Final Exam Study Notes Week 5-6

SENG 460
Spring 2021

5 Security Awareness, Privacy

5.1 Employee Onboarding

- Roles and Responsibilities
- Work to prevent issues and if you see something, report it
- Ensures employees know that security is everyone's responsibility

5.2 Security Awareness

- Establish and maintain a security awareness, education, and training program
- Content reviews
- Program effectiveness evaluation
- Methods and techniques
  - E.g. Clean desk checks, phishing campaigns

5.3 Phishing Campaigns

- Provide a safe environment for employees to make the right decisions
  - Don't shame them, but educate
- Sending phishing emails to their own employees

5.4 Privacy

- Definition
  - We don't define it in law or policy
  - Contextual, hard to pin down
  - Informational self determination
- You get to choose what happens to your information
- Trust people with information and to make the right decisions once they have the training
- Continually question whether you are applying rules or others are on your behalf
- People don't always make good choices
- Privacy is:
  - Subjective
  - Contextual
  - Negative
- PHI: Personal Health Information
- Privacy is something you negotiate all day
- Personal expectation of privacy does not always translate to the law
- Includes when you combine things - the mosaic effect
- PII: Personally Identifiable Information
  - Info that can directly identify or can be combined with other identifiers

- Context not always dictated by you
  - Eg. Border crossing
- Personal information is
  - Anything **BUT** your contact information
    - Name
    - Phone
    - Address if you are at a business
- FIPPA definition of Personal Information
  - Recorded information about an identifiable individual other than contact information
- Context is important - think about it for yourself
  - Your opinions, things you think
    - Unless they are about someone else and then it is their information
- Law tries to give you a choice to control
  - People ask "can I have the information so I can share it"
- Sometimes you don't have to ask
  - Eg. description of fleeing robber
  - Lost right to privacy - supporting an investigation
- How do you know what they have if you can't get access to it?
  - Anyone who has your info should give it to you
  - You shouldn't have to be in the dark with your information

- As individuals not bound to same laws though you can't set up a camera in your front yard pointed at neighbour's bedroom
- Some cases the information will not be corrected if it was correct on that day
- Individual to individual need to ask do I trust this person enough to do the right thing
- Organizations have a requirement - they have to listen if the information is wrong
- Some places do not control the information
- Privacy is only dead if
  - You give up your choices and decision making
  - You allow it to be
- Privacy law applies to inmates same as citizens
- Not making good choices if don't know why someone is asking
- Privacy is about limiting the use, disclosure, retention based on what you told someone you want to do with the information
- Surprises are never a good thing
- Force people to not surprise you
- Ensuring accuracy of information is important
- Privacy is a constantly negotiated battleground
- When you have been wronged there is someone to help you with it
  - Eg. OIPC

5.5 "The Right To Privacy" - Harvard Law Quote

... but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.

5.6 Examples of Personal Information

- Name, address, email, phone number
- Age, sex, religious beliefs, sexual orientation, marital or family status, blood type
- Individual's health care history, including a physical or mental disability
- Individual's educational, financial, criminal or employment history
- Personal views or opinions

5.7 3 Kinds of Privacy

- Spatial: Your space and things around you
- Physical: Privacy of body
- Informational: Information about you

5.8 What the privacy team does

- Review initiatives
- Respond to breaches
- Advise on initiatives
- Conducts audits
- Develop policy
- Provide training

5.9 What the privacy commissioner does

- Regulate
- Oversee
- Adjudicate

5.10 Privacy Considerations

- Management
- Notice
- Choice and consent
- Collection
- Use/Retention/Disposal
- Access
- Disclosure to third parties

5.11 Privacy Legislation (Canada)

- Privacy Act
  - Applies to federal governments and agencies
- Personal Information Protection and Electronic Documents Act (PIPEDA)
  - Applies to information-handling practices of many businesses
  - Manitoba, New Brunswick, Newfoundland/Labrador, NWT, Nova Scotia, Nunavut, Ontario, PEI, Saskatchewan, Yukon
- PIPEDA does not apply to organizations operating entirely within the following provinces, unless personal information crosses provincial or national borders:
  - Alberta
  - British Columbia
  - Quebec

5.12 Mandatory Breach Notification

As of November 1, 2018, organizations subject to PIPEDA will be required to:

