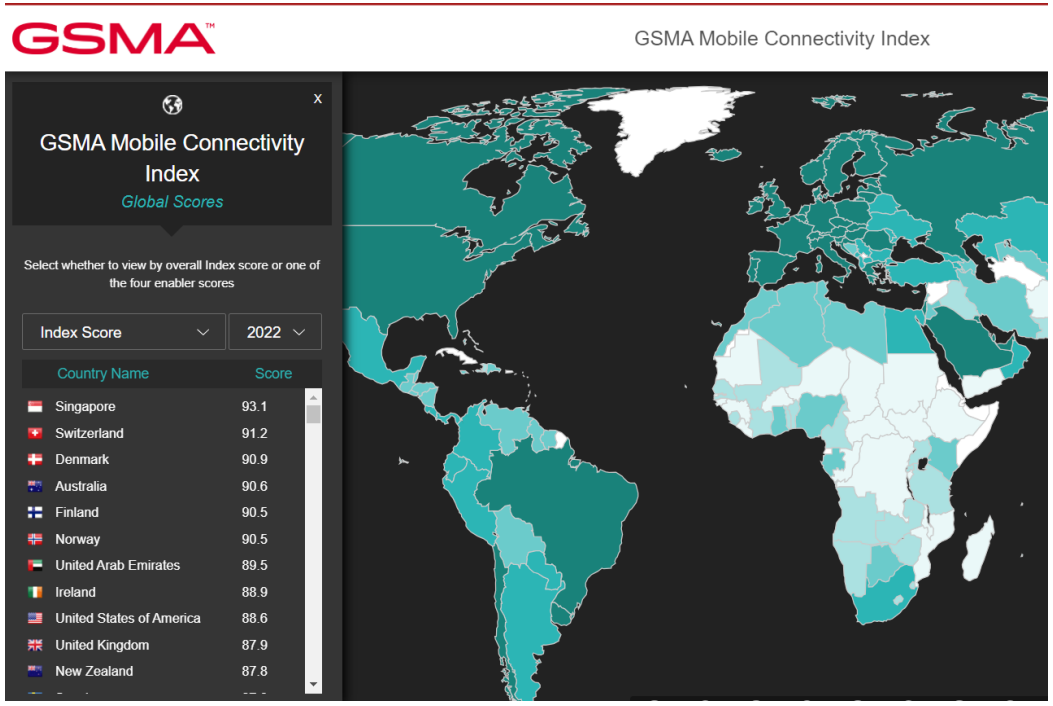
- JPCERT's Project Tsubame



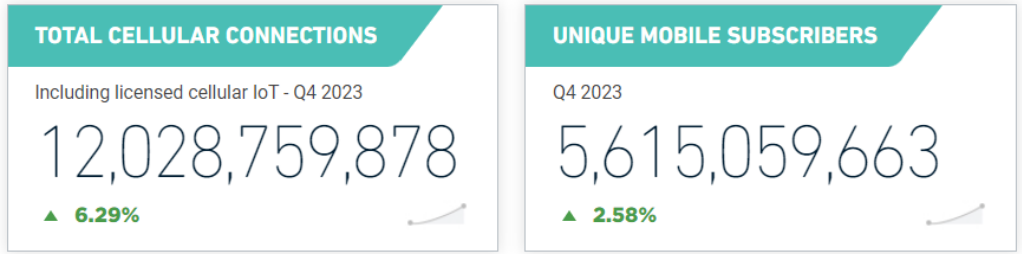
https://www.jpcert.or.jp/english/tsubame/

Data, Statistics and Lessons from Projects

- GSMA Data (e.g. GSMA Mobile Connectivity Index)



