Does Your Cloud Solution Look Like a Mushroom?
1: Asset Identification

2: Identify Risks

3: Countermeasures

4: What risks does solution cause?

5: Costs and Trade-offs
1: Asset Identification
1: Asset Identification
1: Asset Identification
## 1: Asset Identification

<table>
<thead>
<tr>
<th>Bank</th>
<th>Online Banking URL</th>
<th>Header?</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASB</td>
<td><a href="https://fnc.asbbank.co.nz/1/User/LogOn">https://fnc.asbbank.co.nz/1/User/LogOn</a></td>
<td>YES!</td>
</tr>
<tr>
<td>ANZ</td>
<td><a href="https://secure.anz.co.nz/IBCS/pgLogin">https://secure.anz.co.nz/IBCS/pgLogin</a></td>
<td>no</td>
</tr>
<tr>
<td>BankDirect</td>
<td><a href="https://vault.bankdirect.co.nz/default.asp">https://vault.bankdirect.co.nz/default.asp</a></td>
<td>no</td>
</tr>
<tr>
<td>BNZ</td>
<td><a href="https://www.bnz.co.nz/ib/app/login">https://www.bnz.co.nz/ib/app/login</a></td>
<td>no</td>
</tr>
<tr>
<td>HSBC</td>
<td><a href="https://www.hsbc.co.nz/1/2/HUB_IDV2/IDV_EPP">https://www.hsbc.co.nz/1/2/HUB_IDV2/IDV_EPP</a>...</td>
<td>no</td>
</tr>
<tr>
<td>Kiwibank</td>
<td><a href="https://www.ib.kiwibank.co.nz/">https://www.ib.kiwibank.co.nz/</a></td>
<td>no</td>
</tr>
<tr>
<td>Rabobank</td>
<td><a href="https://secure1.rabodirect.co.nz/exp/authenticationDGPEN.jsp">https://secure1.rabodirect.co.nz/exp/authenticationDGPEN.jsp</a></td>
<td>no</td>
</tr>
<tr>
<td>SBS</td>
<td><a href="https://sbsbanking.sbs.net.nz/secure/">https://sbsbanking.sbs.net.nz/secure/</a></td>
<td>no</td>
</tr>
<tr>
<td>TSB</td>
<td><a href="https://homebank.tsbbank.co.nz/online/">https://homebank.tsbbank.co.nz/online/</a></td>
<td>no</td>
</tr>
<tr>
<td>Westpac</td>
<td><a href="https://sec.westpac.co.nz/IOLB/Login.jsp">https://sec.westpac.co.nz/IOLB/Login.jsp</a></td>
<td>no</td>
</tr>
</tbody>
</table>

Python Script by François Marier
## 1: Asset Identification

<table>
<thead>
<tr>
<th>Bank</th>
<th>Online Banking URL</th>
<th>Header?</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANZ</td>
<td><a href="https://www.anz.com/INETBANK/bankmain.asp">https://www.anz.com/INETBANK/bankmain.asp</a></td>
<td>no</td>
</tr>
<tr>
<td>Bank of China</td>
<td><a href="https://ebs.boc.cn/BocnetClient/LoginFrameAbroad.do?_locale=en_US">https://ebs.boc.cn/BocnetClient/LoginFrameAbroad.do?_locale=en_US</a></td>
<td>no</td>
</tr>
<tr>
<td>Heritage Bank</td>
<td><a href="https://online.hbs.net.au/hbsv47/ntv471.asp?wci=entry">https://online.hbs.net.au/hbsv47/ntv471.asp?wci=entry</a></td>
<td>no</td>
</tr>
<tr>
<td>Westpac</td>
<td><a href="https://online.westpac.com.au/esis/Login/SrvPage">https://online.westpac.com.au/esis/Login/SrvPage</a></td>
<td>no</td>
</tr>
</tbody>
</table>
1: Asset Identification

2: Identify Risks

3: Countermeasures

4: What risks does solution cause?

5: Costs and Trade-offs
2: Identify Risks

Non-Hostile
- Info Partner
- Reckless Employee
- Untrained Employee

Hostile
- Radical Activist
- Anarchist
- Vandal
- Disgruntled Employee
- Government Spy
- Mobster
- Internal Spy
- Data Miner
- Government Cyber Warrior
- Legal Adversary

Competitor
- Terrorist
- Sensationalist

Corrupt Government Official
2: Identify Risks

Risk = Likelihood * Impact
2: Identify Risks

Your Organisation

Accountants
Bank 1
Online Trading
Professional Services
Domain and/or Technical Consultants
Telco
ISP
Government Security Orgs
Other Threat agents
Competitor

Dependency
2: Identify Risks

Likelihood

Threat Agent Factors

- Skill level
- Motive
- Opportunity
- Size
2: Identify Risks

Likelihood

Vulnerability Factors

- Ease of discovery
- Ease of exploit
- Awareness
- Intrusion detection
2: Identify Risks

Impact

Technical Factors

- Loss of confidentiality
- Loss of integrity
- Loss of availability
- Loss of accountability
2: Identify Risks

