

My Office

shop **sa**

JUNE 2014 R50. INC VAT

THE OFFICIAL MAGAZINE OF THE STATIONERY, HOME AND OFFICE PRODUCTS ASSOCIATION

PENS AND INKS

**ENERGY MANAGEMENT
AND BACKUP TOOLS**

**ESSENTIAL
FIRE SAFETY**

**BREAKROOM
APPLIANCES**



crystal™
Xtra Life

Writes over 2km



BIC®

For more information visit www.bic.co.za

My Office Magazine is the official magazine of the Southern African Association for Stationery, Home and Office Products. It is read by over 25 000 buyers and sellers of stationery and office products each month.

PUBLISHER

Rob Mathews - robm@icon.co.za

Kathy Gibson - kathy@futurewave.co.za

EDITOR

Mercédès Westbrook - mercedes@shop-sa.co.za

CUSTOMER RELATIONSHIP MANAGER

Wendy Dancer - wendy@shop-sa.co.za

NATIONAL OFFICE

Web Master: Neil Caetano

Design and Layout: Vanessa Bentley

New Membership: Rachel Skink

Reception: Ruth Montsho

Johannesburg Office

PO Box 3226, Parklands, 2121

6 Edward Street, Kensington B, Randburg, 2194

Tel: + 27 11 781 0370

Fax: + 27 11 781 2828

Email: info@shop-sa.co.za

Website: www.shop-sa.co.za

Cape Town Office

PO Box 48431, Kommetjie, 7976

Tel: + 27 21 780 1209

Cel: + 27 78 970 7633

Email: info@shop-sa.co.za

CONTRIBUTIONS

Letters and editorial contributions are welcomed and should be addressed to the editor at editor@shop-sa.co.za. Publication cannot be guaranteed and is subject to space and the editor's discretion.

THE LEGAL BIT

Whilst every effort is made to ensure accuracy the publisher and editor cannot accept responsibility for supplied material. The opinions of contributors are not necessarily those of shop-sa. Copyright is strictly reserved and no part of this magazine may be reproduced in whole or in part without the written permission of the publisher.

NEWS

34 | INDUSTRY NEWS

Industry-related news and trade business announcements

36 | ECO PAGES

A green sustainability update, sponsored by Mondi

SALES SAVVY

06 | MURPHY HAS NOTHING TO DO WITH IT

Aki Kalliatakis reveals that Murphy's Law is no excuse

26 | FURNITURE: STYLISH PAPER SAVERS

Recycling paper in the office is a necessary and beneficial exercise – and it can be stylish too

30 | BREAKROOM: SKIP THE CHORES

Life in the home and office has become mostly automated, thanks to light work appliances

BUSINESS SAVVY

04 | LESS IS MORE

Less is more is a tough concept when you are trying to do just about anything, says Gavin Moffat

08 WRITS OF EXECUTION

Dr Ivan Israelstam shows how parties who are not happy with the decision of a CCMA arbitrator can apply to the Labour Court to review the arbitrator's conduct

20 | POWER UP WITH A UPS

Invest in a quality UPS system that will protect your data and your components

28 | LEADERSHIP AS THE MANAGEMENT OF CULTURE

Colin Browne focuses on what makes a good leader

29 | TO CHANGE YOUR LIFE, CHANGE YOUR WORKDAY

Rethink your habits to boost your productivity



24 MOBILE DATA DEVICES AND POPI
If you have a business which uses mobile data devices, POPI will affect you



10 AS INK IS TO A PEN
A look at pens as the worker bees of the stationery industry



SPECIAL FEATURES

31 | FIRE RISK

Displaying the correct signage in a building can save lives

32 | OPI SPECIAL FEATURE: GOING DIRECT

A new go-to-market strategy in Europe is selling directly to resellers rather than via the merchant channels

47 | WIN THIS

Write in and win giveaway products

IN EVERY ISSUE

02 | EDITOR'S WELCOME

03 | CRIME ALERT

23 | WEB BUTTONS

33 | PERSONABILITY

38 | PRODUCT SHOWCASE

40 | BUYERS' GUIDE

48 | PUNCHLINE

Stationery sponsored by



Office paper sponsored by



Member of the Audit Bureau of Circulation



Published by



PRINTED BY

Colorpress (ptv) lth

Top tips to reduce retail risk



Reduce retail risk by addressing these five key areas

Remote access – ensure that you understand exactly who is accessing your network remotely at all times. If you have third parties managing your IT network, ensure they only access your systems when required and that you have full visibility of all their activities. You should insist they have dedicated user accounts for all their staff and confirm they use unique passwords. Ask and confirm that remote access is authenticated using two factors. This means that the remote user must provide two means of identification.

Firewalls – by segmenting general office or store systems that are used to access e-mail and the Internet away from business systems (such as back office payment systems), an organisation will significantly

reduce their risk of the payment systems being affected by unwittingly downloading malware via the Internet. Additionally, risks can be significantly mitigated by ensuring people on the network can only visit sites and locations you stipulate and explicitly allow for your business.

Passwords – ensure that passwords are never shared or used in more than one place. Passwords should be at least seven characters long and comprise of numbers, letters (upper and lower case), special characters or punctuation marks to make them harder to guess and therefore increase their strength. Also ensure passwords are implemented on the operating system and in the applications themselves.

Patching of systems – ensuring that your systems are fully up to date with software patches will reduce your business risk by eliminating the known vulnerabilities that software providers have identified and fixed. Hackers target systems that are out of date. Enabling auto-updates is a fairly simple task.

