How I Learned to Stop Worrying and Love the Cloud

A Newbie Federal CISO’s Painful Cloud Security Education
Overview

- The United States Mint
- Software as a Service (SaaS) Cloud Computing
- How to Outsource and Sleep Well at Night
Who I am..

- Previous team lead for security assessments and penetration testing for an intelligence agency
- Created a penetration testing program for the Library of Congress
- Currently serving as the United States Mint CISO
The United States Mint

- We make the circulating coins
- We are the only Federal mint in the United States
- The Mint had over $700 million dollars in numismatic sales in 2011
- The current commerce system is aging and needs replacement
- We are required to maintain PCI & FISMA compliance
Software as a Service (SaaS)

- SaaS is a fancy name for managed hosting
- The vendor is responsible for providing a stable and current solution
- They are also responsible for securing the solution
- Our goal is risk transference
- OK, it’s more than managed hosting but you get the idea...
The Case for SaaS

- Huge cost savings
- The cloud vendor is responsible for managing your security
- Routers, Firewalls, IDS and updates are all handled by the cloud provider
- Incident response and disaster recovery are also handled by the vendor
The Case Against SaaS

- You lose control
- You are at the mercy of your cloud providers' security infrastructure
- You are dependent on your cloud provider for timely disclosure of security incidents
- You lose much of your system visibility
My Introduction to SaaS

- Outsourcing to SaaS was discussed during my interview for the Mint CISO position.
- Day one of the new job I’m asked to sign off on the SaaS solution as the CISO....
- Many hard lessons of SaaS were learned over the next few months.
Site Visit

- Profile your vendor
- Know your requirements
- Ask for detailed explanations of the security infrastructure including diagrams, procedures and key staff
Site Visit

- Ask to speak with the security team
- Be prepared for resistance or unpreparedness
- Ask for the ROC, SSP and testing results BEFORE you sign a contract
Foreign Vendors

- In a global economy it is increasingly difficult to find a solely US based host
- Negotiating with a provider with a foreign presence can pose regulatory and security issues
- Your organization’s policies may prohibit foreign hosting
Foreign Vendors

- You will need to make a risk based decision that suits your needs
- Don’t be afraid to ruffle feathers to get what you need!
- The political ramifications of foreign hosting must also be weighed
- Get management buy in if possible but understand you may have to go it alone
- Get the decision in writing!
A Federal agency that accepts credit cards gets the double PCI and FISMA compliance whammy.

FedRAMP is a great idea that is light on specifics.

Make sure your vendor understands the regulatory compliance your organization must meet.

Mandate contractor support if necessary.

Hold them to it!
Pre-Contract Testing

- Ask for access to a demo site
- Make sure this site is representative of how yours will be hosted
- Use aggressive testing...
Pre-Contract Testing

- Identify and get access to the administrative interfaces as well
- If the vendor will absolutely not give you access until after contract award test as soon as the contract is signed!
Contract Negotiations

- Understand this is business
- Security is not the business objective
- However, security problems can shut the business down
- Use transaction based models to your advantage
- Try to avoid being locked in a room with the vendor over the weekend while negotiating....
Disaster Recovery

- Understand what constitutes an disaster in the cloud and request an appropriate solution
Disaster Recovery

- Know where your data goes in a disaster
- Decide if you can live with where your data goes in a disaster
- Negotiate hard to make sure that solution meets all your needs
Cloud vendors do not provide separate customer logs.

Everybody knows this and talks about it, nobody offers a solution.

The data is there... ask for it!

You need the visibility for FISMA continuous monitoring.

You’ll save the vendor and yourself a lot of hassle in the long run.
Monitoring

- If your vendor can’t filter out your data there is a problem
- Solution should include at a minimum:
  - Firewall logs for all your IP’s
  - Web Server logs for all your IP’s
  - Database logs for all your IP’s
- You need a way to make sure incidents are disclosed in a timely manner
Incident Response

- Clearly identify what your providers incident response capabilities are
- Ask for specific incidents and results
- Clarify response times and when the vendor will notify you of a breach
- Create an SLA to nail down response actions and times
Make sure YOU pentest the vendor
Ask for the last two penetration test reports
Be mindful of delays in providing those reports...
Negotiate both internal and external penetration testing
If the vendor let their contractor in to test they can let you in as well
Service Level Agreements (SLAs)

- Define what’s important to you
- Don’t put too much emphasis on the SLA
- Rely more heavily on the contract language
- Understand the true impact or lack of impact from SLAs
Have an Escape Plan

- Make sure you can get your data if something goes wrong
- Get a Data Escrow vendor to hold your data
- Choose a trusted third party provider
- Preferably with an automated online solution
Know what you need
Ask the tough questions and demand the answers
If the answers don’t meet your needs don’t be afraid to recommend walking away
Keep the same approach after the contract is signed
Remember, you are the customer!