- Report to the Privacy Commissioner of Canada breachers of security safeguards involving personal information that pose a real risk of significant harm to individuals
- Notify affected individuals about those breaches
- Keep records of all breaches

5.13 What is a breach of security safeguards?

The loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards that are referred to in clause 4.7 of Schedule 1 of PIPEDA, or from a failure to establish those safeguards

5.14 Does this apply to small businesses?

Large and small businesses will be subject to PIPEDA requirements to report and notify breaches of security safeguards that pose a real risk of significant harm, and to keep records of all breaches of security safeguards

5.15 Are there financial penalties?

- It is an offense to knowingly contravene PIPEDA's reporting, notification and record-keeping requirements relating to breaches of security safeguards, and doing so could lead to fines
- OPC does not prosecute offenses under PIPEDA or issue fines. What the OPC can do is refer information relating to the possible commission of an offense to the Attorney General of Canada, who would be responsible for any ultimate pros-

ecution.

5.16 FIPPA

- Storage and access must be in Canada
  - **30.1** ... stored only in Canada and accessed only in Canada ...
- Disclosure inside or outside of Canada
  - **33.1** ... (ii) ... the individual is temporarily traveling outside Canada; ...
- New
  - ...(ii) in the case of disclosure outside of Canada, results in temporary access that is limited to the minimum period of time necessary to complete the processing...
- Newer
  - Disclosure outside of Canada
    - **33.1** A public body may disclose personal information outside of Canada only if the disclosure is in accordance with the regulations, if any, made by the minister responsible for this Act
  - Disclosure of personal information in records available to public without request
    - **33.3** (1) A public body may disclose to the public a record that is within a category of records established under section 71(1)
    - (2) A ministry may disclose to the public a record that is within a category of records established under section 71.1(1)

5.17 Privacy Teams

- Can respond when things don't go well
- Investigate Breaches
- Advise on important files
- Recommend others check in with privacy team early and often on projects
- Perform audits, develop policy, provide training

5.18 Privacy Impact Assessments

- Process to make sure personal information collected and used by organizations is protected
- Personal information belongs to the person it's about
- 5 Steps:
  1. Download template
  2. Fill out template
  3. Submit for review
  4. Get signatures
  5. Start project

5.19 Myths

- Privacy doesn't matter because I'm not doing anything wrong

  - This is usually said by people who are about to take your privacy away
  - The point is you get to hide it
  - It's what we choose to share with whom
- You need an individuals' consent to do anything with their information
  - This is not the law
  - You get to choose to the greatest degree possible is the principle
  - Information about you that has your name pulled off
    * eg . hospital visit and how long your stay was - researchers may use the information
    * Privacy legislation has provisions where consent is not required
- Often hear people "wielding" consent
  - Eg. "I never consented to that!"
- It is important to push on the rights
  - Won't always win
  - Sometimes don't have choice
- If information is publicly available anyone can do anything they want with it
  - Eg. employer shouldn't look at Facebook to decide if you get a job
  - Just because they "can't" doesn't mean they "won't"
  - Are digital assistants infringing? Yes!
  - Don't want someone/something listening when doesn't need to be
  - Don't put yourself in a place to be victimized
  - Facts
    * Public body needs authority to collect under FIPPA
      · Authorized under an Act
      · For law enforcement
      · Related directly to and necessary for an operating program or activity
      · Necessary for planning or evaluating a program or activity of the public body
      · The information is collected by observation at a public and voluntarily attended presentation, ceremony, performance, sports meet or similar event
    * How PI is collected
      · Directly from the individual
      · Must notify the individual of the purpose
      · Legal authority
      · Should provide who to contact if there are questions
- The laws alone will protect me
  - Treat it as a dialog, have the conversation
  - Very awkward when someone asks you for something and you say no
  - You can say "I don't think you can ask me that"
  - Push to the point so they have to prove it
  - Force them to demonstrate
  - If they are entitled they should be able to prove it

5.20 Week 5 Summary

- To be inquisitive is a positive thing
- Be critical, analytical and do so as much as you can
- People often rely on laws but incidents do happen
- Because incidents happens doesn't mean ramifications of incidents are not very serious

- Administrative errors by far are the most common issue
  - Eg. sent to wrong address, wrong name, double-stuffed envelopes
- Privacy as an industry is not going away
  - Get involved in drones, AI, genomics, biometrics, etc
  - Everyone should have someone responsible for privacy
  - Free resource to call: BC Privacy and Access Helpline

