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.