

SECURITY AND MOVING TO THE CLOUD

Stewart James
7/9/2011

vu.edu.au

CRICOS Provider No: 00124K

WHO AM I

- Geek. With a functional personality.
- InfoSec specialist
- ICT Security Manager at VU
- CISSP and GIAC Certified (8 with 2 Gold)
- Passionate about InfoSec

ROAD MAP

- **INFORMATION SECURITY AND ICT**
- **CLOUD TYPES**
- **RISK**

- **CHALLENGES IN THE CLOUD**

- **QUESTIONS. IF YOU HAVE ONE LET THE CHAIR KNOW**

INFORMATION SECURITY

- Information Security
- A maturing field, fast moving
- 3 core principles
- Information is the concern not the technology

CLOUD TYPES

SaaS

PaaS

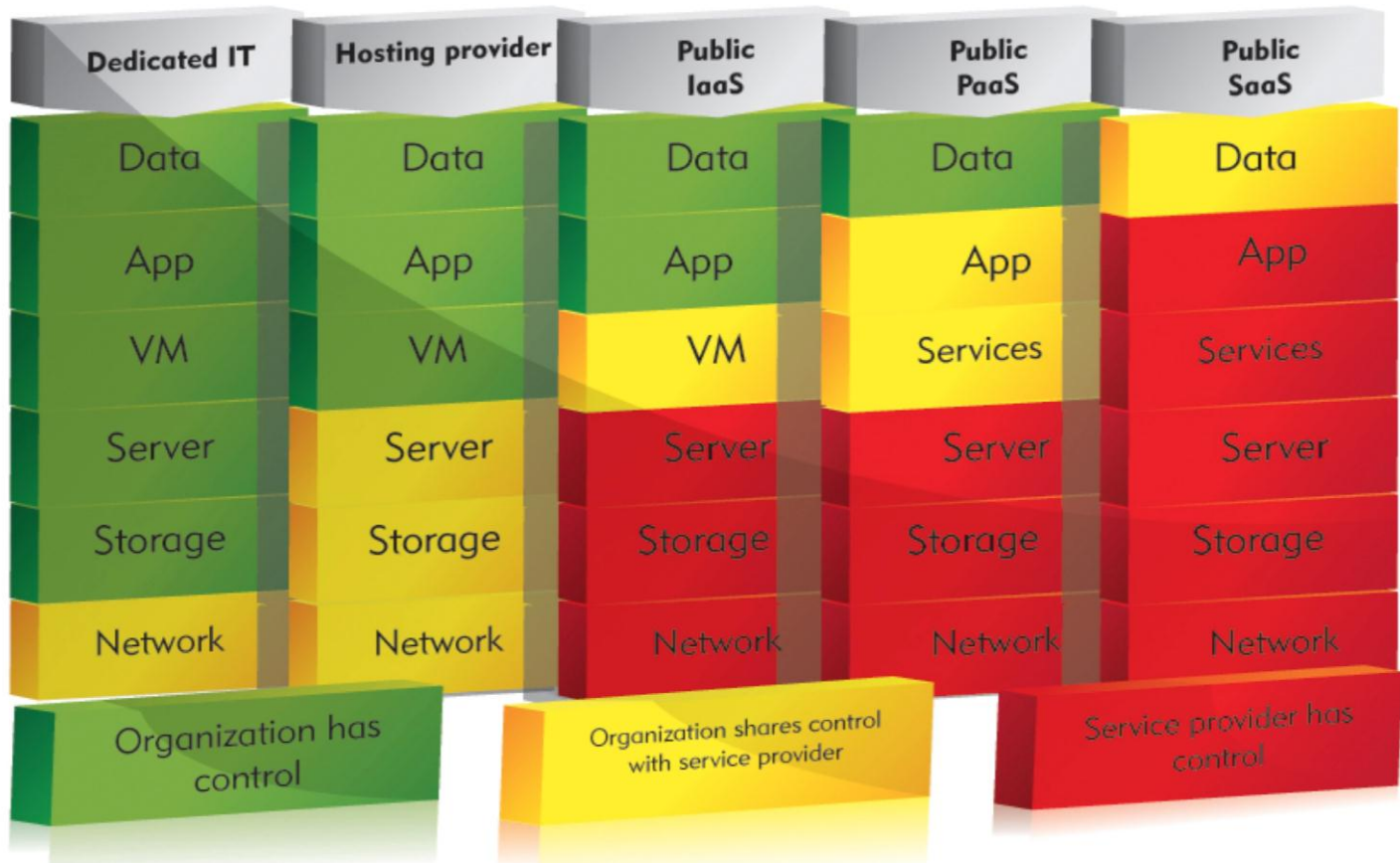
IaaS

CSP - Cloud Service Provider

TRUST



Security - Who is in control?



