SSM 3

I.G.Batten@bham.ac.uk

16217082

Recap

- Policies define objectives and outcomes
- Procedures define methods and measures
- Audit checks everything is being obeyed
- But how do we choose the things that fall into scope?
- Asset Registers

Asset Registers

- Register of all the information assets in the business
- Therefore define the scope of an information management system
- Should include everything that can affect the security of information

Multi-Layed

- Data set (“the HR information”)
- Application (“the Oracle instance”)
- Platform (“Solaris Server number 6”, “EMC Array”)
- Locations (“Birmingham data centre”)
- Infrastructure (“AD Server”, “UPS”)
- People (“HR Director”, “Cleaner”)
- …

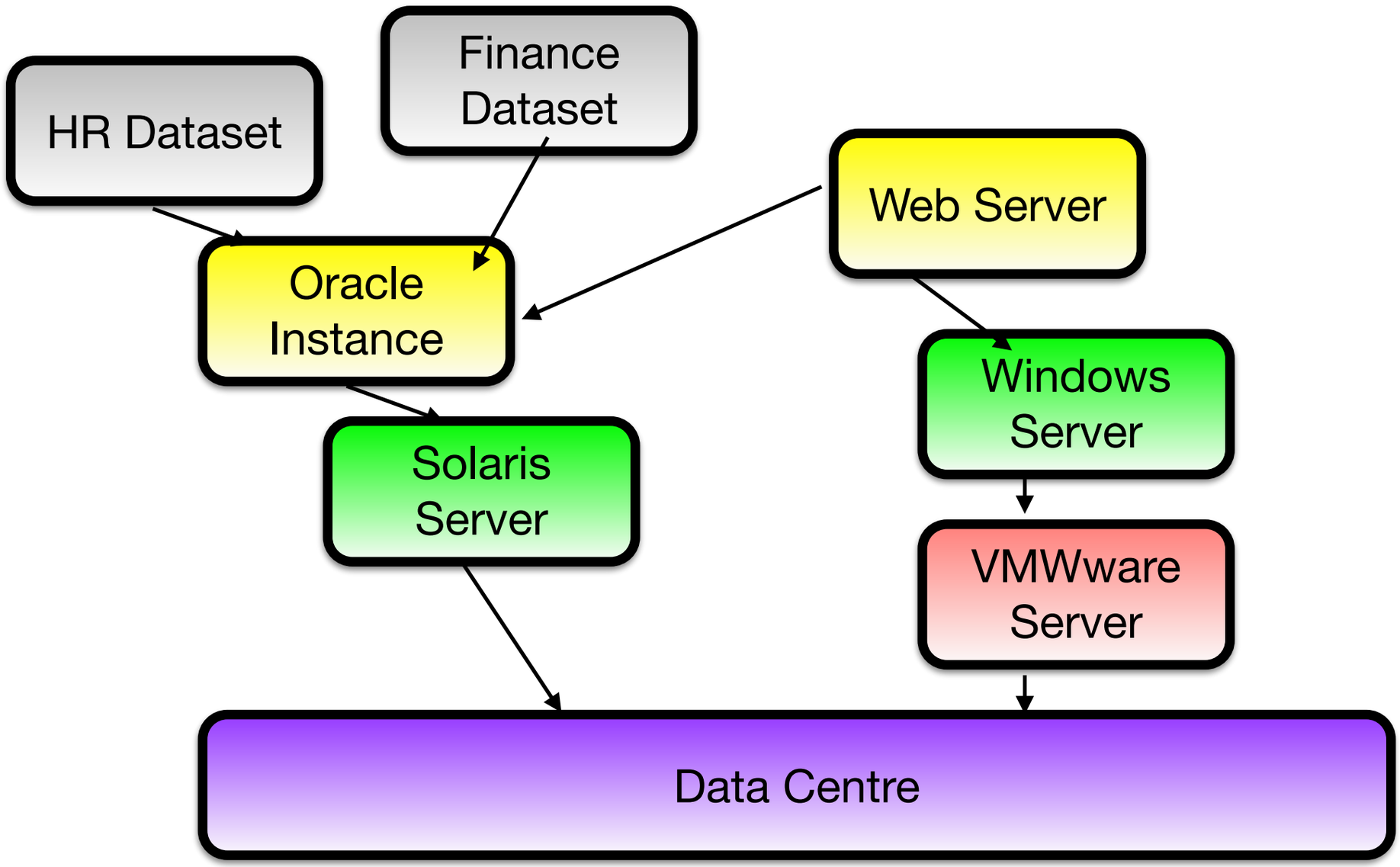
The full scope

- Everything you might want to record a **threat** against
  - Everything an attacker might want to control / destroy / compromise
  - Everything that might stop working
- Everything you might want to apply a **control** to
  - Everything you need to consider, in other words

Benefits

- Asset registers are sometimes not this deep: they cover only the information assets in terms of data sets
- But it is much better if you can unambiguously identify the things you are going to measure risk for and apply controls to.
- And many things are shared between data sets

Dependencies



And everything depends on AD, Firewall, networking, power…

Asset Register Construction: an approach

- First step: systems and databases
  - Payroll, HR, source control…
- Then expand downwards
- Second step: “what you can see”
  - Boxes (“tin”), Buildings, People, Cabling
- Then expand upwards
- Maybe meet in the middle?

Reality intrudes

- Experience of doing this exercise is that you find a lot of things you didn't really know about, or didn't realise still existed
- Lots of legacy systems and, worse, legacy infrastructure
- "Mature" computer installations are subject to the 2nd law of thermodynamics
  - 27001 (etc) can be opportunity to simplify: removal better than controls

And iterate…

- You won’t get it right first time, and shouldn’t feel bad when you don’t
- When you come to do a risk assessment, you will realise that your asset register isn’t quite correct
  - Not fine grained enough
  - Missing some infrastructure
- It’s OK to iterate and improve

Exercise

- Think about a business that has an HR system, a finance system, a public webserver and some engineering systems (source control)
- Sketch a graph like the one we've just looked at.

