CS 458 — Module 7: Non-Technical Aspects of Security/Privacy

1 Ethics

- Just because something is possible/legal doesn't mean you should do it.
- Codes of professional conduct may be expectations that one is expected to uphold.
- In Canada, there is CIPS, DHC.

2 Security Plans

- A security plan is a document put together by an organization that explains what the security goals are, how they are to be met, and how they'll stay met.
- A security plan should generally have these parts:
  1. Policy — a high-level statement of goals, responsibility, and commitment.
  2. Current state — A risk analysis describing the current status of the system, what assets/controls are there, what vulnerabilities are possible, what might go wrong, what one should do if new assets/vulnerabilities appear, etc.
  3. Requirements — what needs does the organization have? Who is allowed to do what? What audit logs should be kept?
  4. Recommended controls — where you list mechanisms to control vulnerabilities listed in Current State, satisfying needs in Requirements, taking account the priorities in Policy. These could be, for example, security controls in this course!
  5. Accountability — who's responsible if security controls aren't implemented (properly), or something fails?
  6. Timetable — how and when are elements of the plan performed?
  7. Continuing attention — security plans should evolve and change as the organization and world change.
- More than one person/team should be in charge of a security plan.

2.1 Business Continuity Plans

- AKA "Disaster Recovery Plans".
- A BCP is a security plan where the focus is on availability.
- This is what your organization will do if it encounters a situation that is:
  - Catastrophic — a large part of a computing capability is suddenly unavailable.
  - Long duration — the outage is expected to last long enough that business will suffer if left unattended.
- Some examples of a catastrophic failure is a natural disaster, a utility failing, pandemics (*cough cough COVID-19*); the IST in UW does have a pandemic plan, for example!
- Writing the plan isn't enough though — you might also need to:
  - Acquire redundant equipment
  - Arrange for backups regularly
  - Stockpile supplies

  - Train employees so they know how to react — this may involve live testing the BCP, but this may be problematic:
    * May be too disruptive to do
    * May not be accurate enough of a test since it's *only* a test, not the real deal
    * No BCP during the *testing* of the BCP!

- We can also have an incident response plan, where this might not directly be affecting our business but could get worse.
- So for example, a batch being tampered, website being defaced, etc.
- These might need to consider things like:
  - Legal issues
  - Preserving evidence
  - Records
  - Public relations
- What potential coping methods could we do for, say, an incident involving the loss for our data centre?
  - Hot sites — a complete duplicate data centre.
  - Cold sites — like a hot site but no computers (ie: IBM shipping you new machines if yours fail).
  - Mobile hot sites — a hot site that you can move, so people don't, say, have to travel to a hot site that may be very far away.

2.2 Choosing Controls

- We need some risk analysis to know how to choose controls, comprising of:
  - Identify assets — hardware, software, data, people, documentation, supplies.
  - Determine vulnerabilities — think like an attacker, what things might be attacked?
  - Estimate likelihood of exploitation — there are experts to do this as it's hard, but how likely are certain risks going to occur?
  - Compute expected loss — what could be the impact of a risk?
  - Survey applicable controls — for each risk, how can we control the vulnerability?
  - Project savings due to control — for each control, the cost of control is its direct cost (buying, training, etc.) pus the exposure of the controlled risk. Savings are the risk exposure minus the cost of control. Hopefully, this will be positive.
- The TRA (Threat and Risk Assessment) Process is managed by the RCMP for all federal government departments.
- Steps for the TRA:
  1. Make a list of threats that could affect IT assets
  2. Make a list of controls that could mitigate/eliminate the threat
  3. Calculate the total expected losses if no controls are implemented.
  4. Evaluate the cost of buying various combinations of the possible controls.
  5. Select and implement the package of controls that results in the lowest total expected losses (note that "no controls" is a totally valid response).

2.3 Physical Security

- Firewalls can't stop someone just making off with your actual machine.
- Two major classes of physical threats — natures and humans.
- We can kinda mitigate against natural disasters by building based on likely natural disasters.
- Vandals, thieves, and targeted attacks can be examples of human physical threats.