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