SENG 460 / ECE 574
Practice of Information Security and Privacy

Week 10

Cryptography, PKI, Business Continuity Planning,

Disaster Recovery Planning, Review

Gary Perkins, MBA, CISSP

garyperkins@uvic.ca

University of Victoria

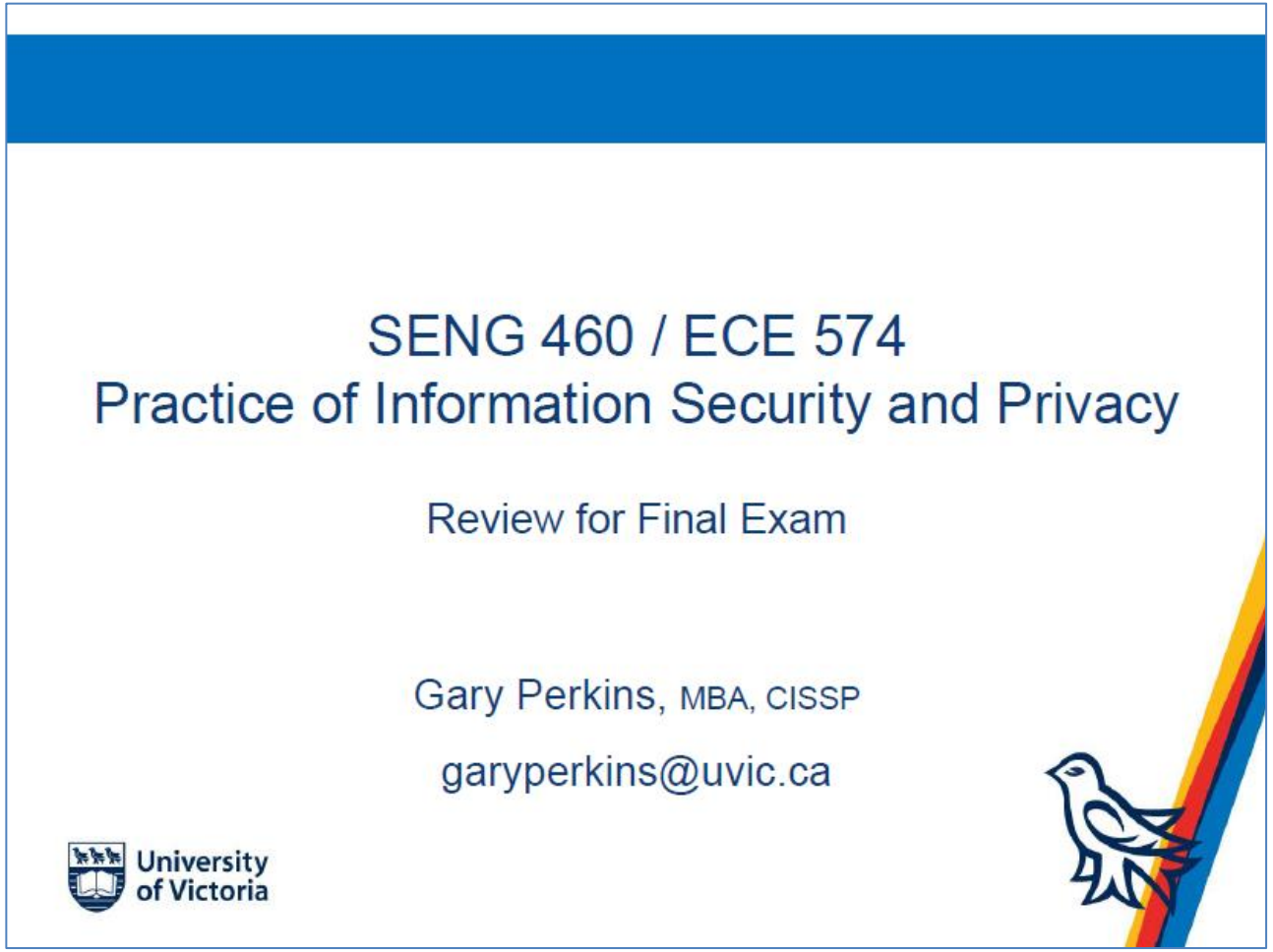
Final Exam

- What: SENG 460 / ECE 574 Final Exam (cumulative)
- When: April 11th to 26th online (BrightSpace)
- How: Multiple choice, true/false, with scenarios
  - >10000000 questions

University of Victoria

Final Exam

- posted review slides online including a number of terms



University of Victoria

Course Survey

- online Course Experience Survey (CES)
  - https://www.uvic.ca/learningandteaching/students/course-experience-survey/index.php
  - https://ces.uvic.ca

- please fill it out – I read every entry and use the results to improve the course
- include things to keep doing, start doing, stop doing

University of Victoria

Security News Digest

www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/info...