6 Legal, Breaches, Investigations, OSI, Darknet, Foreign Threats

6.1 Software Licensing

- Shrink-wrap agreements
  - Clause stating you acknowledge agreement simply by breaking the seal on the shrink-wrap
- Click-through agreements
  - States you agree when clicking the button you agree
- Written, signed, negotiated contracts
- Cloud services license
  - Click-through agreements

6.2 Law Prosecution

- Jurisdiction is a problem
- Evidence is a problem
- Having the skills and maintaining talent supply is a problem
- Prosecution is very difficult - consider you must prove beyond a reasonable doubt
- Technology is evolving so quickly, laws and law enforcement are challenged to keep up

6.3 Four Categories of Intellectual Property (IP)

- Patent
  - Legal ownership of an invention (Eg. bottle design)
- Copyright
  - Expression of the idea of the resource instead of the resource itself (Eg. book on Coke)
- Trade Secret
  - Something proprietary to the company and essential for its survival and profitability (Eg. Coke recipe)
- Trademark
  - Word, name, symbol, sound, shape, colour, or combination of these which represent the company (brand identity) to a group/people/the world (Eg. Coca Cola™)

6.4 Liability

- Liability
  - Being responsible to an entity because of your actions or negligence
- Negligence
  - Organization was careless and as a result some person or organization was negligent and may be found liable
- Due care
  - Degree of care a reasonable person would exercise (eg. request patch vulnerabilities) .. putting measures in place to protect
- Due diligence
  - Reasonable steps taken by someone to satisfy a requirement (eg. follow-up and determine vulns were patched) ensuring measures remain in place

6.5 Evidence

- Best evidence
  - Original or primary evidence rather than copy or duplicate
- Secondary evidence
  - Copy of evidence or oral description (Not as reliable as best evidence)
- Direct evidence
  - Proves or disproves a specific act through witness's five senses (e.g. saw harassment); testimony from firsthand witness
- Conclusive evidence
  - Evidence that cannot be contradicted by any other evidence; incontrovertible; overrides all other evidence
- Circumstantial evidence
  - Inference of information from other, immediate, relevant facts; evidence to support circumstances/other evidence
- Corroborative evidence
  - Supporting evidence used to help prove an idea or point; used as a supplementary tool to help prove a primary piece of evidence; not on its own
- Opinion evidence
  - Expert: may offer opinion based on personal expertise and facts
  - Non-expert: May testify only as to facts
- Hearsay evidence (3rd party)
  - Oral or written evidence that is presented in court that is secondhand and has no firsthand proof of accuracy or reliability (usually not admissible in court)
- Real evidence
  - Physical evidence, tangible (Eg. hard drives but not the information on them)

6.6 Headlines

- When there is a new incident
  - People want to know if they are affected
- Understand how attacks happen
  - What they did, how they did it, why they did it
  - Should we blame the companies?
  - Who is the victim?
- Understand how to prevent them
  - There is a lot to learn from incidents
  - What they did, how they did it

- When there is new vulnerability
  - New website pops up with information
  - It's new (WHOIS), no reputation, why do you trust it?
  - Often has a tool to check if your website is vulnerable
  - How do you know they won't say it's good and send the results to the bad guys?

6.7 Company Breaches

REVIEW THE SLIDE DECK STARTING AT SLIDE 19 OF WEEK 6

- Clearview AI
- Yandex
- LifeLabs
- Saskatchewan eHealth
- Government of Saskatchewan
- City of Saskatoon
- University of Saskatchewan
- Ontario Hospitals
- WannaCry
- NotPetya
- Maersk
- Atlanta, Baltimore, New Orleans, Florida
- Ottawa, Adobe
- BC Municipalities
- Nunavut
- Power Grids
- Ontario Municipalities
- Desjardins (insider!)
- Capital One
- Health Breaches
- Bangladesh Bank
- Canada NRC
- Nova Scotia
- PEI
- Casino (IoT...)
- Various
- Australia, UK
- Stuxnet (Awareness)
- DoorDash
- Yahoo
- AdultFriendFinder
- UnderArmour
- eBay
- Equifax
- TransUnion
- Quora
- TJX
- Anthem
- Sony
- JP Morgan
- Target
- Tumblr
- Uber
- Home Depot
- Facebook
- Ashley Madison
- US Office of Personnel Mgmt (OPM)
- Google
- Cathay
- Dropbox
- LinkedIn
- Swedish Transport Agency
- Cellebrite
- Hollywood hospital
- University of Calgary
- Canada Treasury Board
- Toyota
- Bayer

