Morning:

China syndrome movie will be in exam, must watch

Content:

* When something goes wrong, we do a Root Cause Analysis:
  + Attempt to identify root cause so that we can prevent something going wrong again -> works if done like an engineer, not like a reactive, patching peasants
  + Causes in descending order of how often they’re told:
    - #1 Human/user error: sack the person, because the system is fine
      * Humans like a villain so we often accept this
      * Attacks will be because of human error, but not just one human
      * ‘Last touch’ – someone who comes through the door last is the dogs favourite
    - #2 Culture – we don’t have the right culture is a cop out as well since it’s no one’s individual fault, we can all be blamed and all not take action
      * “Let’s pay heaps of money to consultants to educate our staff to improve our culture”, “all our traders are now ethical, they passed the multiple-choice quiz”.
  + There first 2 have truth, but you can’t focus on them
    - **#3 The whole system** – at fault, too complex, tightly coupled

More human weakness:

* **Dishonesty:** people lie, especially to themselves
  + Honour code – sign up to a uni pledging that you wont cheat or plagiarise and such. Do a test, and then mark your own and report what you got to the uni. If you do the test and sign the honour code at the end, you are less honest than if you sign the honour code before, and then sit the test.
    - If you put the reminder at the top of the page, the Stamford and Princeton were both honest, and if you didn’t, they weren’t, even though Stamford didn’t actually have the code, if you told them they did, they were as honest as Princeton.
    - For Princeton who was the honour code, you’ve shoved full of the honour code, made no difference.
  + Most people get away with dishonesty by convincing themselves that they aren’t
* **Misdirection and limited focus:** we can’t focus on many things:
  + in any situation, there are usually more salient points than we can focus on. Like the lights are out, a crisis occurs & we can only look at areas of crisis with a torch.
  + Then we are subject to misdirection: humans should focus on what is logically important, but we tend to focus on salience (what grabs our attention)
  + Social engineers and magicians take advantage of this -> get you to focus on the wrong things.
  + Similarly matching: try to match what is happening to something you’ve seen before and then respond in the same way without thinking.
    - We have small working memory – so our brain tries to move things out of focus as early as it can so our body can automatically respond
  + Frequency gambling: we are trying to recall a pattern that describes what is happening now. But when we see something new, our brain still tries to pick a pattern, so if there are 17 patterns, we pick the most commonly used pattern in the past, which might not be useful.
    - Quite natural and can be useful – as soon as we here a lion roar, we run as fast as possible away from the sound
    - Asking physics postgrads and random people a practical physics question in the real world – they all got it wrong, but the physics students in a theory/exam environment think logically and get it right
    - Dropping a pencil, can usually grab it mid-air in a split second by pattern matching
    - This works, but bad when a new threat occurs, this might be detrimental
  + Attacks vs. Accidents – attacks have intent, but accidents are somewhat random
    - An adversary is adaptive and clever, we assume when we program security that everything, we aren’t controlling will be exploited against us.
    - Programming Satan’s computer – if you engage in a strategy that is unsafe, you will be caught
* Satisficing and bounded rationality: we generally accept that good enough will do, we don’t go for the best possible outcome
* We tend to try to verify a generalisation not falsify it
  + Confirmation bias
* Groupthink syndrome – how your behaviour changes when you are in a group
  + When you value group membership and acceptance more than getting things right, you don’t want to cause problems and feel pressure to comply
* So we design systems such that if we experience human error, it isn’t catastrophic

System Error:

* A normal accident: this is just going to happen, we can’t really stop it from happening
  + Someone is hit in a car crash, ambulance is diverted, given the wrong drugs and died -> it’s not always last touch, it’s everything/the whole system is at fault
  + If your culture punish/blame, you’ll never learn from these & fix your system
  + What is the best way to solve a problem? Pick from a set of solutions/algorithms -> we know we can solve it, but what is the best design of a solution.
    - High coherence, low complexity, loose coupling in a design, means the code is not brittle and can respond to changes better
      * Your security system is resilient in response to adverse circumstances
        + Resilient to common-mode failure (1 cause -> lots of problems)
* Cassandra and Apollo – you can see the future, but no one will ever belief you
* Hindsight: Chekov’s gun: if there is something notable, it will be used e.g. a shotgun in a case on the wall in a play.
  + Looking back, everything seems clear – every little point seems salient because you know the outcome, but when you’re actually dealing with a case study, you need to look for the important things
* Humans simplify - as we tell stories again and again, we simplify more, drop things we don’t think are salient and exaggerate things that we believe are
  + Plan for less contingencies than actually occur
* Ability to control outcomes –> belief we have control
* Hindsight bias: seen the event impact before -> tend to overestimate it’s likelihood
* Latent errors: immediate response to something bad, but the impacts or it aren’t felt until late -> these are the hardest to detect and remedy since the failure was invisible
  + Can make defence in depth more dangerous – since if something goes wrong but the impact is saved by something else, you can’t detect a fault in the initial thing
* Automatic safety devices -> operators losing their skill. If something then goes wrong, we don’t have enough skill to deal with the crisis. Humans as the last line of resort isn’t good, all these extra systems to prevent crises -> worse crisis response from people
* As we plan for the future, we are really planning for reoccurring past events
* Learn about **Chernobyl accident** for exam

Evening:

Digital Forensics:

* Stages of investigation:
  + Acquisition – duplicate the data source so you can take a clone away
    - Put a write blocker on the data so it can’t be changed after acquired
  + Analysis -
  + Reporting
* Types of forensics: memory forensics, data forensics
* Tools for Digital Forensics:
  + For taking snapshots of target and analysing the snapshot
* Image of a USB: FAT 32 file system: 0xE5 (sigma) first character of deleted data shows that it is deleted, it isn’t fully removed from the system

Content:

Continuing with systems: Richard Tells a 45 minute story

* 3-mile island – look at accidents & consider the biases of people leading to the accident
  + Nuclear reactor – very complex -> problems when first starting up
  + 2 people running the machine sued each other each for incompetence
  + If the core got too hot, components would start to melt and become unsound
  + China syndrome – melts so hot that that it burns through ground that it goes to China -> h/w where in China is Opposite where in America
  + Done a check of the system 2 days before, and left the system in a state that couldn’t perform emergency task – latent error (no indicator of pumps going into closed pipes)
  + When you’ve made a mistake, you’re likely to make it again, and only a new set of eyes can notice it
  + Computing, nuclear reactors, sea vessels, etc: these are all complex systems – and we see that humans cause/don’t notice these systems failure’s
    - Everything’s in a rush to be made, and so the quality/integrity can suffer
* You cannot make a complex system failsafe, we can only build a system and make it harder for them to fail
  + We should not focus on scapegoats, we focus on “if something does go wrong, how can we limit the impact”
  + Work out important assets and put all resources into defending them
  + Assume you’re going to be breached, & set it up so it won’t cause disaster
  + Don’t build a data lake, where the attacker can access everything