SENG 460 / ECE 574
Practice of Information Security and Privacy

Review for Final Exam

Gary Perkins, MBA, CISSP

garyperkins@uvic.ca

University of Victoria

Definitions

- **Information Security** – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

- **IT security** - "safeguards" to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information

- **Cybersecurity** – The ability to protect or defend the use of cyberspace from cyber attacks.

- **Cyber Attack** – An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

- **Cyberspace** – A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

University of Victoria

Sources: NIST and Government of Canada Policy

Security Threat Landscape

- significant shortage of jobs in cybersecurity
- cybersecurity has never been as imperative as it is today
- cybersecurity is not solely an IT problem – it is a business enterprise risk
- security is not just the responsibility of the security team, it's everyone's responsibility
- impacts of cyberattacks is much greater than simply a virus on a computer
- incidents are increasing in frequency and are more sophisticated and targeted than ever
- no organization globally is immune to attack
- organizations will be judged not only on their ability to prevent but detect and respond
- doing the basics well will stop 80% of the problems
- security is not just an IT problem, it's business enterprise risk
- cyber attacks are more frequent, effective, targeted, sophisticated, profitable, elusive
- threat actors include juveniles, insiders, hacktivists, organized crime, nation-states, cyber terrorists
- threat actors have different motivations, sophistication, and access to resources
- juveniles are typically associated with the lowest sophistication and nation-states the highest
- organizations do not get to choose whether they are targets – they are targeted whether they have something of value or there is the perception they do
- organizations are targeted to gain economic advantage, get access to financial or personal data (eg. health) for fraud, identity theft, take over systems as a launch point against others, retribution or make a statement, cause damage or distraction, surveillance and other reasons
- impacts to businesses include direct impact to clients/customers, disruption of operations, financial/value loss, litigation/regulatory, data breach and loss, brand and reputation, lost/stolen intellectual property, lost productivity

Security Threat Landscape

- insiders: people who the enterprise has trusted to access and operate with company data
  without trustworthy insiders the organization cannot function
  2 types: malicious insider, unwitting insider
- some example of attack vectors/methods include phishing, smishing, vishing, social engineering, spearphishing, whaling, malware, cryptoware, ransomware, scareware, malvertising, waterholing, pharming, weak/no passwords/brute force, supply chain/vendors/partners, distributed denial of service (DDoS), poor coding hygiene (SQL inject, buffer overflow), exploiting other vulnerabilities
- there are many "pew pew maps" on the internet such as Norse and Kaspersky and Digital Attack Map and others that visualize some attacks
- Shodan is the search engine for the Internet of Things and provides information on what devices are connected to the internet and what ports are open without having to touch the targets directly
- goals of Information Security are Confidentiality (preventing unauthorized disclosure), Integrity (preventing unauthorized modification), and Availability (preventing disruption of service and productivity) – this is referred to as the CIA Triad
- 5 tenets of security include:
  strong authentication, least privilege, non-repudiation, separation of duties, defence in depth
- mandatory vacations: insisting that employees take vacations helps employees balance work-home life but also if they're not at work, those filling in may realize they have been committing crimes

University of Victoria

Five tenets

- **strong authentication**: more than one type of authentication (two-factor)
- **least privilege**: individual, program, or system is not granted any more information than necessary to perform the task
- **non-repudiation**: one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction
- **separation of duties**: ensures that an individual can not complete a critical task by himself. For example: an employee who submits a request for reimbursement should not also be able to authorize payment or print the check.
- **defense in depth**: layering on and overlapping of security measures is called defense in depth - the strength of any system is no greater than its weakest link - the failure of any one defensive measure should not cause failure of the system

