Secure System Management

i.g.batten@bham.ac.uk

Check Panopto!

- Is it running?
- Is it running?
- Seriously, is it running?

The Course Title

- Probably better named “Security Management Systems”
- Title was a placeholder in the accreditation process and changing it uses up our metaphorical with the accreditor without much benefit.
- Not about systems administration
- “Management systems” are things like ISO 9000 Quality, not things that use SNMP.

Logistics

- Lectures: Mech Eng B05, 9am Tuesday and 2pm Thursday
- Office hours: Wednesday, 10–12 in CS 132
- I.G.Batten@bham.ac.uk
- https://igb.batten.eu.org/
- Canvas/Panopto will contain full recordings
- So far as I know, there will be no cancelled lectures

Purpose

- Teach you about the management systems that sit behind computer security systems
    - It isn’t just technology, you need to organise it as well.
- How do we decide what to secure, how to secure it, and check we have secured it?
- No security is perfect, no security is free, how do we balance cost, risk and effectiveness?
- And how do we convince other stakeholders that are are doing sensible things, and doing those sensible things properly?

Reasons

- Security people are often bad at business and risk judgements
- Knowing your “Risk Appetite” is crucial, but in the absence of the debate it’s too often assumed to be zero (cf. Birmingham University)
- We focus on **risk reduction** and sometimes **mitigation**, but should consider risk **transfer** and, last but very much not least, **acceptance**.

Threats and Risk

- Much research into risk of fraud against contactless payment,
    - Risk to individual is capped at somewhere between £0 and £90, depending on whether you trust your bank.
    - Not nice if you are a poor cash-strapped student, but rarely existential.
- From the criminal's side, it's a lot of work to get £30 at a time
    - not easy to convert to cash
    - risk of conviction for fraud and similar offences.
- **WHY NOT JUST SHOPLIFT WHISKY FROM SUPERMARKETS?**
    - Petty criminals do not need to get a paper in CSF in order get a post-doc, they just want £30 now.
- We have to look at risk, motivation and threat actors, not just consider the risks in the abstract.

Who should be here?

- People doing the cyber security MSc (this course is compulsory, so you must pass it)
- Is there anyone else sitting in?
  - I know I have agreed to a conversion MSc and as of yesterday two MSci students.

Background Knowledge

- What do you know about security? Has anyone worked under…
  - ISO 27001 (or BS7799)?
  - ISO 9000 (or BS5750, if you are very old)?
  - Common Criteria
  - What?
- What experience do you have other than a computer science degree?
- Or something else?

Enterprises

- Who has worked in an enterprise (university, large business, government department?)
- What security training did you get?
- Do you think it was well thought out?

Basic Content

- Asset registers
  - **What** are we securing, and **why**?
- Risk and threat analysis and modelling
  - What are we securing the assets **against**?
- Change management
  - How do we deal with **new** assets and threats?
- Metrics and Audit
  - How do we know **how well** we are doing? Or **whether** we are doing it at all?

Methodologies

- ISO 27001 for Information Security Management Systems
- ISO 27005 for risk modelling
- HMG Information Security Standard #1 for comparison (UK-specific, but similar to other government standards and after all, this is a UK government certified programme)
    - Currently being phased out, but the “son of IS#1” replacements aren’t easily available.
- BS 25999, now ISO 22301/22313, for business continuity, if we have time.

Week 1

- This introduction and getting to know each other session
- A walk through some security technologies at a very high level (we are going to need to talk about them)
  - Essentially an executive summary of next semester's Network Security course

Week 2

- Quality management systems, Plan Do Check Act
- Governance
- Policies, Procedures, Work Instructions, etc
- Class Activity: writing a simple policy, procedure and audit scheme

Week 3

- Building an asset register, defining the Trusted Computing Base
- Class activity: designing a small enterprise we can use for future exercises (groups of three or four)

Week 4

- Risk assessment, threat modelling, attack trees
- Adversarial Thinking
- Class exercise: attack our enterprise

Week 5

- Controls: what can we put in place to improve matters, and how do we choose and justify them?
- Residual Risk Statements
- Reduce/Mitigate/Transfer/Accept
- Class exercise: controlling our risks

Week 6

- Evaluating our work: metrics and audit
- Tiger teams / red teams
    - This is **not** a pen-testing course
    - You will gather at various points that I am sceptical about the merits of pen-testing
    - GCHQ big noise: “*the problem when recruiting is trying to find people who **don’t** just want to be pen-testers*”.
- Class exercise: designing an audit plan for our controls

Week 7

- Continuous improvement: how do we make things better?
  - Plan do check act, but we need to think about what this means
- Class exercise: make things better

Week 8

- Formal risk assessments: ISO 27005 and HMG #1

Week 9

- ISO 27005 and HMG #1 continued
- Class exercise: HMG #1 risk assessment for our enterprise, complete with threat actors

Week 10

- Putting it all together: writing a top-level policy and a coherent set of procedures, getting management support and training
- Class exercise: a security policy in less than 500 words, and how to justify it

Week 11

- Presentation to senior management and to staff (depends on numbers how long this will take)

Assessment

- I’d like to do this as team exercises, and maybe mix the teams up a couple of times if there are concerns about fairness.
- If this is going to upset people, let’s talk, but this isn’t really the sort of stuff people do on their own.
- I intend to give the same mark to everyone in each group. This has worked OK for two years so far.
- Groups of 4–5, at most 6, preferably with a mix of experience and background.

Outcomes

- You’ll know what a 27001 stack looks like
- You’ll know how to fulfil the ISMS requirements
- You’ll be able to say “threat actor” and know what it means
- You’ll be able to say “risk appetite” and not look silly
- You’ll have written a presentation to management about residual risk statements
    - This is the main take-away: these are the best personal insurance policy you can have.,

Assessment

- Sequence of reports, mirroring (as much as we can) activities you would carry out when doing an ISO27001 or similar activity.
- Problem is that we don’t have an enterprise to play with.
- As I said, Groups, if that’s OK by you.

Things to do now

- Get a copy of ISO27001 and ISO 27002 and read them
- Get a copy of HMG Infosec standard #1 (might tax your Google skills!)
- Look at ISO 9000 management systems
  - The documents are very dry; you will find commentaries perhaps easier going.

Exams

- The past papers are available
- I don’t guarantee that the next exam will be the same format, but the general idea (“here’s a scenario, here’s a problem, respond”) is likely to remain.
-

SSM Lecture 2

I.G.Batten@bham.ac.uk
https://www.batten.eu.org/~igb

Check Panopto!

- Is it running?
- Is it running?
- Seriously, is it running?

Purpose

- I want us all to have a similar understanding of *adversarial thinking*
- I want us to work through a simple example of information security, and highlight the *technology* and *process* issues at each point.
- This isn’t going to be formal, I just want us to have a taste of the issues.

Format

- Later, I want you to break into groups of three or four
- Ideally, people you don’t know and aren’t from the same country / university / etc as you (to get some different perspectives)
- I’m going to set a series of 5 minutes exercises

Problem

- Imagine I have three pieces of data on my laptop
    - “Market affecting” information about a company which will allow anyone who knows it to make money on the stock market
    - A spreadsheet containing the bonus payments to be made to the staff of my company.
    - Information from a whistle-blower which will harm another company when I give it to the government.

CIA

- Confidentiality (like market affecting data)
    - Can this data only be **read** by authorised actors?
- Integrity (like bonus plans)
    - Can this data only be **changed** by authorised actors?
- Availability (like whistle-blower data)
    - Is this data always available to **authorised** actors?

Adversaries?

- Confidentiality (like market affecting data)
  - Adversaries want to read the data, so they can make money from derivative trading
- Integrity (like bonus plans)
  - Adversaries want to change the data, to make their bonus better.
- Availability (like whistle-blower data)
  - Adversaries want to delete the data or make it temporarily unavailable, so they can avoid embarrassment.

Conventional Ratings

- Each of these is rated on a 5, or sometimes 6, point scale of “impact” — what are the consequences of the security property being violated (monetary, safety, national security)
- 1 means “no or trivial impact”
- 5 can mean “major loss or life or vast economic harm”
  - Scales are decided for the domain you are working in

CIA Triples

Note these classifications are now deprecated, but the numerical ratings remain

- 334 is UK “RESTRICTED”
- 444 is UK “CONFIDENTIAL”
- 554 is UK “SECRET”
- **66**4 is UK “TOP SECRET”

IL 3

- “Risk to an individual’s personal safety or liberty”
- “Loss to HMG/Public Sector of £millions”
- “Undermine the financial viability of a minor UK-based or UK-owned organisation”

IL 6

- “Lead directly to widespread loss of life”
- “Major, long term damage to the UK economy (to an estimated total in excess of £10 billion)”
- “Major, long term damage to global trade or commerce, leading to prolonged recession or hyperinflation in the UK

Exercises

- I realise that the answers to these exercises are the stuff we are going to learn about over the coming weeks.
- I just want you to start thinking **adversarially**: start thinking like an attacker, and start thinking like a defender.

Exercise 1

- Think of the people who might want to attack my laptop.
    - How **skilled** are they?
    - How **motivated** are they?
        - Motivation includes willingness to break the law, willingness to take risks and the size of the possible pay-off.
    - How **resourced** are they?

Suggestions

- Fraudsters
  - Could be very skilled and motivated, but resources?
- Business competitors
  - All three?
- Employees
  - Skilled and motivated, might be able to use my resources against me
- My government?
- Other governments?

Exercise 2

- Think of threats to my laptop and to the data on my laptop.
  - Do they affect **integrity**, **confidentiality** or **availability**?
  - Do they require **skill**, **resource** and **motivation**?
  - Don’t just think of subtle crypto attacks: be inventive, and be crude!

Suggestions

- Phishing
- A wide variety of protocol attacks we will talk about in Network Security
- Theft
- Blackmail / Coercion
- Cameras / Keyloggers / etc

Exercise 3

- How would you stop these attacks?
- How difficult, expensive, intrusive are the counter-measures (we are going to call them **controls**)?
  - Think of costs and unintended consequences?
  - Will users accept them?

Suggestions

- Passwords
- Encryption
- Locks
- Tamper Resistance
- Stuff we’ll talk about in Network Security :-)

Exercise 4

- How would you **measure** the benefits of your controls?
- How would you **audit** whether people were following your controls?
- What problems might arise?

Suggestions

- Virus incidents detected
- DLP
- IDS / IPS
- Surprise visits

The cycle of quality systems

- Plan
- Do
- Check
- Act

Plan

- Identify assets, risks, threats
- Associate controls

Do

- Run the system with the new controls applied

Check

- Design and collect metrics
- Design and collect audit information
- Assess the success of the system

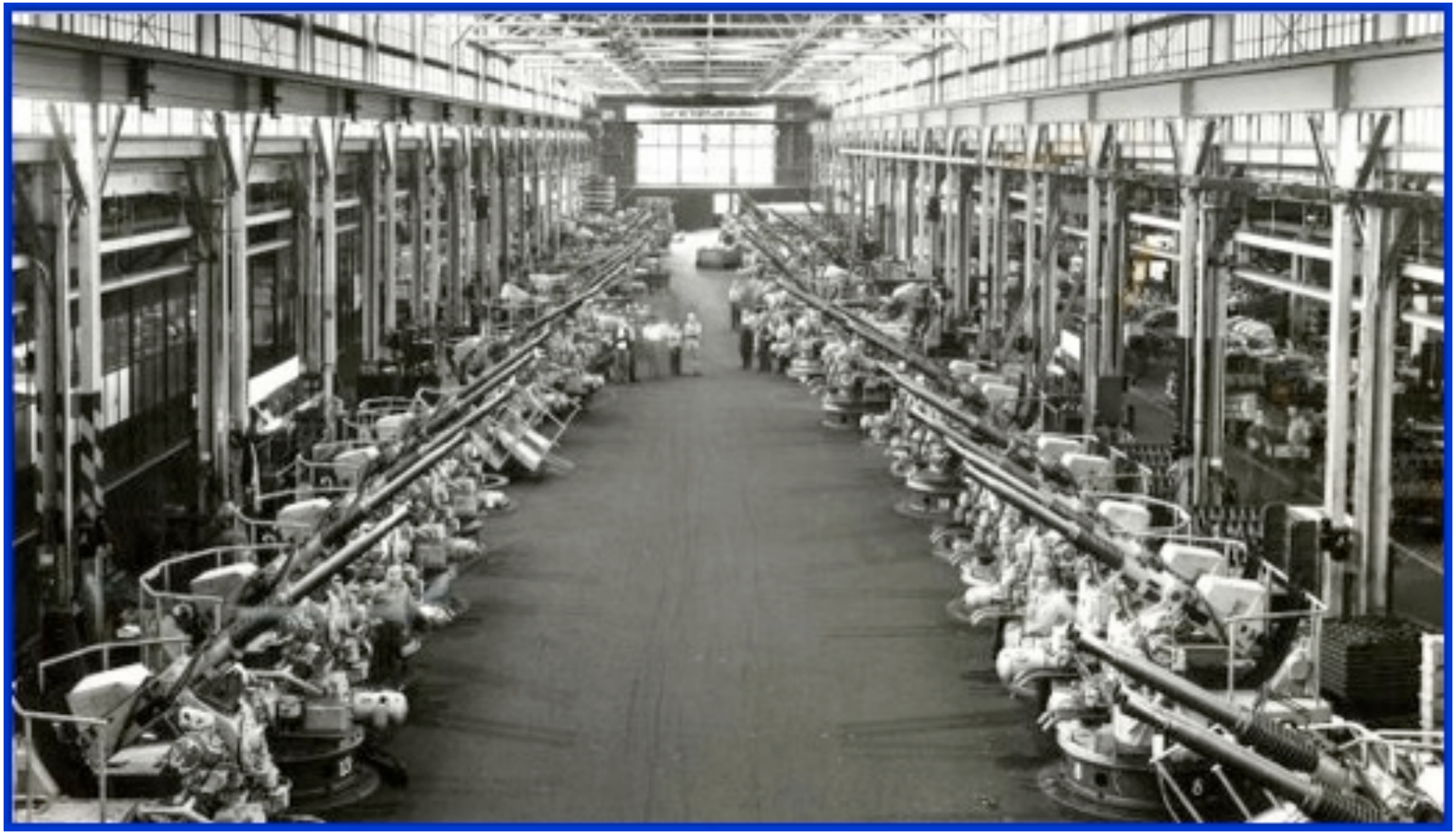
Act

- Improve the system
- Return to “do” (or “plan”, depending on your taste)

Basic Cycle of Quality Systems

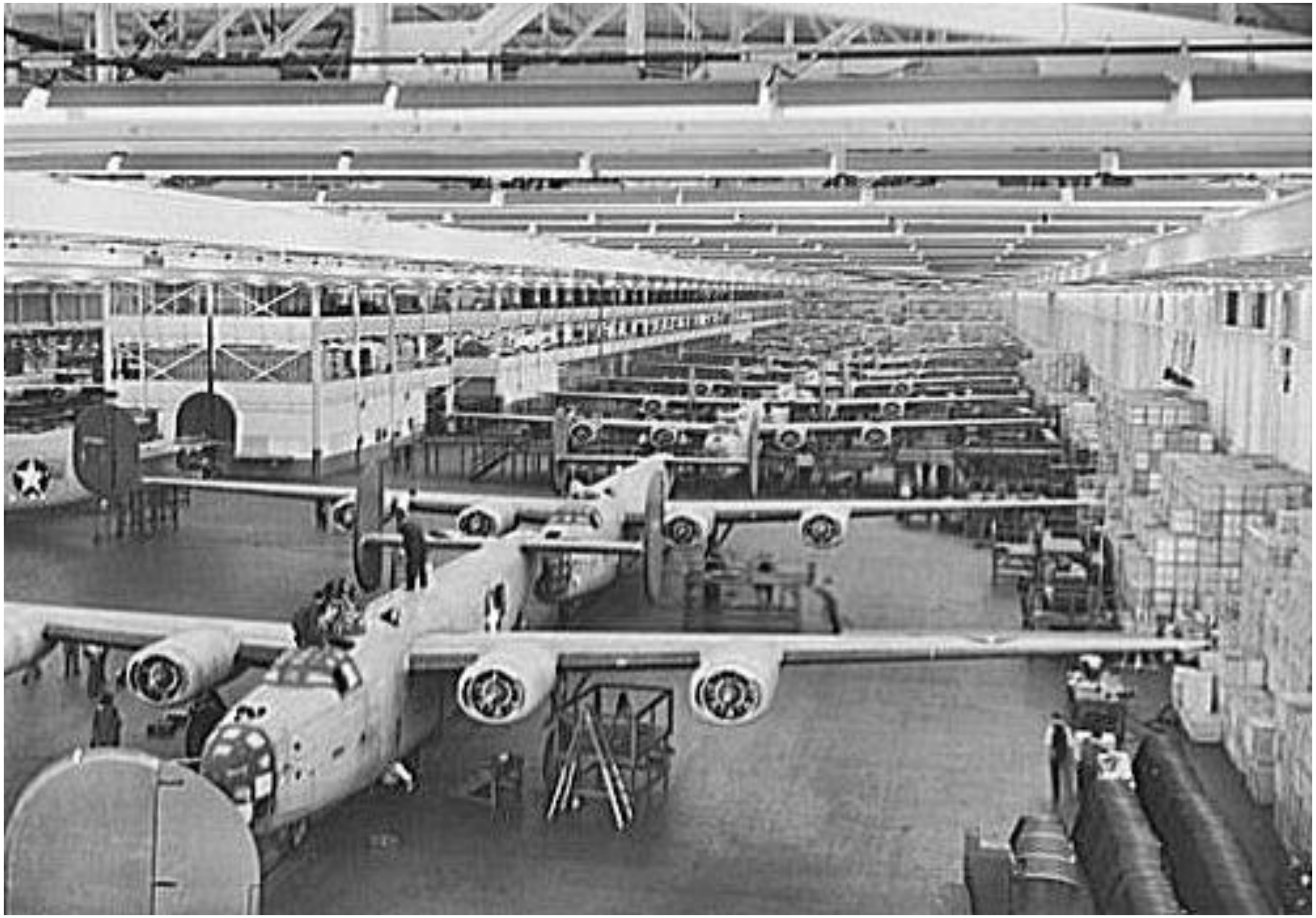
- Ironically, modern quality standards stem from wartime manufacturing as refracted through Japanese manufacturing after the war.
- BS5750 and before that MIL-Q-9858 led to ISO 9001.

