NAME : Lethukuthula Gumede
COUNTRY : South Africa
REGISTRATION NUMBER : 6760

Question 2.1: What is the industry's experience in planning, implementation, and evaluation of, as well as compliance with cybersecurity regulations, standards, measures, or procedures?

There are no regulations governing cybersecurity for electric distribution utilities in SA. We have the National Cybersecurity Policy Framework (2015) that addresses cybersecurity at a national level. There is also a national critical infrastructure cybersecurity plan that is in progress. However, no regulatory framework has been enforced for electric utilities. Therefore, compliance to regulations is non-existent. Each organ of the state is responsible for in protecting its critical infrastructure, therefore choice of cybersecurity standards and procedures are left to each organisation.

The electric power grid is a highly interconnected system that cannot be protected taking a siloed approach. There is no single national strategy for information security for critical infrastructure - no consolidated strategy that talks to the objectives and frameworks under which regulatory measures can be enacted.

Contextual risk models are required that are objective enough to drive risk adjusted capital investment programs. This is where most of the difficulty lies. Trying to understand the threat landscape at the national level facing the power sector as a whole. A holistic approach that takes into account the various threat actors and their intent. This in turn can drive cyber investments.

There is also a general lack of governance and regulation around data sovereignty for ICS. As suppliers drive the move to fog or cloud based solutions, EPUs are seeking guidance on how to make this transition

EThekwini Electricity (EE) Communication Networks Branch (CNB) has formulated a cybersecurity strategy that draws best practice from international standards such as SANS/ IEC 62443-2-1, NERC CIP 002-011, IEC 62351. The risk-based cybersecurity strategy focuses on people (creating cybersecurity awareness and cybersecurity culture), processes (cybersecure business processes) and technology (security by design).

Three strategic goals of

- SG 1: Protect CNB information and communication assets to ensure the availability, integrity and confidentiality of communication services,
- SG2: Develop a Cyber Security knowledgeable workforce,
- SG 3: Improve cyber security situational awareness across the branch, were chosen to improve the cybersecurity posture of the branch.

CNB had undertaken a cybersecurity awareness assessment to establish a baseline level of cyber security awareness within the branch with the aim of identifying training needs to improve the situational awareness and security practices within the branch. Cybersecurity awareness presentations/campaigns were held to increase cybersecurity awareness.

Cybersecurity risk assessment according to SANS 62443-2-1 asset/ scenario-based approach. Risks were ranked by the number and severity of the consequences. Recommendations have been made and some of their implementation is under way.