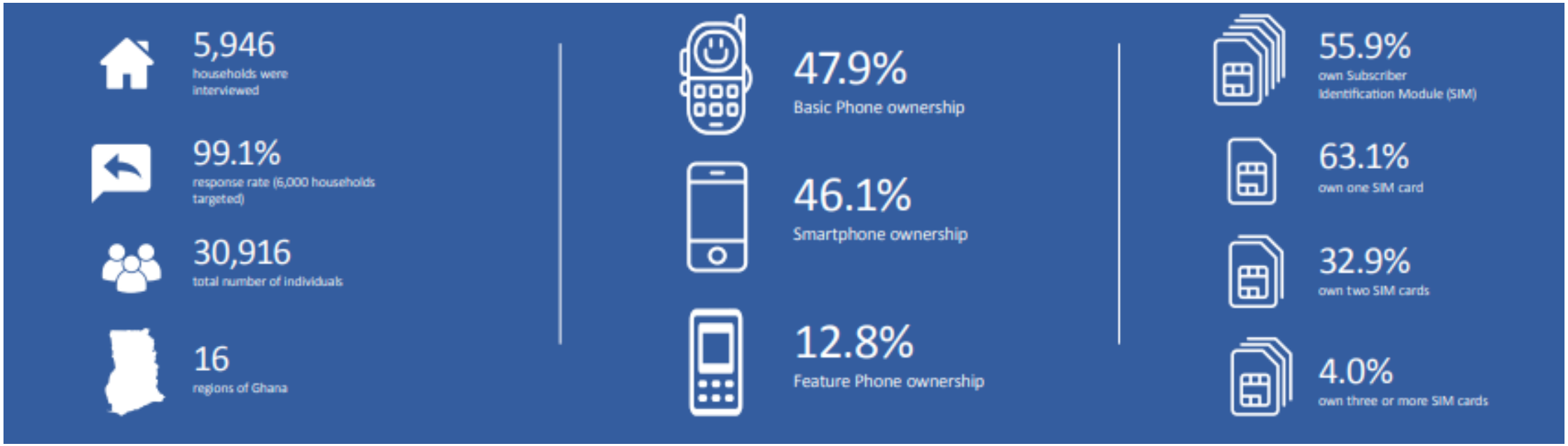
https://www.mobileconnectivityindex.com/index.html



https://www.gsmaintelligence.com/data/
https://www.gsma.com/futurenetworks/all-ip/statistics/

Case and Examples in Ghana

- Ghana ICT Household Survey (working across sectors – Ghana Statistical Service and National Communications Authority)



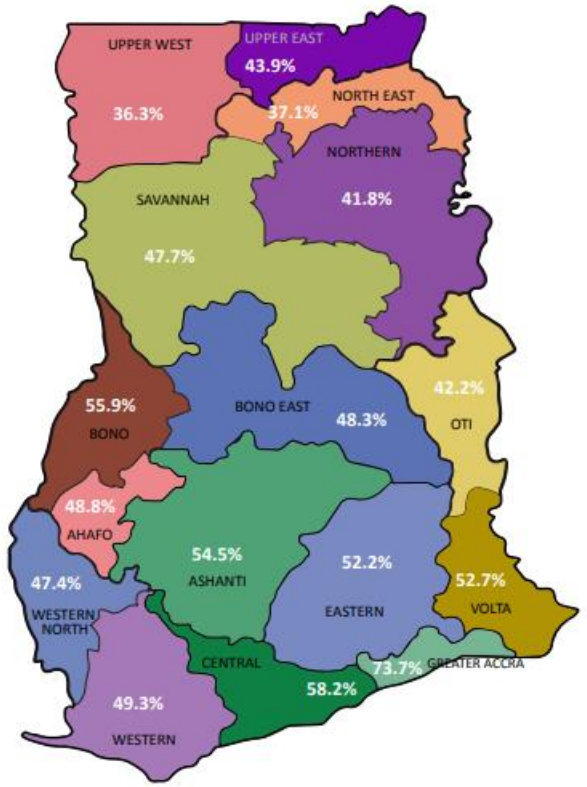
Case and Examples in Ghana

- Ghana ICT Household Survey(continued)

2.3 Regional distribution of mobile phone ownership in Ghana (Individuals five years and older)

From Figure 2.3, ownership of mobile phone is highest in the Greater Accra Region (73.7%) and lowest in Upper West Region (36.3%) .

