Morning Lecture:

RISK: Is ‘what is’ the same as ‘what out to be’?

* **High-probability low-impact:** likely to take the risk, you would usually have seen the outcome in your past and be aware
* **Low-probability:** we lack past experience, so we usually underestimate the risk (treat 1 in 10000 the same as 1 in 1mill since we’ve never seen the impact of either)
  + This matters if the event is **high impact** – if there’s a chance of it happening, we are bad at estimating the danger of low probability events
* Risk is **invisible**: you don’t know you’ve taken it, unless you experience the negative impacts of it; Laptop repair:
  + Hand in your laptop to a repair shop who take it behind a screen, and you don’t see how they are repairing it. Imagine their repair process in high risk and the process could break it, if you could see behind the scenes, you’d pay more for the safely repaired shop next door.
  + Suppose they break a laptop – you would be angry, but we usually only get angry when the risk goes wrong
    - THE BAD THING IS TAKING THE RISK – TAKING THE RISK AND IT PAYING OFF IS JUST AS BAD AS WHEN IT GOES WRONG
  + It’s just as dangerous every single time you don’t wear a seatbelt, but it’s only on the news when there is a crash and injury/death
* **Humans are bad at assessing risk**:
  + We don’t have enough resources to fully eliminate risk, so we make tough choices about where to allocate funds to mitigate risk
  + Human Nature – obsess about a risk or ignore it, i.e. cleanliness
    - Hard to make a nice balance
* Terrorism – over last 20 years, the amount of Australian deaths from terrorism is around the same as 1-year road toll around the Easter holidays
  + But we spend billions of $s on preventing it, is this good resource allocation?
* Risk Matrix: x = impact, y = probability, graph exposure of everything to rank threats
* Lots of things can be measured, but risks cannot – so there’s a certain amount of arbitrary decision making
* Compliance is a good minimum standard for processes for minimising risk – bad if compliance isn’t used with extra measures to make it better, it can actually be harmful by making you complacent by ticking off the boxes & not actually quality.
  + Better to have no compliance culture and live in fear to make your own processes more safe
* **Managing Risk:**

1. **Prevention:** **Elimination of the threat** such that the undesirable event is guaranteed not to occur. Inherent safety prevents undesired events. E.g. removing the bolt and bullets from a rifle to prevent it from accidentally firing.
2. **Limit:** In situations which the threat could not be eliminated, mechanisms are implemented to **minimize the impact resulting from the event** (fault tolerance) or reduce the likelihood of it occurring (probabilistic safety). E.g. a castle with concentric walls: one wall is breached -> limited portion of castle compromised.
3. **Passing the risk to a 3rd party:** Generally taking out an insurance policy is used minimize or negate financial loss in an event of a failure.
4. **Wear – accept potential to cop the impact if the event occurs**

Evening Lecture:

* *Human weakness -> corruptibility (look for a unique one)*
* *Make a data breach prediction that you expect to happen before term’s end*
* *Make a generally bold prediction*
* Reversing tragedy: the bad thing is the risk not the outcome, outcome is luck
  + She didn’t hit anyone, but if she did, we’d be upset – she cut corners and is just as much to blame when she hits someone and when she doesn’t
* **Centralisation:** single point of failure if cloud or google get compromised
  + While Google’s security is much better than any we could make, if it was compromised it would be very high impact
* **Bits of Work:**
  + Space/time trade-off: with more space you can store previous breach attempts and hence re-use parts of attempts to save time
  + You want the amount of work to do a bad thing to cost more than the benefit/be too arduous, so people don’t bother
* **Insiders**:
  + Are generally the biggest problem but often overlooked -> people try to ignore them because we don’t like to think we let people on the inside that would harm us
  + Who’s watching the watchers -> who polices the police?
  + **Blind spot Examples:**
    - Kim Philby – Soviets knew everything w/in British intelligence
    - Gordievsky – KGB kept missing that he was an insider and he was a double agent with proper allegiance to Britain
    - Michael Bettany (M15),
    - Aldrich Ames (CIA) – moved between heaps of roles and came to understand how multiple things work together (*tranquillity principle*)
    - Robert Hanssen (FBI)
    - American one’s seemed to be motivated by money while UK’s and Soviets motivated by anti or pro-communism ideology
  + Insider risks are only possible when people are corruptible, but EVERYONE is

**Cryptography:**

* **The Private Key Problem:** if I’m talking to 100 people, I need 100 keys to make every channel secure i.e. me and bob don’t have same key as me and Jill. If 100 people all talk to each other, you need 100C2 keys for secure communicate.
  + Key increases at rate n^2 for n people in the system
  + Setting up new keys; all this other mgmt hassle for a non-trivial # of people
* Solve with **Public Key Cryptography:**
  + Each message has an encode and decode key – everyone can know me encode key and then everyone write to me, but no-one can decrypt and read each other’s messages
  + **Merkel solution – puzzles:** B generates lots of messages containing, "This is message X. This is the key Y", where X is a randomly generated identifier, and Y is a randomly generated encryption key. Hence, both X and Y are unique to each message. All the messages are encrypted in a way such that a user may conduct a brute force attack on each message with some difficulty. B sends all the encrypted messages to A.
    - A receives all the encrypted messages, and randomly chooses a single message to brute force. After Alice discovers both the identifier X & the secret key Y inside that message, she encrypts w/ the secret key Y & sends that identifier (plaintext) w/ her cipher text to Bob.
    - Bob looks up the secret key paired with that plaintext identifier, since he's the one who generated them in the first place and deciphers Alice's cipher text with that secret key.
    - Note that the eavesdropper E can read the identifier X sent back (in cleartext) from A to B, but has no way to map that to the secret key Y that B & A are now using for their ongoing encryption, because the value of X within each message was randomly generated (entropy).
  + **RSA** –
    - <https://web.archive.org/web/20130829080627/http://doctrina.org/Why-RSA-Works-Three-Fundamental-Questions-Answered.html>
    - <https://www.youtube.com/watch?v=GSIDS_lvRv4>
    - 3^4 -> ^7 = 3^7 -> ^4: you get your message as a big number
    - Raise it to a power and mod it
    - The number you get is jumbled so much that you can’t reverse it
      * Very hard to get original number -> favourable work ratio to get confidentiality
      * Message (= base) get raised to Power (= Encryption key) to give Number (= encryption text)
      * Receiver raises to another power to get original text (Decrypt)