Mass production of complex guns



40mm twin Bofors, “The Big Room” at Chrysler

B24s at Ford Willow Run



And even ships!

Why is manufacturing hard?

- Requires accurate control over sub-contractors, so they deliver stuff to you that is the right size and quality
- Chrysler had thousands of sub-contractors, as did Ford, as did Kaiser.
- But you need a way to ensure that sub-contractors have a quality process which matches their processes and gives them freedom to innovate and improve: profit motive!
- How do you check their quality process is credible, without imposing inflexible systems?

Basic Components

- **Policies**: state the objectives and criteria of the system
- **Procedures**: state how to do things, checked to ensure they fulfil policy objectives
- (Sometimes) **Work Instructions** or **Method Statements** which are more detailed
- **Quality Records** can be **audited**, as can compliance with policies and procedures

Compliance

- External auditors check that policies are adequate, that procedures support the policies, and that procedures are being followed, with the help of the quality records and internal audit.
- Internal auditors check that procedures are being followed.
- External auditors issue a certificate to say the quality system is fit for purpose.

Governance

- Documents need to be approved by named individuals who are accountable.
- Documents need to have review dates.
- Documents need to be issue/version controlled.
- There needs to be some way to get an “up to date” copy, and protection against out of date copies (hence review dates).
- Documents need to flow from requirements

Document Hierarchies

- The precise taxonomy of documents may vary from business to business:
    - 27001 offers some guidance, but a business may have existing practices, may have to consider other standards, may have historic requirements.
- What I will describe is one way of working.

Policies

- Describe how things should be, not how to do them.
- Set out objectives and high-level operational requirements
- Written by senior managers, approved by other senior managers or board-level directors.
- Short in length, long in duration.

Examples of Policies

- Why are we securing things, and who from?
- Do we prefer cloud or on-premises solutions?
- What legislation do we need to comply with?
- Who approves changes to our security system?

Policies:

- Are clear and unambiguous
- Are as short as possible, but no shorter
- Cover the majority of cases, with a process for dealing with exceptions, rather than trying to deal with everything
- Do not contain lengthy background material

Procedures

- Describe how to do something correctly
- Can be checked against procedures to confirm that they implement the requirements and objectives (and should state which procedures they are derived from)
- Generate quality records
- Written by operational managers
- Approved by their line managers, or ideally by owners of policies.

Examples of Procedures

- How to deal with new staff
- How to manage the departure of staff
- Who should be let into the building by night security?
- How do we provision a new laptop?

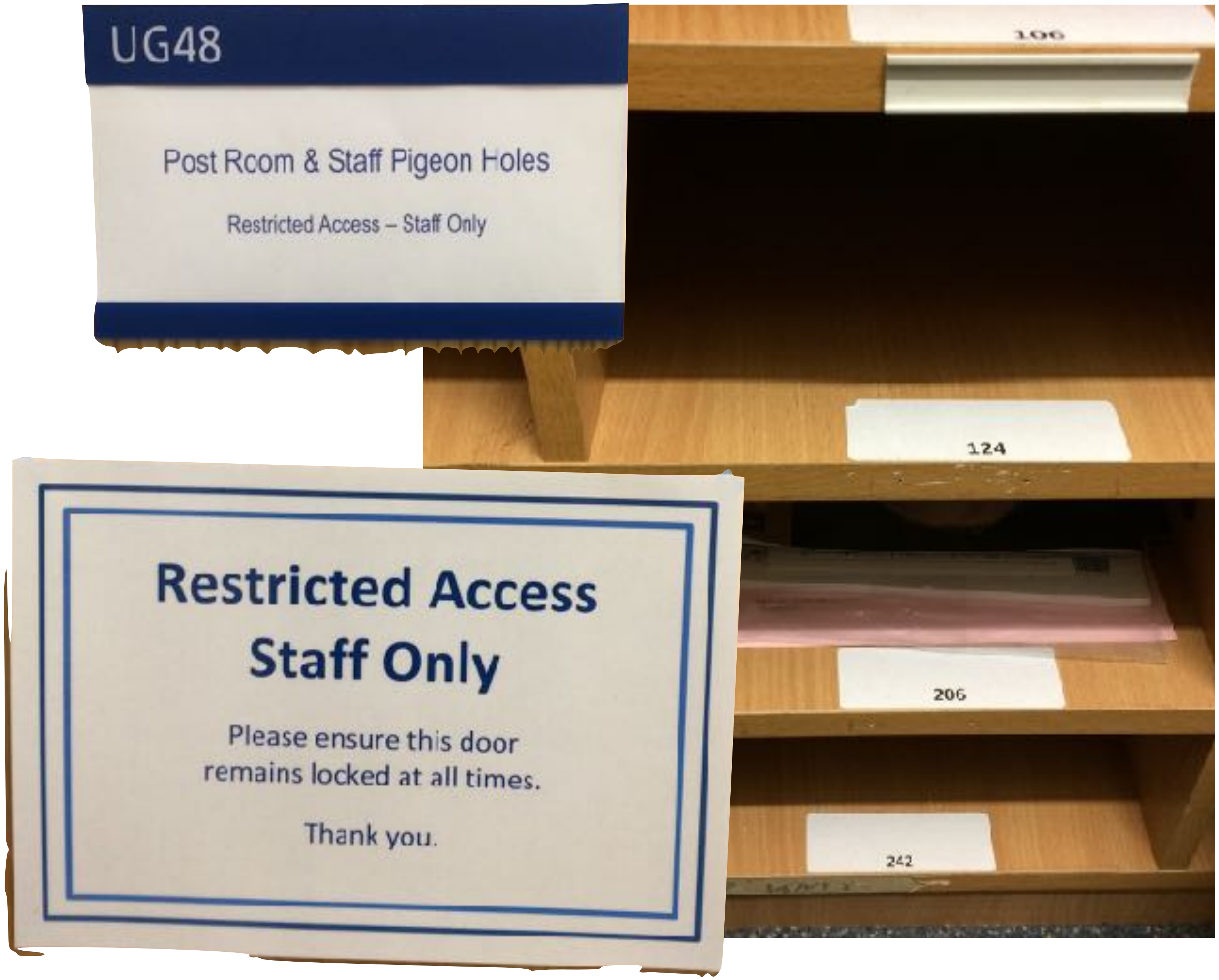
Procedures:

- Are step-by-step descriptions of what needs to be done
- Are always accurate and up to date
- Are immediately flagged for review if they don’t work
- Minimise opportunity for people to make decisions which may be inconsistent

With good policies and procedures:

- You should **NEVER** have to tell someone “oh, that’s not right, but if you go and ask Dave he can get Steve to sort it out”.

For example…



UG48

Post Rcom & Staff Pigeon Holes

Restricted Access – Staff Only

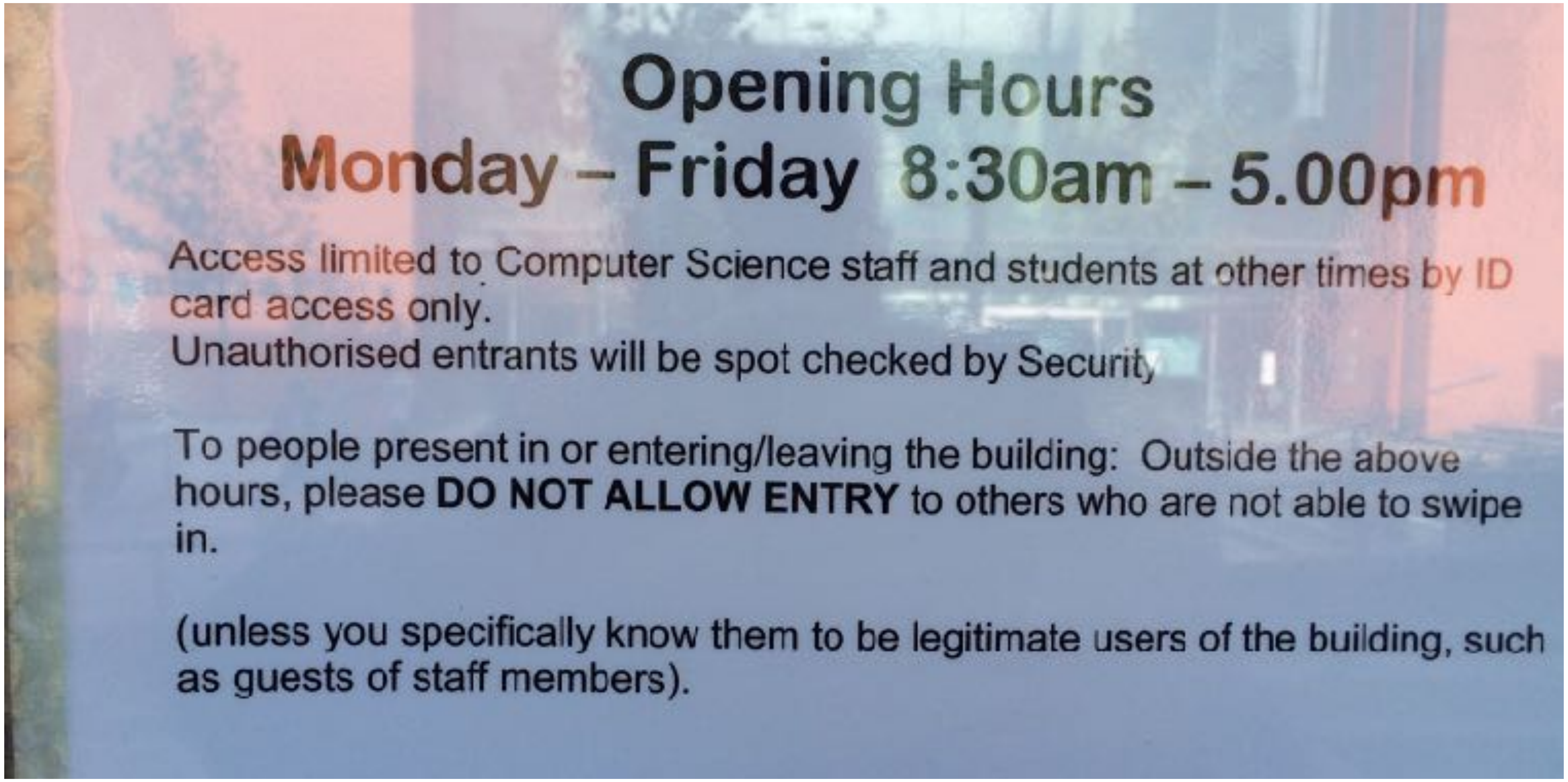
Restricted Access
Staff Only

Please ensure this door
remains locked at all times.

Thank you.

PhD Offices

For example



Opening Hours

Monday – Friday 8:30am – 5.00pm

Access limited to Computer Science staff and students at other times by ID card access only.
Unauthorised entrants will be spot checked by Security

To people present in or entering/leaving the building: Outside the above hours, please **DO NOT ALLOW ENTRY** to others who are not able to swipe in.

(unless you specifically know them to be legitimate users of the building, such as guests of staff members).

Document to critique

- https://intranet.birmingham.ac.uk/it/documents/public/Information-Security-Policy.pdf
- Consider its length
- Consider how easy it is to check it is enforced
- Look at its revision history
- How easy is it to use?