Partnerships – work with a security partner that understands the risks being faced by the industry and promotes best practice through simple solutions that cater to your business.

Contact Foregenix on support@foregenix.com or (010) 500 8622 if you want more information, or if you suspect that your business has experienced a breach. ■

PLATINUM SPONSORS:



Silveray
Stationery
Company
Love Stationery

GOLD SPONSORS:



SILVER SPONSORS:



Keeping shop-sa members abreast of criminal and fraudulent activity in the stationery and office products industry
To sponsor the Crime Alert page contact 011 781 0370

REPORT CRIME AT info@shop-sa.co.za

Renew your Crime Alert sponsorship today! Call Wendy Dancer on 011 781 0370 to book your logo placement on the Crime Alert page as an industry leader in transparency, information sharing and anti-crime business ethics.

DR PETER TOBIN is a consultant at IACT-Africa. He can be contacted on 083 922 3444 or peter@iact-africa.com.

Mobile data devices and POPI

If you have a business which uses mobile data devices, POPI will affect you

On 11 April 2014, the government initiated the first steps towards the full implementation of the POPI Act (2013) across South Africa. One aspect that is receiving particular attention is how mobile digital devices capable of storing personal information (PI) and data are deployed.

"South Africa, in common with other countries, has seen an explosive growth in the use of mobile data devices (MDD) in line with the BYOD trend, from smartphones to tablets, all impacted by the need for personal information (PI) protection as demanded by the POPI Act," says Dr Peter Tobin, consultant with IACT-Africa.

"Now that PI is stored on privately-owned devices used for business

purposes, the demands placed on the information officer as defined in the POPI Act represent a major challenge and a significant component of the overall risks associated with protection of PI."

Tom Carter, business development manager at iStorage-Africa, has first-hand experience of the value that comes from securing such mobile data devices. "Many of our clients recognise the negative impact that data loss or inadvertent destruction can have on vital business data. That's why the range of secure mobile devices we offer has proved so successful with clients with demanding applications such as military-grade mobile data protection."

Colin McCarthy is MD of Uthanda ICT, a Microsoft partner and managed service provider which offers professional IT support for small to medium sized businesses. He is adamant about the need to treat MDD seriously. "Our company policy clearly states that we will ensure that mobile devices with on-board storage, such as laptops and tablets, need to be encrypted as just one of the steps to secure the data they contain."

"Not only that, we recognise that flash drives (memory sticks) are often ignored or forgotten, and we have evaluated the best way to ensure that devices such as these and other portable back-up devices need the same level of encryption.

Uthanda has begun advising its clients about POPI Act compliance as part of their broader approach to adding value in client service delivery," says Eben Müller, IT director at Uthanda.

"We know our clients treat us as trusted advisors, and we are not willing to put our reputation at risk in this key area of data privacy and POPI Act compliance, so what we say is what we do," adds Colin.

From the perspective of one of South Africa's leading growth areas, advocate Louis Nel says POPI is upon us and the entire spectrum of travel, tourism and related industries and their use of MDD are affected.

"Each sector, from the travel agent (face-to-face or online), to the conference organiser, conference venue and accommodation and transport providers, capture personal information addressed by POPI. The entire industry needs to

take stock and implement urgent steps to ensure proactive compliance, or face extremely adverse implications ranging from R10-million fines and imprisonment to civil action and publication of IT breaches with concomitant, severe reputational damage."

Digital forensics is another area impacted by the POPI Act. Alan Evan-Hanes, forensic investigator and consultant with Althair, has extensive experience in the implications of poor security practices in the area of MDDs. "My colleagues and I have seen too many cases where regret overwhelms forethought. Too often clients realise too late that a more formal approach, such as the use of encrypted technology, while appearing to be a significant investment in the short-term, actually pays huge dividends very quickly. Just one incident of loss or data breach could destroy a huge amount of value and reputation (hard to build and too easy to destroy) which could easily have been avoided."

Frik Kitching, forensic investigator of CLAMP, says, "Clients need to track MDD movement, for devices such as laptops, tablets and cell phones, not only for the potential physical asset value loss but increasingly because of the value of the data contained in those devices. Our forensic work has taken on an additional dimension now that POPI Act compliance demands organisations take seriously how and where they store personal information, protect it from unauthorised access and recover it intact whenever possible."

Information security and privacy governance mechanisms for MDD also need to be put into place, says John Cato, Information Security and Governance consultant at IACT-Africa. He says that many organisations believe that by implementing technologies such as encryption and data loss prevention they are protected against losing information. While this is true to an extent, good security and privacy governance steps also need to be taken as many information leakages are caused by staff members, either unintentionally or for malicious reasons.

Good governance for MDD starts with building mobile device responsibilities into information security, privacy and BYOD policies. By making staff members aware of their responsibilities for protecting PI (and other company information), the risk of losing information will be reduced as they know they will be held accountable for any information losses.

So what should organisations do about personal information protection on mobile data devices?

"Take minor steps to avoid a major data breach," suggests Dr Tobin. ■

Five tips to avoid a data breach:

- Minimise the amount of PI stored on MDD;
- If you must use an MDD, ensure you know what PI you are storing on your MDD in case it is lost or stolen;
- Notify your information officer as soon as a loss of your MDD with PI occurs;
- Only use an MDD with device encryption for storing PI; and
- Remember to comply with POPI, or suffer the consequences.

