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.) plus 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.

3 Intellectual Property

- Intellectual property differs from "real" property (like a house or car), in that:
  - It is non-depletable — even if someone took it, it's still mine!
  - It is replicable — I can make more copies of my IP.
  - It has a minimal marginal cost — while the first copy might be expensive to build, the cost of making more copies after this should be small.
- *Trade secrets* are the simplest kind of IP — there is no protection other than "nobody else knows".
  - Now, of course, this isn't totally possible, since you'll probably have to tell someone how to make it to, well, make more.
  - Note you can't really protect the secret outside of hoping it doesn't leak, though you can sue if someone divulges the secret without permission.
  - People can also reverse-engineer trade secrets!
  - For example, RC4 was reverse-engineered, and since it relied on keeping it proprietary and secret as part of its protection...
- *Trademarks* protect names, brands, and logos.
  - This lets you sue others who use that name in a confusing manner.
  - So, even if RC4's algorithm isn't protected, the *name* still is!
  - In Canada, you can now register a trademark before using it, and you can register non-traditional things like smell, taste, etc.
  - However, it costs more now.
- *Patents* applies to inventions.
  - They must be:
    - Novel (nobody has done it before)
    - Useful (usually)
    - Non-obvious to somebody who knows about the topic
  - However, you get a monopoly for this invention for 20 years, but now, you must tell the world how it works. This tries to incentivize improving knowledge for the rest of humanity by sharing what would otherwise be kept secret.
  - Many cryptographic algorithms are/were patented — this doesn't violate Kirchoff's/Shannon's in any way, it just means you have to pay licensing fees to use said algorithm.
- *Copyright* protects expressions of ideas in a tangible medium, but not the ideas themselves.
  - There is no filing requirement, though you can get additional benefits if you do file.

  - These last a limited time — in the US, it's for your life + 70 years; in Canada, it's the life + 50 years.
  - The copyright holder has monopoly rights over certain uses of the work.
- There is also *fair use*. These are copying exceptions for purposes like criticism, comment, news reporting, etc.
  - There are four tests that must be met to decide of fair use is allowed (in the US):
    1. The purpose and character of the use (is it commercial, non-profit, educational, etc.)
    2. Nature of copyrighted work
    3. The amount and substantiality of the portion used in relation to the copyrighted work as a whole
    4. The effect of the use upon the potential market/value of the copyrighted work
  - In Canada, we don't have fair use — we have *fair dealing*.
    * This applies to private study, research, criticism, review, news, education, parody, and satire.
    * This is an *exhaustive* list!
    * And things like time-shifting, backups, copying for private purposes, mash-ups, etc. are also legal.
    * For example, downloading songs is probably legal in Canada; *uploading* is probably not though!
- Paracopyright: the Digital Millennium Copyright Act (DMCA) made it so that if there was some kind of copy protection mechanism, even if you were within your rights for fair use, it is illegal to break the copy protection!
- In Canada, it was made illegal to, for example, lock a cell phone, as that could be locked via similar rules.

4 Computer Crime

- Rules of evidence: how do we manage digital evidence?
  - Chain of custody for digital evidence?
  - How do we preserve electronic evidence?
- How do we deal with computer crime that (often) spans across countries?
  - The Council of Europe cybercrime treaty (Canada and the US are signatories) stipulates that member countries pass laws making it easier to enforce laws in regards to telecommunications traffic.
- What about some Canadian laws?
  - C-30 was originally an act to combat child pornography, but it was criticized for allowing ISPs to hand over customer information without warrent and give the government authority to inspect packets. Abandoned.
  - C-13 allowed any public officer can demand computer data in a person's control to not be deleted, and lowers the standard for seizing computer/transmission/tracking data.
- Backdoors:
  - Clipper chip
  - The main criticism with a backdoor is that if there is an intentional backdoor, people will usually find a way to use it.

5 Software Failure

- If you buy a product and it fails, you can get a refund or get a new one usually.
- With software? Not as easy. EULAs usually make you agree that software might not work.
- Usually this isn't the case with embedded software.
- So, how should you report software failures?
  - Most vendors would like you to tell them and nobody else, as well, they don't want people exploiting their software.
  - Some of them back this up by legal rammifications!
  - But... what if the vendors don't fix said failures?
  - There are thus two approaches to software failure reporting:
    * One approach is full disclosure — if a problem is found, post it to a full disclosure mailing list of security professionals.
    * The reasoning is that if you have found it, people who are potentially looking to do harm may have done so, and by publicly "shaming" the vendor, the are more inclined to fix the problem.
    * The flaw is that now, the vendor may have to race against the clock to fix the problem even though they may have just learned about it, and now people are going to be upset.
    * The other approach is responsible disclosure — tell the vendor first, and if no fix comes out (or at least some announcement of the flaw), then contact a coordinating centre like CERT to decide what to do next.