Evaluation of Online Resources on the Implementation of the Protection of Personal Information Act in South Africa

Johnny Botha, M.M. Eloff, Ignus Swart

Abstract:
The recent adoption of the privacy law, Protection of Personal Information (PoPI) Act in South Africa, mandates notable changes from both government departments and the public sector when dealing with personal identifiable information (PII). Recent research has shown that the level of change still required to comply with the new Act is significant. Surveys indicated that approximately only forty percent of organisations in South Africa have started with the compliance process. Private empirical research has found widespread leakage of PII within South African cyber infrastructures. The leaked information affected well over two million South African citizens in some or other manner and with penalties instituted by the PoPI of up to R10 million, it is crucial for organisations to clean up these incidents of non-compliance. Even without the monetary incentive, leaked PII holds a significant threat, not only for individuals but also for companies and governmental organisations alike. Several documented instances exist where targeted phishing attacks, that has a 70% success rate once PII is included, has been successfully used against organisations. While technical controls may limit the leakage of PII, significant security vulnerabilities exist that allows for the circumvention of these controls. Cyber security awareness is still the primary defence against these technical control failures, but the notable challenge remains in educating users and responsible personnel. As with any cyber activity, there is a human factor that requires a significantly diverse skill set to understand the infrastructure that comprises an organisation. With cyber security education a continuous developing field, there is a dire need for additional research to supplement this knowledge base. This paper examines online resources available for individuals, organisations and governmental departments to comply with the PoPI Act. The approach used will be to examine content made available through popular social media platforms such as YouTube (YouTube, N.D.), Facebook (Facebook, N.D.), Twitter (Twitter, N.D.) and search engines. These data sources were chosen since it may be the most likely common route individuals will take to gain fundamental understanding of the requirements the PoPI Act places on them. Identified resources will be evaluated for the audience they serve (e.g. business owners, privacy officers, managers and employees), technical content (e.g. informative, guidelines or step by step instructions) and finally the cost involved to access or download resources (e.g. free or commercial).

Keywords: Cyber security awareness, education, online resources, PII disclosure, PoPI.