People 65+ and Indigenous peoples 18+ can **register to get vaccinated** | **Province-wide restrictions** are in effect

BRITISH COLUMBIA

Menu

Home > British Columbians and our governments > Services & policies for government > Information Management & Technology > Information Security >

- Privacy & Personal Information
- Information Security
  - Security Schedule
  - Professional Development
  - Information Security Classification
  - Defensible Security
  - Awareness
  - Cyber Security Alerts & Notifications
  - Information Incidents
  - Security Threat and Risk Assessment
  - **Security News Digest**
  - Provincial Security Advisory Council
  - Cyber Security Incident Response Process
  - Security Roles and Responsibilities
  - External Security Services
  - Information Security Quick

Security News Digest

What's Happening in Security...

A weekly security news brief from various news sources, the Security Ne
are interested in being added to the distribution list please contact us.

Current Digest: April 6, 2021

Archive

If you are interested in a previous issue (not listed below) of the Security

March 30, 2021

March 23, 2021

March 16, 2021

March 9, 2021

March 2, 2021

February 23, 2021

February 16, 2021

February 9, 2021

February 2, 2021

January 26, 2021

April 6, 2021

Try our April Working Remotely Quiz

This week's stories:

U.S. looks to keep critical sectors safe from cyberattacks

Stolen Data of 533 Million Facebook Users Leaked Online

Facebook takes down troll farm linked to Iranian opposition group

Data scraped from 500 million LinkedIn users found for sale online

Hackers From China Target Vietnamese Military and Government

Conti Gang Demands $40M Ransom from Florida School District

UC Berkeley confirms data breach, becomes latest victim of Accellion cyber-attack

GitHub investigating crypto-mining campaign abusing its server infrastructure

How the quick shift to the cloud has led to more security risks

How To Defend the Extended Network Against Web Risks

Hackers Targeting professionals With 'more_eggs' Malware via LinkedIn Job Offers

Sensitive Student Data leaked online by Ransomware Gang

In a rare step, Activision warns CoD players of malware hidden in cheat apps

North Korean Group Targets Security Researchers - Again

OCIOSecurity@gov.bc.ca
or Sophos

Security Day

REGISTER

The Province organizes and hosts two "Security Day" events each year (spring and fall), free of charge. Government employees, representatives from the broader public sector, school districts, post secondary institutions, municipalities, crown corporations, and the general public are encouraged to attend via webcast.

The theme this May is Vulnerability Management: To Patch or Not to Patch? Silly Question!

Stay tuned for updates - the Information Security Branch will provide an agenda in the coming weeks.

Previous Events

- November 2-3, 2022
- May 10, 2022
- November 3, 2021
- June 23, 2021
- May 27, 2020
- November 20, 2019
- June 13, 2019

