“Trust Me, I’m a Cloud Vendor”

Bruce Cowper
Co-Founder of SecTor, TASK, OASK, CSA Seattle
and Senior Security Strategist, Microsoft
Deciding to Trust Takes Time and Evidence
Drive to the Cloud

Scalability

Flexibility & Agility

Lower Cost of Ownership

Efficient Deployment & Operations

Robust Infrastructure

InfoWorld: Cloud security's PR problem shouldn't be shrugged off

Computerworld: Cloud computing still raises security, reliability concerns

Cloud Computing Journal: Cloud Reliability Will Be Bigger than Cloud Security for 2010-11

CNET News: Privacy panic debate: Whose data is it?
Cloud Trends

- Mobile
- Social / Identity
- Government
- Consumerization of IT
- Big Data
Cloud Questions

- **Security and Reliability** – what practices are in place?
- **Privacy** – is my data protected?
- **Loss of control** – how does my workflow change?
- **Global compliance** – what is my risk?
Off-loading Threats to the Cloud?

- Security fundamentals guard against most attacks
- Industry vulnerability disclosures are declining
- Less than 1% of vulnerability attacks were “zero-days”
- 99% of attacks impacted vulnerabilities that have updates

Microsoft Security Intelligence Report V11: www.microsoft.com/sir
The most commonly observed type of exploits were those targeting vulnerabilities in the Oracle (formerly Sun) Java Runtime Environment (JRE).

Detections of operating system exploits result of CVE-2010-2568 (.lnk).

More than 934,000 detections of exploits targeting Adobe Flash.
Exploit Detections

- Exploits that affected Adobe Acrobat and Adobe Reader accounted for most document format exploits
  - Win32/Pdfjsc
  - Ichitaro less than 0.1%
Types of Malware / Threats

% of Computers Cleaned by Country/Region

- Adware
- Misc. Trojans
- Trojan Downloaders & Droppers
- Viruses
- Backdoors
- Misc. Potentially Unwanted Software
- Worms
- Exploits
- Password Stealers & Monitoring Tools
- Spyware
Malware / Threats in Canada

- Adware
- Misc. Trojans
- Trojan Downloaders & Divers
- Exploits
- Worms
- Backdoors
- Password Stealers & Monitoring Tools
- Viruses
- Spyware

Canada vs Worldwide
## Threat Families - Canada

<table>
<thead>
<tr>
<th>Family</th>
<th>Most Significant Category</th>
<th>% of Computers Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Win32/Hotbar</td>
<td>Adware</td>
<td>17.0%</td>
</tr>
<tr>
<td>2 Win32/FakeRean</td>
<td>Misc. Trojans</td>
<td>12.8%</td>
</tr>
<tr>
<td>3 Win32/ClickPotato</td>
<td>Adware</td>
<td>11.9%</td>
</tr>
<tr>
<td>4 Win32/OpenCandy</td>
<td>Adware</td>
<td>11.3%</td>
</tr>
<tr>
<td>5 Win32/ShopperReports</td>
<td>Adware</td>
<td>11.3%</td>
</tr>
<tr>
<td>6 JS/Pornpop</td>
<td>Adware</td>
<td>10.9%</td>
</tr>
<tr>
<td>7 Win32/Zwangi</td>
<td>Misc. Potentially Unwanted Software</td>
<td>10.0%</td>
</tr>
<tr>
<td>8 Win32/Winwebsec</td>
<td>Misc. Trojans</td>
<td>6.9%</td>
</tr>
<tr>
<td>9 Java/CVE-2010-0840</td>
<td>Exploits</td>
<td>6.4%</td>
</tr>
<tr>
<td>10 Win32/Alureon</td>
<td>Misc. Trojans</td>
<td>4.6%</td>
</tr>
</tbody>
</table>
Email Threats
The volume of spam blocked by FOPE decreased dramatically over the past 12 months, from a high of 89.2 billion messages in July 2010 to a low of 21.9 billion in May 2011, due in large measure to takedowns of two major botnets: Cutwail and Rustock.
Spam Messages Blocked by Type

