

# POPI is beneficial for SA companies

POPI is being seen as a compliance nightmare, but it could also be highly beneficial for South Africa, delegates heard at the recent IDC - Fortinet Advanced Threat Protection Network Security Conference in Sandton.

The Protection of Personal Information (POPI) Act is raising concern among South African enterprises. Compliance is expected to add cost and complexity to securing personal information, and the potential penalties for non-compliance are significant. "POPI is being seen as a compliance nightmare," said Kerri Crawford, Associate of Norton Rose Fulbright South Africa. On the other hand, POPI also presents an excellent opportunity for local organisations to improve their security practices and for South Africa to improve its attractiveness to foreign investors, said Crawford.

Crawford noted that while the right to privacy is already enshrined in the constitution, protecting this right in court could prove complex and expensive for individuals. POPI provides accessible mechanisms for protecting the constitutional right to privacy in respect of personal information. In addition, it protects personal information relating both to individuals and corporates.

A key benefit of the new legislation is the potential impact on foreign investment and business into South Africa, said Crawford. "Currently, legislation in many foreign countries prevents companies from sending their information to countries where it will not be adequately protected," she said. "POPI, when it comes into effect, is a comprehensive piece of legislation and may well be recognised abroad. This will be good for local business."

## Expected to incentivise organisations

More importantly, she said, POPI is expected to incentivise organisations to step up their IT security measures. "South Africa is a recognised target for cyber-crime. Before POPI, South Africans have not been legally obliged to be risk aware. POPI requires us to focus on security awareness, which should have the effect of reducing South Africa's exposure to cyber risk," she pointed out.

Crawford said that POPI does not prescribe the security tools required to secure personal information, but it does require 'appropriate and reasonable measures' to protect both electronic and physical information. Generally accepted practices and procedures should be applied. This requires that, as cyber risks evolve, organisations must steps to apply advanced threat protection to mitigate those risks.

"Effective information protection and compliance with POPI is not just about IT," she noted, "it impacts on the entire organisation. Until now, the legal consequences of data breaches or loss in South Africa have not been severe in comparison with global counterparts. But as legal liability increases, so will security awareness." She added that POPI also demands that any organisation contracting a service provider in the collection or handling of personal information, must

contractually oblige that service provider to take the same measures the organisation is required to take under POPI to secure this data.

Crawford advised organisations to start their journey to compliance by assessing what personal information they hold and for what purpose; whether this purpose is legitimate; where and how they use, store it; who they share it with; and how and when they delete or destroy it.

During a panel discussion at the Security Conference, data security experts said the increasing sophistication of cyber-attacks meant that organisations should assume they had already been breached, and take a proactive, multi-layered approach to mitigating risk.

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