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.
Multi-Phased and Multi-Staged Attacks
Multi-Phased and Multi-Staged Attacks

Headquarters Data Center
Regional Office
Roaming Users
Security Stack

Linkedin
Pinterest
Dropbox
Gmail
Amazon
iCloud
GoToMyPC

Personal Devices
The Cloud Office — Coming Your Way

- **2013**: 10%
- **2017**: 33%
- **2022**: 65%

**Source**: Gartner 2014

Email, Chat, File Share, Conferencing, Social, Office Apps (Archive, Device Management, Loss Prevention, Discovery)
Benefits of Cloud come with Security Challenges

Reality
774 apps\(^1\)

Perception
40-50 apps

72% of employees admit to using unapproved apps\(^1\)

Source: \(^1\)Elastica Q2 2015 Shadow Data Report
\(^2\)CIO Insight
Benefits of Cloud come with Security Challenges

Who Controls Sharing?
Cloud apps democratize sharing permissions, no longer governed by IT

Source: Ponemon, 2013 Cost of Data Breach Study

90% of organizations lost sensitive data via file sharing

Copyright © 2018 Symantec Corporation SYMANTEC CONFIDENTIAL – INTERNAL USE ONLY
What is **Shadow Data**?

**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.
Shadow Data

Of total files stored in the cloud per user (average) **25%** files per user are broadly shared (average)

**74%** of these files contain compliance related data

**9%** public

**17%** all company

**12.5%** external

**54%** SSN

**31%** PHI

**15%** PCI
The Need for Cloud Data Protection

Data governance in the Cloud Generation

- **PRIVACY**: Multinationals face an array of legal requirements governing data privacy and regional data residency.

- **COMPLIANCE**: Data compliance guidelines make cloud adoption a challenge across multiple regulated industries.

- **SECURITY**: Many enterprises want the security of knowing their most sensitive data is never outside of their control.
Data Residency & Sovereignty

Data cannot cross borders and be placed in cloud-based systems
**Encryption**

- Protection via “transformation”
- Mathematical link

**Tokenization**

- Protection via “replacement”
- **No** mathematical link
Office 365: Exchange, OneDrive, Sharepoint, Yammer, More apps...

78% of organizations currently use or planning to use Office 365

Source: Gartner 2016 survey

Most Popular Apps Trends Over Time

Number of Customers with App Provisioned

Source: Okta – Business @ Work Report – March 2016
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 Predictions for 2016

"...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

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.


Bob shares that file with others

O365 Salesforce ServiceNow other

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

23% of files per user are broadly shared (average)

12% of these files contain confidential data

48% of confidential data includes:

- SSN (33%)
- PII (33%)
- PHI (14%)
- PCI (5%)
## Loss of Data can be Expensive

<table>
<thead>
<tr>
<th>Compliance Fines</th>
<th>Files with acquisition plan details stolen — $2.4B acquisition deal lost</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>$1.7M</strong> - HIPAA</td>
<td>Product source code stolen &amp; used by competitor — cost $800M</td>
</tr>
<tr>
<td><strong>$4.8M</strong> - HIPAA</td>
<td>Lost authentication technology requiring reissue of 40M tokens — cost $66M</td>
</tr>
<tr>
<td><strong>$13.3M</strong> - PCI</td>
<td>Designs for new product stolen -- counterfeit products forced drastic price reductions — cost $9.2M</td>
</tr>
<tr>
<td><strong>$25M</strong> - PII</td>
<td></td>
</tr>
<tr>
<td><strong>$3.5M</strong> - PI</td>
<td></td>
</tr>
</tbody>
</table>

Does NOT include costs for mandated remediation

---

**Recent News!**

- February 2016: FCC releases PII violation orders for $8M, $7.6M, $9.6M, $4.3M, $1.7M, $1.8M, $1.8M
- 2015: Hackers plead guilty to stealing more than $100M in intellectual property & proprietary data from Microsoft and others...

---

Copyright © 2018 Symantec Corporation SYMANTEC CONFIDENTIAL – INTERNAL USE ONLY
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
Attacks on Cloud Accounts

- **Steal** company data
- **Hijack** data with ransomware
- **Infiltrate** your org w/ malware via shares & downloads
- **Leverage** your resources to host their “business”
Risk of **Account Takeovers IT May Never See**

- Additional internet bandwidth (based on an organization of ~3500 people)
  - Exchange Online + 200MB
  - Exchange & OneDrive + 300MB
  - ProPlus + 500MB

- Additional concurrent internet connections per user
  - Exchange + 7 (on average)
  - Yammer + 40 or more
How do you solve for shadow data, malicious attacks, and performance?
What Cloud/SaaS Vendors Typically Don’t Provide

Automated Classification

Granular Real-time Controls

User Behavior Analytics

By 2018, 40% of Office 365 deployments will rely on third-party tools to fill gaps in security and compliance...

Source: Gartner “How to enhance the security of Office 365”
Start Planning Now

- **Risk Analysis:**
  - What is your risk of data exposure?
  - What is your threat risk?
  - What are your compliance risks?

- **Identify gaps in your security**
  - Data governance
  - Threat protection

- **Review your current security provisioning**
  - Can your existing security solutions handle the additional traffic demands of O365?

- **Establish budget and implementation plan**

---

By 2018, 40% of Office 365 deployments will rely on third-party tools to fill gaps in security and compliance...

Source: Gartner “How to enhance the security of Office 365”
Innovation for the Cloud Generation:
Ensuring Safe Cloud Usage

Headquarters Data Center
Regional Office
Roaming Users

salesforce
Office 365
ORACLE
successfactors
workday
Gmail
LinkedIn
Dropbox
serviceNow

Personal Devices
IOT Devices