Contact Information

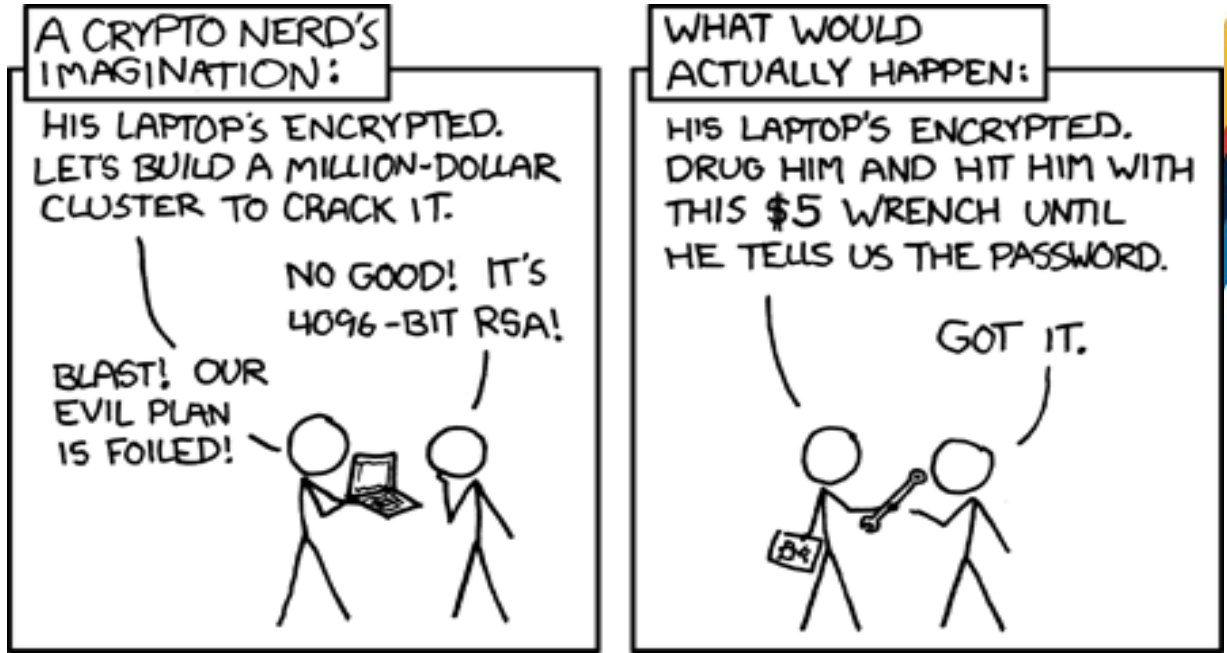
Contact the Security Day organizers.

Cryptography

Tales from the Crypto:

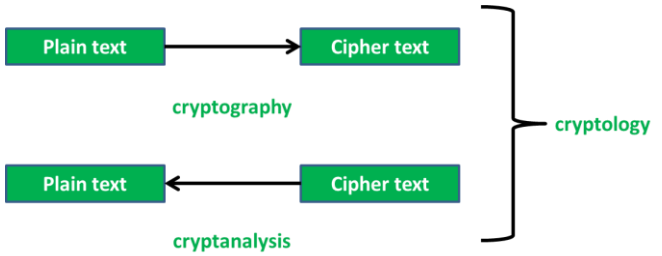
https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/professional-development
Or
https://youtu.be/lJvFfwgeKu8
Or
https://www.youtube.com/watch?v=lJvFfwgeKu8

University of Victoria



Terms

- cryptology — cryptography & cryptanalysis
- cryptography — science of codes
- cryptanalysis — science of breaking codes
- plaintext — message in original format — unencrypted message
  clear text
- ciphertext — message in encrypted format — encrypted message
  cryptogram



https://www.geeksforgeeks.org/difference-between-cryptography-and-cryptology/

University of Victoria

Terms

- encryption — transform data into unreadable format
  encipher
- decryption — transform data into readable format
  decipher
- encoding — changing data into another format
- decoding — changing data back into original format

University of Victoria

Cryptography

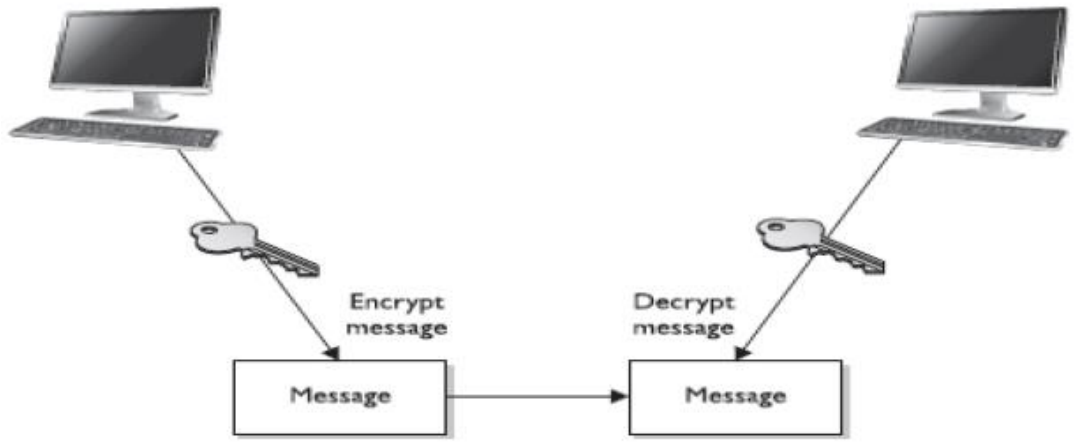
- **symmetric (private key crypto)**
  - one key to encrypt and decrypt
  - block ciphers AES, DES, 3DES, Blowfish, Twofish
  - stream ciphers RC4