University of Victoria

Security Controls, Standards, Audit

- passwords do not provide adequate security alone – **if you must use a password then make it long or strong** (complexity with lower case, upper case, numbers, punctuation), have password aging, history, and lockout after unsuccessful attempts
- two factor or multifactor authentication refers to something you know (eg. password), something you have (eg. hardware token), or something you are (eg. biometrics)
- AAA refers to authentication, authorization, and accounting
- 3 types of security controls are administrative, logical or technical controls, and physical
- security technology includes, firewalls, VPN, intrusion detection/prevention, web content filtering, email content filtering, DDoS prevention, anti-virus/anti-malware, Security Information and Event Management among others
- cyber insurance can help transfer risk, other options are to avoid, accept, or mitigate
- standards/frameworks include ITIL, COBIT, NIST, NERC, HIPAA, ISO 17799/27001, ISO 27002
- audits include SOX, SAS70/SSAE16, PCI
- audit, certification, accreditation
- breaches like Home Depot were attacked through supply/chain/vendors they used, malware installed on Point of Sale (PoS) devices and stole unencrypted credit card numbers
- binary, TCP/IP, IPv4, IPv6 addressing, routing, Class A/B/C/D/E
- subnetting is used to reduce network congestion, increase performance, and create smaller network chunks
- **DHCP** provides IP addresses, subnet mask, gateway, DNS servers; dynamic and static IP addresses
- **DNS** resolves hostnames to IP addresses and IP addresses to hostnames
- MAC address, ARP, RARP, CIDR, localhost, broadcast, ping, traceroute, nslookup, dig, whois, telnet

Ports, Network Security, OSI

- hub, switch, router, default route, routable and non-routable IP addresses
- NAT, PAT, proxy
- **difference between NAT and proxy is that the proxy is ‘application aware’ and the traffic often stops and starts again – transparent proxy is the exception**
- TCP vs UDP, SYN, SYN-ACK, ACK
- well known ports are 0-1023, registered 1024-49151, dynamic/private 49152-65535
- common ports are 20/21 FTP, SSH 22, telnet 23, SMTP 25, DNS 53, DHCP 67/68, TFTP 69, HTTP 80, POP 110, IMAP 143, HTTPS 443, SQL 1433, MySQL 3306, RDP 3389, VNC 5800-5900+, IRC 6667+
- secure protocols vs not – best examples of unsecure protocols are telnet and FTP (there are secure equivalents in SSH and SFTP)
- firewall and rules are often formed on source/destination/port/action
- 5 tuple is: source IP, source port, destination IP, destination port, protocol/port/service
- cleanup rule is any any drop at the bottom of the firewall policy
- stateful inspection firewalls track the record of the connection in the connection table to know if the return packet should be allowed
- OSI model – application, presentation, session, transport, network, data link, physical
- hub/repeater is at physical, switch at data link, router at network
- Man in the Middle, spoofing
- virus, worm, trojan, spyware, DoS, DDoS through reflection attacks, amplification
- hacktivist method of operations – DDoS, defacement, doxxing
- privilege escalation, remote code execution

University of Victoria

OSI Model will be tested

Attacks

- ping flood, ping of death, SYN flood, UDP flood, smurf, fraggle, teardrop, land, bonk, boink, jolt, ssping, pepsi, jizz, ICMP nukes
- buffer overflow, heap overflow, stack overflow, ARP poisoning, BGP hijacking, SQL injection
- amplification, reflection, browser hijacking, backdoors, rootkits, password attacks (brute force, dictionary attacks, rainbow tables)
- social engineering, phishing, smishing, vishing, spearphishing, zero day exploits, cross-site scripting (XSS), malvertising, waterholing
- examples of viruses, trojans, malware – Melissa, ILoveYou, CodeRed, Nimda, SQL Slammer/Sapphire, Sasser, MyDoom, Conficker
- other attacks: HeartBleed (discovered affecting CRA tax agency in Canada), ShellShock, Poodle, Freak, Beast, Drown
- Stuxnet, Duqu, Flame, Gauss
- Cryptolocker, Cryptowall, Cerber, Locky, Wannacry, NotPetya
- common security certifications – most requested ones by employers are CISSP, CISM, CISA
- if a pentester then LPT, GPEN, CEH
- if just starting out maybe Security+ or CSX Fundamentals
- FOIPPA – freedom of information and protection of privacy act
- hygiene procedural controls include information security policy, risk register, risk assessments, incident response plan, incident response team, security education and awareness, threat modelling
- conduct risk assessments on new systems and material changes to existing ones
- hygiene technical controls include: firewall, intrusion prevention, website content filtering, email content filtering, anti-virus/malware