- Pharmacy – Non sexual: 33.7% in January, 27.9% in June
- Non-Pharmacy Product ads: 15.3% in January, 18.1% in June
- 419 Scams: 10% in January, 5% in June

% of blocked messages
Spam Messages Blocked by Type

% of blocked messages

- Financial Phishing
- Phishing
- Gambling
- Dating/Sexually explicit material
- Pharm. - Sexual
- Malware
- Get Rich Quick
- Image-only
- Stock Software
- Fraud. Diplomas
## Malicious Websites and Spam

<table>
<thead>
<tr>
<th>Metric</th>
<th>3Q10</th>
<th>4Q10</th>
<th>1Q11</th>
<th>2Q11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing sites per 1000 hosts <em>(Worldwide)</em></td>
<td>N/A (N/A)</td>
<td>N/A (N/A)</td>
<td>2.05 (0.33)</td>
<td>1.02 (0.38)</td>
</tr>
<tr>
<td>Malware hosting sites per 1000 hosts <em>(Worldwide)</em></td>
<td>N/A (N/A)</td>
<td>N/A (N/A)</td>
<td>1.93 (2.24)</td>
<td>2.29 (2.02)</td>
</tr>
<tr>
<td>Percentage of sites hosting drive-by downloads <em>(Worldwide)</em></td>
<td>0.040% (0.229%)</td>
<td>0.049% (0.131%)</td>
<td>0.877% (0.223%)</td>
<td>0.872% (0.273%)</td>
</tr>
<tr>
<td>Percentage of world spambot IP addresses</td>
<td>0.000</td>
<td>0.000</td>
<td>0.842</td>
<td>0.351</td>
</tr>
</tbody>
</table>
Reliability: Operations Investment

Design Considerations
- People
- Security
- Electrical Power
- Environmental Control
- Connectivity
The Japan Disaster

- On March 11, a magnitude 9.0 earthquake struck at 14:46 (local time) 81 miles (130km) east of Sendai, the capital of Miyagi Prefecture (Japan),
- This was followed by a 7 meter tsunami.
- At least 15,000 confirmed deaths with and more than 11,000 unaccounted for.
- There are more than 130,000 people still living in evacuation shelters.
- The estimated cost is as much as US$309B.
- Major critical infrastructure damage was reported in the area impacted by the tsunami with disruptions to travel, electricity, communications and mobile networks stretching throughout Japan.
In the aftermath of the Earthquake and Tsunami, communications were impacted:

- NTT East Japan - 879,000 telephone lines out of service, as well as 475,400 fiber-optic lines
- More than 11,000 wireless base stations belonging to DoCoMo, KDDI and Softbank were also out of service
- Numerous undersea cables were damaged
Japan’s Nuclear Reactor(s) Crisis

Fukushima Daiichi Nuclear Plant Impact

- March 11: Cooling system malfunctions
- March 12: Explosion at No. 1 Reactor
- March 14: Explosion at No. 3 Reactor
- March 15: Explosions at No. 2 & 4 Reactors
- March 16: Fire at No. 4 Reactor
- Ongoing power outages and mandatory rolling blackouts
Incident Response Capability

READINESS
- Companies are being remembered for how they handled an incident

RESOURCES
- Customers are typically looking for a consistent experience and a standard set of resources

INQUIRY
- When something goes wrong, people want to know where to go to find more information
Cloud Trust Checklist

What process and technology investments are you making in security, privacy and reliability?

How do you ensure my applications and data are protected against vulnerabilities?

What certifications and other industry standards do you continually achieve for your cloud environment?

What business continuity plans do you have in place, and have you tested them?

How do you monitor your quality of service, and what do you do when things go wrong?
Thank-you