NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY

FACULTY OF APPLIED SCIENCE
DEPARTMENT OF COMPUTER SCIENCE

A CYBER SECURITY FRAMEWORK FOR SMART GRID ASSETS

A DISSERTATION SUBMITTED BY

AGATHAH MUKUMBIRA

Student Number: N01416113W

Supervisor: Mr. S. M NLEYA

NOVEMBER 2016, BULAWAYO

This dissertation is submitted in partial fulfillment of the requirements of the Master of Science in Information Systems Degree Program

ABSTRACT

A cyber security framework is a set of industry standards, guidelines and best practices that help organisations manage cyber security risks. Cyber security is essential to the nation's economic health, its critical infrastructure and its national security since the nation depends on the reliable functioning of all its critical systems. This study set out to propose a cyber-security framework for use by power utilities in addressing security challenges in smart grid assets. This was driven by the need to distribute electric power to profitable consumers in a transparent manner hence the initiative by ZETDC, which is the major power utility distributor in Zimbabwe, on modernisation of electric power consumption with an Advanced Metering Infrastructure (AMI). Leveraging on the efforts of other standard bodies like NIST, previous work on cyber security is considered in the literature review with a narrowed scope to cyber security in smart grid assets, thereby highlighting the main theme of the study. Case study approach is articulated in research methodology and semi-structured interviews, content analysis and focus groups were used as data collection instruments. The cyber security framework proposed comprises of five major functions: Identification function, Protection function, Detection Function, Response function and Recovery function. The proposed framework will help the power utility in articulating its management of cyber security threat by organizing information, enabling risk management decisions and addressing cyber-threats against the AMI. A deductive approach is used to discuss the results and carry out a comparative analysis of literature findings with data found from the case study. The conclusion drawn is that protection of smart grid from cyber-attack is not only a concern of the engineers, researchers and the power utility operators, it is also the responsibility of the government to ensure the security of this national critical infrastructure. The main contribution of this study is a cyber-security framework for smart grid assets which can be used both for generic and specific guides by power utilities since it takes into consideration the broader SADC cyber security vision. The proposed framework can be used to assist industry utilities, vendors, academia, regulators, system integrators and developers and other smart grid stakeholders to manage cyber security risks and for future decision making. For instance by reducing and better managing cyber security threats and vulnerabilities, saving as a model for critical infrastructure and as the framework is put into practice, lessons learned will be integrated into future versions.