Network Security

- network architecture
- approach to improving security – assess present state, determine future state, gap analysis, prioritize/plan, execute, communicate, measure/, report
- Lockheet Martin Killchain – reconnaissance, weaponization, delivery, exploitation, installation, command & control (C2), actions on objectives
- blue team, red team, purple team
- DMZ, VPN client to site with IPSec or SSL, Site-to-Site
- intrusion detection, intrusion prevention
- host-based, network-based
- signature-based, anomaly-based
- email filtering – blacklist/whitelist, reputation-based, anti-spam/anti-malware
- web content filtering and categories to block
- anti-malware signature-based and behaviour-based
- anti-DDoS on-prem and cloud; manual, hybrid, automatic
- SIEM enables correlation of security events and incidents across devices

Vulnerability, Risk, Privacy

- advanced persistent threats (APTs) are intended to gain access, maintain persistence, go undetected for long periods of time while trickling out data
- vulnerability identifies then it's discovered, reported, communicated, vulnerability may be theoretical at first and then exploit exists, exploit seen in use in the wild, exploit seen by company
- crown jewels: critical systems and data
- costs of a data breach went from 3.5M in 2014and up to 4M in 2016 and down to 3.86M in 2018
- risk appetite, risk register, risk assessments
- people are the single biggest risk, biggest weakness, biggest vulnerability
- privacy means people should get to choose what happens to their information
- privacy is subjective, contextual, no one definition exists
- 3 kinds of privacy: spatial, physical, informational
- reasonable expectation of privacy
- examples: age, marital status, name, email, net worth, car owner, voting habits, clicks/downloads, political party, purchases, astrological sign, DNA, internet searches, average spending, home owner, kids in house, criminal record, usernames
- identify purpose, limit collection, get consent, limit use/disclosure/retention, reasonable security, be accountable, be open and transparent, ensure accuracy, right of access and correction, provide recourse
- it is not law that you need an individuals' consent to do anything with their information – the principle is you get to choose to the greatest degree possible
- the laws alone will not protect you

Risk, Vulnerability, Exploits, Threats

- risk, vulnerability, exploits, formula risk = probability * impact, threat
- quantitative risk assessment, qualitative risk assessment (eg. low/med/high)
- asset value AV, exposure factor EF, single loss expectancy SLE, annual rate of occurrence ARO, annual loss expectancy ALE
- AV x EF = SLE and SLE x ARO = ALE so (AV x EF) x ARO = ALE
- risk appetite, tolerance, register, assessment
- exploit, threat, incident, risk owner
- controls, compensating controls, countermeasures, safeguards, mitigations
- inherent risk, residual risk
- risks can be ignored/rejected, accepted, avoided, transferred, mitigated/reduced/treated
- risk treatment, remediation, transference
- common issues: weak encryption, buffer overflows, lack of input validation, SQL injection, cross-site scripting, broken authentication or session management, misconfiguration
- control types: administrative, logical / technical, physical
- control functions: deterrent, preventive, corrective, recovery, detective, compensating

Privacy, Security, Insurance, Breaches

- **privacy**: appropriate collection, use, and sharing of personal information
- **security**: protecting such information from loss or unintended or unauthorized
- privacy policy should state:
  1) personal info you will collect
  2) why it is collected and how it will be used and shared
  3) how you will protect the data
  4) explanation of consumer benefit from collection, use, sharing, and analysis of data
- companies should give clear opt-out at every stage
- cyber insurance can play a role in organization's overall protection – you should insure against cyber the way you would insure against other risks like fire, flood, earthquake
- causes of top breaches commonly include: poor security awareness to defeat phishing, offline backups, poor patching and vulnerability management, supply chain
- Stuxnet labelled as the first cyber weapon given physical destruction (targeted Siemens PLCs in use in only one place in the world)
- Yahoo is the biggest breach on record with 3 billion records lost

