Grant Thornton

An instinct for growth™

BY MICHIEL JONKER, DIRECTOR: IT ADVISORY, GRANT THORNTON JOHANNESBURG – AUGUST 2014

In the public eye

POPI requires a new look at ICT security

The new Protection of Personal Information (POPI) Act is going to force government institutions to change their attitudes towards ICT security. Data privacy which is built upon solid ICT security practices will no longer be negotiable and South African citizens are going to become more hostile towards government organisations that do not treat personal data appropriately in terms of the eight principles of POPI.

The POPI Act; gazetted in November 2013 and currently waiting an effective date, requires widespread reforms that both the private and public sector must introduce to ensure that the personal information and data they collect are protected. The Act also provides strict guidelines, among other things, on what data can be collected, how it can be used, and the requirement for it to be kept up-to-date.

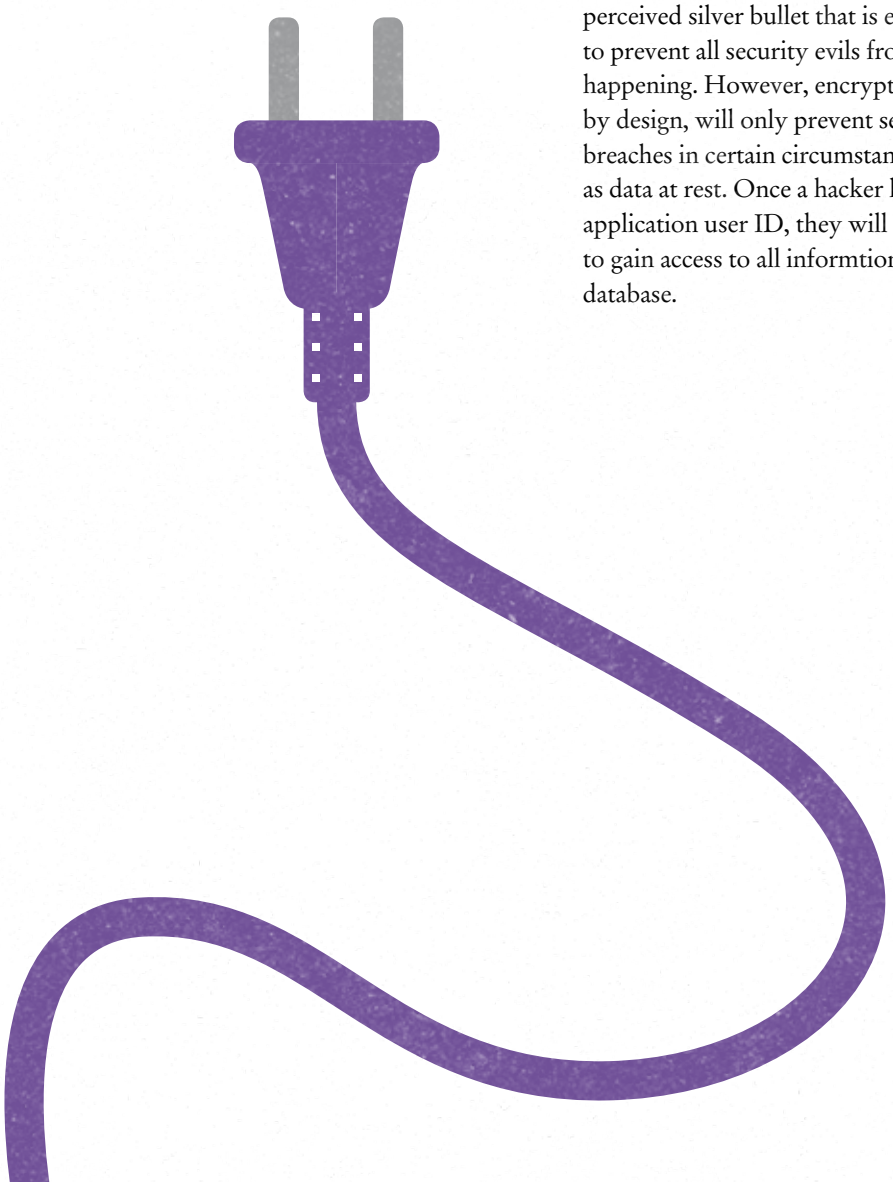
The private and public sectors have been plagued by dramatic security breaches in the past few months both in South Africa and abroad. Internationally, in the private sector the recent security incidents at retail company Target as well as at renowned e-commerce group eBay are only two examples.

And at home it's been reported that the Sanral website (e-toll account management website) was hacked, the ANC Youth League's website was defaced while both the City of Joburg and police websites and databases were also identified as not safe or even hacked. In the case of SAPS' website hacking, 16 000 whistle blowers have had their private details exposed. These breaches have caused great concern and anxiety amongst company board members in the private sector and accounting authorities and accounting officers in the public sector.

The lesson learned is that none of these entities' IT security practices were adequate or effective enough to prevent security incidents from occurring.

The myth: 100% ICT security is possible

Public sector accounting authorities might have high expectations that "ICT security" will equal 100% security. But unfortunately, no organisation can achieve this, unless they unplug all computers.



A classic example is the firewall. There is a misconception that a firewall fulfils the same function as a brick firewall: that it can prevent a fire threat jumping from one section to another. But unlike the physical structure, firewalls in the ICT world will allow unauthorised traffic through – in some circumstances. Encryption is another example of a perceived silver bullet that is expected to prevent all security evils from happening. However, encryption, by design, will only prevent security breaches in certain circumstances, such as data at rest. Once a hacker has a valid application user ID, they will be able to gain access to all informtion in a database.

