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.
-