Attacks, Policies, Standards, Audit

- steganography is used to conceal information in another file
- john the ripper is used to crack passwords by encrypting and comparing
- rainbow tables are a list of already encrypted passwords to compare against
- ping, traceroute, nslookup, dig, telnet
- nmap is a port scanner to determine what ports are open on a server
- policy and policy components, standards, guidelines
- personnel security, information systems and devices, access to info systems and devices, information encryption, physical security, operations security, computer network and communication security, information system procurement/development/maintenance, supplier relationships, cloud services security, supplier relationships, assurance and compliance
- security standards and frameworks: ISO/IEC 27001, ISO/IEC 27002, NIST
- audits: Sarbanes Oxley/SOX, SAS70/SSAE16, PCI DSS
- SOC 1, 2, and 3 reports, Type 1 and Type 2
- PCI and significance of the Cardholder Data Environment (CDE)
- vendor security requirements
- DarkNet, TOR browser (assist with being more anonymous but anonymity is not guaranteed)

Incident Response

- security is NOT an IT problem it is a business enterprise risk
- security is the responsibility of every employee
- cybersecurity incidents have real world harm
- there is very much a talent shortage in security
- organizations will be judged not only on their ability to prevent but detect and respond
- incident handling: logistics, communications, coordination and planning functions needed in order to resolve a security incident in a calm and efficient manner
- incident response: all of the technical components required in order to analyze and contain a security incident
- incident handling and incident response are two sides of the same coin
- incident management, investigations
- breach, compromise, vulnerability, exploit
- exploits turn vulnerabilities into incidents
- during an incident you have to think on your feet, be decisive, subscribe to deductive logic,
- in an incident you want to prevent, detect, deny, disrupt, degrade, deceive, corrupt or destroy the attack by any legal means possible
- PICERL = preparation, identification, containment, eradication, recovery, lessons learned
- incident response plan, incident response team, roles and responsibilities, exercises
- communications plans, agreements with 3rd parties
- note-taking is a key component, there are many roles to staff: incident handler, incident response, forensics, communications, media relations, note-taker, investigations, law enforcement, intelligence, privacy, legal, regulatory, vendor management, etc

University
of Victoria

Incident Response

- do not capture details in general ticketing systems
- controlling flow of communications is critical
- event vs. incident (refresh here, there will be examples)
- event is an observable occurrence in a system or network
- incident is an adverse event in an information system and/or network or the threat of the occurrence of such an event
- types of incidents (policy violation, unauthorized access, denial of service, unauthorized or inappropriate use, changes without owner’s consent, malicious code)
- containment is to prevent further damage and stop the problem from getting worse
- chain of custody
- eradication is to completely remove all traces of infection or other incident
- compromised machines cannot be trusted
- lessons learned is a critical step of the process not to be missed
- types of attacks: spam, phishing, spearphishing, malware, denial of service, DDoS, exploiting vulnerabilities, credential theft, website defacement, ransomware, extortion, compromised hosts, data breach, others
- know the difference between Denial of Service (DoS) and Distributed Denial of Service (DDoS)
- IOC is indicator of compromise

Incident Response

- DevOps or DevSecOps can allow security to be built in at every level
- security by design – built in from the beginning is easier, faster, cheaper, and more effective
- **security is not a destination, it's a journey**
- trust and verify
- cyber threats pose a real risk to the democratic process in countries around the world
- elections are increasingly using technology
- most effective defenses against ransomware are user awareness and offline/disconnected backups
- if you pay the ransom you may get your data back – the decision should be up to the business
- risk: probability that a vulnerability will be exploited and the impact if it does
- threat: any potential danger associated with the exploitation of a vulnerability; anything that has the potential to do harm
- vulnerability: absence or weakness of a countermeasure in place; flaws or weaknesses in systems, software, or procedures
- risk register: list the risk, the inherent risk, the risk trend, residual risk (know how to recognize a risk register) and the importance of a risk register
- risk appetite, tolerance, register, assessment
- exploit, threat, incident, risk owner

