Dr. Phil Legg

Associate Professor in Cyber Security

Information Risk Management

3: Risk Concepts

Date

UWE Bristol | University of the West of England

Recap

- Last week we introduced the Information Security Management System (ISMS)

- ***Today, we will continue to discuss Risk Concepts***

Managing Risk

- Not all risks are bad (…even the bad ones!)
  - https://thomlangford.com/2014/04/09/not-all-risks-are-bad-even-the-bad-ones/
  - "Sharkmageddon" - more people are killed every year sitting on the beach by falling coconuts than those by sharks, but there is an almost universal fear of sharks. We irrationally consider swimming in the sea safer (less risky?) than sitting under a coconut tree.

It is crucial to assess our risks suitably to determine the ***probably frequency and probably magnitude of future loss***

Managing Risk

- One of the most misunderstood approaches to treating a risk is to *accept* or *manage* it. Most people are comfortable with mitigating, transferring or avoiding a risk as they involve some kind of act to deal with them, something we are all familiar with.
- …However, it often feels wrong to simply accept a risk, in essence *to do nothing*. Although this is not strictly the case, it is essentially how we feel we are dealing with it. You are accepting that there is either nothing you can do, or nothing you are willing to do to reduce the risk. However, you are not blindly accepting it at face value; rather you are being cognisant of the risk as you continue your operational activities. You know it is there as you carry on your day job. These activities and the very environment you are operating in can change without notice, and make the decision to accept a risk now the wrong course of action.

https://thomlangford.com/2014/04/09/not-all-risks-are-bad-even-the-bad-ones/

Managing Risk

- Suppose we accept a risk, and then observe a future change
  - E.g., contract expiry with a competitor
  - E.g., lower cost solution has come to market

- Maybe given some change, it is best to now mitigate the risk
  - *It may now be cheaper to introduce the mitigation too!*

- Risk / Reward Spectrum
  - https://en.wikipedia.org/wiki/Risk–return_spectrum

Why Risk Management Matters

- Risk management exists to help us to create plans for the future in a deliberate, responsible and ethical manner. This requires risk managers to explore what could go right or wrong in an organisation, a project or a service, and **recognising that we can never fully know the future** as we try to improve our prospects. [NCSC]

Question

- When my wife asks ”What time will I be home?” – what should I say?
  - If I say 9:30pm, how likely will I be correct?

Question

- When my wife asks ”What time will I be home?” – what should I say?
  - If I say 9:30pm, how likely will I be correct?
  - How about if I say between 5pm and 11pm?

Question

- When my wife asks ”What time will I be home?” – what should I say?
  - If I say 9:30pm, how likely will I be correct?
  - How about if I say between 5pm and 11pm?
  - How about if I say between 9pm and 10pm?

Question

- When my wife asks ”What time will I be home?” – what should I say?
  - If I say 9:30pm, how likely will I be correct?
  - How about if I say between 5pm and 11pm?
  - How about if I say between 9pm and 10pm?

A distribution (i.e., a range) is much more likely to be correct than a single value

It also informs about how confident I am about my answer (i.e., a large range equals a low confidence)

Uncertainty

- The purpose of risk management is to enable us to make the best possible decisions, based on our analysis of future events and outcomes. The future can be anticipated, but within limits defined by our **uncertainty** in our analysis.

- Risk is a part of everything we do. You not only 'take risks' that you are aware of, but you also 'run risks' that you're *unaware* of all the time. This introduces an important point about risk; because of this uncertainty, it is impossible to know and understand *all* of the risks that any person, organisation or network is running at any one time. You will always run risks that you are not aware of. [NCSC]

Probability, Possibility

- What if we are told that there is a 63% chance of rain?

Probability, Possibility

- What if we are told that there is a 63% chance of rain next week?

Probability, Possibility

- What if we are told that there is a 63% chance of rain on Friday?

e.g. What's the probability of our production server experiencing a Denial of Service attack **in the next 3 days**?

"on a long enough timeline the survival rate for everyone drops to zero" Fight Club

To truly benefit from a probability we need to consider the time period in question

… otherwise it becomes just a possibility.

Likelihood, Frequency

- Virus infection on a computer system vs Facility power outage
    - Both events may be "highly likely" on a risk matrix – but one is almost certainly going to occur more frequently than the other.
- Probabilities can be expressed as frequencies – e.g., a 5% probability of an external system being hacked this year is equivalent to a frequency of once every 20 years.
- Limitation of frequency – can't use it for events that will happen only once (e.g., if the sun turned into a white dwarf) – so we use probability in these 'only once' cases.

Prediction, Forecasting

- A risk analysis is a **forecast**, not a **prediction** – never call it so!
  - *In the same way that we know a weather forecast may be right or wrong.*

- A risk analysis is a forecast of the events being probable within a given period of time
  - *Your analysis may be out of date by tomorrow.*

- Forecast and probability can help to quantify uncertainty around how often the event may happen.
  - *E.g., we know the probability of a 6-sided dice rolling a 3, but we don't know exactly when this will occur.*

Measurement Quality

Measurement Quality

- How tall am I?
- What do you all think?

Measurement Quality

- How tall am I?
- What do you all think?

- How did you arrive at your answer?
- Was that a subjective or objective decision?

Measurement Quality

- How tall am I?
- What do you all think?

- How did you arrive at your answer?
- Was that a subjective or objective decision?