SSM 3

I.G.Batten@bham.ac.uk

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”)
- …

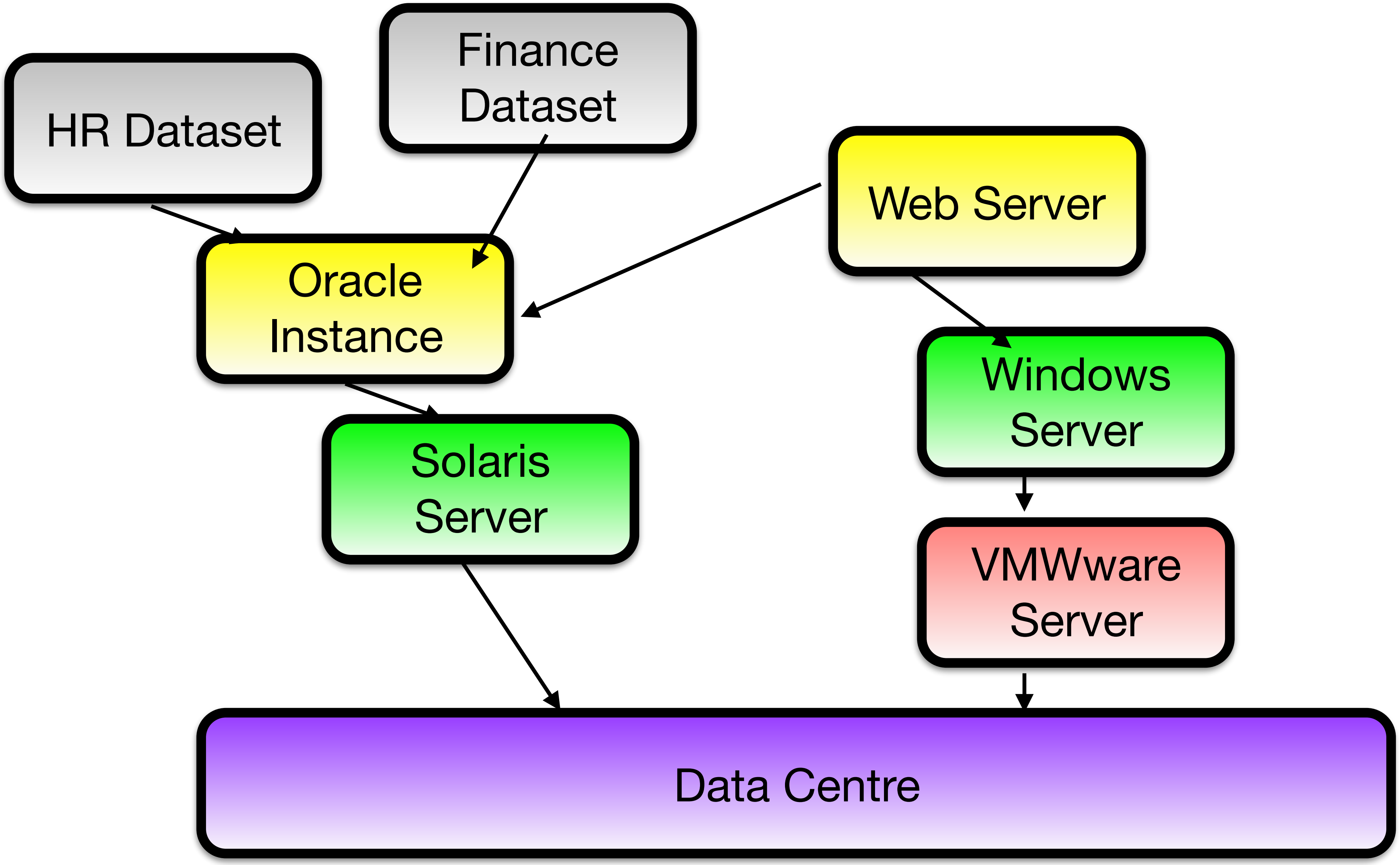
The full scope

- 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

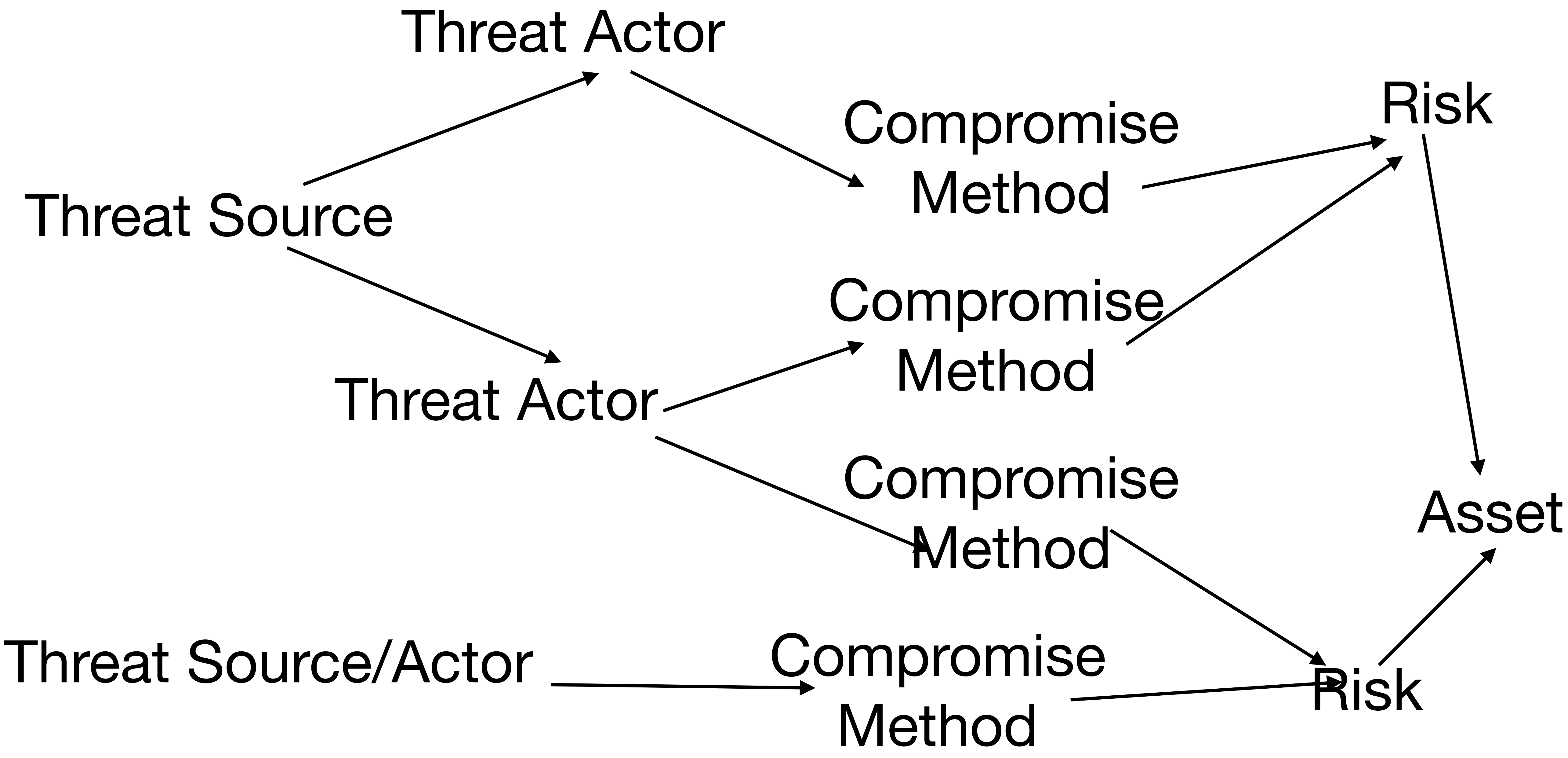
SSM Week 3: Risks and Threats

I.G.Batten@bham.ac.uk

Threats, Risks, Compromise Methods

- The language is confused, and the concepts are often treated in different ways
- I am going to use one set of definitions broadly from HMG IS1; other sources may use different definitions.
- In general:
  - **threats** are people who might do things
  - **compromise methods** are how they might do things
  - **risk** is the potential consequence to the defender of those things succeeding.

Overview


Threat Actor
Risk
Compromise Method
Threat Source
Compromise Method
Threat Actor
Compromise Method
Asset
Threat Source/Actor
Compromise Method
Risk

Threats

- A threat is something that an attacker (“threat actor”) might attempt to do to an asset.
- One way to assess this is by looking at capability (**can** the attacker do this?) and intent (**will** the attacker do this?)
- Attackers need both to be a danger

HMG #1 says

- A **threat source** is a person or organisation that desires to breach security and ultimately will benefit from the breach in some way.
- A **threat actor** is a person who actually performs the attack or, in the case of accidents, will cause the accident.
- For example a criminal may wish to breach the confidentiality of some HMG data. The criminal wishes the breach of security to happen and thus is the threat source. If the criminal persuades a system user to release the desired information to them then the user is actually carrying out the attack. They are the threat actor.

“Will benefit”?

- That includes “feeling good about themselves” or “getting props” or “LoL”.
- I think we underestimate the economic incentives and literacy of attackers, but we must be careful not to assume they are all rational actors.
- Old joke about economists and the twenty pound note.

What HMG #1 says

- The threat level is a value attributed to the combination of the capability and motivation of a threat actor or threat source to attack an asset. It takes into account any clearances that may apply to the threat actors and whether they are considered Deterrable.

Deterrable?

- Threat to lose job, clearance, livelihood, liberty…
- Alternatively, appeals to “better nature”, ethical codes, etc.
- Unfortunately, cybercrime (a) is not well prosecuted and those that are prosecuted are low-hanging fruit and/or guilty of something else as well and (b) seen by many to be victimless, so does not engage social taboos about theft and vandalism.
  - Nerdy young men who won’t spraypaint trains will deface websites, and claim it’s different.

Compromise Methods

- How an attacker might carry out an attack
- Can start at a high level (“Compromise Network”) and be refined to much more detailed level (“use CVE 1234 to penetrate system ABCD”).
- Only considers compromise methods that are plausible for identified threat sources.

What HMG #1 says

- A compromise method is the broad type of attack by which a threat actor may attempt to compromise the C, I or A of an asset. Once the threat actors' types have been determined it is straightforward to identify from Appendix C, the compromise methods they might use, and then consider which of those are actually plausible.
- We will look at Appendix C as an example of compromise methods on Thursday

Risks

- The risk to an asset is things that might happen to an asset, combining likelihood with impact.
- So a 1% chance per year of $10 000 of damage might be thought to be worth $100 per year (although it’s not as simple as that: 1% of $10 000 is not the same as 0.01% of $1 000 000, as most businesses can absorb the former but rather fewer the latter)
- Risks for ISO 27001 include things like accidental fire and flood which don’t have threat actors; **IS1 doesn’t consider this.**

HMG #1

- In general terms an information risk can be thought of as the likelihood that a threat will exploit a vulnerability leading to a business impact. IS1 aims to define all risks and estimate a risk level for each.
- Within IS1 a risk can be thought of as consisting of a number of components:
  - Threat actor and threat actor type;
  - Threat source;
  - Compromise method;
  - Property (C, I or A) of an asset … and business impact level associated with the compromise of that property.

Risk Assessment

- A Risk Assessment is a list of things that might happen to your assets, looking at likelihood and impact.
- Multiplication is OK, but breaks down for high impact / low likelihood events (cf. self-insuring)
  - Sometimes, you need to consider high impact events even if they are very low likelihood
- Idea is to weigh outcomes in the light of likelihood

But…

- Beware of claims to be precise and numeric, as there is too much uncertainty and subjecivity
- *“For the purposes of this Standard, risk level is defined on a six-point scale: Very Low; Low; Medium; Medium-High; High; Very High. The step-by-step process in Chapter 4 indicates how to estimate risk levels.”*
- Six point scale, eh?

Threat Assessment

- A threat assessment is a list of the people (groups of people) you think may attack you, looking at their capability and their motives.
- Nation states have (massive) capability, but for most people have limited intent (depends on the nation!)
- The guy you sacked yesterday has lots of intent, but probably fairly limited capability (assuming a competent exit process)

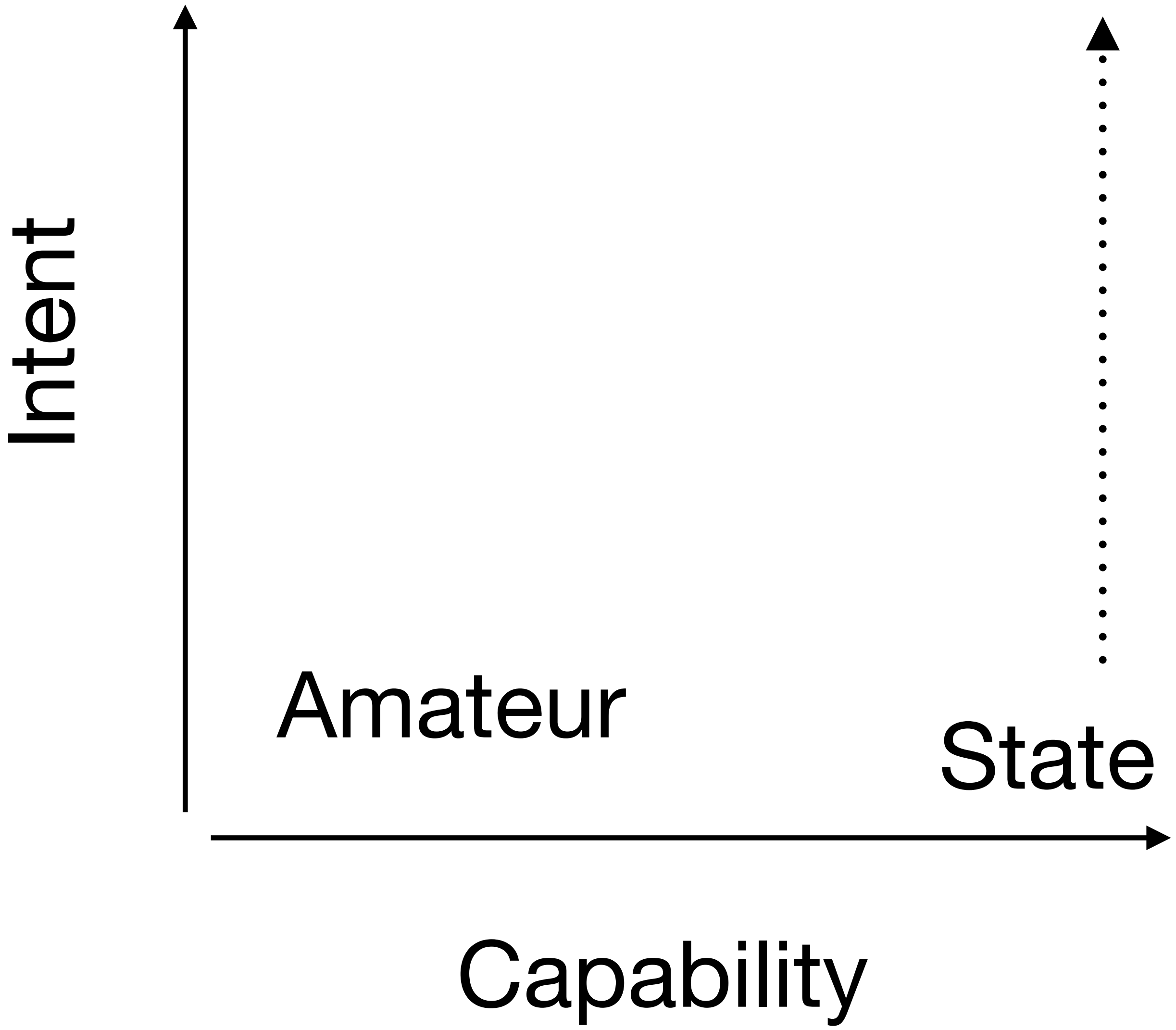
Exercise: Threat Actors

- Think about four different people or groups of people who might want to attack your business.
- Write down some statements about their capability: what can they do, and how well can they do it?
  - Think about this qualitatively (list the things) and informally quantitatively (how strong or weak?)
- Write down some statements about their intent: what might they want to do, and how likely are they to do it?

Examples

- Nation States: capability high, motive ?
- Fraud/Blackmail: capability medium, motive high
- “Script kiddies”: capability low, motive low
- Employees: capability medium, motive medium
- It’s difficult to enumerate them, isn’t it?

Examples



HMG #1 says

- Bystander (BY)
- Handler (HAN)
- Indirectly Connected (IC)
- Information Exchange Partner (IEP)
- Normal User (NU)
- Person Within Range (PWR)
- Physical Intruder (PI)
- Privileged User (PU)
- Service Consumer (SC)
- Service Provider (SP)
- Shared Service Subscriber (SSS)
- Supplier (SUP)

Bystander

- A Bystander is someone with authorised physical access to a place where the equipment within the focus of interest is located and/or account holders work, but with no business need to handle equipment or logically access the system. Typically this will include cleaners and visitors but could (for example) include hotel staff if portable equipment is left on hotel premises. (People with a need to physically handle equipment would normally be of type Handler).

Handler

- A Handler is someone whose business role requires physical access to the equipment within the focus of interest, but who is not a registered user and does not usually have logical access to the operational system, but may have temporary supervised access for test purposes. This includes people who transport equipment, test repair or replace hardware or dispose of obsolete or damaged equipment. This may also include postal or courier services.

Indirectly Connected

- An Indirectly Connected threat actor does not have legitimate or authorised business connectivity to the FoI. They may however, be able to access or make use of business or network connections because of onward connections from business partners or through networks to which the FoI has a direct connection e.g. the Internet. Where Departments have direct or indirect connections to the Internet this threat actor type could include all Internet users. This indirect connectivity could allow threat actors to mount business traffic-borne or network based attacks against the FoI.
- (FoI => Focus of Interest)

Information Exchange Partner

- An Information Exchange Partner is someone who needs, as part of their business, to exchange information with the focus of interest, whether through direct or indirect electronic connection or media exchange. The person may be an originator, recipient or both, of information in support of normal business. Note there must be a need to exchange information, not merely an ability to exchange information; people with the ability but not the need are Indirectly Connected.

Person Within Range

- A threat actor of type Person Within Range is someone who is in range of electronic, electromagnetic and any other emanations from the equipment within the FoI. This applies whether the emanations are unintentional, intentional or as the result of tampering, and hence is very broad ranging. In addition this threat actor type due to their presence within range of emanations, transmissions and communications may be in a position to jam communication paths. This type could be considered as including people who may:
- (TEMPEST, radio attacks, etc)

Normal User

- A Normal User is a registered user or account holder who uses the applications, services and equipment within the FoI to store, process, handle and exchange information in support of business objectives. These users would be provided with ‘standard’ facilities and system privilege as defined in the Departments [sic] policy.