University of Victoria

avoid using the term hacker to refer to a cybercriminal
if someone has committed a crime you call them a cybercriminal

Incident Response

- privacy has different meaning to stakeholders based on context, societal norms, geographical location
- no consensus definition of privacy
- organizations should communicate good privacy work – publish data principles that communicate how data is gathered, protected, and shared
- compliance: company's program for ensuring adherence to cybersecurity policies, laws, regulations
- cyberinsurance – pros and cons, challenges with making successful claims and demonstrating diligence
- good advice: know what you have and who has access to it; keep only info needed to conduct business; protect info in your control, dispose of info that is no longer needed, prepare plan for responding to security incidents
- 4 categories of IP: patents, trademarks, copyrights, trade secrets
- trade secrets are the only one to maintain their value
- know when and why to engage law enforcement
- importance of background checks
- compliance is not equal to security
- clean desk policy: desk is free of sensitive information
- OSINT – open source intelligence – there are many sources
- Maltego is a tool to gather OSINT
- liability, negligence, due care, due diligence
- best evidence, secondary evidence, direct evidence, conclusive evidence
- circumstantial evidence, corroborative evidence, opinion evidence, hearsay evidence

Incident Response

- hash, salt, encryption
- don’t store passwords in plain text
- virus, worm, trojan, rootkit, keylogger, adware, spyware, bots, RAT, logic bomb, backdoor
- DoS, DDoS, man-in-the-middle, buffer overflow, SQL injection, cross-site-scripting, privilege escalation
- amplification, reflection, ARP poisoning, BGP hijacking, DNS poisoning, domain hijacking
- hijacking (clickjacking, session hijacking, typo/squatting)
- zero day vulnerability, zero day attack/exploit, replay, pass the hash
- scareware, ransomware, cryptomalware, cryptomining, social engineering (phishing, spearphishing, whaling, vishing, smishing)
- tailgating, dumpster diving, shoulder surfing
- waterholing, malvertising
- zombies, bots, botnets, white hat, black hat, grey hat
- nmap – portscanner
- Nessus – vulnerability scanner
- Metasploit – penetration testing tool
- Armitage – frontend for Metasploit
- false positive, false negative, true positive, true negative
- netcat – tool to open reverse shell from target back to attacker
- penetration testing, external, internal, blind testing, double-blind test, blackbox texting, whitebox testing

University
of Victoria

Physical Security

- physical and personnel security – **RUN HIDE FIGHT**
- guards, fences, gates, cages, locks, safes, bollards, astragals
- threat categories: natural environment, supply system, manmade, politically motivated
- fences: 3-4 ft deter casual intruders, 6-7 ft too tall to climb easily, 8+ ft deter more determined intruders
- gates: class 1 residential, class 2 commercial, class 3 industrial, class 4 restricted
- locks: warded, tumbler, combination, electronic, proximity, biometrics
- fire suppression: wet pipe, dry pipe, preaction, deluge, halon gas
- power outages: surge, brownout, fault, blackout, sags
- **CPTED – crime prevention through environmental design**

