SaaS Security Checklist: Data, Management, and Liability

Diana Kelley, SecurityCurve

Agenda

- **Data and Transferability Issues**
- **Can Risk be Transferred?**
- **Understanding Hidden Costs**
- **Quantifying Cost of Downtime and Other Loss**

Data and SaaS

- **Data is stored / transferred via the provider**
  - **For both software (CRM, HR) and security as a service**
- **Software as a Service Data**
  - **Customer contact lists**
  - **Private customer information**
  - **Intellectual property**
  - **Proprietary corporate information**
    - **Salaries**
    - **SSNs**

The Data and the SaaS

- **Security as a Service Data**
  - **Log information**
    - **What's in your log files?**
  - **Vulnerability information**
    - **Where the enterprise may be exposed**
    - **Roadmap for an attacker?**
  - **Compliance readiness**
  - **Corporate email**
  - **Corporate surfing statistics**
    - **Really, you'd be surprised…**

Data and Transferability Issues

- **Who Owns the Data?**
  - **It was yours**
  - **But now the SaaS has it**
- **Who is Responsible if it is lost?**
- **Can it be moved?**
  - **To another provider?**
  - **Back on-prem?**

Can Risk be Transferred?

- **Yes**
  - **Insurance - cost exposures / loss**

- No
  - Your time and reputation
  - Public perception
  - Customer relationships
  - Regulatory liability

Myth: Outsourcing Your Liability

- **Consider the Rules of Disclosure**
  - **In the event of theft of property (perhaps containing PII?)**
  - **How about a break-in?**
  - **Is there an SLA governing unauthorized disclosure?**

*The service provider provides the service but ultimately **you are accountable** for your data*

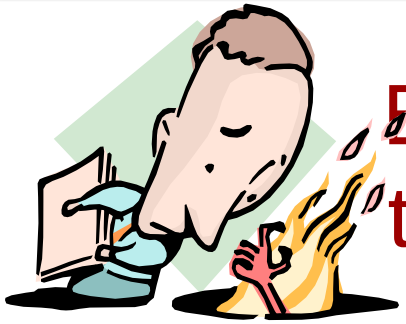
Who Do You Trust with your Data?

- **Our Lady of the Lake Regional Medial Center, August 27, 2009**
  - **Former Medical Center employee arrested for allegedly stealing the personal information of 46 patients. He opened credit cards and fraudulently filed federal income tax returns.**
- **Battle Ground Urgent Care / Prompt Med, August 21, 2009**
  - **Bags of medical records (~623 patients) including social security numbers, copies of driver's licenses, and sensitive information were found, all unshredded in a dumpster behind a building.**
- **Wells Fargo Bank, August 14, 2009**
  - **A Wells Fargo Bank employee working inside a bank call center was arrested on August 14, using customer account access to pay her own debts.**

Source: Identity Theft Resource Center, 2009 Breach List, www.idtheftcenter.org

"Worst Case" Example Scenario

- **Example**
  - **SMB signs on with mail hygiene and archive service provider**
  - **Also using mail server as part of SaaS agreement**
- **What they think they're getting**
  - **Low cost "clean" mail**
  - **Secure protection of corporate communications**
  - **Archive compliance**



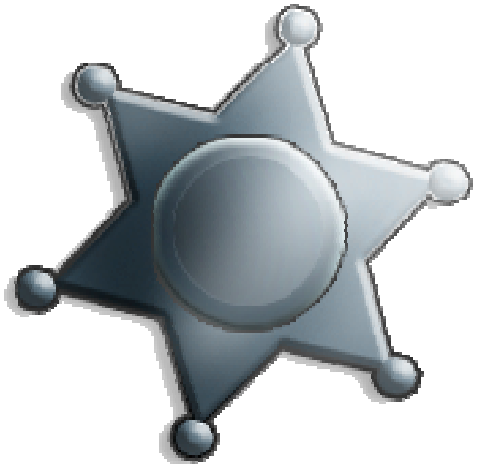
Example Scenario: Devil's in the Details

- **What they're *really* getting**
  - Poorly protected portion of a shared mail server
  - Insecure connection to remote mail server
  - Overzealous spam filtering
- **Result – Remember this is "worst case"!**
  - Passwords are stolen and private emails accessed
  - Exposure of customer data
  - Critical business emails are lost