Physical Intruder

- A Physical Intruder is someone who gains unauthorised physical access to equipment within the FoI, typically by breaking in to the premises in which the FoI equipment is sited. This may include the traditional office, data centres or locations where remote working is carried out.

Privileged User

- A Privileged User is a registered user or account holder who manages the applications, services, equipment and security defences within the focus of interest. A threat actor of this type can usually not be constrained in the same way as a Normal User and as such is modelled as a separate threat actor type.

Service Provider

- A Service Provider is someone who provides services to the FoI, including but not limited to, communications, shared databases, Internet access, web-site hosting, resource sharing, archive services or intrusion detection services and who by virtue of controlling that service could compromise any Security Property of the FoI.

Service Consumer

- A Service Consumer is someone who makes use of services advertised or provided by the FoI. Services provided by the FoI may require that consumers are registered for access control purposes or allow unregistered physical or logical access to a publically available service (e.g. an Internet website or ‘walk in’ kiosk). Service Consumers may use services provided by the system (such as view a website) but are not Normal Users.

Shared Service Subscribers

- A Shared Service Subscriber applies only where a shared service is within the reliance scope. A Shared Service Subscriber is someone who is an authorised user of services used by a FoI, but who is not a registered user of systems or services within the FoI. This threat actor could compromise the FoI by attacking the shared service. For example, a FoI may rely upon a shared service such as power distribution. If actions of other customers of that power distribution network make in unavailable, this could in turn affect availability of the FoI.
- Could this cover cloud tenants?

Supplier

- A threat actor of type Supplier is someone in the supply chain who provides, maintains or otherwise has access to software or equipment. This threat actor type may be aware of the system and its security characteristics and be in a position to provide equipment deliberately modified or configured to allow or facilitate compromise of any security property.

SSM 6: Defence in Depth

i.g.batten@bham.ac.uk

Recap

- Logging tells us what happened, and might allow us to spot patterns early

- Patched systems have fewer security problems

- Services that aren’t running can’t be broken into

- Services which aren’t listening are hard to break into

Defence in Depth

- Idea is that multiple defences add (multiply?) together to improve security
- If one defence is breached, there are others still standing
- Model has a long history…

Castles

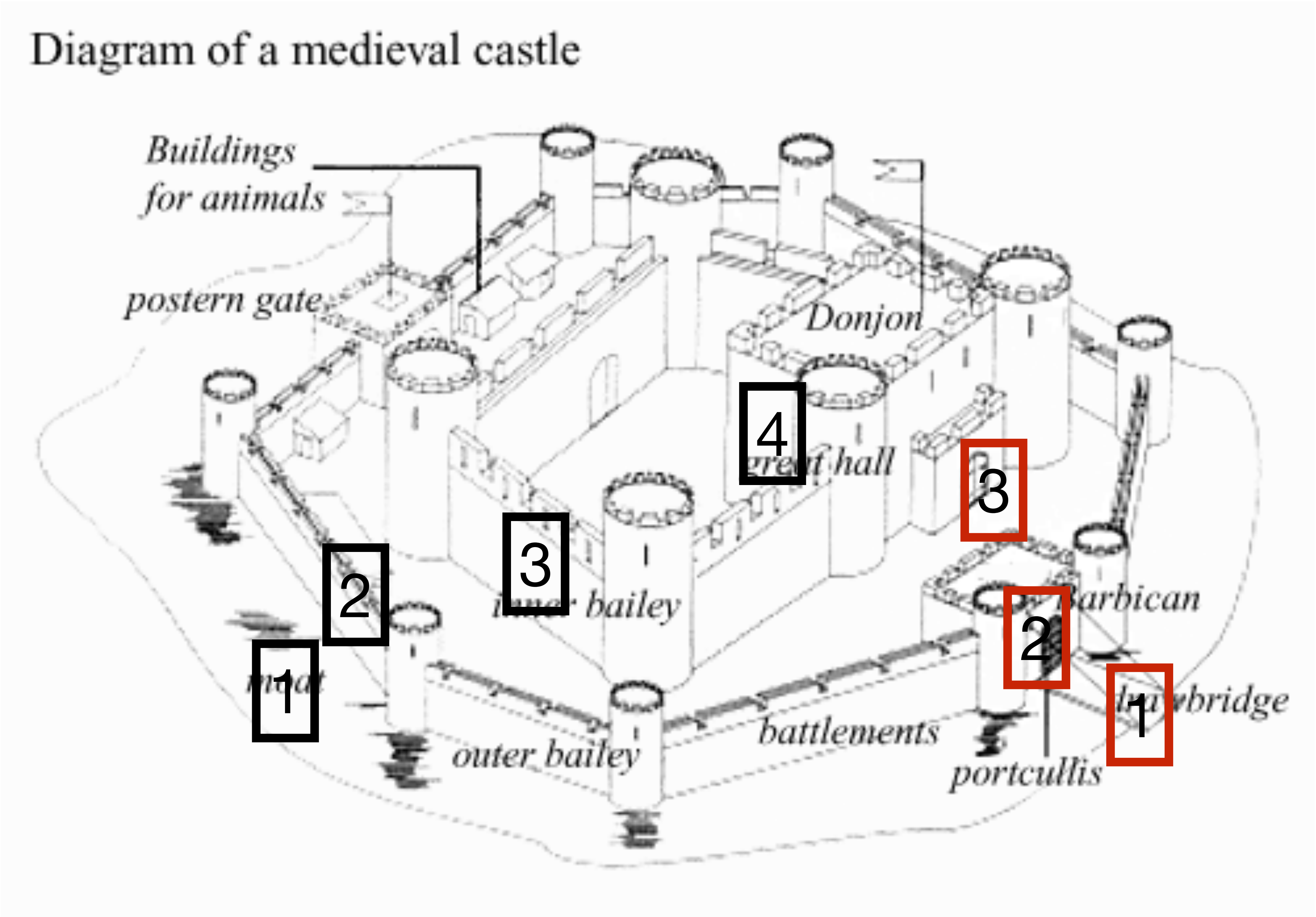


Diagram of a medieval castle

Problems

- Assumption that defences are independent
  - Not just physically or logically, but in terms of tools needed to break them
  - Attacker who can knock down one wall can knock down others
  - Attacker who can brute-force one encryption key and brute-force orthers

And can be counter-intuitive: which is safer?

When do planes crash?

- Takeoff is the riskiest phase of flight
- An aircraft accelerates down the runway until it reaches speed V_1, at which point it cannot stop before the end of the runway.
- It needs to get to V_2 (usually greater than V_1, except on ten mile runways), which is minimum safe climb-out speed.
- At some point (usually between V_1 and V_2) it will reach V_R, at which point it “rotates” (starts to take off).
- Engine failure between V_1 and V_2 is very dangerous
- Certification rules are “must be able to get from V_1 to V_2 with one engine failed”. Twins therefore have 200% power installed, Fours 133%.

Twin v Four not obvious

- Twin will crash on takeoff or goaround if two engines fail
    - (0.01 + 0.01) * 0.01 = 0.0002
- Four will crash on takeoff or goaround if two engines fail
    - (0.01 + 0.01 + 0.01 + 0.01) * (0.01 + 0.01 + 0.01) = 0.0012
    - Six times greater risk!

Reality much more complex

- Reality is much more complex, and complicated by the certification regimes for twin-engined aircraft over water (ETOPS) being much stricter than for fours, while fours can fly on two engines and often land.
- But having 200% of minimum take off power is preferable to having 133%

Independence

- But if a plane runs out of fuel, or enters a cloud of volcanic dust, all the engines fail, whether there are one, two, three, four or eight engines

For Information Security

- It is very tempting to think that having lots of defences equates to having defence in depth.

- But one strong lock is preferable to ten weak locks, as an attacker who can break a weak lock can break ten.

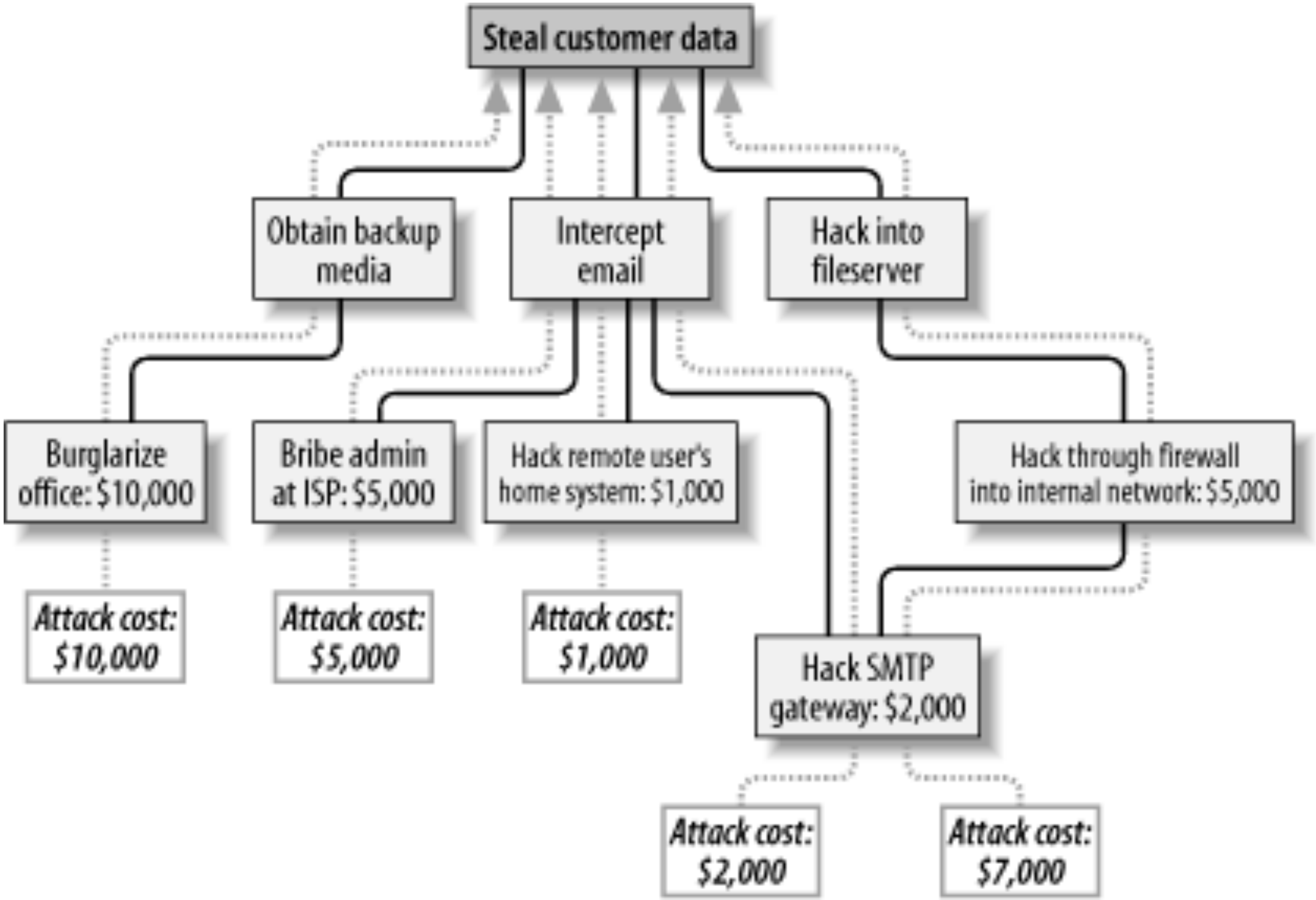
    - And a door with ten locks is weakened by ten sets of holes drilled in it.

- We need to make sure we are getting increased protection.

Attack Trees

- Build a tree, with the attacker’s goal at the top, and the various ways he might achieve that descending from it.

Example


Steal customer data

Obtain backup media

Intercept email

Hack into fileserver

Burglarize office: $10,000

Bribe admin at ISP: $5,000

Hack remote user's home system: $1,000

Hack through firewall into internal network: $5,000

Attack cost: $10,000

Attack cost: $5,000

Attack cost: $1,000

Hack SMTP gateway: $2,000

Attack cost: $2,000

Attack cost: $7,000

For each risk, controls

- Backups can be encrypted
- Hackable systems can be made less hackable
- Bribeable staff can be vetted, their jobs divided in two, etc.

Building attack trees is hard

- There is research work both on building them and on analysing them (ripe field for PhD).
- Looking for independence is hard, too

Exercise

- Take five minutes, and build an attack tree for changing your end of year marks on a marks database.

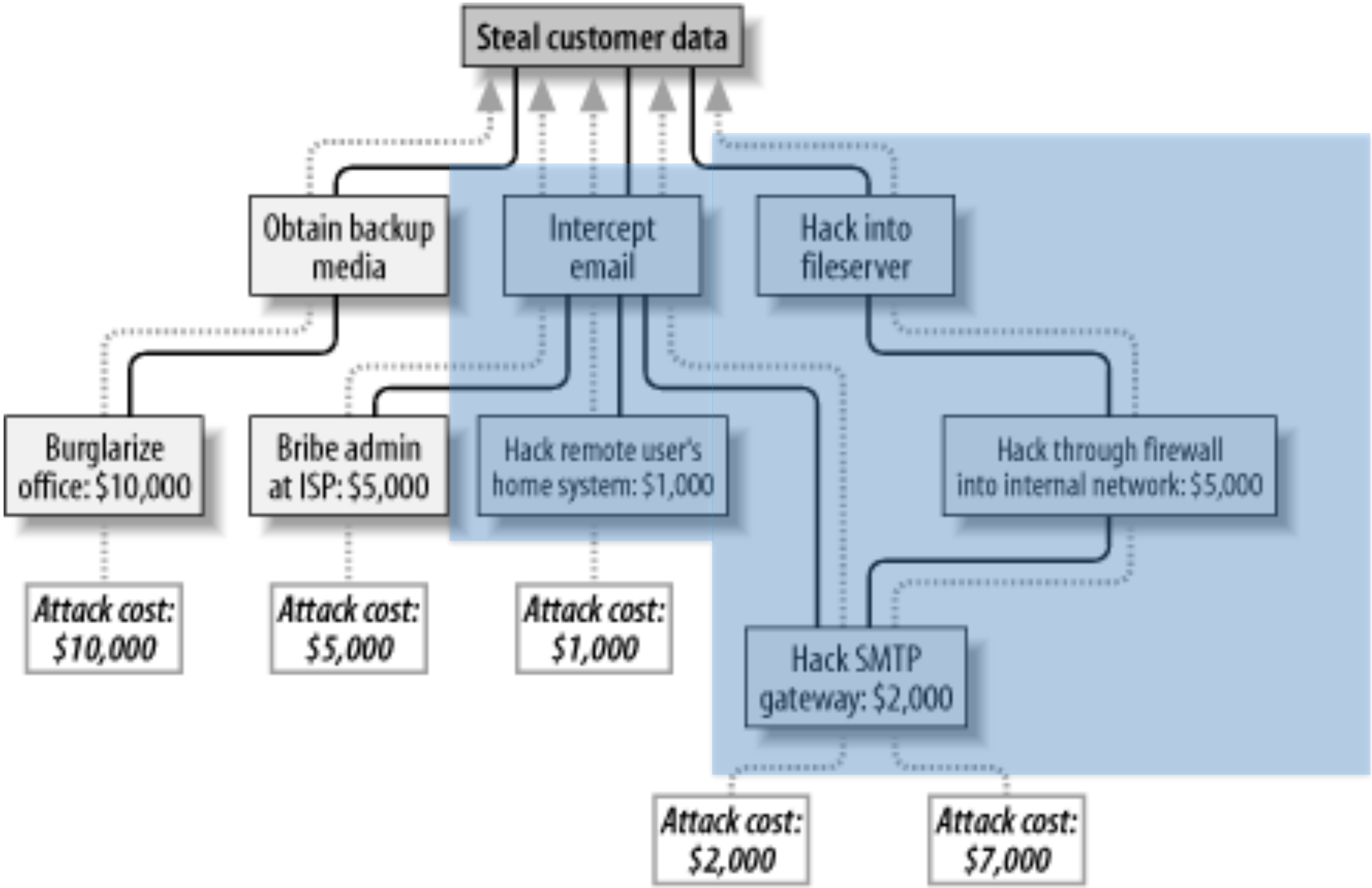
- Assume the database is on a computer, which is behind a firewall, which is administered by an administrator and used by lecturer