Figure 2.3: Regional distribution of mobile phones in Ghana - Individuals five years and older



Case and Examples in Ghana

- Cybersecurity Reporting across sectors
  - Ministry requests key indicators, National and Sector CERTs engage and customize templates, terms are agreed for information exchange, NCA progressively develops and automates reporting
- Operators' Engagements on Cybersecurity in Communications
  - NCA outlines key issues and indicators, Operators and Service Providers engaged, Templates developed and aligned across Divisions

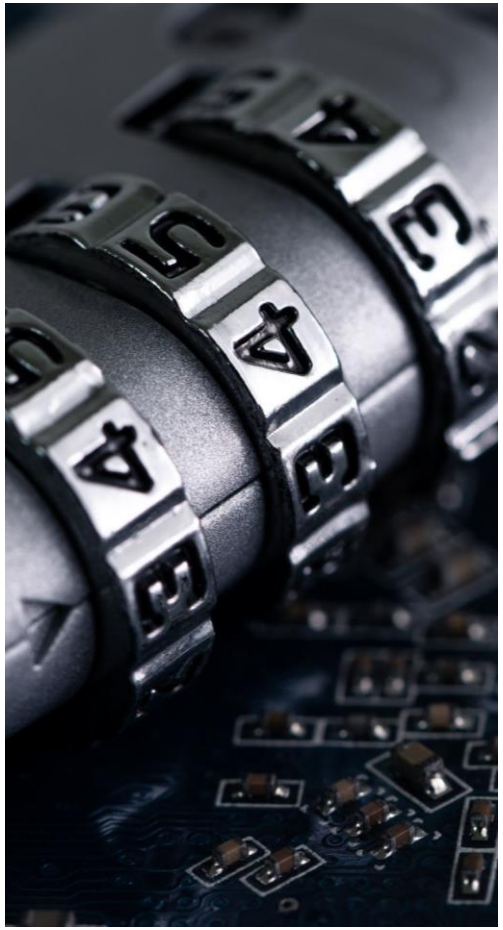
Case and Examples in Ghana

- Cybersecurity Reporting on Regulatory Data
  - Cybersecurity reporting and indicates (as included in licenses, directives and communications)
  - SIM Registration Data analysis (forensics audit and monitoring) for subscriber statistics
  - Started small (table-top; laptops and computers; algorithms to software, programmes and statistical databases)

Case and Examples in Ghana

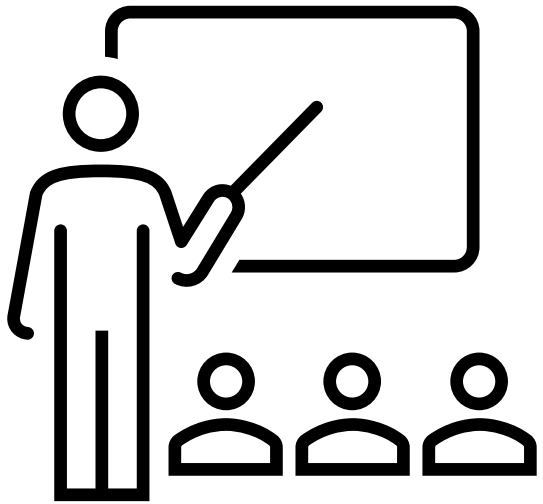
- Research, Innovation and Policy Division of NCA
  - Tracks strategy, policy and objectives of divisions
  - Divisions (e.g. Cybersecurity) make quarterly inputs into organizational strategy and objectives
- Consumer and Corporate Affairs Division of NCA
  - Documents and keeps database of complaints

Case and Examples in Ghana



- NCA Internal Security
  - NCA Cybersecurity Security Engineering Unit performs assessments, vulnerability assessments, and maintains database of assets and vulnerabilities
  - NCA Cybersecurity Security Operations Unit contributes to database of incidents and reports (including threats on dark web)
  - NCA Cybersecurity Communications Team tracks engagements for awareness (e.g. which staff is trained in which division)
  - NCA Data Protection team tracks assessments and reports on data protetion

