Wait and see approach could be detrimental

Many organisations have taken a wait and see approach to the Protection of Personal Information (PoPI) Act. This is largely due to the delay in the appointment of an information regulator, who has the power to investigate and impose penalties for breaches to the Act. The PoPI Act stipulates how companies may collect, handle, store and discard information, with heavy penalties for those that fail to comply. Once the commencement date of the PoPI Act is announced, organisations will have 12 months to comply with the Act. Xperien CEO Wale Arewa says the reality is that if there is a breach, the financial implications can possibly cripple an organisation. "If found guilty, companies will face potential civil claims, fines and reputational damage." "The Act enforces companies to introduce strict measures and guidelines that will safeguard the processing, usage and handling of sensitive information. It places a strict onus on businesses when it comes to handling personal information about their clients, staff and customers," he adds. Cybercrime is growing at a rapid pace, it's geared towards stealing personal information for financial gain. Once criminals have access to personal information, they can use it for identity theft or to commit fraud. Many people use their personal mobile devices for work purposes and this is a huge concern for organisations as confidential information is at risk of leaking. Company executives need to take measures to ensure that all personal information is protected on all mobile devices including smartphones, tablets and laptops. Arewa says knowing what information to protect is vital. "Once you know where this information resides, you can put a plan in place to secure it. Data encryption will help control what data leaves the organisation and also ensure that data is not accessible." When it comes to data leakage, employees are probably one of the weakest links in any organisation. Confidential information is often mistakenly sent to wrong email recipients and as a result, the company could be legally liable. If not properly protected, cybercriminals easily take

advantage of code vulnerabilities to gain access to data on these devices. It is crucial that businesses adopt a mobile workforce strategy with a security policy to effectively secure the data on all devices. Not only is the introduction of mandatory protection of personal data a huge challenge for companies, but now organisations are being prompted to rethink how they approach the reuse, recycling or recovery of their eWaste. Although the PoPI Act does not explicitly mention IT assets at all, the PoPI Act Condition 7 (section 19 to 22) requires a responsible party (the organisation that processes personal information) to prevent loss or damage to personal information (section 19 (1) of the Act) and (section 19 (2) of the Act) to conduct a risk assessment and establish and maintain appropriate safeguards (section 19 of the Act). Arewa says most organisations have very little or no idea when it comes to the protection of personal information when disposing of redundant IT assets. "By retiring technology assets wisely, customers can offset the cost of a secure IT asset disposition programme. Rather find yourself a third-party specialist with deep experience in secure IT asset disposition." Technology holds all kinds of proprietary company data as well as confidential customer and employee information. Data breaches are hard enough to control within the four walls of any organisation, but when they toss old computers in the trash or 'erase' the hard drive of old laptops, they could be releasing confidential data into the wild. "This trusted partner can help you find the metrics to convey a secure asset disposition plan's ROI to budget-minded superiors. You'll rest assured that security regulations are being met," he concludes. For more information contact Xperien on (011) 462-8806 or email itad@xperien.co.za or visit www.xperien.com