Identity

- web access management, single sign-on, Kerberos, AS, TGS, KDC
- account management, onboarding, transfer, offboarding
- differences when employees leave voluntarily and involuntarily
- aggregation of privileges, separation of duties, least privilege
- SAML: open standard for exchanging authentication and authorization data between parties (eg. identity provider and service provider)
- Oauth: open standard for access delegation (used for internet users to grant websites or apps access to their information on other websites without giving them the passwords)
- federation: arrangement between enterprises to let subscribers use same identification data to obtain access to networks
- logging, retention, review, correlation, alerting, monitoring
- information classification – important to know what your sensitive data is and where it is and who owns it – then label it – can use whatever scheme works for you – federal government is public, confidential and if confidential protected A, B, C
- access control – only allowing authorized users programs or other computer systems to gain access
- multi-factor, biometrics, fingerprints, retina, iris, vascular, gait, typing, voice, etc.
- false reject/type 1 error, false accept/type 2 error, crossover error rate, false positives, false negatives
- mandatory access control: central security grants access to specific users
- discretionary access control: data owner grants access to others as they choose
- non-discretionary access control: central authority determines – may be role-based or task-based
- role-based access control: restricting access based on role – role determines what access a person should have

Cryptography

cryptology:	cryptography & cryptanalysis
cryptography:	science of codes
cryptanalysis:	science of breaking codes (with enough time and compute, encryption will fail)
plaintext/clear text:	message in original format
ciphertext/cryptogram:	message in encrypted format
encryption/encipher:	transform data into unreadable format
decryption/decipher:	transform data into readable format
encoding:	changing data into another format
decoding:	changing data back into original format
running key:	this cipher is an encoding scheme that uses a secret key that is a string of words (often from a book or any text agreed to)
concealment:	message within a message
substitution:	replacing data to hide original text
transposition:	(permutation) shuffling/reordering to hide original text
one-time pad	(OTP) plaintext + OTP = ciphertext
product ciphers	using more than one cipher to deal with weaknesses introduced by our language
collision	different messages produce same hash
key clustering	different keys generate same ciphertext from same plaintext
avalanche	small changes in key or plaintext significantly change ciphertext
diffusion	small changes in plain text create significant changes in ciphertext
confusion	small changes in key lead to significant change in ciphertext
ways to protect data	**encryption, tokenization, obfuscation**

Cryptography

symmetric	private key crypto uses a single key to encrypt and decrypt; much faster than asymm
examples	block cipher: AES, DES, 3DES, Blowfish, Twofish stream ciphers: RC4
remember	you need a secure way to share the keys
asymmetric	public key crypto uses a different key to encrypt and decrypt; slower than symmetric
examples	Diffie-Hellman Key Exchange, RSA, DSA, Ellpitic Curve, PGP/GPG
stream cipher	treats message as stream of bits and performs math functions on each bit individually
block cipher	original message divided into blocks of bits and blocks are put through functions one block at a time (best example is DES)
RSA	each user generates public/private key pair; publish public key, keep private key secret user A encrypts message with user A's private key and user B's public key
hash	message integrity to ensure a message has not been altered (examples: MD5, SHA1, SHA2)
PKI	set of hardware, software, people, policies, and procedures needed to create manage distribute use store and revoke digital certificates; provides confidentiality/encryption, message integrity, authentication, and non-repudiation components include: certificate authorities CA, certificate revocation list CRL, registration authorities RA
note	third parties can check the CRL to determine if cert is valid – if cert is no longer valid then it is no longer trusted
types of certs	user, device, SSL
certificates	can be used for digital signatures, encrypting email, encrypting files, authentication
digital signature	supports non-repudiation and integrity
cross-certification	when two certificate authorities CA issue certificates to each other for trust
certificates	can be used to sign, encrypt, sign and encrypt

X.509 is a standard for the format of a certificate

Cryptography

- certificate policy (CP) where all the agreed upon rules sit that build trust in the environment
- key management ensuring keys are protection during creation distribution transmission, storage, and destruction
- note you need to keep old keys in order to decrypt files and data
- self signed another type of certificate with low assurance level as the company signed itself
- wildcard certs rather than have a cert for tulip.flowers.com and roses.flowers.com have a cert for *.flowers.com – this is a bad practice as anyone using the certificate could leak it and expose the other users
- attacks:
    - ciphertext-only: attacker has ciphertext of several messages
    - known plaintext: attacker has plaintext and corresponding ciphertext of one or more messages
    - chosen plaintext: attacker has plaintext and ciphertext and can choose plaintext that gets encrypted to see corresponding ciphertext
    - chosen ciphertext attack: attacker can choose ciphertext to be decrypted and has access to resulting decrypted plaintext
- birthday paradox probability that 2 or more people in a group of 23 share the same birthday is greater than 50.7%
- birthday attack exploits math behind birthday paradox in probability theory

