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

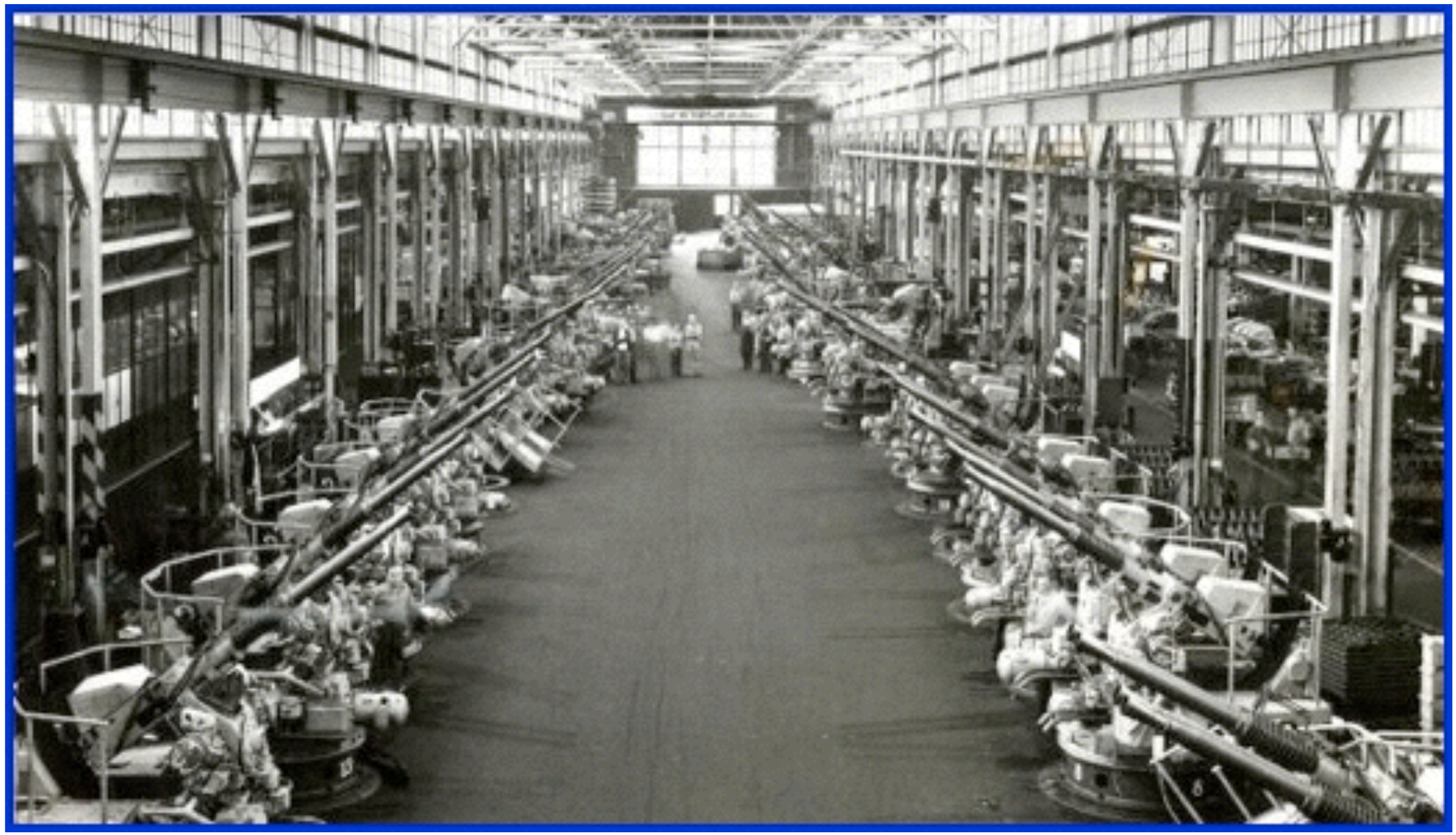
Act

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

Basic Cycle of Quality Systems