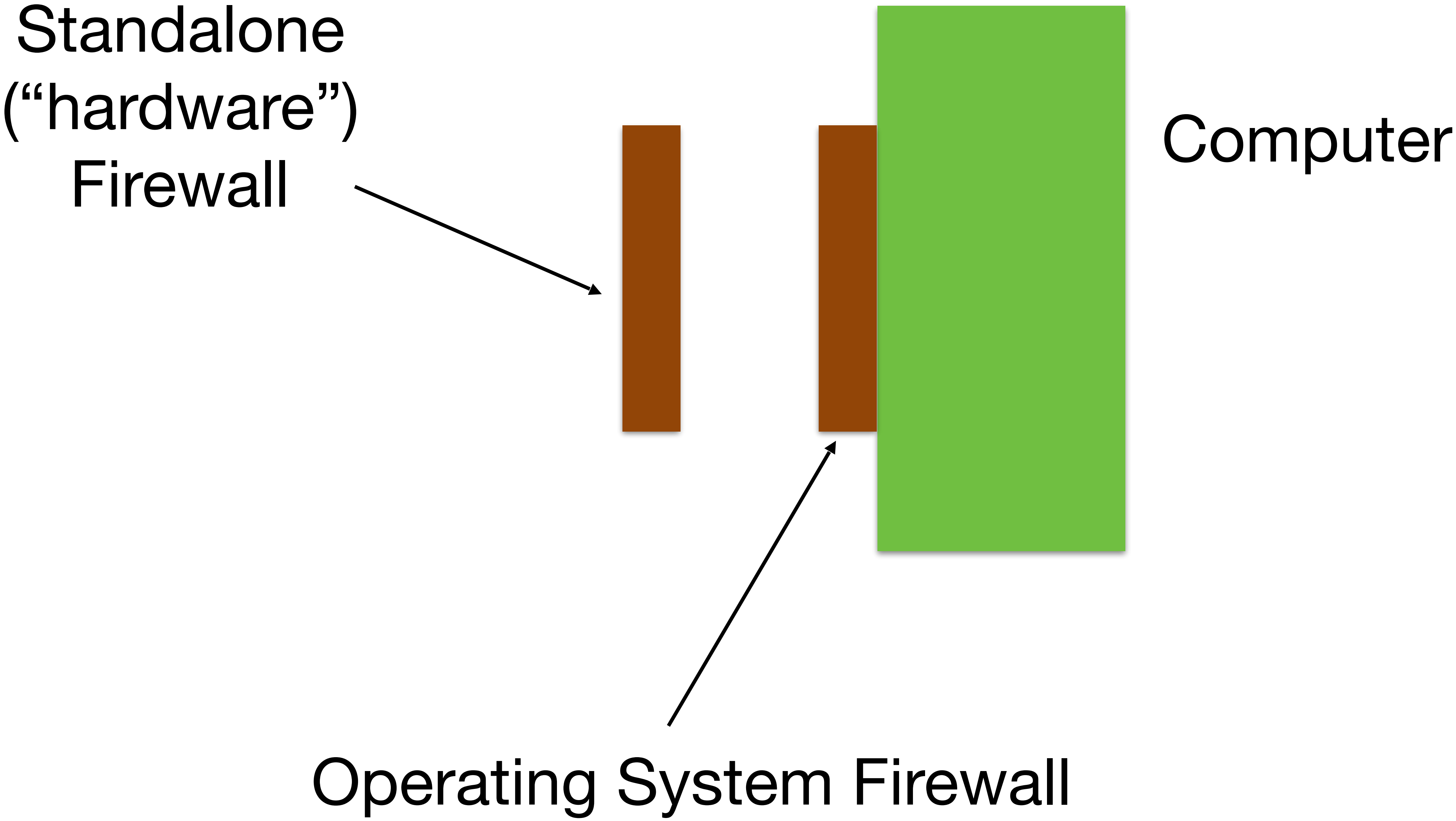
- Be imaginative

Depth?

- Tempting to think that a system protected by two firewalls (or whatever) both of which need to be hacked is more secure that a system protected by one.

Are these independent?





Standalone (“hardware”) Firewall

Computer

Operating System Firewall

Firewalls and Attack Surfaces

- You can filter packets using a firewall on a computer

- You can configure the services on that computer securely

- But an attacker who has a get-root privilege escalation attack can bypass both

Firewalls and Attack Surfaces

- You can filter packets using a firewall in a separate box, placed in front of a server

- However, if there is an authentication server which permits users to log in to the firewall and to the computer, an attacker who can attack the authentication server is admin on the firewall and the computer.

Complexity is hard

- In general, the more devices and elements are involved in a security solution, the less likely that it is accurately analysed

- Tradeoff between simplicity (and therefore ease of analysis) and defence in depth is not one that can be given a general answer.

Subsidiary Protocols

- Attack trees often miss attacks on “subsidiary protocols”.

- Classic example is DNS.

- Suppose I configure some access control mechanism (Apache .htaccess) to permit access to a sensitive document from secure.bigcorp.com.

DNS PTR records

- How do you find out the name of a machine from an IP number?
- For address 1.2.3.4, you form this name:
    - 4.3.2.1.in-addr.arpa
- And you look up the PTR record for that name.
- The 3.2.1.in-addr.arpa “zone” is controlled by the owner of 1.2.3.0/24.
- So they can add this record to the DNS.

Solution

- Attacker controls 3.2.1.in-addr.arpa, but does not control bigcorp.com.

- Solution is to follow up any query IP->name by looking up the name and checking that the IP number is one of the address records.

Example

```
ians-macbook-air:~ igb$ nsupdate -k update-key
> server offsite7.batten.eu.org
> update add 215.150.187.81.in-addr.arpa. 86400 in ptr gromit.cs.bham.ac.uk
>
> ians-macbook-air:~ igb$
```

```
ians-macbook-air:~ igb$ dig -x 81.187.150.215

; <<>> DiG 9.8.3-P1 <<>> -x 81.187.150.215
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4764
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;215.150.187.81.in-addr.arpa.  IN PTR

;; ANSWER SECTION:
215.150.187.81.in-addr.arpa. 86400 INPTR    gromit.cs.bham.ac.uk.

;; Query time: 107 msec
;; SERVER: 147.188.244.250#53(147.188.244.250)
;; WHEN: Tue Jan 27 14:26:00 2015
;; MSG SIZE  rcvd: 79

ians-macbook-air:~ igb$
```

```
ians-macbook-air:~ igb$ dig gromit.cs.bham.ac.uk

; <<>> DiG 9.8.3-P1 <<>> gromit.cs.bham.ac.uk
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32162
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;gromit.cs.bham.ac.uk.		IN	A

;; ANSWER SECTION:
gromit.cs.bham.ac.uk.	85439	IN	A
;; Query time: 6 msec
;; SERVER: 147.188.244.250#53(147.188.244.250)
;; WHEN: Tue Jan 27 14:27:02 2015
;; MSG SIZE  rcvd: 54

ians-macbook-air:~ igb$
```

Other Protocols

- NTP can be abused (but rarely is): if you really need accurate time and rely on it, then you need your own reference clock

- DHCP and other configuration protocols can be abused, but it is difficult to do remotely

SSM 8: Risk Appetite and Residual Risk

I.G.Batten@bham.ac.uk

Catchup

- We’ve been looking at risk assessment and risk treatment plans.

- **Risk Assessment** is the process of looking at our enterprise and evaluating the set of **risks** (undesirable things that might happen), how **likely** they are, and their **impact** (the cost of their happening).

- A **Risk Treatment Plan** is the process of choosing and applying a set of **controls** to address these risks.

Controls

- We talked about controls that **reduce** risks, such as firewalls, encryption, staff vetting and clear desk policies;

- And we talked about controls that **mitigate** risks, such as backups, anonymisation and segregation of duties.

  - Note that the distinction between reduction and mitigation will often depend on the detailed wording of the risk.

Today’s Topics

- Today we’re going to talk about the reality of producing an effective risk treatment plan
  - The difficulty of assessing the cost of controls
  - The difficulty of assessing the cost of failure
  - The issue of risk appetite: how willing an enterprise is to accept residual risk.
  - Why enterprises decide to accept risks they could in principle control.

Alternatives to controls

- Another approach to risk is to **transfer** it. By taking out an insurance policy, or outsourcing the function with an appropriate penalty regime, the consequences of failure become someone else's responsibility.
    - We will talk about this in more detail next week, but for example, by doing credit card handling via Paypal you pay additional margin in exchange for not needing to process sensitive financial information.
- And finally, you can **accept** the risk. Today I hope to convince you that this can be an active strategy, rather than an admission of failure.

Choosing Risk Treatments

- Development of a risk treatment plan is iterative
  - Apply some controls to reduce likelihood and/or impact
  - Look at the **residual risk**, ie the remaining likelihood and impact
  - Assess whether the residual risk is OK
  - If not, repeat.

How do we do this?

Goals of Risk Treatment

- Each step in a risk treatment plan should reduce either the likelihood of a risk occurring or the impact of that occurrence.
- The cumulative effect of all the controls should be to reduce the residual risk to an acceptable level.
- **So why isn’t the eventual outcome zero risk?**
- Security failures at high-security installations (intelligence agencies, for example) are not unknown, cf. Snowden.
- No-one cannot ignore cost, in the broadest sense.
- Some residual risk will always be present, either known and explicitly accepted, or unknown and implicitly accepted.

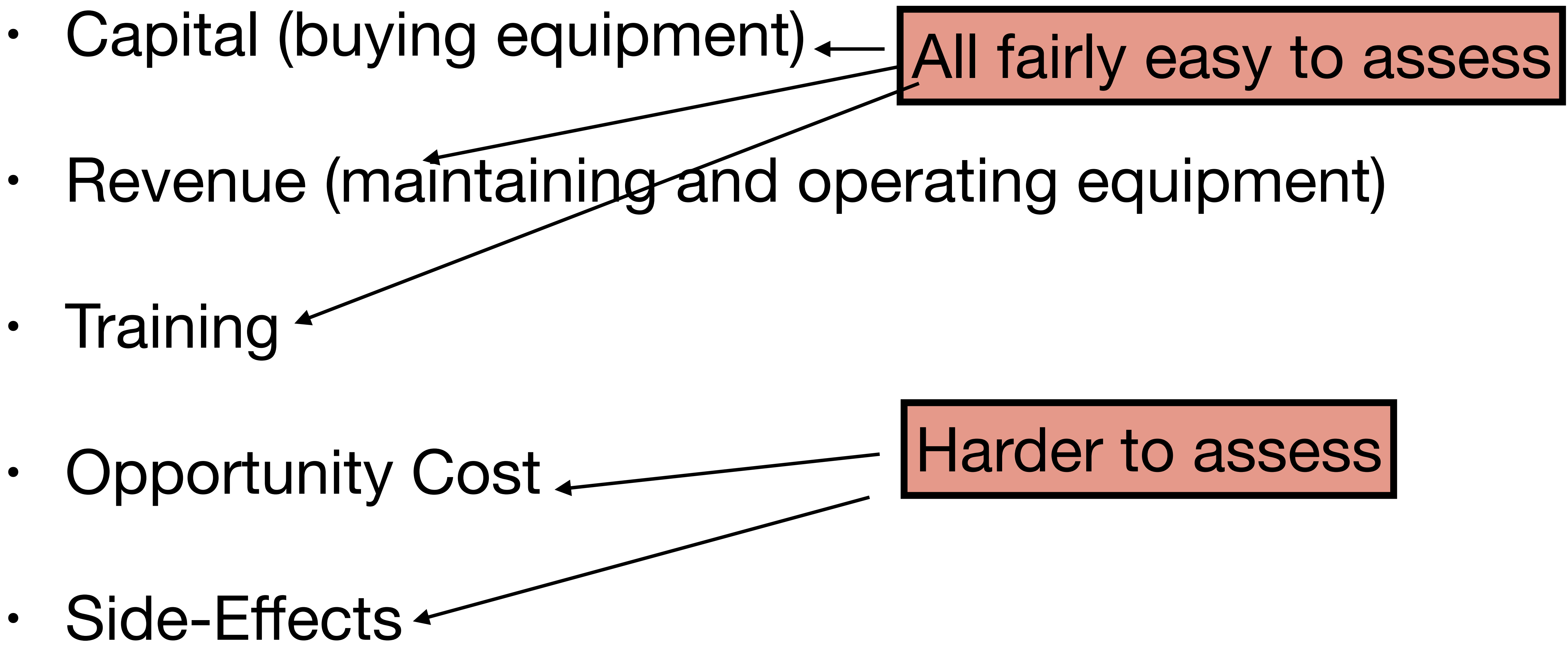
Zero risk is unachievable

- The concepts of risk assessment and risk treatment come from health and safety practice
- You might hope that workplace deaths are never acceptable, but in reality cost and practicality intervene.
  - **ALARP**: As Low As Reasonably Practical
  - It does often reduce to “putting a price on a life”.
  - Removing risks can be both expensive and difficult.
  - Consider North Sea drilling platforms: helicopter operations are inherently risky

Who decides *reasonably*?

Costs of Controls

- Very few controls are free to implement



  - Capital (buying equipment)
  - Revenue (maintaining and operating equipment)
  - Training
  - Opportunity Cost
  - Side-Effects

All fairly easy to assess

Harder to assess

Financial Case

- Direct cost of implementing a control is fairly straightforward to evaluate as it is “just another IT project”.

- Unfortunately, the payback is often harder to assess, as we cannot easily place a value on a security improvement which reduces the probability or impact of an already unlikely event.

Standard Cost Case

- Businesses make investment decisions based on:
  - the balance between cost and return
    - discounted by how long it takes to make a return (ie could you just put the money in the bank and get interest?)
    - discounted by how likely the project is to deliver its goals (is it a long shot or a sure thing?)
    - and weighed against what else could be done with the money (**opportunity cost**).
  - This is often done intuitively, rather than in fine detail.
- Problem for security controls (and compliance more generally) is that the costs are hard to quantify and return is very uncertain in size and timescale.

Opportunity Cost of Controls

- In standard business terms, this is “what else could I do with the money”.

- But also we need to consider “what are the **other** effects of this control on the business”.

  - Unintended consequences or **side-effects**

Side Effects

- **Direct**
  - These are consequences of imposing the control, irrespective of the way users respond
  - For example, tighter email policies may result in problems when staff are travelling, which cost money
- **Indirect**
  - These are the consequences of imposing the control caused by users working around it or other displacement of risk
  - For example, tighter email policies may result in problems caused by staff redirecting email to gmail, or even using it as their main account.

Indirect Side Effects

- Most staff, including managers, do not support information security policies if they impact on “real work”.
  - Compared to the security function, staff often assign lower probabilities and impacts to risks.
  - There are exceptions to this, and some organisations have very strong security cultures. But they are exceptions.
- Therefore, staff will sometimes attempt to work around controls, perhaps even with their managers’ support
- **The workaround may be worse than the original risk**

Email Policy

- Risk: access by threat actors to either an individual's email or the email of a larger group of people

- Impact: email can contain the most sensitive discussions within an enterprise

- Controls: encryption and other endpoint protection measures; VPN for access to servers.

- Example: competitor obtains CxO's laptop and tries to read email; cannot read data at rest because of encryption, cannot get more mail because of VPN with two-factor protection.

Problems

- CxO can’t read email as easily on the train (his phone doesn’t work as well as it did)

- CxO can’t read email at home as easily (doesn’t work on his own iPad while watching TV)

- CxO finds setting up the VPN “a bit of a faff”.