Internet of Things (IoT) & Cloud

- issue raises significant security and privacy concerns as the devices were not created with security and privacy in mind – projected to have 10’s of billions of devices
  often sold by companies that don’t understand privacy and security
  may use no password, weak password, or hardcoded password
  may have default, generic, or undocumented accounts
- **use cases be able to identify possible security/privacy concerns for a given IoT device (eg. Nest)**
- security know what devices you are using, buy from reputable vendor, put them on a separate network, best to have visibility into what they might do
- cloud delivering hosted services over the internet with flexibility, scalability
- 3 types Software as a Service (SaaS), Platform as a Service (PaaS),
  Infrastructure as a Service (IaaS)
- note cloud **can** have greater security given large providers can invest so much in security
  often comes down to how the cloud is configured and whether users are using security controls they have access to properly
- approaches to securing cloud – standards based leveraging a cloud standard or framework like CCM, ISO 27017, NIST 800-53
- north-south in and out of the data centre
- east-west within the data centre

Mobile Device Security

- BlackBerry Enterprise Server (BES)
- ActiveSync
- Mobile Device Management (MDM)
- Enterprise Mobility Management (EMM)
  - examples include AirWatch, MaaS 360, MobileIron
- jail-breaking, rooting devices
- side-loading apps
- whitelisting, blacklisting apps (not a good method of security given how many apps there are and how many updates – eg. an app that was good may not be good after next update)
- containerization
- device ownership – personal or employee
- common models are bring your own device BYOD, choose your own device CYOD and here's your own device HYOD

University of Victoria

Privacy

- expectation of privacy
- reasonable use
- appropriate use policies
- Personal Information Protection and Electronic Documents Act (PIPEDA) applies to many provinces **except** for Alberta, British Columbia, and Quebec as they have private-sector laws that are deemed substantially similar to PIPEDA
- Personal Information Protection Act (PIPA) applies to private sector in BC
- Freedom of Information and Protection of Privacy Act (PFIPPA) applies to public sector
- mandatory breach notification (as of Nov 1, 2018 organizations subject to PIPEDA required to report, notify affected individuals, keep records of breaches)

Business Continuity Plan (BCP)

- BCP plans and framework to ensure business can continue in an emergency
  minimize cost associated with disruptive event and mitigate risk
- 4 elements scope and plan initiation, business impact assessment (BIA), business continuity plan development, plan approval and implementation
- 3 goals criticality prioritization, maximum tolerable downtime estimation, resource requirements
- BIA detailed/documented process to identify and prioritize business functions and workflow including establishing RTO by assessing impacts over time that might result if organization was to experience a disruptive event
- process information gathering, risk analysis and threat assessment, determine key metrics (MTD, RTO, RPO), develop impact statements
- other business priority service, critical services
- backups full (all files backed up), incremental (changed files; archive bit reset), differential (changed files; archive bit not reset)
- RPO recovery point objectives – point in time at which available data from backup can be restored (maximum amount of data loss or work loss for a given process)
- RTO recovery time objectives – amount of time a business ufnction can withstand an interruption before a negative or unacceptable consequence occurs
- MTBF how frequent are failures
- MTTR how long to repair equipment on average
- availability (total time – downtime)/total time
- WRT time required to configure systems
- MTD maximum tolerable downtime MTD = RTO + WRT
  period of time after which the organization would suffer considerable pain if process were unavailable

Disaster Recovery Plan (DRP)

