Grant Thornton

An instinct for growth™

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

In the public eye

Data hoarding puts an increasing number of SA organisations on the wrong side of the law

As yet another barrage of data leakages made news headlines recently – this time publicly exposing FNB and Gautrain customers' personal details – organisations need to consider whether these security incidents are as a result of data hoarding issues or due to operational oversight, especially as the new POPI legislation and its strict guidelines loom.

Recent security breaches raise the alarm again while new POPI legislation looms

A balance has to be achieved between the availability and security principles within an organisation.

One of the core reasons for the increase in large-scale security incidents is as a result of the phenomenon of "big data". For the past decade companies have been processing and analysing more and more data.

A huge concern is that there is a very fine line between big data with effective, excellent intelligence tools to mine the data versus the issue of 'data hoarding' with no purpose.

We need to ask the question: When do businesses and government begin to collect masses of data without clear, specific objectives, and with no strategy regarding the security consequences of this information?

Unfortunately, organised crime has also grasped the value of big data as they continue to target companies and governments with big repositories of personal data on a more regular basis.

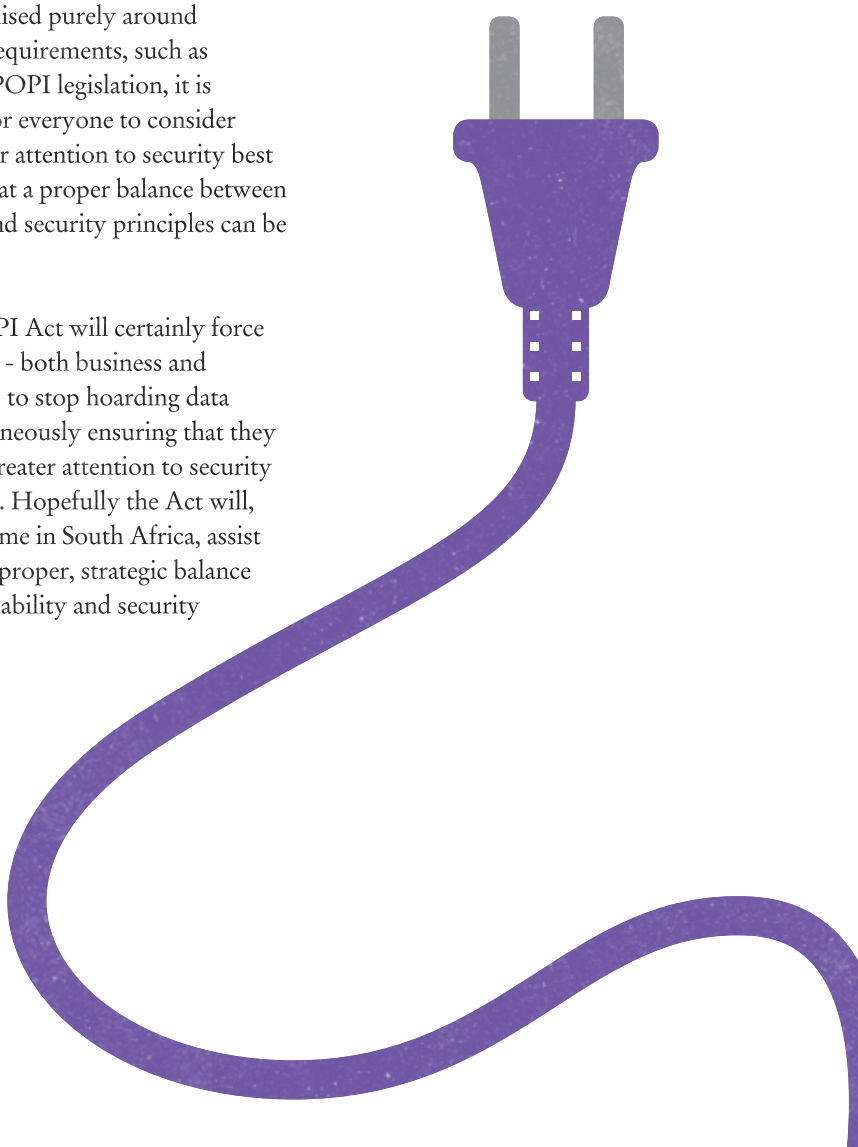
Unfortunately, organised crime has also grasped the value of big data as they continue to target companies and governments with big repositories of personal data on a more regular basis.

POPI defines data hoarding as illegal
When POPI comes into place, data hoarding will be illegal in South Africa, because POPI requires that data is only processed for as long as there are clear and defined reasons to do so. In addition, all security breaches will have to be reported directly to those individuals that have been impacted and to the Regulator.

The new Act provides an almost certain guarantee that more organisations will end up with egg on their faces very soon, never mind the fact that senior representatives will need to appear in court to face criminal charges and civil claims.

While it's completely logical that organisational and IT strategy should not be formalised purely around compliance requirements, such as the pending POPI legislation, it is paramount for everyone to consider paying greater attention to security best practice so that a proper balance between availability and security principles can be achieved.

The new POPI Act will certainly force organisations - both business and government - to stop hoarding data while simultaneously ensuring that they start to pay greater attention to security best practices. Hopefully the Act will, for the first time in South Africa, assist us to strike a proper, strategic balance between availability and security principles.



What can you do to minimise security incidents?

- **At an operational level**
  - Developers need to become more skilled and technically aware of security issues and applications will have to be developed from a security perspective from the start – i.e. security risks must be part and parcel of the phase where business requirements and functionality are considered.
  - More focus should be placed on the pre-testing of applications. The text book approach should be enforced – proper testing should be done at different levels (i.e. the old, good practices of unit testing, integration testing etc.). Different levels also include different types of users – from developer testing right through to user interface testing.
  - Very few companies perform quality assurance (QA) on source code. A separate QA function should be implemented in order to analyse and test source code logic. Research indicates that any piece of software could contain logic errors for nearly every 40 lines of source code.
  - Businesses and government need to reinforce "negative testing" so that systems are tested to prove that they are properly delivering the required business specifications to its users and handling valid user input, while also being tested to "think and execute the unthinkable" whereby testers interact with the system in a seemingly invalid way in order to try and force it to act outside of its defined ways of dealing with user input. By acting outside its design framework, this could force the system to allow full access for the user to the back-end.
  - Especially when it comes to external web facing applications, proper expert and manual penetration testing ("white hat hacking" or "ethical hacking") must be performed by professionals on all web applications. However, Internet-facing systems should also be monitored on a continuous basis by making use of different scanning tools.

- **At a strategic level**
  - Boards in the private sector and Accounting Authorities and Accounting Officers in the public sector cannot afford to treat IT security as an operational issue anymore. IT strategy should be an integral part of business strategy. For example, organisations need to incorporate cybercrime scenario planning into their regular strategic and risk assessment procedures.
  - Business and government has to realise that although big data presents many benefits and that business intelligence is important, huge data sets do pose a security threat too. Big data increases an organisation's risk of attack because organised crime also places a premium on big data. How can we protect data if we are hoarding and cannot tell what data we possess in either a structured or unstructured form? Hoarding makes it extremely difficult to identify and classify data assets according to data sensitivity and risk assessments schemes.
  - SLAs with software vendor companies must enforce security arrangements.

Contact 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