SSIRC 2021-126

CYBER SECURITY RISK CULTURE: TELECOMMUNICATIONS RISK REPORTING

Gerrit Maritz
Cyber Security, North-West University, Vanderbijlpark, South Africa
ORCiD: 0000-0003-1741-1968

Emmanuel Mulambya
Faculty of Economic and Management sciences, North-West University, Vanderbijlpark, South Africa
ORCiD: 0000-0003-2796-5534

Abstract:
In a digital world, telecommunications companies provide computer-based technology (referred to as cyber technology) that allows people and businesses to communicate and conduct business. To protect these users against the dangers and threats associated with cyber technology, cyber security must ensure that the technology is operating as expected, cannot be tampered with, and is available when required. The present risk culture study investigated perceptions of internal risk reporting for decision making by two groups of participants: cyber security practitioners working in a cyber-security unit, and senior managers responsible for cyber security but not working directly in the cyber security unit. The research used a qualitative approach to collect data in a telecommunications company, based on a review of the literature, document analysis, and semi-structured interviews, followed and underpinned by qualitative data analysis. Cyber risk reporting that fails to meet the objective of enhancing decision making could result in risks to the organisation and its customers. Our findings showed that although the company's cyber security unit had all the textbook policies and procedures in place for risk reporting, in practice the guidelines for risk reporting seemed not to be adequate to the task. It is recommended that organisations in which cyber security is a key pay close attention to appropriate reporting guidelines for risk data aggregation and reporting. As this was an exploratory study on internal cyber risk reporting, the findings highlighted interesting areas for further research. These include challenges in cyber risk reporting, the monitoring of the contribution of cyber risk reporting to enable decision making, the importance of the accuracy of information gathered, risk reporting to internal audiences, and organisational structures and responsibilities for risk reporting.

Keywords:
Risk reporting, risk data, risk management, risk culture, risk awareness, cyber security