- **asymmetric (public key crypto)**
  - uses pair of public and private key to encrypt and decrypt
  - Diffie-Hellman Key Exchange
  - RSA
  - also: DSA, Elliptic Curve, PGP/GPG

University of Victoria

Cryptography

- symmetric ciphers
  - sender and receiver use **two instances of same key** for encryption and decryption
  - much faster than asymmetric
  - need secure mechanism to deliver keys
  - each pair of users needs unique key (key management issues)
  - confidentiality but no non-repudiation

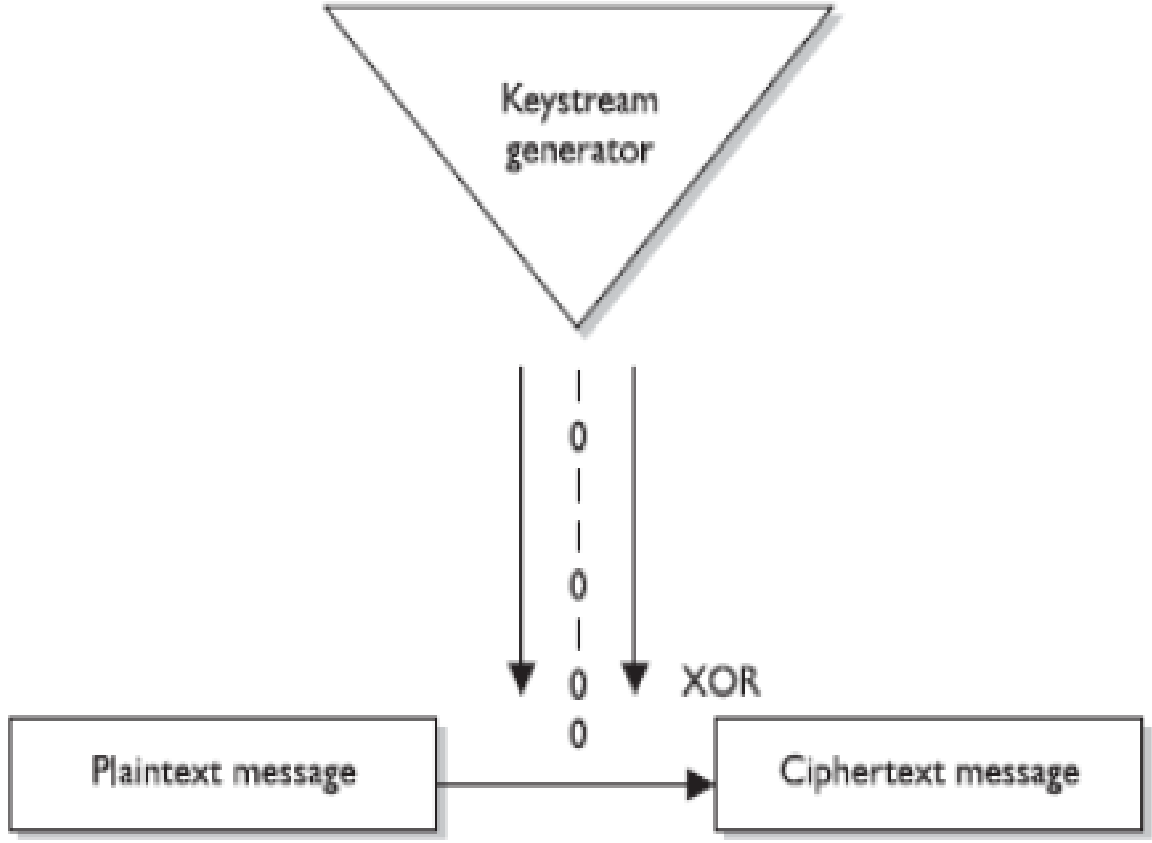


University of Victoria

Cryptography

- stream ciphers
  - treats message as stream of bits and performs math functions on each bit individually (usually XOR)
  - long periods of no repeating patterns
  - statistically unpredictable keystream
  - keystream not linearly related to key

eg. RC4 (web SSL/TLS, WiFi WEP)

