

Cellular companies must protect clients' personal data

With the promulgation of the Protection of Personal Information Bill (POPI) later this year, the protection of consumers' personal information is becoming increasingly important. In light of the increase in cellphone banking fraud in South Africa, this has become particularly relevant for companies in the telecommunications space.

Recent statistics released by the South African Banking Risk Information Centre (SABRIC) revealed that cases of illegal SIM-swaps, which resulted in subscribers being defrauded of their money, increased by 900% from under 100 cases in 2011 to around 1000 cases in 2012.

"With around 29 million cellphone subscribers in South Africa, according to Nielsen, cellular service providers must implement practices to help reduce the number of incidences, one of which is the proper destruction of documents containing client's personal details," said Gianmarco Lorenzi, MD of Cleardata, a group company of Metrofile Holdings.

"Cellular network providers handle and store thousands of clients' personal information on a daily basis and need to ensure that this information is protected at all times in order to comply with the POPI."

Forgotten branches

He said that while head office may already be working closely with legal teams to ensure compliance, they may be forgetting about an often overlooked aspect of the organisation: its network of branches across the country. "It is crucial to ensure that regulatory requirements extend to all areas of the organisation, regardless of their location, as non-compliance with legislation governing data protection branches could potentially lead to the downfall of the organisation."

"The POPI standards require that personal information is not only securely stored and managed, but also properly disposed of in a manner in which the information cannot be reconstituted," said Lorenzi. "Every company that has access to personal information relating to their employees or clients has a responsibility to dispose of that information in a proper manner. Risks are faced by all industries; however financial institutions, such as the banks, are faced with an even greater risk due the vast amount of personal information they have relating to their clients."

He said that if documents are not disposed of effectively the organisation could face legal, reputational and financial consequences. "Telecommunications companies can be held liable for identity theft if client's information falls into the wrong hands. Casually discarding information shows a callous disregard for customer and shareholder interests."

"It is advisable to ensure that all organisational branches are reviewed constantly with regards to data protection regulations and necessary steps are taken to ensure adequate levels of compliance."

Need to protect trade secrets

Lorenzi said that besides compliance with information protection legislation, telecommunications companies also need to protect trade secrets from competitors. "If confidential information about a new product line or strategic plan is left lying in an exposed rubbish bin, it is vulnerable to the eyes of competitors and companies may find their competitive advantage is lost."

"Shredding unwanted documentation remains the most effective data destruction method as it ensures the documentation cannot be reconstituted in any way," said Lorenzi. "Employing the services of a reputable data destruction company that is compliant with international standards of data destruction is the most reliable way of ensuring that confidential documentation does not fall into the hands of unauthorised parties."

"In light of the impending POPI coming into law, it is essential for all businesses to protect their information at all transaction points and employ strict governing principles at all branch locations to ensure that no documentation is left exposed to avoid the consequences of non-compliance," concluded Lorenzi.

For more, visit: <https://www.bizcommunity.com>