- CxO loses two factor token

Possible Workarounds

- CxO asks secretary to forward email to personal gmail account
    - No two factor, accessible to Google for data mining, data protection and other issues
- CxO starts to use gmail account as shadow email account for “real work”
    - Data outside any corporate governance, audit, etc. Illegal in some contexts (ie, Sarbox, FCA/PRA regulated businesses).

Total Cost is not just money

- Direct costs easy to evaluate under standard project management assumptions
- Side effects require thought to work through, and can be hard to predict and value
  - You should never underestimate the ingenuity of users in foiling your best intentions

But even if we know costs…

- …we often struggle to value the benefit the business will get from our additional control. What is it worth to reduce a risk of catastrophic failure from 1% per annum to 0.1% per annum?
- Much security work is about reducing the incidence or impact of already rare events
- Justification often involves even rarer worst case outcomes.
- The extent to which we worry about worst cases is one of the factors making up our **risk appetite**.

Let’s go on holiday

- Suppose we are travelling to the USA

- In our bags we will have our laptop, the usual assortment of electronics, our elegant designer wardrobe, etc.

- American medical costs are very high; a broken arm can be tens of thousand of dollars, a heart attack hundreds of thousands.

- Do we need travel insurance?

- If travelling on business, does our company need travel insurance for us?

What is insurance?

- At its simplest, insurance is a bet on an event happening

- The person taking out the insurance “wins” if the event occurs and they receive a payment; the insurer “wins” by keeping the premium otherwise.

- The insurer prices the bet at their view of the likelihood, multiplied by their view of the potential payout, plus a margin to make the business worthwhile to them.

Self-Insurance

- So if you can afford the **maximum** payout, and are going to be travelling frequently, a rational view is to **self-insure**

  - I’ve never claimed on travel insurance in thirty years, and can afford to re-buy my luggage, elegant wardrobe and all.

- Some people may regard paying a small premium as worthwhile to avoid the risk of a larger cost; others may reckon that over time the sum of the premiums will be greater than the sum of the payouts (as will be the case if the insurer is pricing accurately). This reflects their **risk appetite**.

Risk Acceptance

- Very few people, or companies, could afford the maximum medical bill that might be incurred (potentially tens of millions of dollars) but the chances of this are very small

- You might feel able to self-insure broken arms, and a business certainly could if they had many staff travelling

- Although an employer who just **accepted** the risk of not being able to pay larger medical bills would be acting illegally, an individual might opt to do so.

Risk Appetite

- The decision as to which risks you insure against is a matter of **risk appetite**. Insuring against everything costs money, but removes the risk of being out of pocket. Insuring against nothing saves money if nothing goes wrong.
- Individuals, small businesses, large businesses may make different decisions.
- For example, very large organisations (BCC, BT) don't carry buildings insurance; until recently, BT didn't carry car insurance. UK government carries no insurance.
- Companies often take out policies with very large excesses to reduce the cost of the insurance. They partially self-insure.

Security Risk Appetite

- The decision to buy or not buy insurance is just a matter of expense: in general, there is no downside to taking out an insurance policy other than not having the premium available to buy other things. The total cost is just the monetary cost plus any opportunity cost.
    - Risk homeostasis probably less of a risk than for individuals, as commercial policies have huge excesses and people taking the risk don't know about the insurance
- Unfortunately, additional controls in your security management system will usually have side-effects which are harder to price.

Cost and Return

- So far we have been talking about how hard it is to cost the controls
- But we also need to cost the impact, and again here we have problems
- The tendency is to over-state cost of failure.

The CxO’s Mail

- Assume our threat is “CxO’s mail device is lost”
- The most likely outcome is “it gets wiped and turns up in Cash Converters”, which is a £500 failure; most businesses self insure the loss of portable equipment.
- Even if the email is read, the chances of it being read by a hostile and interested opponent is small
- And even if your key competitor reads your most secret plans, the business effect may be quite small: it will assist their competitor intelligence people, but they already know a surprising amount (sometimes more than you do!)
- The downsides described earlier are there every day.

Confidentiality Failures

- Suppose that a university leaked its entire student record system

- It is safe to say that it would be excruciatingly embarrassing

- But students can obtain most of their record via the Data Protection Act, and the concrete impact on a student of others seeing their record is small

- The value to the university of reducing this risk is more than zero, but would they be willing to spend a million to make it a “once a century” event?

Integrity also important

- Suppose a student were instead able to modify their student record (not a theoretical risk!)
- It could result in the granting of a degree that the university should not have granted.
- One “bad” degree per year would be a failure rate of around 0.01%. Other errors in assessment and process may be more significant.
- Again, the cost to the university is more than zero, but should they spend a million pounds to prevent it?

Costs of Failure

- Maximum fine from ICO, which will only be payable in the case of egregious negligence, is £500 000. GDPR raises the maximum, but the actual fines imposed are as yet unknown.
- Having an approved ISO 27001 security management system will usually satisfy the ICO that reasonable steps had been taken, even if there has been a breach.
- Reputational harm is difficult to measure, but anecdotally most enterprises survive (people are surprisingly willing to accept security cannot be perfect)
- Financial costs arising directly from failure depend on nature of business, but in many cases are small and/or extremely unlikely, and amenable to insurance (**transfer** of risk).
- Failure **is** an option.

Who sets appetite?

- Risk appetite is a function of strategic management
- In a business, usually CEO or board level
  - Financial organisations have risk appetite committees at senior level, as it is fundamental to their business and is part of their regulatory obligations.
  - Other enterprises should consider security risk appetite at an equivalent forum.
- Residual risk statement also approved at this level.

What do security staff do?

- Security staff liaise with senior management to establish risk appetite.
    - Senior management will not expect zero risk, and will not want risk concealed.
- Worst case for a CSO: an untreated risk occurring which senior management were not given the opportunity to consider treating.

Perverse Incentives

- This is the observation that sometimes staff are driven by their own targets to do things which are bad for the enterprise overall.
- Security policies must improve the overall operation of the company, not just reduce theoretical risks at the expense of the wider good.
- Measuring security staff only on security is a bad idea!

Summary

- Controls cost money, and also have other impacts on the enterprise
- Failures are difficult to cost, but simply assuming the worst case may not be sensible
- Risks can be transferred or accepted rather than controlled
- Risk appetite and hence residual risk is a function of senior management, who should be given options.
- Incentives for security should be aligned with the enterprise.

Testing the system

I.G.Batten@bham.ac.uk

“Tiger Teaming”

- aka Red Team, “ethical hacking”, penetration testing, etc, etc.
- Very popular, very trendy, probably great fun to do

Objective

- People with skill are employed to “break” your security
- Tests both security policy and security execution
- Can be done by your own staff, by small outside companies, or offered as a service by large audit and security companies
  - Who might outsource it, of course

Positive Results

- If they don’t break in, you presumably don’t have gaping open doors in your security
- Provides some confidence that your security policy is capable of providing some security
  - Of course, that assumes the tiger team aren’t idiots

Negative Results

- Shows you that there is at least one flaw in your security, how it was exploited and (ideally) how to fix it.
- Might be policy, might be implementation, might be execution…but you should be able to figure it out.

Problems

- Tiger team **motivations** are potentially different
- Tiger team **resources** and economic **incentives** aren’t realistic
    - (particularly, “give up and try the next company” less attractive to them)
- Tiger team **legal position** different
    - Less likely to use firearms and kidnapping: they don’t have a “Get out of jail free” card

Freedom to Break Law?

- Extremely unlikely tiger team will be granted permission to commit criminal offences
- Companies can give *de facto* permission by failing to report or provide evidence, but cannot give *de jure* permission in case of assault, document fraud (in UK law, at least, possession of forged ID documents is an offence in its own terms) etc.

Problems

- More likely to end up finding obscure technical weaknesses whose economic value to an attacker may not be great
- Less likely to find internal process and personnel weaknesses, as not their focus
- Also cannot blackmail, bribe or otherwise suborn staff without possible legal consequences
- Great fun for managers, though.

War Gaming

- Like a tiger team, but a paper exercise
- Instead of trying to break into the real enterprise, an exercise is conducted in a room, with the paperwork to hand, and referees to adjudicate “battles”.
- Has the disadvantage of being entirely unrealistic
- Has the advantage of allowing examination of illegal acts
- Expensive, and not as exciting for managers

Hostile Audit

- Usually there is tacit understanding with auditors that they aren’t there to tear the whole system apart
- Most auditors are being paid by the people being audited, and want repeat business
- Sometimes you can get auditors who don’t have those sort of constraints, for example internal security people in a large multi-national
- They can “white box” examine systems and processes and report

Learning Lessons

- Main problem with all these approaches is **WHAT DO I DO NEXT?**
- Is a security system which consists of patches applied to fill individual holes worthwhile?
- Hence continuous improvement needs to look at root causes

Exercise

- Suppose a tiger team penetrated the network by using a security vulnerability on a machine which hadn’t been patched.
- That’s all you know: “there was a machine, it wasn’t patched”.
- What might be the reasons it wasn’t patched?

Causes

- Failure of patching
- Failure to try to patch
- Failure to include in list of machines to match
- Failure to include in list of machines that matter
- Failure to firewall
- Failure to audit
- …

Root Cause Analysis

- Is the solution:
  - apply the patch?
  - revisiting patching policy?
  - revisit security awareness?
  - revisit top-level security policy?
  - What else?

Not on Asset Register

- Just add it to the asset register?
- Look at the scope document?
- Check how the asset register was built?

AAIB / RAIB

- Air accident investigation board (used to be "branch")
- Rail accident investigation board
- Their reports are detailed, dispassionate and find root, root causes

G-BJRT, June 1990

- Windscreen failed on a BAC 1-11 flying out of Birmingham airport
- Pilot partially sicked out (this is not a real photograph, it's a reconstruction)
- Problem was traced to careless use of bolts that fitted but weren't long enough, uncalibrated torque wrenches, a whole host of issues
- "84 of the 90 windscreen retention bolts were 0.026 inches (0.66 mm) too small in diameter, while the remaining six were 0.1 inches (2.5 mm) too short."

Root Cause Analysis

- Time consuming
- Expensive
- “What’s the point, we know anyway?”
- Absolutely vital

SSM: Metrics

I.G.Batten@bham.ac.uk

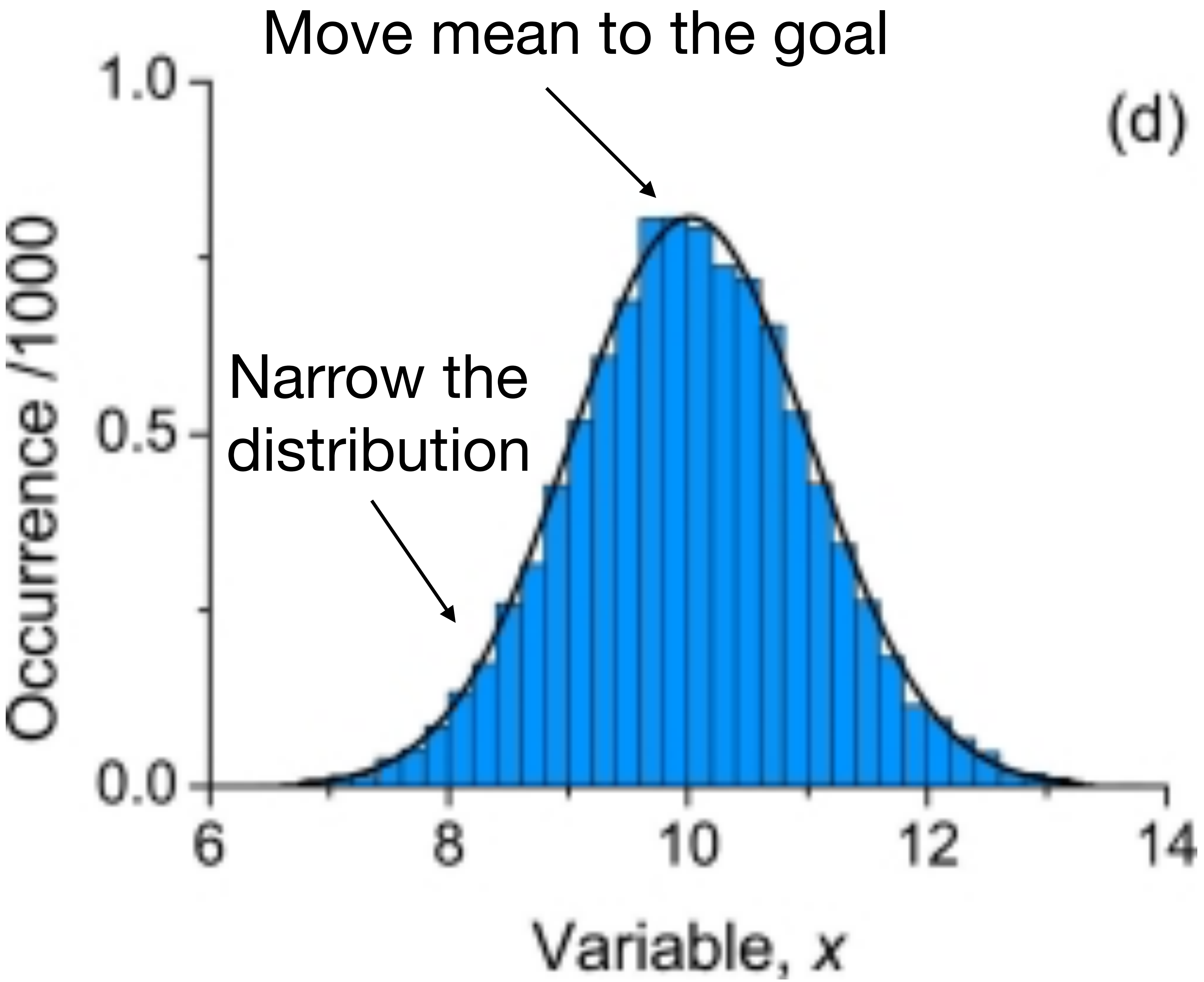
Purpose

- ISO 27001:2005 talks about plan-do-check-act improvement (which comes from ISO9001)
- ISO 27001:2013 is less prescriptive about the *how*, but still demands continuous improvement (so six-sigma, for example, is now compliant)
- How do we measure the effectiveness of our security system so that we can improve it?

The Problem

- Most of the things we are really worried about are rare, high-severity incidents
  - A few viruses (virii or viri is both wrong and very pretentious), the occasional phishing email: are these serious?
  - There will be constant ratting of the background radiation of the internet against your firewalls
  - And people will be constantly trying to break into ssh and web servers
- What should we measure?

Manufacturing is easy (!)