Example Scenario: Conclusions

"Buyer Beware"

- Impacts
  - **SB 1386 Disclosure of breach to customers**
    - PR repercussions
  - Loss of Revenue
    - **Fall out from breach**
    - And deleted business emails
- **Who is accountable?**



Understanding Hidden Costs

- **Pay as You Go**
  - **And keep on paying**
  - **One time start-up fees (perpetual license) v. ongoing subscription**
  - **Usage models can mushroom**

Understanding Hidden Costs

- **Determine**
  - **What is the annual cost?**
    - **On prem has a steep start up fee**
    - **But maintenance is ~10-15% over time**
  - **Usage frequency?**
    - **One scan a year for compliance probably fits service**
    - **Daily scans may price out better on-prem**
  - **How does the price point change with additional users/services/targets?**

Understanding Hidden Costs

- **What's not included?**
  - **Migration**
    - **User lists and entitlements**
    - **Legacy information**
    - **Also consider: time to migrate and what that may cost the company**
  - **Archive and storage**
    - **On going backups of data**
    - **Does the SaaS charge an additional fee?**

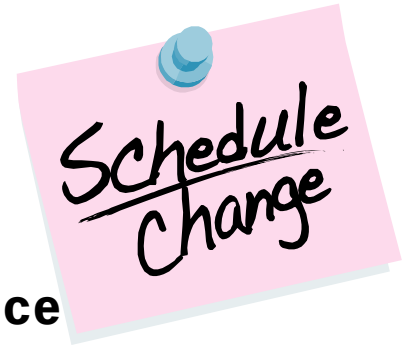
Understanding Hidden Costs

- **Headcount**
  - **Reduction not elimination of headcount and education overhead**
- **Determine**
  - **Cost (if any) of educating users on new system**
  - **Liaison and response headcount**
    - **Manage the SaaS**
    - **Review logs, reports**
    - **Initiate changes is necessary (ex: mitigate a vuln)**

Understanding Hidden Costs

- **Vetting and Governance**
  - **Due diligence on the SaaS provider**
  - **Remember who's still accountable for the data…**
- **Determine**
  - **What certifications and processes are in place?**
  - **Existing customers?**
    - **Are they in your vertical?**
    - **Have similar requirements?**

Understanding Hidden Costs



- **Scheduled Maintenance**
  - **Does the provider go off-line during maintenance**
  - **Will this impact your business?**
- **Software Upgrades**
  - **What is the upgrade schedule?**
  - **Will you be using outdated software?**

Understanding Hidden Costs

- **Is support included?**
  - **Is it 24/7?**
  - **Will better levels of support cost more?**

Quantifying Cost of Downtime and Other Loss

- **What is the real cost to the business if the service fails?**
  - **Consider both downtime**
  - **Coverage failures**
    - **Especially with scanners**
  - **And exposure from data loss**

Quantifying Cost of Downtime and Other Loss

- **Mail Hygiene**
  - **Provider's server crashes**
  - **Mail does not get through for X number of hours**
    - **During a work day**
  - **What would that cost?**

Quantifying Cost of Downtime and Other Loss

- **Vulnerability Assessment**
  - **Provider missed critical exposure on application server**
    - **SQL Injection attack results in database leakage of credit card numbers**
    - **PCI RoC = failed**
  - **Or, provider scan brings down web server for X hours**
    - **It is the ticketing web server**
    - **Transactions can not be completed**

Quantifying Cost of Downtime and Loss

- **If loss has occurred**
  - **Your organization may already have these numbers**
- **Green field?**
  - **Some extrapolation may be required**
  - **Calculate based**
    - **On type or server or service**
    - **Actual transactions on server / application**
    - **Cost of inactive employee (hourly rate)**

Quantifying Cost of Downtime and Loss

- **Ask the SaaS provider**
  - **They may have conducted a business impact analysis**
  - **And have some example numbers for you**
  - **These numbers are often used in negotiations for remuneration fees in service level agreements**

Key Take Aways

- **Get Data Smart**
  - Understand where your data is stored
  - Who has access
  - How it's protected
- **Know The Costs**
  - Factor in "hidden" fees
  - Quantify impact of downtime / exposure / loss