Impact

Business Factors

- Financial damage
- Reputation damage
- Non-compliance
- Privacy violation
2: Identify Risks

The Cloud vs In-House Security Comparisons

<table>
<thead>
<tr>
<th>The Cloud</th>
<th>In-House</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secrets not safe</td>
<td>Potential for greater security</td>
</tr>
<tr>
<td>Have to trust others</td>
<td>Trust yourself and your experts</td>
</tr>
<tr>
<td>Only some risks can be mitigated</td>
<td>Control over what to fix when</td>
</tr>
<tr>
<td>Lack of empathy</td>
<td>You control amount of empathy</td>
</tr>
<tr>
<td>Coerced, forced to give up secrets</td>
<td>Your decision. A lot less likely</td>
</tr>
</tbody>
</table>
2: Identify Risks

The Cloud vs In-House Security Comparisons

<table>
<thead>
<tr>
<th>The Cloud</th>
<th>In-House</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inherent lack of security</td>
<td>Your decision</td>
</tr>
<tr>
<td>Out-sourcing their out-sourced</td>
<td>You decide what goes where</td>
</tr>
<tr>
<td>Physical location unknown</td>
<td>Can see your rack</td>
</tr>
<tr>
<td>Physical security \textit{uncertainty}</td>
<td>Physical security certainty</td>
</tr>
</tbody>
</table>

We also use third party software (such as customer relationship management and accounting software) that holds your information, sometimes overseas.
2: Identify Risks

The Cloud vs In-House
Security Comparisons

<table>
<thead>
<tr>
<th>The Cloud</th>
<th>In-House</th>
</tr>
</thead>
<tbody>
<tr>
<td>No knowledge of your domain</td>
<td>Domain expert</td>
</tr>
</tbody>
</table>
2: Identify Risks

Control Lost

Duffy said that because it was a bulk request, Trade Me could have notified members whose details had been released.

Trade Me considered "at length" whether to do so, but "eventually made the decision not to inform members directly so as not to create undue panic or distress members unnecessarily."

Senior lawyers and the Privacy Commissioner have told the Herald of concerns over the practice which sees the companies voluntarily give the information to police.

Instead of seeking a legal order, police have asked companies to hand over the information to assist with the "maintenance of the law", threatened them with prosecution if they tell the person about whom they are interested and accept data with no record keeping to show how often requests are made.

The request from police carries no legal force at all yet is regularly complied with.
2: Identify Risks
1: Asset Identification

2: Identify Risks

3: Countermeasures

4: What risks does solution cause?

5: Costs and Trade-offs
## 3: Countermeasures

<table>
<thead>
<tr>
<th>The Cloud</th>
<th>In-House</th>
</tr>
</thead>
<tbody>
<tr>
<td>On top only</td>
<td>Full control</td>
</tr>
</tbody>
</table>
OWASP AppSensor

IMPLEMENT REAL-TIME INTRUSION DETECTION WITHIN YOUR SOFTWARE

ATTACK DETECTION

RESPOND AUTOMATICALLY

Free, open source, DevOps friendly and cloud compatible
3: Countermeasures

- Avoid Commercial
- Use Public-Domain
3: Countermeasures

Hardening VPS's

- Create Multiple Partitions
- Review Password Strategies
- Disable Remote Root Logins
- Harden SSH
3: Countermeasures

Hardening VPS's

- Disable or Remove Services
- Schedule Backups
- Keep Systems Up to date
- Logging to Off-site
3: Countermeasures

Hardening VPS's
3: Countermeasures

Hardening VPS's
3: Countermeasures

Hardening VPS's
New Zealand Security Incident Management Guide for Computer Security Incident Response Teams (CSIRTs)

Robin Ruefle
Ken van Wyk
Lana Tosic

May 2013

New Zealand National Cyber Security Centre
Government Communication Security Bureau

Developed in cooperation with the CERT® Division of the Software Engineering Institute at Carnegie Mellon University
3: Countermeasures

Break Your System
1: Asset Identification
2: Identify Risks
3: Countermeasures
4: Risks that solution causes
5: Costs and Trade-offs
4: Risks that solution causes

New Risks

<table>
<thead>
<tr>
<th>The Cloud</th>
<th>In-House</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hack CSP -&gt; Prosecution</td>
<td>Hack Yourself -&gt; Find Holes -&gt; Harden</td>
</tr>
</tbody>
</table>
4: Risks that solution causes

New Risks

<table>
<thead>
<tr>
<th>The Cloud</th>
<th>In-House</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hack CSP -&gt; Prosecution</td>
<td>Hack Yourself -&gt; Find Holes -&gt; Harden</td>
</tr>
</tbody>
</table>
4: Risks that solution causes

New Risks
4: Risks that solution causes

New

Mitigated
5: Costs and Trade-offs

Establish Value

Loss of Convenience
5: Costs and Trade-offs

Staying on Top
Resource Compilation

- Cloud Security Assessment
- Automation
- Security Focused Facility
- In-house Cloud Planning

Total Web Security Solution
Binary Mist Limited

Where Passion, Quality and Technical Expertise meet