ABSTRACT

It is unclear how government departments have incorporated cybersecurity in their strategic planning processes, policies and operations to promote organisational and operational resilience. The government stores a significant amount of data and often uses legacy systems vulnerable to complex cyber threats and attacks. Vulnerabilities mitigated through cybersecurity frameworks, standards, people management and backed up by good vulnerability intelligence can provide an understanding of how and why threat actors are targeting particular vulnerabilities.

The case study method was chosen as it was considered highly suitable for the research setting because this method provided a provincial government department view by focusing the study on cybersecurity practice in government departments in an unidentified province. This data enabled the researcher to understand the current vulnerabilities, needs and historical responses as the basis for designing future cybersecurity responses to ensure operational resilience.

The research methodology identified the appropriate methods which the researcher exploited to address the research purpose and research questions. Methods of research design were examined in relation to the research diagram. Qualitative constructivism method research approach allowed the researcher to comprehend the provincial government's cybersecurity challenges. Constructivism was selected as new knowledge that needed to be collected rather than merely acquiring it via memory or solely communication from those who know to those who do not know about cybersecurity in the provincial government. A systematic mapping study provided an unbiased and systematic mechanism to answer research questions by finding the research outcomes. The lighter systematic mapping method was chosen as a more comprehensive systematic literature review was not required at this research level. Using systematic mapping, existing research on cybersecurity was better understood by identifying the limitations and gaps of current research.

One of the main findings is that provincial government departments are exposed to cybersecurity vulnerabilities and threats because they do not have adequate controls in place. The provincial government visibility of cybersecurity vulnerabilities and threats has been identified as lacking. A critical implication is that there is no alignment between provincial departments regarding cybersecurity. The outcome of the research is that the provincial government is not in line with the national cybersecurity policy framework because the identification of cybersecurity risk is low. These factors can potentially influence the availability of government information systems and affect the department's operational resilience. The Government Information Technology Council, which is involved in the investigation, formulation and development of ICT security policies, e-government and strategy, and ICT procurement, has key objectives which focus on the alignment of ICT and ICT Security (Cybersecurity) in the province with government business objectives.

The identification of cybersecurity vulnerabilities and threats is critical for the provincial government to respond to cyberattacks, this cybersecurity risks can be mitigated by incorporating people management with programs such as cybersecurity awareness. Cybersecurity vulnerabilities, responses and people management are interlinked and need to be aligned to improve the provincial government's operational resilience.

The GITO council should be making departments HOD's and the premier aware of non-compliance in departments and implement measures to ensure that cybersecurity incidents in the departments are reported to the provincial GITO council to ensure that the cybersecurity incidents get a response and cybersecurity controls amended to mitigate future incidents.