Protection of Personal Information (PoPI): Impacts & an Implementation Approach

29 January 2013

Wayne Webner CISSP & Arnold Okkenburg B.Com, PMP

The leading, independent management consulting firm in South Africa
1. Protection of Personal Information Overview
2. Cost of Non-Compliance
3. Origins of PoPI
4. PoPI in the World
5. PoPI Challenge
6. Further Considerations
7. Typical Areas of Impact
8. Business Approach to PoPI
9. An Implementation Approach
10. Suggested End To End Approach
11. Key Deliverables
12. Critical Success Factors
13. Proposed Business Impacts
• **Forrester: Average Cost Per Data Record Loss based on 28 case studies:** Between $90-$305 USD “After calculating the expenses of legal fees, call centres, lost employee productivity, regulatory fines, stock plummets, and customer losses, it can be dizzying, if not impossible, to come up with a true number” said [Khalid Kark](#): Research analyst at Forrester

• **Symantec Research Corporation/Ponemon: Exploitation techniques used:** The Symantec Ponemon study found that the number of data breaches that were caused by malicious attacks increased from 31% in 2010 to 37% in 2011. The leading cause (in 50% of cases) was malware, followed by malicious insiders (33%), device theft (28%), SQL injection (28%), and phishing attacks (22%). Interestingly, 17% of all data breaches also involved social engineering attacks. "We think about the evil hacker, which is pretty serious stuff, but in our study, we find that it's really the malicious insider--someone who's nefarious or angry at the organization--that presents the real danger to the company," said Ponemon

• **Estimated Amount of PI records lost in the States per year:** A new report from the Privacy Rights Clearinghouse (PRC) notes 535 breaches during 2011, involving 30.4 million sensitive records.
PoPI legislation dictates that an “organisation will safeguard an individual’s constitutional right to privacy”.

The PoPI Bill outlines 8 fundamental conditions organisations need to observe when collecting and processing Personal Information (PI):
1. Accountability
2. Process Limitation
3. Purpose Specification
4. Further Process Limitation
5. Information Quality
6. Information Security
7. Openness
8. Data Subject Participation

There are also some Additional Considerations that should be looked at like; Prior Authorisation, Exemptions, Codes of Conduct, Direct Marketing, Trans-Border Information Flows, Enforcement, Offences and Penalties
Origins of PoPI

- Article 8 of the European Convention on Human Rights, which was drafted and adopted by the Council of Europe in 1950 and meanwhile covers the whole European continent except for Belarus and Kosovo, protects the right to respect for private life: "Everyone has the right to respect for his private and family life, his home and his correspondence." Through the huge case-law of the European Court of Human Rights in Strasbourg, privacy has been defined and its protection has been established as a positive right of everyone.

- Article 17 of the International Covenant on Civil and Political Rights of the United Nations of 1966 also protects privacy: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

- Shortly, the South African government will be enforcing the Bill for the Protection of Private Information Act (herewith “PoPI”). This Bill gathers its origins from the Constitution of the Republic of South Africa, section 14 (herewith “Privacy”), as requested by the South African Law Reform Commission, which prescribes that everyone has the right to privacy and that
  - the right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information
  - the State must respect, protect, promote and fulfil the rights in the Bill of Rights

- The PoPI act will have significant implications for both the citizens whose information is processed and for the companies and public bodies who do the processing. PoPI formalizes the requirements for Privacy Protection and therefore introduces the concept of Data Protection to South Africa. This concept, whilst mature in the developed world, has been a long time coming to South Africa.
• PoPI will be mandatory for private and public bodies
• New legislation therefore unprecedented in South Africa
• Much like its PCI parallel, PoPI is a “grudge” project and therefore the goal is compliance with minimal business and financial impact
• Requires the manifestation of a Corporate Privacy Culture using Policy, Process, People and Technology as a toolset
• PoPI compliance must be achieved or corporations face stiff penalties
Further Considerations

• Performing a Comprehensive Privacy Gap Assessment of existing legacy systems and Technologies, Infrastructure, Business Areas, Policies, Procedures and Partnerships which may be impacted by PoPI.

• Identifying interdependencies and integration capabilities with in-house project initiatives (e.g. PCI-DSS)

• Regulatory Cohesion (e.g. CPA, NCA and ETC)
Data Privacy typically impacts on organisations in the following areas:

<table>
<thead>
<tr>
<th>Business Area</th>
<th>Typical Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Relations</td>
<td>Collection and processing of customer personal information e.g. Call centre processing customer personal details for returned or defective items and queries.</td>
</tr>
<tr>
<td>Human Resources</td>
<td>Collection and processing of employee personal information e.g. New employee banking details processed and stored in a database repository.</td>
</tr>
<tr>
<td>Governance</td>
<td>Detailing who has overall accountability for compliance e.g. Appointing a Chief Privacy Officer and deputy</td>
</tr>
<tr>
<td>Information Management</td>
<td>Developing Policies for Information Security, Data Classification and Retention e.g. Personal Information must be desensitised before being hosted in a QA environment.</td>
</tr>
<tr>
<td>Contract Management</td>
<td>Identification and Management of 3\textsuperscript{rd} party processing and hosting partners e.g. All service providers hosting Personal Information will be subject to yearly privacy audits.</td>
</tr>
<tr>
<td>Marketing</td>
<td>Maintenance of opt-out registers, restrictions on direct marketing e.g. Marketing to maintain a audited database for users opting out of promotional campaigns.</td>
</tr>
<tr>
<td>International Transacting</td>
<td>Identification and restrictions on cross border information transfers e.g. Woolworths Africa sending account information to Woolworths Australia.</td>
</tr>
</tbody>
</table>
The Business approach adopted for PoPI should be on a practical level with a grounded framework to assist the organisation with a path to compliance and beyond.
An Implementation Approach