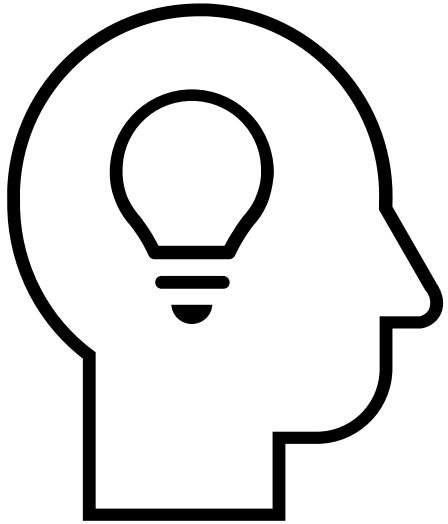
Localized Lessons



- Consider laws, regulations, standards and management systems
  - Ghana's National Communications Act, Electronic Transactions Act, Data Protection Act, Cybersecurity Act
  - Directives on Critical Information Infrastructure (from Ministry of Communications and Development through the Cyber Security Authority)
  - Information Management Systems for Business Continuity and Disaster Recovery, Risk Management, and Information Security

General Lessons

- Data and Statistics helps with empowerment, communication, and impact
- Stakeholder buy-in including support at all levels including board, management and staff

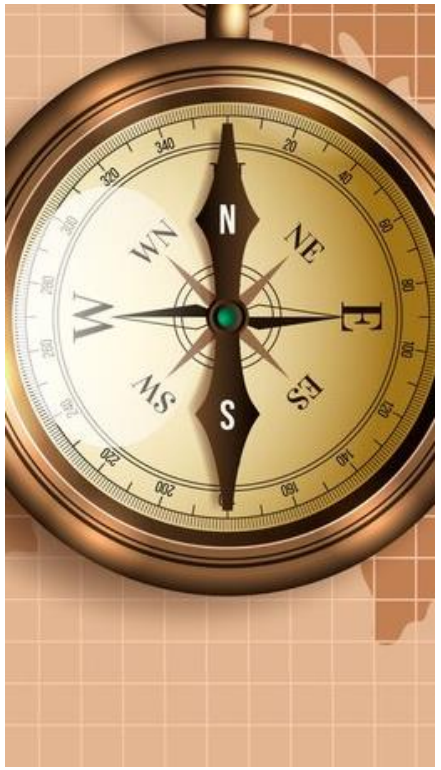


General Lessons

- Culture of Data and Documentation
- Awareness and training
- Collaboration and teamwork (with resource use)
- Incremental and directed (do not be afraid to fail or do not have to be perfect)
- Listen, share and discuss (different views and uses of data but important to be aligned)

Where are we headed

- Collaboration (information sharing platforms, agreements and processes for information/data exchange)
- Technology (build on existing tools within organizations – e.g. CRM, Ticketing, Monitoring)
- Automation, AI/ML
- Further Integration into strategy, policy and operations

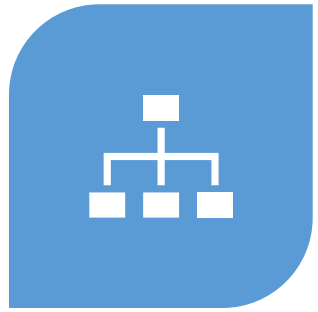


Things to watch out for

OVERLAPS AND CONFLICT (OPPORTUNITIES FOR SHARING, LEARNING AND EFFICIENCY)

OVERHEADS (BALANCING SUPPORT AND ENABLING BUSINESS OPERATIONS)

RESOURCES AND COST (USING OPPORTUNITY/RISK-BASED APPROACH)



BIG PICTURE (SUPPORTING THE ORGANIZATION)

Questions?

Thank you!