6.8 Company Breaches Summary

- Insiders are threat actors that operate within the organization and have legitimate reason to be there and legitimate access and knowledge
- They may use this access and knowledge to do illegitimate things They may do this knowingly or unknowingly - intentionally or unintentionally Difficult to detect, can be very harmful
- They may do this knowingly or unknowingly - intentionally or unintentionally
- Difficult to detect, can be very harmful

6.9 Open Source Intelligence (OSINT)

- Is there a lesson to be learned even though it isn't true?
- Some open source, some not
- Many sites with information available
- Just need to know where to look (E.g. courts)
- For articles and studies - check your sources
  - Exercise critical thinking
  - Who wrote the article or sponsored the study?
  - What do they have to gain?
- There are many sources of information, intelligence
- When you correlate the available information can synthesize or determine additional pieces of information (Example was a video for Maltego)
- Is the story legitimate? Is it fake news?
  - Is the person knowingly spreading false information?

6.10 DarkNet

WARNING: Don't go there

- Often accessed through ToR browser*
- Difference between surface web, deep web, dark-web
- Take precautions
  - Use VPN
  - Turn off all scripts

6.11 Surface Web

- Bing
- Google
- Wikipedia

6.12 Deep Web

- Contains 90% of the information on the Internet, but is not accessible by Surface Web crawlers
- Academic Information
- Medical Records
- Legal documents
- Scientific Reports
- Subscription Information
- Social Media
- Multilingual Databases
- Financial Records
- Government Resources
- Competitor Websites
- Organization-specific Repositories

6.13 Dark Web

- A part of the Deep Web accessible only through certain browsers such as Tor designed to ensure anonymity.
- **Deep Web Technologies has zero involvement with the Dark Web**
- Illegal information

- TOR-Encrypted sites
- Political Protests
- Drug Trafficking sites
- Private Communications

6.14 5 Eyes

- 5 Eyes countries include: United States, Canada, Australia, New Zealand, United Kingdom
- Countries and parties to the multilateral UKUSA Agreement, a treaty for joint cooperation in signals intelligence
- Processed intelligence is gathered from multiple sources
- The intelligence shared is not restricted to signals intelligence (SIGINT)
- Often involves defense intelligence as well as human intelligence (HUMINT) and geospatial intelligence (GEOINT)

6.15 Threats to Canada's Democratic Process

- Goal is to prepare for the known so when the time comes can focus on the unknown that arise
- Multiple groups will likely deploy cyber capabilities against future elections ranging in sophistication
- Elections are largely paper-based and have controls in place
- Threat to Canada's democratic process remains at 'low' level
- Highly probable threat activity will increase
- Cyber capabilities are publicly available and cheap and easy to use
- Rapid growth of social media and other factors without sufficient checks and balances means spreading 'fake news' is easier than ever
- Elections are increasingly using technology
- Deterring cyber threat activity is challenging because it is difficult to detect, attribute, and respond to in a timely manner
- Different types of threats: strategic threats and incidental threats
- Cyber threats can be a show of force to deter other nation-states
- Adversaries may seek to change Canadian election outcomes, policy choices, government relationships
- Cyber capabilities to disable a website are simple to buy or rent
- Adversaries may steal a voter database in order to sell it on the DarkWeb
- Convert manipulation of traditional and social media to influence political discussion
- **The most effective defenses against ransomware are user awareness and offline or disconnected backups**
- "Many effective cyber capabilities are readily available, cheap, and easy to use.... Deterring cyber threat activity is challenging. We are unable to attribute about 20 percent of incidents to a particular adversary. Of those incidents that are attributed, most appear to have gone unpunished."
- "The rapid growth of social media coupled with the decline in longstanding authoritative sources of information make it easier for adversaries to use cyber capabilities and other methods to inject disinformation and propaganda into media to influence voters."
- "Elections and election agencies are adopting more online processes, making them more vulnerable to cyber threats."
- "There is a dynamic of success emboldening adversaries to repeat their activity, and to inspire copycat behavior"
- During the 2015 federal election, Canada was targeted by low sophistication cyber activity
- Nation-states have demonstrated the highest sophistication