PoPI Regulation

Compliance Requirement

Privacy Gap Assessment

- Accountability
- Further Process Limitation
- Openness
- Process Limitations
- Information Quality
- Data Subject Participation
- Purpose Specification
- Information Security
- Additional Considerations

Phase 1

Solutions Visioning

- Alignment with other Regulatory Controls
- Integration with Other Initiatives
- Infrastructure Requirements
- Systems and Application Requirements
- Process Requirements
- People Requirements

Phase 2

Develop & Implement a Roadmap

Phase 3

Policy & Process
In order to achieve PoPI compliance, we suggest a 3 phased approach. Phase 1 being the performance of a detailed Privacy Gap Assessment. Phase 2 is the assimilation of artefacts from Phase 1 outlining recommendations required in order to deliver a Solutions Vision. Phase 3 is the development and enactment of the agreed solution recommendations via a People, Policy, Process and Technology approach.
Phase 1: Privacy Gap Assessment

- Plan and execute Kick-off Meeting
- Define and agree roles and responsibilities
- Engage stakeholders
- Gather & understand existing systems & process documentation
- Host work shop sessions to identify processes, systems & people handling or hosting Personal Information
- Perform Privacy Gap Assessment and Compliance Review
- Contextualize business systems, technology, processes and people non-compliance in Spider and Heat Map diagrams for priority determination.
- Describe supplier & partner non-compliance
- Detail POPI overlap with inflight projects
- Determine in-flight project integration capabilities and dependencies for PoPI compliance
- Conduct work shop sessions to validate understanding
- Engage business stakeholders for feedback and agreement
Phase 2: Solutions Visioning

- Conduct Stakeholder “solution” visioning and remediation workshops
- Define technical, functional and operational requirements
- Determine existing infrastructure and process “re-use” feasibility
- Agree stakeholder compliance actions & initiatives
- Articulate or define partner, vendor & supplier compliance activities
Phase 3: Develop & Implement a Roadmap

- Define a programme structure
- Define an implementation approach & roadmap
- Establish a costing model
- Establish a resource plan
- Develop a change management strategy
- Define a stakeholder management plan
- Outline and agree the business case (costs & benefits)
- Implement all of the above
Key Deliverables

- Perform Privacy Gap Assessment
- Identify Business Systems, Processes, Technologies and Partnerships in Non-Compliance
- Determine how PoPI integrates and impacts with in flight & planned projects
- Alignment with other regulatory controls
- Solutions Vision
- Implementation Roadmap
• Clear programme sponsorship and visible executive support
• Clear accountability for PI Information management and decision making
• Clear accountability for timeous decision making, meeting attendance, data validation and KPI management
• Aligned and accessible business stakeholders, e.g.
  — Marketing and Channel Stakeholders
  — Business System, Information and Process Owners
  — IT Infrastructure, Applications and Governance Stakeholders
  — External Service Providers (CEB, DiData, T-Systems, etc.)
• Availability of key resources to deliver domain content, e.g.
  — IT Governance and Security
  — Business Process
  — IT Architecture
  — Business systems
  — Legal and Compliance
• Quality of documentation
• Establishing Chief Privacy Officer
## Proposed Business Impacts

<table>
<thead>
<tr>
<th>Business Role Players</th>
<th>Project Phase 1: Gap Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>SteerCom (Exec level)</td>
<td>2-3 hours pp</td>
</tr>
<tr>
<td>System &amp; Process Owners</td>
<td>24-40 hours pp</td>
</tr>
<tr>
<td>Business Stakeholders</td>
<td>2-3 hours pp</td>
</tr>
<tr>
<td>Legal</td>
<td>2 hours</td>
</tr>
</tbody>
</table>
### Proposed Business Impacts (continued)

<table>
<thead>
<tr>
<th>Business Role Players</th>
<th>Project Phase 2: Solutions Vision</th>
</tr>
</thead>
<tbody>
<tr>
<td>SteerCom (Exec level)</td>
<td>2-3 hours pp</td>
</tr>
<tr>
<td>System &amp; Process Owners</td>
<td>12-20 hours pp</td>
</tr>
<tr>
<td>Business Stakeholders</td>
<td>2-4 hours pp</td>
</tr>
<tr>
<td>Legal</td>
<td>4 hours</td>
</tr>
</tbody>
</table>
## Proposed Business Impacts (continued)

<table>
<thead>
<tr>
<th>Business Role Players</th>
<th>Project Phase 3: Develop &amp; Implement a Roadmap</th>
</tr>
</thead>
<tbody>
<tr>
<td>SteerCom (Exec level)</td>
<td>6-8 hours pp</td>
</tr>
<tr>
<td>System &amp; Process Owners</td>
<td>40-60 hours pp</td>
</tr>
<tr>
<td>Business Stakeholders</td>
<td>12-18 hours pp</td>
</tr>
<tr>
<td>Legal</td>
<td>6-8 hours</td>
</tr>
</tbody>
</table>