- DR disaster recovery refers to IT recovery
- DRP disaster recovery plans (DRPs) document the process to recover and restore the technology needed to support critical business functions
- goal recover from emergency with minimum impact on business; people are the #1 priority
- difference DRP is the effort to recover IT system and applications whereas BCP is the effort to recover business processes
- hot site fully configured, all hardware and data (resume operations in < 1 hr)
- warm site configured, data may not be in real time, backups may be required
- cold site facility available with power and HVAC but no computer hardware or data
- **HVAC heating ventilation and air conditioning**

Security Controls and Alerts

- Superman problem: refers to security use case where a person cannot be in two places at the same time and so if the logs show logging in from Paris and Vancouver it is very suspicious (it is still possible to do from a network perspective, it’s just cause to examine it more closely)
- **alert fatigue:** when analysts are exposed to so many alerts they are overwhelmed and unable to action any
- goal with many security systems is to prevent – however if need intervention from a human then the alert should be actionable
- can test the organization through drills, or red teaming or other penetration testing
- mission for blue and red teams is the same – protect the organization and improve security posture
- can assess the organization through self-assessment or hire an organization to perform an assessment

- zero trust: security posture focuses on only allowing legitimate users and applications as opposed to trying to block everyone – concept that castle and moat doesn’t work – no-one is trusted by default, verification is required for everyone

Secure Coding

- secure coding validate your input, use secure protocols, never store or pass passwords in plain text, don’t proceed with known vulnerabilities and patch new ones that arise
- OWASP: Open Web Application Security Project (guidelines for web app security)
- SQL injection: due to insufficient input validation, attacker is able to input SQL commands that are executed – example: password’ OR ‘1=1
- XSS: due to insufficient input validation, attacker is able to input code that is executed
  <script>alert(‘xss’);</script> (I will totally ask this question a second time)
- session hijacking: attacker sniffs traffic and captures session and replays to target server
- CSRF: cross-site request forgery when victim visits a website and then attackers website and attacker site contains CSRF code and attacker makes victim post code to original website
- buffer overflows eg. writing 10 bytes of data to an 8 byte buffer
  program may become unstable, crash, or return corrupt info – can run other code

How to build a secure organization

Example steps:

1) pick a relevant standard for your organization (eg. ISO, NIST, NERC)
2) conduct a present state assessment
3) determine future state
4) perform a gap analysis
5) prioritize and plan
6) execute
7) measure
8) communicate and report out

- pre-requisites of a security program include:
  - importance recognized by executives
  - roles and responsibilities are identified and assigned
  - crown jewels are identified
  - risk appetite is known and risk register reviewed quarterly
  - risk assessments conducted
  - security assessments conducted
- components of a security program should include
  - asset management, change management, incident management
  - business continuity plan (BCP), disaster recovery plan (DRP), backup & retention
  - logging & monitoring, access control, security governance
  - defence in depth for endpoints and networks
  - vulnerability management & patching, security awareness, vendor security requirements
  - security incident response, security policy, security classification

also physical security and criminal record checks

How attackers attack organizations

- conducting reconnaissance, gathering information
- weaponization – forging something sinister out of the average or commonplace
- delivering the malware to the target
- exploitation happens when the malware is triggered
- installing the malware on the target system and establishing a backdoor
- command and control – can exfiltrate data, do harm, DoS…
- attacker may move laterally to infect another host so won’t get locked out when it is found because they still have the original
- actions on objectives depends on the specific mission
- sophisticated threat actors will be watching to know when you are on to them
- tailgating: gain physical access to organization by walking in behind someone else
- dumpster diving: searching in discarded items/garbage for information
- shoulder surfing: looking over someone’s shoulder/surveilling them to get information
- social engineering: tricking users into doing something

Summary

- cyber attacks are a significant global problem
- increasing in frequency, sophistication, profitability, persistence
- significant shortage of security professionals
- security is not the role of security professionals alone – it’s everyone’s responsibility
- security is not solely an IT problem either

exams will repeatedly test the core security principles to ensure they are very well known.

University of Victoria

University of Victoria