- Two types of threats
  - Known (Those that you can anticipate)
  - Unknown (Those that you are unable to anticipate)
- Two types of attacks
  - Direct (Attacks directly against voting assets)
  - Indirect (Attacks intended to shift perception of voting process)
- Cyber threat activity against the democratic process is increasing around the world (more than tripled)
  - Canada is not immune
  - Small number of nation-states have undertaken majority of cyber activity against democratic process
- 3 targeted areas of democratic process
  1. Elections
  2. Political parties and politicians
  3. Traditional and social media
- Social botnets
  - Series of computers commanded by a single person
- DDoS
  - Distributed denial of service attack could be against political or media website
- Deface a website
  - Attackers could modify the content to embarrass, discredit, or spread false content
- Spear phishing
  - Targeted phishing against a political target or other
- Elections are targeted to
  - Prevent citizens registering
  - Prevent voters from voting
  - Tamper with election results
  - Steal voter database
- Three essential phases
  1. Registering voters
  2. Voting
  3. Disseminating results
- Threats to political parties and politicians include
  - Cyber espionage
  - Blackmail
  - Embarrass/discredit
  - Steal/manipulate voter or party database
- Troll farms
  - Groups of people paid to spread propaganda on social media
- Ransomware
  - Restricts access and compels victims to pay to have access returned
- Redirect/man-in-the-middle attack
  - When the attacker logically inserts themselves between the source and recipient of the traffic
- Possible attack
  - Gain access, move laterally, monitor, analyze, contact rival...
- Goals of threat actors
  - Reduce trust in a free and fair democratic process
  - Shift policy in a preferred direction or promote core interests

Sophistication levels

- Low
  - Single capability
  - Single target
  - Little or no planning
  - No lasting effect
- Medium
  - A few capabilities
  - More than one target
  - Planning
  - Multiple affected
- High
  - Several capabilities used expertly
  - Numerous targets
  - Extensive planning
  - Long impacts

7 Architecture, Cloud, Operations, Network Communications, IoT, Mobile

7.1 Architecture

Look at slide deck, a million photos

- Translate business requirements into solutions that provide security for key assets
- Multitasking, multiprocessing, multithreading
- Security zones
- System components
  - Processors
  - Storage
  - Peripherals
  - OS
  - Etc.
- Architecture
  - Fundamental organization of a system embodied in its components, their relationships to each other and to the environment and the principles guiding its design and evolution
- Build security in from the ground up; security by design (good)
  - Easier, simpler, faster, cheaper, more effective
- "Bolt on" security after the fact (bad)
  - More difficult, slower, causes delay, expensive, less effective
- Architecture = what you need to have
- Design = how you do it
- System architecture, computer architecture, CPU architecture (structure security)
- Operating system architecture
  - Monolithic
  - Layered
  - Microkernel
  - Hybrid microkernel
- Security policy
  - Expresses what the security level should be by setting what the security mechanisms are supposed to accomplish
  - Foundation for specifications of a system and provides baseline for evaluating system

Enterprise architecture

- Sherwood Applied Business Security Architecture (SABSA)
  - Business driven, based on risk, relies on others (e.g. COBIT) for actual controls
  - Create top-down architecture for every requirement, control, process
  - 6 layers
    * Contextual
    * Conceptual
    * Logical
    * Physical
    * Component
    * Security Service Management Architecture (vertical)
- The Open Group Architecture Framework (TOGAF)
  - Defines architecture goals
  - Benefits/vision
  - Sets up projects to reach goals

7.2 Zero Trust

- Concept that castle and moat doesn't work
- Can't count on keeping bad guys out
- Proposes to not trust anything
- No-one is trusted by default
- Verification is required for everyone

7.3 Cloud

- Delivering hosted services over the internet
- Confusion and hype, real cloud vs. fake cloud
- Absence of responsible adoption of the cloud
- Three common types
  - Software as a Service (SaaS)
  - Platform as a Service (PaaS)
  - Infrastructure as a Service (IaaS)
- Adopting for wrong reasons
  - Save money vs. flexibility vs. focus on core business
- Encryption and access control
  - Who has the encryption keys?
- Data classification is key
- Data security in cloud
- Unclear roles and responsibilities
  - Who does investigations?
  - Incident response?
- Cloud can have greater security
  - Scale and ability to invest
  - Requires customer to utilize the controls available

