Designing and Managing Secure Systems

i.g.batten@bham.ac.uk

55795165

Logistics

- Lectures: SportEx LT1, 0900 Wednesday and 1600 Friday (the timetabling Gods hate us)
- Office hours: Tuesday 1430–1530 and Thursday 1000–1100, my office (CS 132)
    - bookable slots https://bit.ly/meetwithianbatten
- I.G.Batten@bham.ac.uk
- Canvas/Panopto will contain full recordings (last years are there, which I will sort out)
- So far as I know, there will be no cancelled lectures (famous last words)

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 £300, 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 £100 at a time
  - not easy to convert to cash
  - risk of conviction for fraud and similar offences.
- **WHY NOT JUST SHOPLIFT RAZOR BLADES FROM SUPERMARKETS?**
  - Petty criminals do not need to get a paper in CSF in order get a post-doc, they just want £100 now.
- We have to look at risk, motivation and threat actors, not just consider the risks in the abstract.

Process Fails, not Tech

- “The vulnerability used to attack Talk Talk was older than the kid arrested for it”.
  - They had patches available, but uninstalled.
- It is rare that security fails for unknown, unpredictable, unfixable reasons: metaphorically, being struck by lightning on a cloudless day.
- And it rarely fails because of exotic technical attacks.
- It fails because of people and process.

Why do we mess up?

- We knew, but decided (or worse, didn’t decide) to do nothing.
- We knew, but we were unable to deploy a fix “because reasons”.
- We had a fix, but staff ignored or subverted it, “because reasons”
- We had a fix, but it wasn’t complete and the criminals got better and we didn't keep up “because reasons”.
- And, and, and. Sometimes the “reasons” are even good ones.

This course intends to…

- Train you to spot “because reasons” and do a better job of convincing management, convincing staff and — perhaps most importantly — convincing yourself to do sensible things.
- Sometimes it’s OK to accept risks, but you should at least do so rationally.

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
- NCSC Cyber Security Risk Management Framework, as a comparison with 27001

Week 7

- A walk through some security technologies at a very high level (we are going to need to talk about them)
- Quality management systems, Plan Do Check Act
- Governance
- Policies, Procedures, Work Instructions, etc

Week 8

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

Week 9

- 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: attack our enterprise

Week 10

- 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: controlling our risks

Week 11

- 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 11

- 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 these 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 three 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 ISO 27001 and ISO 27002 and read them
- Get a copy of the NCSC Risk Management documents
- Look at ISO 9000 management systems
    - The documents are very dry; you will find commentaries perhaps easier going.

55795165