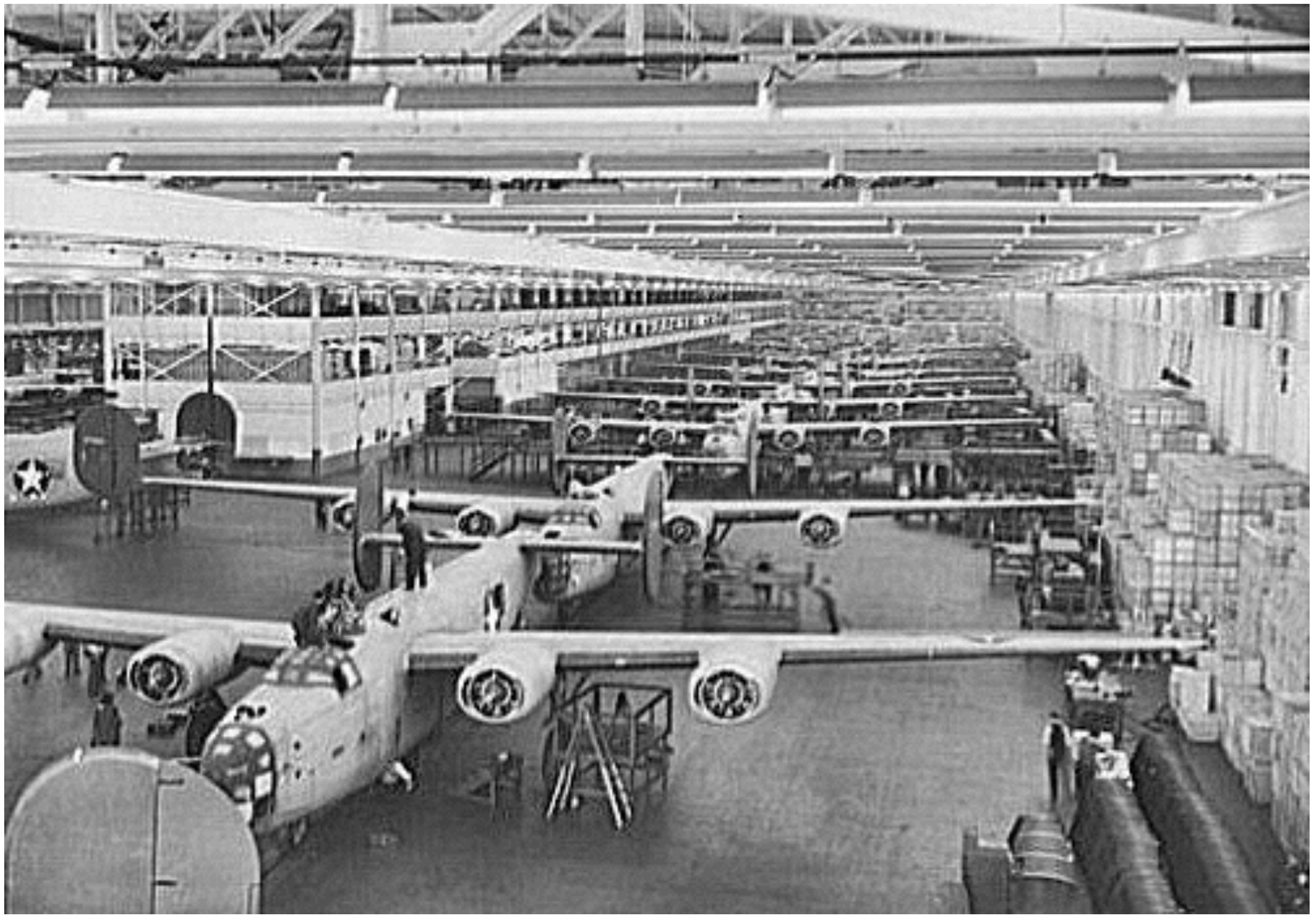
- Ironically, modern quality standards stem from wartime manufacturing as refracted through Japanese manufacturing after the war.
- BS5750 and before that MIL-Q-9858 led to ISO 9001.