Objects in the room help provide a point of reference (comparison)

If you had a tape measure would you still all answer the same?

Measurement Quality

- How tall am I?
- What do you all think?

- How did you arrive at your answer?
- Was that a subjective or objective decision?

Objects in the room help provide a point of reference (comparison)

If you had a tape measure would you still all answer the same?

Both methods (by eye, or by tape) could be valid and repeatable – differ only on precision

Achieving high/perfect precision in InfoSec may be a pipe dream…

UWE Bristol University of the West of England

Measurement Quality

- What makes for a quality measurement?
  - Repeatability – consistent when performed by different means and/or different analysts
  - Validity – measures what it is intended to be measured

Measurement Quality

- Another example: Measure the shoreline of the United States
  - Do we need this to the exact figure?
  - Can we even get it to an exact figure?
  - What if it changes?
  - Generally accepted as 12283 miles – we can call it 12000 miles and have an understanding of this distance.

"A measurement is a reduction in uncertainty"

Risk Analysis Example

- What's the amount of risk to an organization from a database admin "going rogue" and stealing sensitive customer data?

- Most organizations haven't had this happen (that they know of), so trying to estimate the frequency of such an event is challenging. Does this mean they:

1. get to ignore the possibility of it occurring and not make decisions regarding controls that might be useful to manage it, or
2. assume it happens continuously and do everything humanly possible to prevent it?

Risk Analysis Example

- Probably neither – but questions we might ask to help us estimate the frequency of malicious acts by rogue DBAs could include:
  - How many DBAs are there? (a larger population increases the odds)
  - How good is the HR employment screening process?
  - How long have they been with the company? (longer tenure suggests but doesn't guarantee, a stronger personal investment)
  - Have there been any instances of impropriety by any of them that might be a precursor to a more significant event?
  - How tightly knit are they as a team?
  - How good is employee morale in general, and in this team in particular?
  - What kinds of controls exist that might increase the odds of an act like this being prevented or detected (e.g., encryption, logging, joint responsibilities) and how immune are those controls to tampering or circumvention?

All these answers could better inform our decision making

Precision vs Accuracy

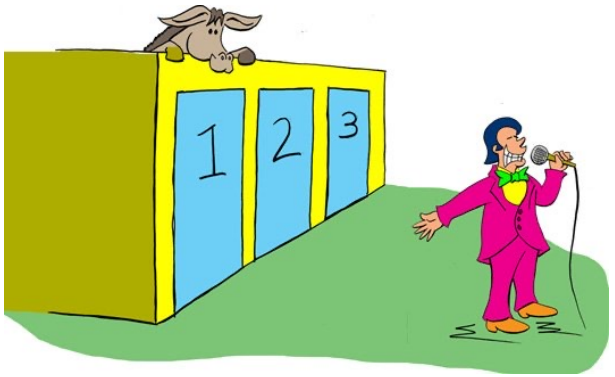
- It is important to recognize the difference between Precision and Accuracy.
- An estimated loss exposure of £501277.15 is highly precise, but also highly inaccurate if the actual loss exposure is £200000.
- If we estimate that the loss exposure is in range £1 - £1000000, we would be accurate but not precise.
- There is always a trade-off between accuracy and precision – however of the two, **accuracy** is king.

Remember the example from earlier about what time I arrive home…

Thinking about Probability: Monty Hall

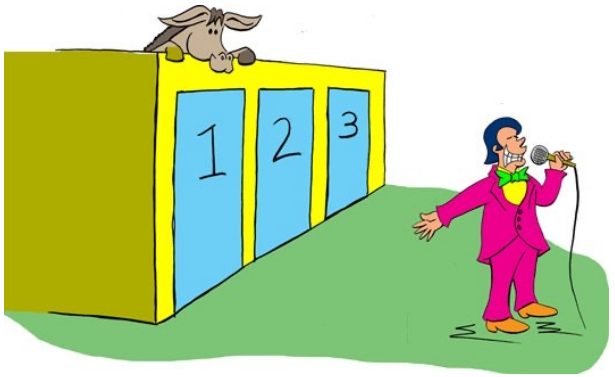
Exercise: Game Show

- The host shows you 3 doors to choose from:
  - Behind 1 door is a CAR
  - The other 2 doors both have a DONKEY



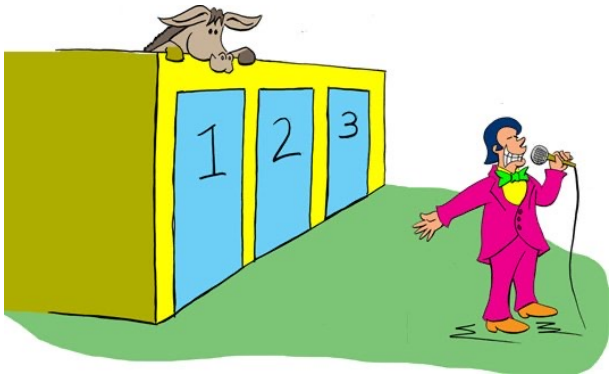
Exercise: Game Show

- You choose a door carefully – let's say door 3!
  - For dramatic effect, the host (who knows where the car is) opens one of the other two doors to reveal a DONKEY.



Exercise: Game Show

- He then asks you to make a decision:
  - **Are you sure it's still Door 3, or do you want to change your mind?**
    - *What should you do?*



Exercise: Game Show