Security is harder

- Not a production line
- Measurement not an inherent part of the process
- Data collection harder and patchier

Proxy Outcomes

- Common problem in health trials
- Because we cannot measure what we want (reductions in long term mortality and long term morbidity) we instead measure a proxy for it (cholesterol, blood pressure, BMI).
- This is fine, as long as the proxy really is a very close correlate of the thing we really want to improve

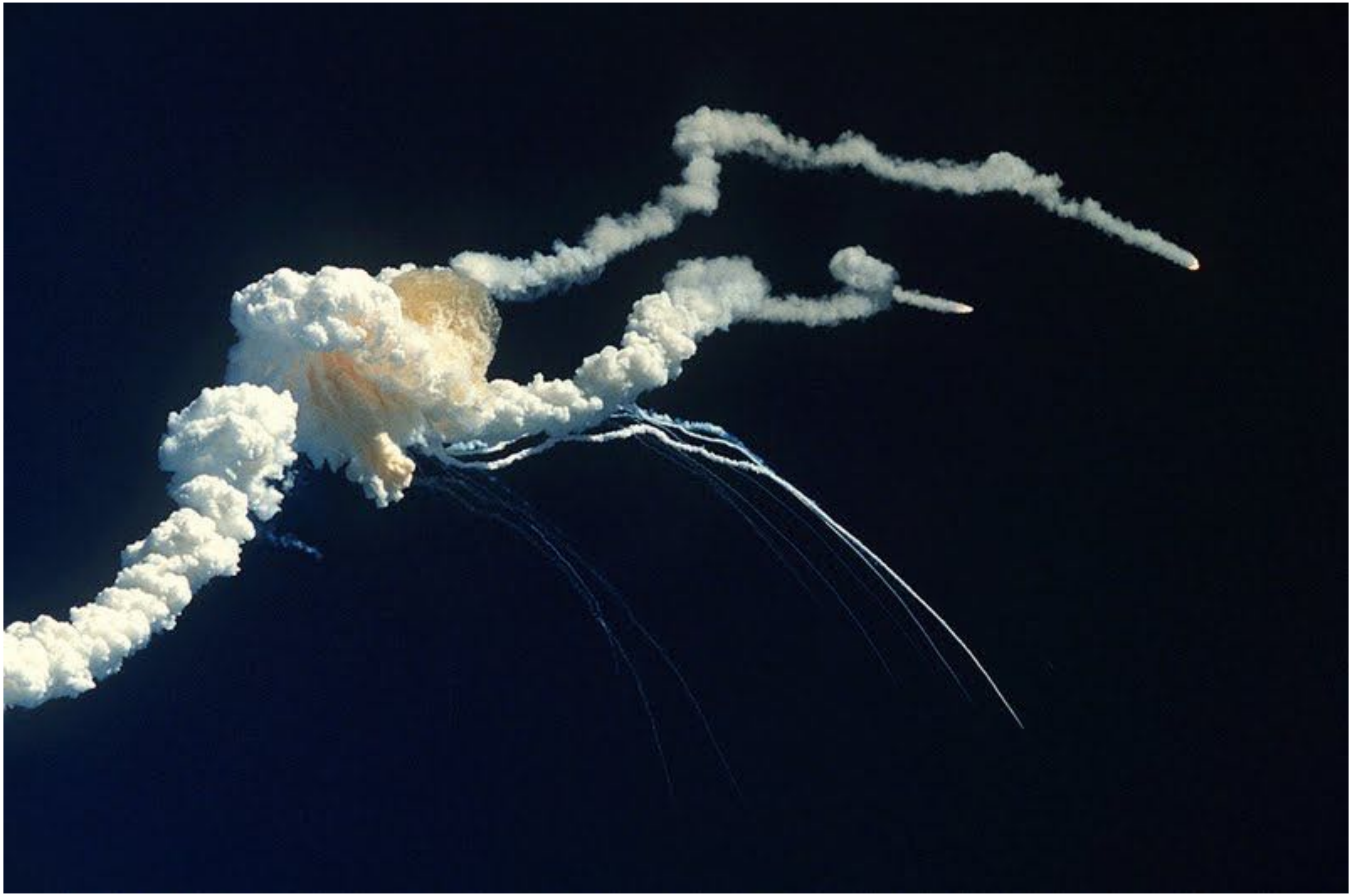
Proxy Outcomes

- Easiest to focus on things that we see a lot of: viruses hitting external email servers, packets hitting firewalls, systems being patched
- Is it better if those numbers go up, or down? Well, it all depends, and that makes use of them very dubious.
- Are we doing better or worse if we double the number of viruses we detect?
- Is our OS vendor releasing more security patches a good thing or a bad thing?

Some are OK…

- Measuring successful restorations (and more importantly failed restorations) is probably a reasonable measure of backup coverage
- Measuring downtime caused by disk failure is a reasonable measure of risk associated with storage redundancy
- But these are tenuous as security: this is more ITIL/ Business Continuity stuff

Who recognises this?

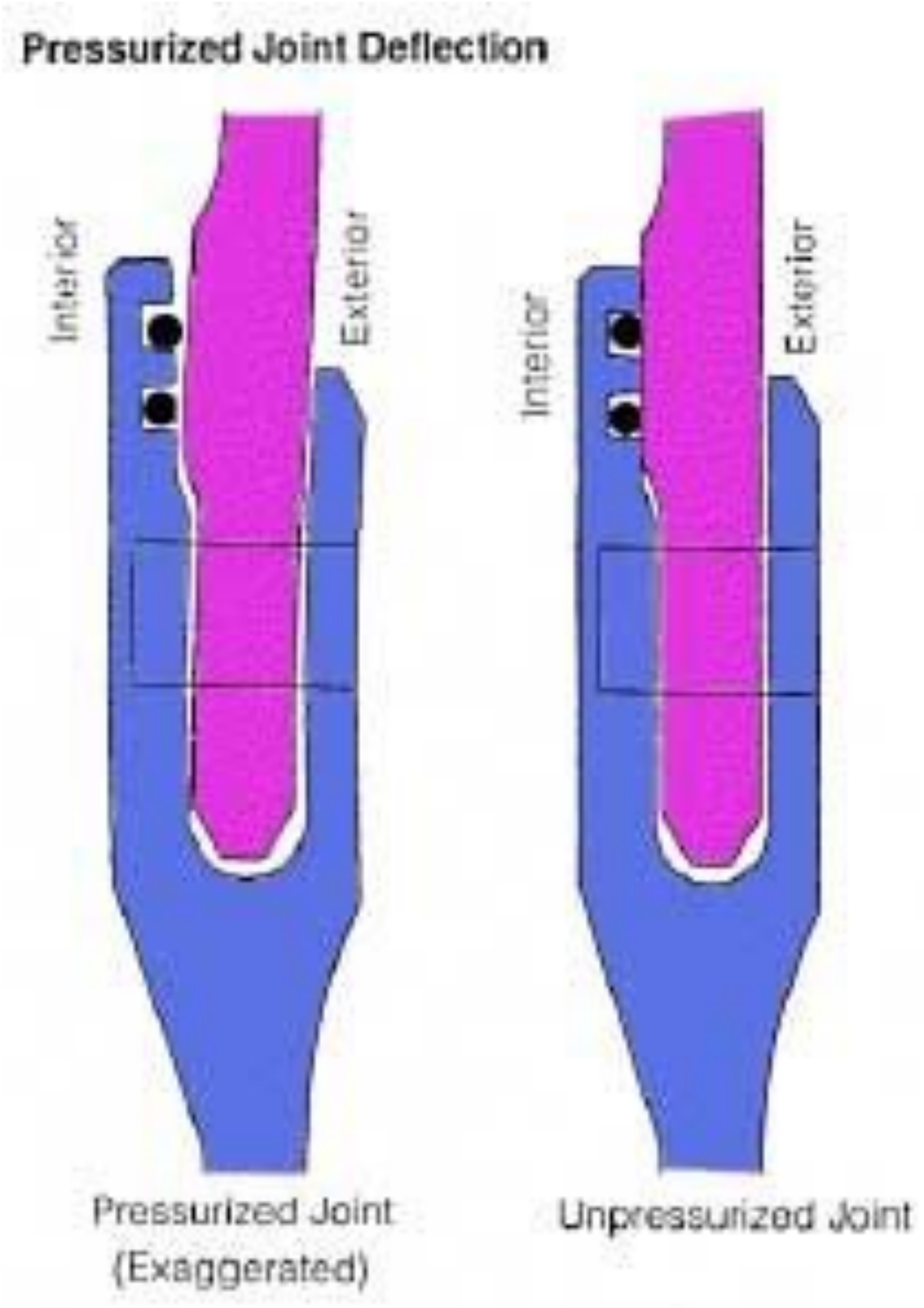


Safety Margins

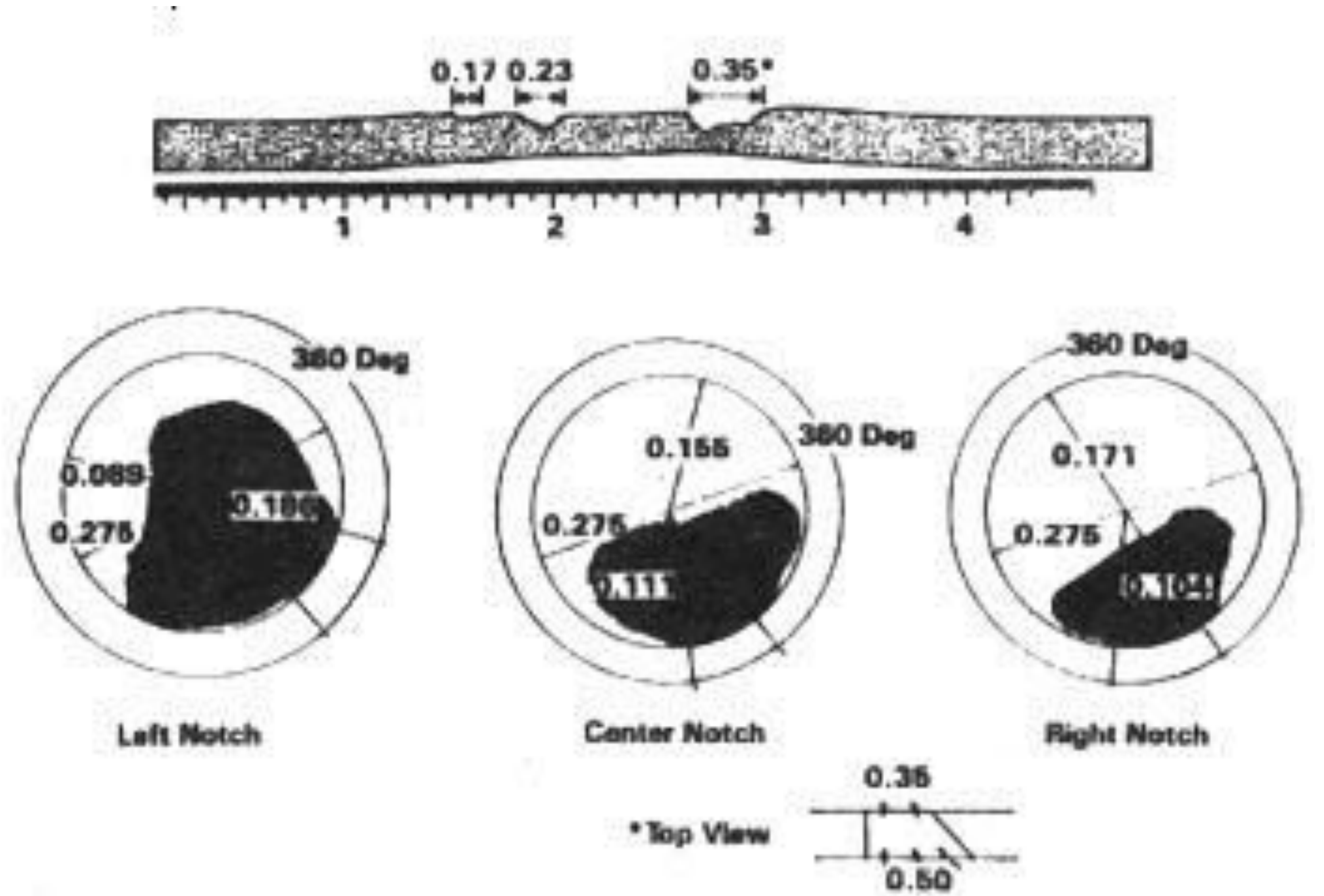
- Challenger accident, Jan 28 1986
- *Challenger*, a US space shuttle, exploded 73 seconds into mission STS-51L, killing everyone on board.
- Complete and utter failure of safety engineering
- Every engineer should read **Feynman's Appendix F** to the report at least once a year
- http://science.ksc.nasa.gov/shuttle/missions/51-l/docs/rogers-commission/Appendix-F.txt

Myth of Safety Margin

- Accident caused by O Rings on large solid-fuel rocket failing
- Design said they should never be eroded



In fact they were being cut through by hot gasses, up to a third of their diameter being eroded.



In spite of these variations from case to case, officials behaved as if they understood it, giving apparently logical arguments to each other often depending on the "success" of previous flights. For example. in determining if flight 51-L was safe to fly in the face of ring erosion in flight 51-C, **it was noted that the erosion depth was only one-third of the radius. It had been noted in an experiment cutting the ring that cutting it as deep as one radius was necessary before the ring failed. Instead of being very concerned that variations of poorly understood conditions might reasonably create a deeper erosion this time, it was asserted, there was "a safety factor of three."** This is a strange use of the engineer's term ,"safety factor." If a bridge is built to withstand a certain load without the beams permanently deforming, cracking, or breaking, it may be designed for the materials used to actually stand up under three times the load. This "safety factor" is to allow for uncertain excesses of load, or unknown extra loads, or weaknesses in the material that might have unexpected flaws, etc. If now the expected load comes on to the new bridge and a crack appears in a beam, this is a failure of the design. There was no safety factor at all; even though the bridge did not actually collapse because the crack went only one-third of the way through the beam. **The O-rings of the Solid Rocket Boosters were not designed to erode. Erosion was a clue that something was wrong. Erosion was not something from which safety can be inferred.**

“Defence in Depth”

- Common metric is to look at systems further in to measure effectiveness of outer perimeter
- So drop in IDS incidents on internal network implies that outer firewall is working
- Or does it imply that the IDS isn’t working?
- Or that the threat has changed?
- After all, the firewall is intended to pass **no** threats!

User Metrics

- Which of these seem like good metrics?
  - How often do users change their passwords?
  - How often do users forget their passes?
  - How often are laptops stolen?
  - How often are desks left unclear?

Good metrics

- Drive sensible behaviour
- Link clearly to security objectives, rather than just controls
- Have clear derivatives (ie, you know whether increase or decrease is better)

Five minutes…

- What would be some good metrics for the work you were doing for the exercise?
- Do they prove controls are working, or are just installed?
- Do they support policy?

Audit

- Internal audit is a very powerful tool
- Difficult in companies that don’t have a strong ISO9000 culture; internal audit teams are expensive and their skills are quite rare
- Also tend to be pariahs in the business: no-one likes the auditor when they turn up

Audit does two things

- Is the process being followed, with controls in place and records being kept?
  - This probably doesn’t require strong domain knowledge, and is about checking documents against reality
- Is the process worthwhile, with controls that meet the objectives?
  - Does require strong domain knowledge, and unlikely that your general-purpose audit team can help. Consultants and/or external auditors

Audit as Metric

- You can graph the number of successful audits, and the number of actions arising and being cleared
- Provided that your audit team is effective, this can work very well
- Probably only a solution for large companies, perhaps with a manufacturing slant

Financial Audit

- Note that today, your company’s financial auditors will want to do an IT security audit as well.
- You need to pass this, but it will probably not be useful as a wider measure of effectiveness: baseline only.

Governance

I.G.Batten@bham.ac.uk

Business Time!

- Several of you have said that you don’t have a background in businesses and would like clarification of terms.
- **Please** stop me and **ask** as we are going along.

Governance

- How are decisions taken?
- How are decisions ratified and embedded?
- How are decisions checked?
- How do we get better?

Small Companies

- The owner, CEO, COO and shareholders may be the same person, or will be the same small group of people.
- Decisions are signed off by them
  - Small companies notorious for poor delegation
  - No oversight on decision making

Large Companies

- Big decisions taken by various committees
  - Board report directly to shareholders via AGM
  - Below that various operational committees reporting to CEO or other board member
  - This isn't a business course: the arrangement at the top will vary, and there may be several layers of "board" like functions.

Governance Matters

- Idea is that decisions are taken by defined people, in a defined way, and generate defined records both of **what** was decided and, more importantly, **how** it was decided.
- If things go wrong, clear audit trail of what was done, and the **how** allows lessons to be learnt.
- 2008 Financial Crisis result of very poor governance, poor decision making, poor record-keeping (CDOs, CDSes aggregate risk)

IT Governance

- Our risk assessment and controls:
  - Expose the company to risk (residual risk)
  - Expose the company to direct cost (the controls)
  - Expose the company to indirect cost (the controls again, as we discussed)
- This needs to be done properly, for the good of the company and of the IT people

Ideal Structure

- A security team headed by a Chief Security Officer (CSO) perform the risk assessment, produce a risk treatment plan and define residual risk (CSO probably has other, non-IT responsibilities as well)
- They present this to the CEO and/or board (note: CEO will probably be a member of the board, other CxOs usually aren't)
- Once agreed, the Chief Information Officer (CIO) does what the board tell him to, with the CSO monitoring.

Reality

- Sometimes the CSO reports to the CIO, rather than directly to the CEO.
    - Discussion: what do we think about this?
- Sometimes the CSO relies on the CIO for staff and resources (ie is independent in name, but not in practice)
    - Discussion: what do we think about this?