Again reality…

- A real exercise like this will uncover a much more complex mesh of dependencies
  - A good reason to get everything under a security management system as quickly as possible is because every year that goes by makes it harder
- Even strongly change-managed businesses are bad at capturing dependencies
- Dependencies aren’t necessarily attack trees, but give clues

Why is this so important?

- New, professionally installed systems on modern hardware locked into a data centre may not be as vulnerable as old, legacy systems running on unsupported hardware under someone’s desk
- But if the latter is holding the system together, it’s a serious point of weakness
- “Development” AD servers, build systems, test systems with access to live data, etc, etc.

Cloud Assets

- How do we do asset registers in the cloud?
- If you are running a service on an AWS instance, what do you put into your 27001 case?
- Your external auditors will advise, but my advice would be that the asset is the information and the contract you have with Amazon, and the audit is of the fitness for purpose of that contract.

Cloud Assets

- Is going to be a huge issue in the future
- At the moment, formal accreditations of cloud services are rare, and businesses that use (say) salesforce.com will adopt a “risk managed” approach
  - Euphemism for relying on a contract, reputation and good luck.
  - Existing audit policies don’t work well
  - “On Prem” cloud attractive to large integrators and government

Maintaining asset register

- Once written, you would like to think that it's easy to maintain the asset register: it's just new stuff, yes?
- But unfortunately new systems and, worse, new dependencies don't require financial approval, or at least don't appear as capital assets
- Requires active co-operation.

Why isn’t this the capital asset register, plus a bit?

- Emphasis starts from systems and functions, not on licenses, bricks and tin
- IT equipment increasing leased, and therefore not a capital asset, or is cheap, and therefore not capitalised
- Financial Asset register usually doesn’t talk about function
- And in any event, most companies are bad about scrapping, so asset register will contain lots of equipment you don’t have or use any more
- A joint project with finance to clean the asset register is good, but will sadly always be low priority.
- Reducing “assets employed” is good for the CIO, even if not the CSO.

With this done, next step…

- Risks and threats