Not all security breaches can therefore be prevented. Public sector entities at all levels are going to have to start to understand that a security breach which was detected in time, and escalated and corrected, must be acknowledged as part of the bigger picture to enforce IT security.

It is when no corrective measures are taken, even when a breach has been detected, that accounting authorities and accounting officers need to step in to address this failure as unacceptable behaviour by the ICT professionals. Failure to deal with basic and well-known vulnerabilities (unless it was a zero-day attack which no one can detect in time and which nobody is able to prevent) must not be treated lightly - hence the need for ICT expertise at accounting authority, board and oversight committee level.

"It is when no corrective measures are taken, even when a breach has been detected, that accounting authorities and accounting officers need to step in to address this failure as unacceptable behaviour by the ICT professionals."

ICT governance must be a priority

In the future, public and private sector organisations could potentially face multi-million rand monetary fines, civil claims and reputational damage if they're found guilty of POPI transgressions.

This makes ICT governance a priority and all members of the public sector tasked with ICT or management responsibility must keep these important points in mind:

- Don't treat ICT security as an afterthought. Security must form an integral part of all business processes. There are still too many systems available in South Africa where no attention was paid to security during development and the focus is purely on functionality – e.g. a financial package was designed to provide proper income statements and balance sheets, not security.
- IT security does make business sense. Recent financial losses endured by retail company Target shows that one security breach can cost an organisation more than the cost of preventative, detective and corrective measures together.
- CIOs and government information technology officers (GITOs) must be appointed at exco level. Many CIOs are not functioning at exco level and many times are not invited to audit committee and accounting authority meetings.
- A holistic approach to security. Security is more than just about prevention. It also entails the capability to detect, escalate and correct breaches. A holistic approach would involve deploying the right technology to prevent and detect incidents, implementing effective processes, having the appropriate structures in place and making sure that people are aware of security risks.
- Security culture. The human element will always thwart the best intentions; continuous awareness must be created. Non-compliance with security policies should not be tolerated. Strict adherence to policies should apply to all levels within an organisation. We still see practices where policies are relaxed for "c-level" executives e.g. CEO's passwords that never expire.
- Data privacy is not only the responsibility of the IT department and its GITO or CIO. The accountability will however, always sit with the CEO or the accounting officer.

"In the future, public and private sector organisations could potentially face multi-million rand monetary fines, civil claims and reputational damage if they're found guilty of POPI transgressions."

Contacts us

Bloemfontein
Terry Ramabulana
Director, Public Sector Advisory
Suite 6 The Park,
14 Reid Street,
Westdene,
Bloemfontein, 9300
T +27 (0)51 430-5368
E terry.ramabulana@za.gt.com

Cape Town
Barry Lodewyk
Partner, Public Sector Assurance
Martin Jansen van Vuuren
Director, Public Sector Advisory
6th Floor, 119 Hertzog Boulevard,
Foreshore
Cape Town, 8001
P O Box 2275
Cape Town, 8000
T +27 (0)21 417-8800
E cape@za.gt.com

Durban
Ahmed Timol
Partner, Public Sector Assurance
Bernadine Galliver
Executive Manager, Public Sector Advisory
2nd Floor, 4 Pencarrow Crescent
Pencarrow Park
La Lucia Ridge Office Estate, 4019
P O Box 950
Umhlanga Rocks, 4320
T +27 (0)31 576-5500
E mail@gtdbn.co.za

George
Charles Minie
Managing Partner
124 Cradock Street
George, 6529
Private Bag X6544
George, 6530
T +27 (0)44 874-2320
E info.george@za.gt.com

Johannesburg
Seth Radebe
Director, Public Sector Assurance
42 Wierda Road West
Wierda Valley, 2196
Private Bag X10046
Sandton, 2146
T +27 (0)11 384-8000

Terry Ramabulana
Director, Public Sector Advisory
137 Daisy Street,
Sandown, 2196
Private Bag X28
Benmore, 2010
T +27 (0)11 322-4500
E info@za.gt.com

Nelspruit
Billy de Jager
Director
No 2 Cherato Place
36 Murray Street
Nelspruit, 1201
T +27 (0)13 752-8084
E info@za.gt.com

Polokwane
Yugen Pillay
Director
130 Marshall Street,
Marshall Chambers Office 16A
Polokwane, 0699
T +27 (0)15 297-3541
E yugen.pillay@za.gt.com

Port Elizabeth
David Honeyball
Partner
125 Cape Road, Mount Croix
Port Elizabeth, 6001
P O Box 63814
Greenacres, 6057
T +27 (0)41 374-3222
E pe@za.gt.com

Pretoria
Johan Blignaut
Managing Partner
Building A, Summit Place
Garsfontein Road
Menlyn, 0181
P O Box 1470
Pretoria, 0001
T +27 (0)12 346-1430
E infopta@za.gt.com

Rustenburg
Seth Radebe
Director, Public Sector Assurance
234-2 Beyers Naude Drive,
Rustenburg, 0300
T +27 (0)14 592-1028
E seth.radebe@za.gt.com

National marketing
Pamela Grayman
Partner and Head of National Marketing
and Business Development
137 Daisy Street
Sandown, 2196
Private Bag X28
Benmore, 2010
T +27 (0)860-GTLINE
E info@za.gt.com

Grant Thornton
An instinct for growth™

www.gt.co.za

July 2014