7.4 Cloud Security

- **Look at OSI model slide for picture and Ports slide (slide 41)**
- Consider traditional defense in depth
- **Look at the slides for all the headlines**

- Contracts
  - Whose 'paper'? (contract terms)
  - Inability to customize agreements (e.g. ref Gartner)
  - Are there any "teeth" (penalties) in the contract?
- Cloud security requires "east-west" controls as well as "north-south"
  - Securing the hypervisor
  - Defense in depth applied at a VM level
  - Controls should follow VM around
  - East-west = Internal to internal
  - North-south = External to internal, internal to external
- Standard-based approach?
  - 3 cloud security standards/frameworks
    - CSA Cloud Controls Matrix (CCM)
    - ISO 27017
    - NIST 800-53
- Consider traditional audit approaches often look for 'air gaps' between machines
  - Air gaps means the webserver and database are on two separate pieces of hardware
  - This is not the way things are done in cloud

7.5 Internet of Things (IoT)

- Aka Internet of Everything
- Aka Internet of Vulnerabilities
- Raises significant security and privacy concerns
- Devices were not created with security or privacy in mind
- "Often privacy and security are not ahead but often in the rearview mirror in danger of catching up" GP
- Those that can't can be used against others
- Sold by companies that don't understand privacy and security
- May use protocols that are not secure
- May have default, generic, undocumented accounts
- Sold online by companies that may not have a reputation or may not have a good reputation
- Saying things are a "game changer" is often overused but Internet of Things is truly a game changer for privacy and security (so are big data and AI) GP
- Explosion of devices, significant number in the 10's of billions
- "70% of IoT devices contain security vulnerabilities"
- If it's connected to the internet it can be hacked
- Everything is being connected to the internet. Therefore, everything can be hacked
- Devices were popularized by
  - Thermostats
  - Fridges
  - Light bulbs
- Cheap to add connectivity they put it in and decide whether to use it later
  - Cars
  - Locks
  - Crockpots
  - Baby monitors
  - Fitbits
- Most IoT devices can surveil you
  - Detect presence
  - Monitor communications

- May have additional inputs, outputs, that were not necessary
- Vendors want to capture as much data as possible
- Devices have no relevant standards
- Devices have no privacy and security requirements
- No way for consumers to discern
- May use
  - No passwords
  - Passwords with low complexity
  - Hard coded passwords
- Devices are often low cost, low margin
  - Purpose built with few extras
  - Revenue trumps security
  - Usability and first to market
- May be so cheap they are designed to be disposable
  - Throw them away, may keep working
  - Imagine if so ubiquitous our oceans are filled with them as are the skies and the sewers
  - Could be so small you excrete them

7.6 Rules for IoT Devices

1. Be able to turn it off
2. Be able to disconnect it
3. Be able to update/patch it

7.7 Top IoT Vulnerabilities

- Weak, guessable/predictable, or hard coded passwords
- Insecure network services
- Insecure ecosystem interfaces (eg. web, api)
- Lack of secure update mechanism
- Insecure or outdated components
- Insufficient privacy protection
- Insecure data transfer and storage
- Lack of device management
- Insecure default settings
- Lack of physical hardening
- Inability to turn on/off
- Inability to update/patch
- Insufficient privacy
- Integration with cloud

7.8 Solutions

- Have to know what is there first
  - Surprising how many devices
- Use reputable vendors
  - Watch out for the apps
- Do your research
  - What features does the device have?
- If you don't need it connected then don't
  - Examine what features it supports (wired, WiFi, infrared, Bluetooth)
  - If WiFi, is it a client, access point, how many of each?
- Update products regularly, patch them
- Protect them with firewalls
- Put them on a different VLAN or SSID
- Monitor the activity (logs or traffic)

7.9 Mobile Devices

- Weak or not authentication
- What are you protecting?
- Jailbreaking, rooting devices
- iPhone, Android, Windows, BlackBerry
  - Which is most secure? Why?
- Side-loading apps
- Whitelisting, blacklisting apps
- Enforcing controls
  - BES (BlackBerry Enterprise Server)
  - ActiveSync
  - Mobile Device Management (MDM)
  - Enterprise Mobility Management
- Containerization
  - Where to authenticate?
- Device ownership
  - Personal device
  - Employer device

Common models

- Bring Your Own Device (BYOD)
- Choose Your Own Device (CYOD)
- Here's Your Own Device (HYOD)