Managing Risk in a Cloud First Government

Michael Davidson
Solutions Architect, Office of the CTO
TeraMach, A Pivot Company

Ajay K. Sood
VP, General Manager / Directeur Général
Symantec Canada
BALANCE

The struggle to find balance between user experience, privacy & security while enabling the business to transform.
LEARN

How do we learn from the past, enhance the future and minimize risk to our citizens and to government data?

Prepare
We should have been better prepared to handle this situation.

Aware
What happened? What is the extent of the damage?

Access
How can we continue to work during an event?

Communicate
Our communication broke down. We didn’t know who to reach out to for help.
ACT

What can you do today to minimize your risk when considering cloud-based services and prepare for journey?

Visibility
Above all, maintain line of sight on where and how your department conducts business in the cloud.

Context
Continuously understand YOUR risk profile. What digital assets are located in the cloud and what is their criticality/sensitivity?

Control
Separate cloud roles and responsibilities. Maintain clear boundaries between systems, services and administration.

Collaborate
Build a centre-of-excellence program that includes vendors, integrators and trusted business partners.
My report comes to the conclusion that cloud technology is of no use to this company. I'll upload it to Drop Box so you can take a look at it.
The Cloud Office — Coming Your Way

<table>
<thead>
<tr>
<th>Year</th>
<th>Not Cloud</th>
<th>Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>10%</td>
<td></td>
</tr>
<tr>
<td>2017</td>
<td>33%</td>
<td></td>
</tr>
<tr>
<td>2022</td>
<td>65%</td>
<td></td>
</tr>
</tbody>
</table>

Email, Chat, File Share, Conferencing, Social, Office Apps (Archive, Device Management, Loss Prevention, Discovery)

Source: Gartner
Benefits of Cloud come with Security Challenges

Reality
774 apps\(^1\)

Perception
40-50 apps

Source: \(^1\)Elastica Q2 2015 Shadow Data Report
\(^2\)CIO Insight

72% of employees admit to using unapproved apps\(^1\)
Legacy Perimeter Architecture
Cloud Redefines the Perimeter

Headquarters
Data Center

Regional
Office

Roaming
Users

Security Stack

Linkedin

Amazon

Yahoo!

Dropbox

Pinterest

Gmail

iCloud

GoToMyPC

Personal
Devices
Quick Cloud Definitions

**Shadow IT**
All the Cloud Apps used in your organization, without the knowledge of IT (unsanctioned apps)

**Shadow Data**
All the sensitive data that may exist in sanctioned or unsanctioned apps, without the knowledge of IT.

PII, PCI, PHI, CODE, LEGAL
Data Residency & Sovereignty

Data can cross borders when placed in cloud-based systems.
Nov 1: Breach Reporting is MANDATORY by law

• Applies to any “breach of security safeguards”

• “The loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization’s security safeguards that are referred to in Clause 4.7 of Schedule 1 or from a failure to establish those safeguards.”

• Personal information is lost, or accessed by an unauthorized individual

• The loss or unauthorized access is the result of someone violating the organization’s security safeguards, or the result of a failure to establish such safeguards
Reporting Obligations under PIPEDA

• Determine if the breach poses a “real risk of significant harm” (RROSH) to any individual whose personal information was involved in the breach.

• Notify individuals as soon as feasible of any breach that poses a “real risk of significant harm”.

• Report any data breach that poses a “real risk of significant harm” to the Privacy Commissioner, as soon as feasible.

• Where appropriate, notify any third party that the organization experiencing the breach believes is in a position to mitigate the risk of harm.

• Maintain a record of the data breach and make these records available to the Privacy Commissioner upon request.
IoT in 2018...

...is following the trajectory of **consumer IT**...

- Social Media
- Personal Devices / BYOD
- Cloud Applications

...into part of our **corporate fabric**:

- Security Systems
- Smart TVs
- Smart Speakers
- Wearable Tech

... And into our collective **consciousness**
IoT is Vulnerable...

Google's camera hackable? wide open
Malicious code sent across Cloud

Research
Infosecurity
SEC Consul.
is most like

Fitbits and
Military

In January
revealed
Pentagon
Internatio
IoT Uses the Cloud...

IoT devices consistently **call home** using sometimes vulnerable protocols.

These devices generally harvest **sensitive** information (PII, photos, location, voice samples etc).

Organizations aren’t contracting or analyzing the **risk** of their IoT providers like their enterprise IT providers.

This leaves organizations **exposed**, and without recourse.
IoT Data is **Shadow Data**...

- Location / Quantity of Personnel
- Voice samples / recordings
- Videos / photos
- Correlated Data (personnel movements)
78% of organizations currently use or planning to use Office 365

Office 365: Exchange, OneDrive, Sharepoint, Yammer, More apps...

MOST POPULAR APPS TRENDS OVER TIME

Source: Gartner 2016 survey
1. Who is responsible for Security in O365?

2. What are the risks?

3. How do you solve for shadow data, malicious attacks, and performance?
Responsibility in the Cloud

95% of cloud security failures will be the customer’s fault

Gartner

“...That result from your unauthorized action or lack of action when required, or from your employees, agents, contractors, or vendors, or anyone gaining access to our network by means of your passwords or equipment, or otherwise resulting from your failure to follow appropriate security practices...”

Microsoft’s Policy
(the fine print)

You are responsible for the data you store and share in the cloud and what actions are performed by your users.
1. Who is responsible for Security in O365?

2. What are the risks?

3. How do you solve for shadow data, malicious attacks, and performance?

- Shadow Data
- Malicious Attacks
- Performance (O365 Bandwidth)

Sanctioned & Popular Cloud
Alice shares a file with Bob

Bob shares that file with others

Typical reasons for accidental over sharing:

- Public
- Entire organization
- Anyone with a link
- Inherited access
- Terminated employees

Miscellaneous Errors and Insider/Privilege Misuse were the #1 and #2 most common reasons for a security incident in 2015.

Risk of **Malware Attacks**

Malware lets the user open the door

Malware infects an endpoint and waits for a cloud app session to jump into

Data stolen
Malware uploaded
Risk of **Account Takeovers**
IT May Never See

Malware infects an endpoint and waits for a cloud app session to jump into

Data stolen
Malware uploaded
IT has zero visibility

Going direct thanks to stolen or weak credentials
Risk of a **Malicious Insider**

It’s just a normal day – or is it?

### Real World Example

Employee & customer/competitor colluded to steal product source code later used in competing products – cost **$800M**

### Real World Example

Employee stole over a thousand documents to give to a foreign competitor – valued at over **$300M**

---

Data stolen  
Data sabotaged  
IT has zero visibility
How do you solve for shadow data, malicious attacks, and performance?
Cloud Security is in the Cloud

- Headquarters Data Center
- Regional Office
- Roaming Users

Cloud Security in the Cloud

- Salesforce
- Office 365
- Oracle
- SuccessFactors
- Workday
- Gmail
- LinkedIn
- Dropbox
- ServiceNow

Personal Devices

IOT Devices
CLX Forum Presents:

Canadian Cybersecurity 2018:
An Anthology of CIO/CISO Enterprise-Level Perspectives

"Whether you are a cybersecurity pro or someone just wanting to learn a bit more about this very important and fascinating subject, this book is for you!"

Danny Pehar, President, Cyber Insurance Education Inc.

WWW.CLXFORUM.ORG