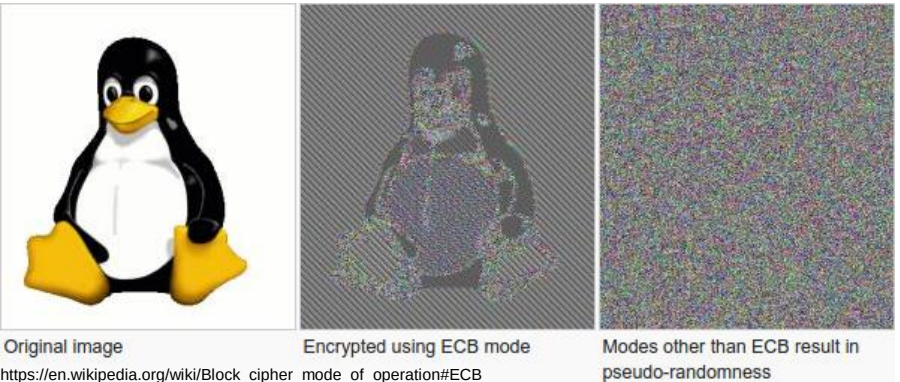


University of Victoria

Cryptography

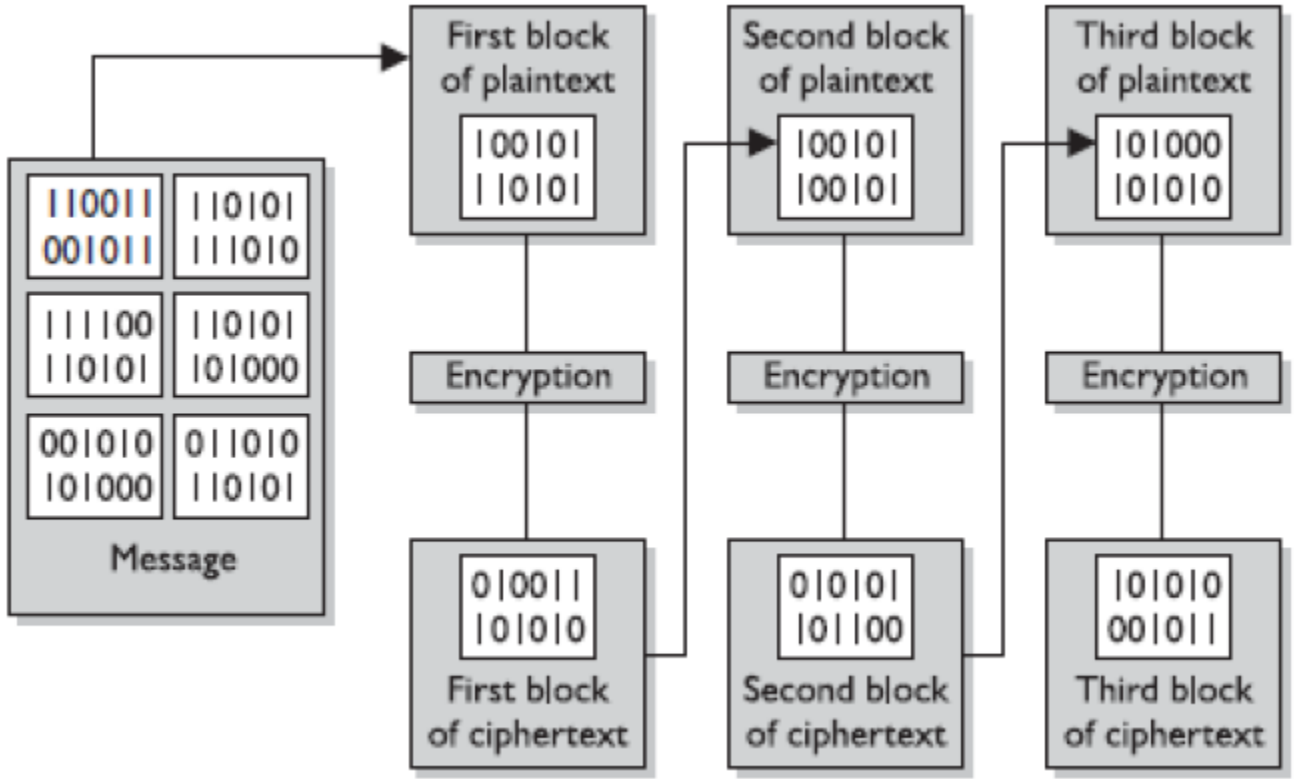
- block ciphers
  - original message divided into blocks of bits
  - blocks put through functions one block at a time