The Wild West

- I have somewhere at home a book entitled “How to lie with accounts”, complete with strategies for mis-using your pension fund
- 1970s, 1980s, companies were free to do what they wanted with “their” money

The background

- Succession of scandals in the UK (“Maxwell”, notably) and the US (“WorldCom”, “Enron”) in which employees, pensioners and shareholders variously lost a lot of money.
- Failures of governance and audit meant CEOs (corrupt and/or stupid and/or malign) and their close associated were able to do what they wanted.

Responses

- In the UK, stronger powers for regulators, particularly the (then) Financial Services Authority and the Serious Fraud Office (power to compel testimony, “regulated persons”, etc).
- In the US, the Sarbanes–Oxley Act of 2002 (aka “Sarbox” and “SOX”).
- In Japan, complex legislation colloquially known as “J-SOX” (Japanese SOX).
- Intent to strengthen audit and shareholder protection.

Section 404: Assessment of internal control

- Requires management, under criminal penalties, to report financial risk to shareholders and the SEC.
- Most large companies have a US presence and are traded in a New York stock exchange, hence SOX 404 is a factor in their operation.
- Similar rules apply in the UK, particularly in the financial sector (“FCA” — Financial Conduct Authority and “PRA” — Prudential Regulation Authority) and elsewhere.

What’s involved?

- Essentially, like an IS1 assessment but for money
- Looks at threat actors who want to take money or are otherwise in a position to harm the company
  - Needs to deal with stupidity, well-intentioned bad decisions, etc, as well as criminals
- Looks at controls
- Establishes residual risk

IT is a component

- The IT controls are obviously a key part of this
  - Access to funds and stock
  - Access to customer data
  - **Accuracy of reporting**

Reporting

- This is something on the edges of this course, but worth talking about for a few minutes
- When we look at information assets, one thing we are concerned with is threat actors altering the data (Integrity).
- But a bigger risk is that the data was wrong to start with (missing a warehouse, using the wrong currency, using incorrect formulae for net present value, Y2K, Y2k38, etc).

Just as an aside

- Year 2038 problem occurs at **03:14:07 UTC on 19 January 2038**
    - Peak of your careers
    - I hope to make some money in retirement, doing remediation
- Unix timestamps were historically seconds counted from 00:00:00 1 Jan 1970, using a **signed** 32 bit quantity
- Rough calculation: 2^31/(86400*365.25) = **68**.04, 0.04*365.25 = **18**.13, 0.13*24 = **3**.12, 0.12*60 = **8**.
- That's right to within a few minutes (it's also complicated by leap seconds, 365.25 not quite being right, etc).
- Thankfully 2000 was a leap year!
- Wraps around to 1/1/70 - 68.04 years = 13 December 1901.

Risks in Reporting

- Finance and IT usually maintain large ERP reporting solution (Oracle, SAP, etc).
- Heavily audited, likely to be as correct as it can be
- However, most actual reporting done by extracting data from central system, putting it in a spreadsheet and “doing stuff”. Staff doing this are often neither IT nor accountants, and very rarely both.
- Cf. the missing warehouse

Finance meets IT

- So as part of a Sarbox exercise, reporting will be analysed from where it is used all the way back to central systems
    - Confidentiality, Integrity, Availability, with Integrity including Correctness
    - Will throw massive pressure onto security of some laptops

Suddenly…

- IT decision making is part of a legally-accountable corporate structure
- Board and others can receive **criminal penalties** (America is notoriously tough on White Collar Crime, cf. the Nat West 3).
- So our IT governance needs the same controls and accountabilities as our financial governance

Structure

- Security Governance Committee, drawing from over the whole business
  - Required by ISO 27001, but not really specified in enough detail
- IT, Finance, HR as a bare minimum
- Should ideally report to board or CEO
- **Should not** report to CIO (mistake I made)
- CEO will need to resolve conflict

Delegation

- Day to day, the CSO and CIO will need to do their jobs without asking the committee for detailed permission to do small tasks
- But strategic decisions must be taken with agreement of committee, although CSO will obviously lead (ie, present a paper for approval).
- Committee can refer really difficult stuff upwards
- Key point: **detailed minutes**.

Don’t…

- Conceal decisions
- Lie
- Assume you know better
- Pick favourites amongst departments
- Assume that because you look after the data you own the decisions

ISO 27005 Risk Management

I.G.Batten@bham.ac.uk

27005 supports 27001

- On Thursday we will start reading 27001, because we will understand all of it from other things we have done
- 27005 is a later, supporting standard but worth reading first (it’s a lot clearer, for a start off)
- Although it has its flaws, following 27005 is beneficial

Purpose

- Not a method, “guidelines” … “support” … “assist” (p. 1)
- Provides a vocabulary and talking points for designing your own risk management system
- Draws heavily on ISO 31000
- Linked to older version of 27001 (“Plan Do Check Act”) rather than 2013 revision (which permits 6 Sigma and others)

Intention

- Provides a means to check that a risk management strategy is broadly sensible
    - Enterprises can ensure their in-house method is compliant
    - Auditors can check that a scheme is sensible
    - You can’t sensibly get a 27005 certificate in isolation

Section 3: Vocabulary

- Should be clear definitions of often-used terms.
- What do you think?
    - Consider 3.7 “likelihood”
    - Consider 3.18 “stakeholder”
- Definitions might require tightening in your system.

Sections 4–6

- 4: Structure
- 5: Background
- 6: Overview
  - Table 1 is a very good summary of an ISMS process

Section 7: Context Establishment

- 7.2 is roughly equivalent to writing IS1 impact levels etc from scratch!
- 7.3 is determining the scope / focus of interest
- 7.4 is again re-writing parts of IS1

So why not use IS1?

- Aimed at government and organisations that need to protect government-classified data
- Emphasis is on protecting labelled material of high classification in clear environments against well-resourced, well-motivated, capable threat actors
- As we found in the exercise, “real” enterprises are all at IL2
- If we pretend that our most sensitive data is IL5, we get absurd risk outcomes

Section 8: Risk Assessment

- Note: “A risk is a **combination** of the consequences…and the likelihood” (my emphasis)
- 8.2.2 asset register, 8.2.3 threat actors (sort of), 8.2.4 and 8.2.5 existing position, 8.2.6 will produce impact levels for CIA.
- 8.3 is an IS1 activity, but done against the backdrop of your own criteria
- The “combination” bit is up to you, rather than coming from IS1’s matrices.

Section 9: Risk Treatment

- Slightly different taxonomy:
  - Modification, Retention, Avoidance, Sharing
- Still leading to residual risk
- Note p.21 where paragraph 2 is concerned with cost while paragraph 3 is much more wide-ranging.

9.2 Risk Modification

- Combines risk **reduction** and risk **mitigation**

9.3 Risk Retention

- aka Risk **Acceptance**
- Note that it superficially implies simply accepting risk, when in fact what it means is reducing the risk under 9.2 and then accepting what is left
- Note also how short the section is

9.4 Risk Avoidance

- Combines risk **transfer** amongst other things
- Would include both “do credit card processing with PayPal” and “stop accepting credit cards”.
- Again, note how short it is.

9.5 Risk Sharing

- Also covers amongst other things risk transfer
- 9.2 > (9.3 + 9.4 + 9.5)
- Very clear the assumption is the main controls you use are about risk modification (reduction and mitigation)

10 Risk Acceptance

- Again, residual risk statement needs to be formally signed off (later we will read 27001!)

11 Communication and Consultation

- Motherhood and apple pie
- Covers training, governance and discussion
- But very important

12 Monitoring and Review

- 12.1: is the environment changing?
- 12.2: is the ISMS working within the environment?

Annex A: Scoping

- Picks up things you might not have thought of
- Note focus on regulation and legislation

Annex B: Assets, Impacts

- Very similar to IS1
- But covers much wider range of situations

Annex C: Example Threats

- Starting point, not finishing point

Annex D: Compromise Methods

- Again, a starting point

Annex E: Approaches

- Very similar to IS1 (I think I heard it came from the same people)

Annex F: Constraints

- Side effects and costs

Tentative

The Real World Intrudes

I.G.Batten@bham.ac.uk

Green Field Sites

- **Scope** the ISMS
- Build **Asset Register**
- Analyse **Threats**
- Build **Risk Register**
- Impose **controls** to control risks
- **Operate** and **measure**
- **Improve**

Plus: **respond** to unexpected events (incidents) and **learn** from them

But…

- It’s rare that you build an ISMS from scratch at the same time as building an IT infrastructure from scratch.
- And even if you were doing this, you probably would not have a clear enough understanding of the landscape to get either right first time.
- Normally, we are retrofitting an ISMS to existing infrastructure.

Case #1: Finance

- Strong security culture
    - although more about shotguns, internal fraud and customer fraud than information risk.
- The IT might not be part of it, but there is staff culture to build on.
- And there is an internal control and audit function and culture you can leverage.
- Security is seen as core, or core-ish, and therefore gets management attention and investment.
- Although IT is often semi-detached and/or outsourced.

Case #2: UK Healthcare

- Worryingly lax attitude to privacy, for deep cultural reasons outside the scope of this course
    - Low priority, until it goes wrong, when it’s a mad panic
- Complex, “evolved” IT environment with a lot of interacting systems which were procured in isolation, a lot homegrown, a lot on obsolete platforms.
- Minimal audit, and almost entirely related to medical outcomes and costs (NHS “Counter Fraud” don’t really do IT).

Case #3: SME

- For example, solicitors and builders subject to invoicing fraud.
- Low priority as compared to paying the bills and keeping customers happy
- “Nothing we have is worth stealing”
- IT is mostly bought-in, and operated by people who don’t know and don’t care much more than how to do their daily tasks.

Common Problems

- Management focus
- Legacy
- Staff training and attitudes

ISMS on a Brown Field

- Building on brown field sites starts with remediation: removing the toxic waste from the past.
- You will almost certainly have things in the infrastructure you take over which are giant waving red flags for an ISMS.
- But how do you manage the change?

Side track

- Just going to run over a few management fallacies and problems which make our lives in IT much harder than they need to be.
  - Technical Debt
  - Sunk Capital Fallacy
  - Stranded Capital Fallacy
  - Reluctance to Rent
  - Reluctance to Change

Technical Debt

- It’s cheaper, in immediate cash-flow terms, to keep paying the interest on your credit card than it is to pay off the capital debt. Even though it’s cheaper in the long run.
- Similarly, businesses accumulate **technical** debt, which they have to pay the “interest” on (ie, the cost of maintaining broken / wrong / expensive things) in preference to the larger, in the short term, cost of fixing it.

This year’s best example

- Apple’s on-disk filesystem, HFS, was designed in the early 1980s to support hard drives of a few tens of megabytes (and floppy disks!)
  - HFS+ conceptually the same, 1998, MacOS 8.1.
- Ported into Unix for OSX, and primary OSX filesystem until 10.12 (2016).
- Hideous: slow, poor crash recovery, **encryption a nasty bolt-on**, poor behaviour on SSDs.

Several failed attempts

- Port of Solaris’s ZFS (itself a 2001–04 response to late 1970s filesystems) done but stalled for political / business reasons before being abandoned. ZFS supports native encryption, with lots of features of interest to security-conscious users.
- Multiple in-house projects failed
- Finally apfs rolling out in 10.13 starting last month (on everything from Watches to Pros).
- For older readers, see also the OSX transition

For security?

- Cheaper and easier to patch and mend rather than reimplement
- Quality lower and you are carrying the technical debt of not doing the job properly
- When building an ISMS, you would like to tear up everything and start again: effectively, **repay all the technical debt in one transaction**.
- Good luck with getting the resources for that!

Sunk Capital

- Suppose you have spent £1m on development costs for a project, and it has failed. Every year it costs £1m more than it brings in.
- Only the small amount of equipment you bought to do the projects with is saleable.
- What should you do?

Sunk Capital

- Rationally, you should give up and scrap the project, writing off the million pounds.
- You have spent the development costs whatever happens, but you don’t have to keep funding the losses.
- However, businesses aren’t rational, and a lot of messy excuses are often made to keep past failures going
  - Sometimes concern about the accounting implications of the write-off, forgetting the old business dictum that **Cash Is King** (see also “turnover is vanity, profit is sanity but cash is reality”).

For Security

- Often you want to move from an old system to a new one as part of imposing new controls
- But the old system cost a lot of money, so even if the new system is cheaper, it still involves writing off the old one.
    - Ironically, this is worse for companies which recognise the non-capital (time, effort) which went into the old system!

Stranded Capital

- Variation on Sunk Capital
- Suppose you have just bought a new car.
- It will cost you £30 to drive to London and park, but you can go by train for £10 (and you can, by the way, at the weekend).
- Which do you do?

Stranded Capital

- A lot of people would take the car, because otherwise it is "wasted" by being sat "unused".
- Similarly businesses spend money to keep using things that can be done cheaper by (often) newer technologies.
- Famously, CS bought an interface card to keep using a disk drive on a new machine. Which cost **more** than replacing the disk drive with a larger, faster, more modern one.
- Again, fear of write-off, and irrational attitudes to "waste".
  - A glance at my hi-fi reveals this tendency.

For security

- Often, a good security approach is outsourcing (risk transfer)
- Sunk and Stranded capital fallacies often make people reluctant to move from in-house solutions to outsource solutions
  - Often a mask for sentimental attachment
  - One of the reasons why incoming management can turn around businesses: much less sentiment.

Reluctance to Rent

- There is a very British thing about not wanting to pay rent. It is seen as “waste”.
- So the British are obsessed with buying holiday homes (hence why they are the #1 target for timeshare scams) even if it makes absolutely no financial sense.
  - They assume the capital is at least recoverable, ideally an investment in its own terms, and therefore over-estimate the cost of renting.
- Also fear that the rent might increase

Reluctance to Rent

- So if you can buy in credit card processing for 7%, many people will see that as 7% waste and pay irrational amounts of money to avoid that cost.
- As we know, a fully-compliant PCI-DSS solution (on which you still pay merchant fees to the card processor, by the way) is expensive and difficult.

For security

- Businesses of all sizes accumulate lots of small, in-house solutions which mask a lot of risk.
- Their costs are hidden in general IT overhead.
- Taking them out requires spending explicit money and often paying a regular monthly or percentage charge.

Reluctance to Change

- Taken together, these factors make people reluctant to change equipment and processes.
- There is some historical precedent, and I am caricaturing the position: change projects tend to **understate costs** and **overstate benefits** — cf. High Speed Two.
- But when rolling an ISMS out, you are often asking for a lot of change in a short period, and you need to think about how to manage this.

Existing Process

- Small companies often have no IT process at all. Kevin in IT deals with it all, and it’s all in his head.
- But let’s assume there is some process in place.
  - Is it being followed?
  - Is it fit for purpose?
  - Does it (or could it) generate records?
  - Could it be adapted?

Existing Process

- Some might address risks you have identified, or could be changed to do so.
- Some might address risks you don’t think are worth treating, or don’t even appear on your risk assessment.
  - There is then a delicate balance: keeping the process is arguably stranded capital fallacy, but is the argument worth the saving?
  - Choose your battles.

Existing Equipment

- Similarly, you will have equipment that was bought for purposes you don't want to continue dealing with in-house.
    - For example, that very expensive PCI-DSS solution for card processing, when you're pretty sure it would be better to go to WorldPay.
- You want to tell the business to accept paying 7%.
- Can you find something else to do with the equipment? That stops people fixating on the write-off.

Existing Staff

- This is where it gets very difficult
- If you are imposing a new ISMS, you may need new staff with new skills, and you may no longer need older skills (particularly in maintaining those old systems you plan to get rid of).
- The cost of change, and the willingness to change, will vary with company culture and legal position (Texas and Frankfurt have wildly different employment law!)
- In the UK, TUPE is a substantial issue.

Existing Staff

- Young dynamic management underestimate the value of institutional memory, particularly when there is change.
- And more experienced staff will be more trusted in the enterprise, so can front-up the changes you are making.
- Wholesale change for a new team is probably the wrong answer, but I am not a management consultant.

Starting the Process

- So we have an idea of the challenges we will confront, so what do we do next?