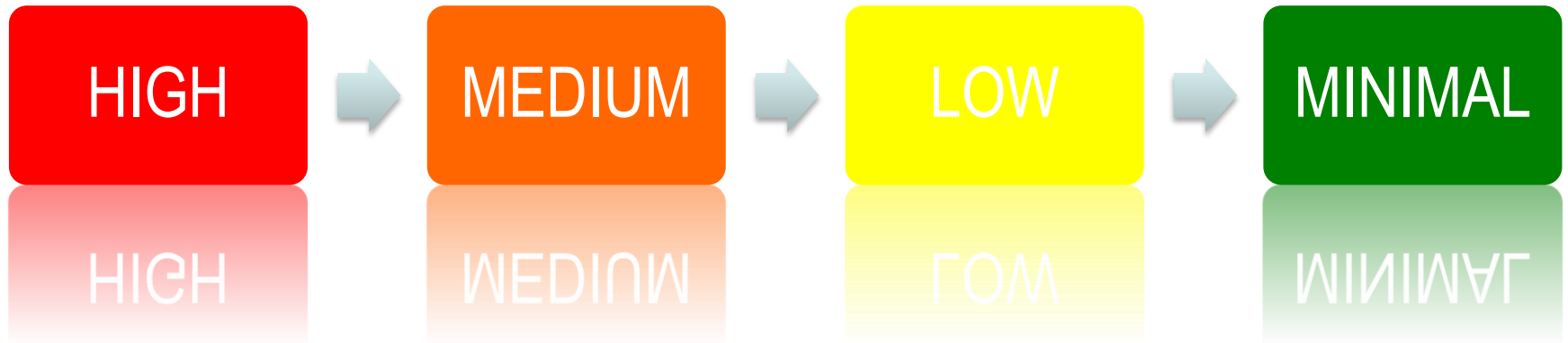
IS IT OUTSOURCING?

- Depends...
- Many of the risks and concerns for outsourcing seem similar to cloud services.

IDENTIFY INFORMATION TYPES

- What type of data do you have?
 - Private (PII)
 - Trade Secrets
 - Commercially sensitive
 - Public
-
- Where is the line for your company?

MEASURE YOUR RISK



CHALLENGES

- Lets look at some of the challenges that may face companies migrating to the cloud

DATA SECURITY AND SAFETY

- At rest
- In transit
- Where processed

EXISTING POLICIES

The University may make a record of your visit and log any of the following information for statistical and business purposes- the user's address, the user's domain name, IP address, the date and time of the visit, the pages accessed and documents downloaded, the previous site visited and the type of browser used. Identification of the user may also be requested and logged.

Information about your visit to a University website may also be logged by Nielsen//Netratings Pty Ltd to provide the University with de-identified statistical analysis about users' online experiences and trends.

(Monash University Privacy Policy)

DATA SPREAD

- Data no longer in a single location
- Data may be spread across multiple cities and countries
- Ability to look at a server, rack or room as containing your data sacrificed. Not necessarily a big deal.

OTHER CUSTOMERS

- Are other customers trustworthy?
- Are the other customers staff trust worthy?
- What level of access to other customers have to your data?
- Are they common attack targets?

LEGAL JURISDICTION

- Which laws are relevant?
- A customer in Britain and a server in the US.
- If another customer's data is subpoenaed, how will the CSP ensure your data is safe?
- Are log files exported to yet another country?

BACKUPS

- Is backup medium per customer or a shared resource
- How are the devices secured?
- How are the devices wiped before reuse?

CUSTOMER EXPECTATIONS

- In Germany using google analytics may be illegal
- In Germany, facebook facial recognition may be illegal
- In Italy sniffing network traffic is legally difficult
- What did you tell your customers when they signed up for your service?

EXIT CLAUSES

- Getting your data back
- Breach of contract
- With hold for non-payment
- Time frame
- Cleansing

REPORTS ON ATTACKS

- IDS Feed
 - IPS Feed
 - Real time log data
 - Firewall logs
-
- Integration with your existing log aggregation aka SIEM system

REPORTS ON INCIDENTS

- Are there reports on confirmed incidents?
- Are they delivered in a timely fashion?
- What information is shared?
- Who else do they report incidents to?

AUDIT AND CERTIFICATIONS

- The right to audit
- Review any external audits they have performed
- Review their certifications

- The more sensitive your data is the more frequently you need to do this

SUMMARY

- Take deliberate action to measure the changing risk profile
- Ask lots of questions
 - Vendors
 - Security Folk
 - Legal Guys
 - Customers
- Better to address these things at the start than after a breach

CONTACT DETAILS

STEWART JAMES

INFORMATION TECHNOLOGY SERVICES

PHONE +61 3 9919 4688

FAX +61 3 9919 4800

EMAIL stewart.james@vu.edu.au

TWITTER @stootles