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

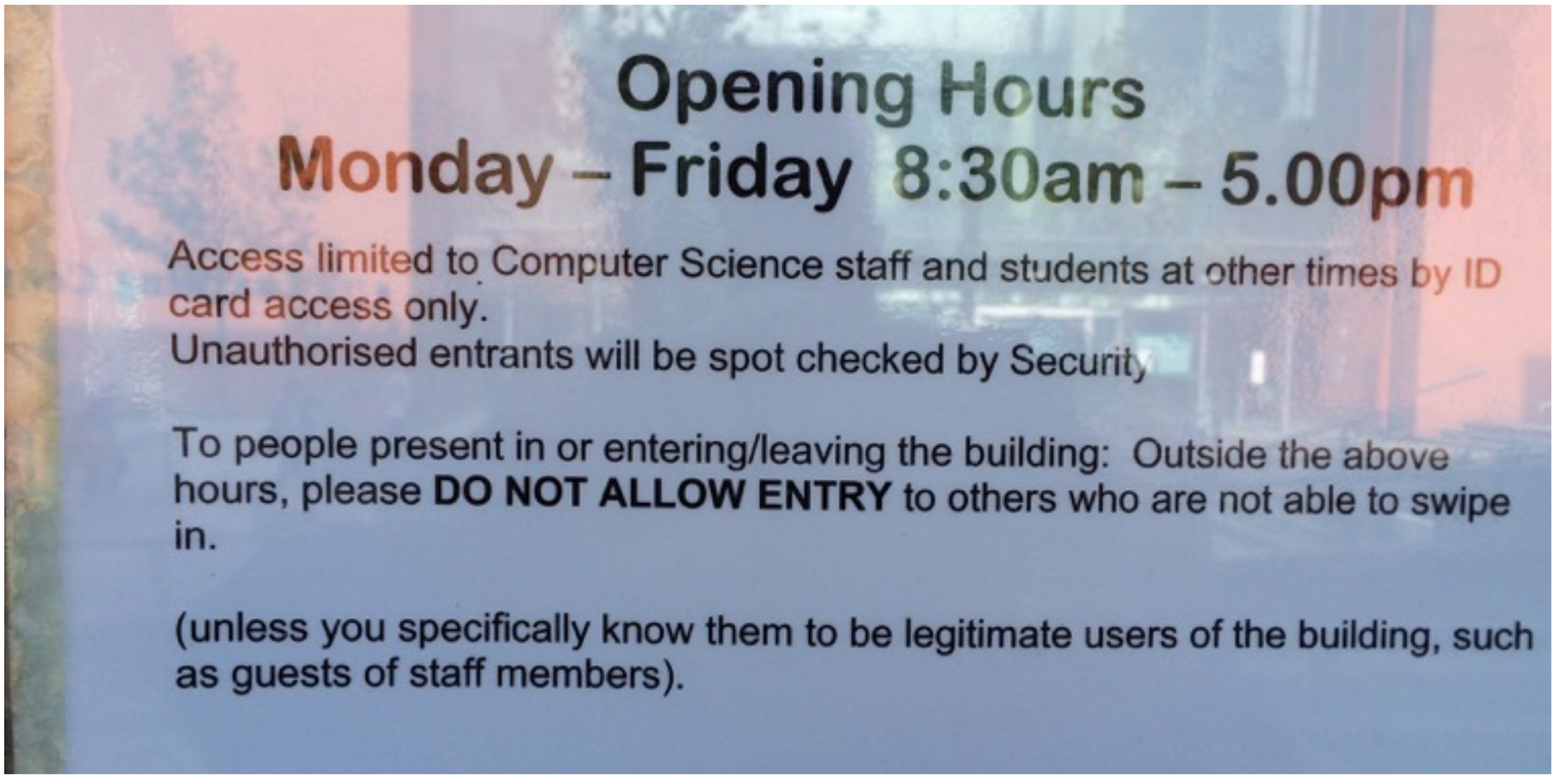
With good policies and procedures:

- 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…

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?