POPI's effects on IT asset disposal

Many organisations have a limited understanding when it comes to IT asset disposal (ITAD) and the dire consequences the Protection of Personal Information Act 2013 (POPI) could have on failure to comply with the requirements of the Act. The POPI Act when in effect will hold organisations liable for the safety of the information they process. Fines for non-compliance can be up to R10-million, with civil claims and reputational damage implications as well.

Not only is the introduction of mandatory protection of personal information a potentially huge challenge, but now organisations are being prompted to rethink how they approach the re-use, recycling or recovery of their e-waste. In addition, the National Environmental Waste Management Act 2008 (NEMWA 2008) and the Consumer Protection Act 68 of 2008 (CPA) also have a bearing on sound IT asset disposal.

How will the act change the role of IT asset managers?

The POPI Act will see the IT asset manager play a more active role in the overall security posture of the organisation, and play a role as a compliance officer rather than being simply a financially-oriented or operations-oriented professional. Asset managers will need to understand the requirements of the POPI Act and develop their own knowledge and skills as well as those of their organisations.

What are the biggest challenges facing organisations in managing their IT assets?

There needs to be the right level of funding to protect IT assets by using appropriate tools, techniques and technologies, while recognising that there is not unlimited budget to achieve the required level of protection. Balancing the security issues associated with IT assets include those owned by the organisation; and those which are "bring your own device", which the organisation does not own but is nonetheless liable for if these devices are permitted to process (capture, store, distribute) the organisation's personal information.

What does the POPI Act say about ITAM?

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). ITAM forms a key part of both the risk assessment and appropriate safeguards. This applies to assets either directly owned by the organisation, BYOD devices or devices used by Operators (service providers).

The significance of ITAM is that where IT assets are not appropriately managed organisations are likely to expose themselves to additional preventable risks of loss of personal information. This should be expected to result in action by the Information Regulator as well as other stakeholders. ITAM should be clearly seen as part of the whole personal information ecosystem, part of the information lifecycle.

Auditability is paramount to maintaining control and also provides the necessary feedback that will reduce costs, shortages and negate the whole compliance process. For example, if a hard drive is lost during transportation, it may contain the personal information of thousands of clients or employees. The loss of personal information could be detrimental to any business, this is why it is so important to be fully compliant.

There are companies that offer ITAD as a core function. These players can help you find the metrics to convey a secure asset disposition plan's ROI to budget-minded superiors. Moreover, once the job is under way, your partner will provide complete documentation of the disposal process. You'll rest assured that security regulations are being met.

Reputable asset disposal service providers should develop effective solutions to address everyday challenges, beginning with the risks associated with data loss. Handover of retired equipment should be immediate to avoid the inevitable loss that occurs in IT storerooms.

Ideally, there should be a project management system that offers the following:

- Developing a secure chain of custody for the assets;
- Minimising storage to prevent shortages;
- A call centre to schedule hardware collection;
- Packaging;
- Secure transportation;
- On-site data elimination;
- Mobile hard drive destruction;
- Data destruction compliance certificates;
- E-waste disposal compliance certificates;
- Asset buy-back;
- Trending reporting; and
- An audit trail.

If your service provider can deliver all this with clear and transparent charges, you are on the right track. However, if you don't have a service provider that understands that data loss may lead to reputational loss, you are probably at risk. ■

ACKNOWLEDGEMENT
DR PETER TOBIN WITH WALE AREWA OF XPERIEN
@SAPOPITALK