Types:
electronic code book (ECB)
cipher block chaining (CBC)
cipher feedback (CFB)
output feedback (OFB)
counter (CTR)
…others



Original image
Encrypted using ECB mode
Modes other than ECB result in pseudo-randomness

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#ECB



Cryptography

- cryptosystems provide confidentiality to ensure data cannot be read except by valid recipient
- cryptosystems provide integrity by allowing valid recipients to verify data has not been altered
- cryptosystems provide authenticity by providing the key to a valid user after that user is authenticated
- cryptosystems provide accountability by proving the origin of data – preventing sender from denying they sent the message (**non-repudiation**)

Hash

- one way encryption using algorithm and no key
- message integrity ensures a message has not been altered
- hash functions:
  - MD5 produces 128 bit hash values (not considered secure)
  - SHA1 (Secure Hash Algorithm) produces 160 bit hash
  - SHA2 produces 224/256/384/512 hash values

Terms

- **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

University of Victoria

Public Key Infrastructure (PKI)

- set of hardware, software, people, policies and procedures needed to create, manage, distribute, use, store and revoke Digital Certificates
- **different types of certificates: user, device, SSL**
  - demo SSL and user certificates
- **main components of PKI include**
  - certificate authorities (CA)
  - certificate repository and certificate revocation list (CRL)
  - registration authorities (RA)

Review - PKI

- uses for PKI
  - digital signatures
    - cryptographically ‘prove’ it came from the sender
  - email encryption
    - encrypt the contents of the email
  - file encryption
    - encrypt the contents of the file
  - authentication
    - grants access to a system

can be signed
can be encrypted
can be signed and encrypted

X.509 Standard
OCSP

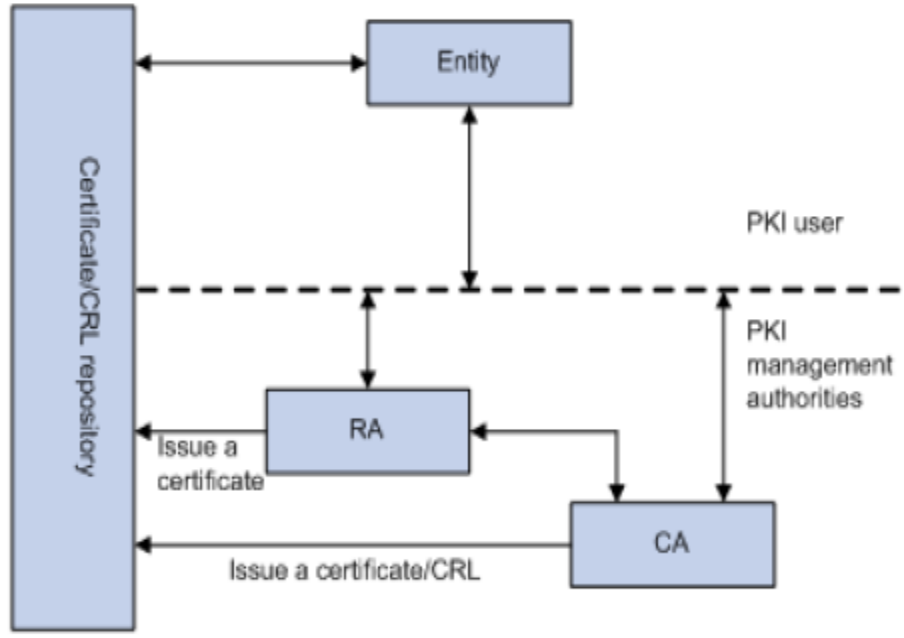
Public Key Infrastructure (PKI)

- certificate request
  1) user requests a digital certificate from RA
  2) RA verifies and validates user's identity info
  3) RA forwards certificate request to CA
  4) CA creates certificate and publishes certificate in repository
  5) user receives certificate (including public key) and private key

certificate authorities (CA)

certificate repository and certificate revocation list (CRL)

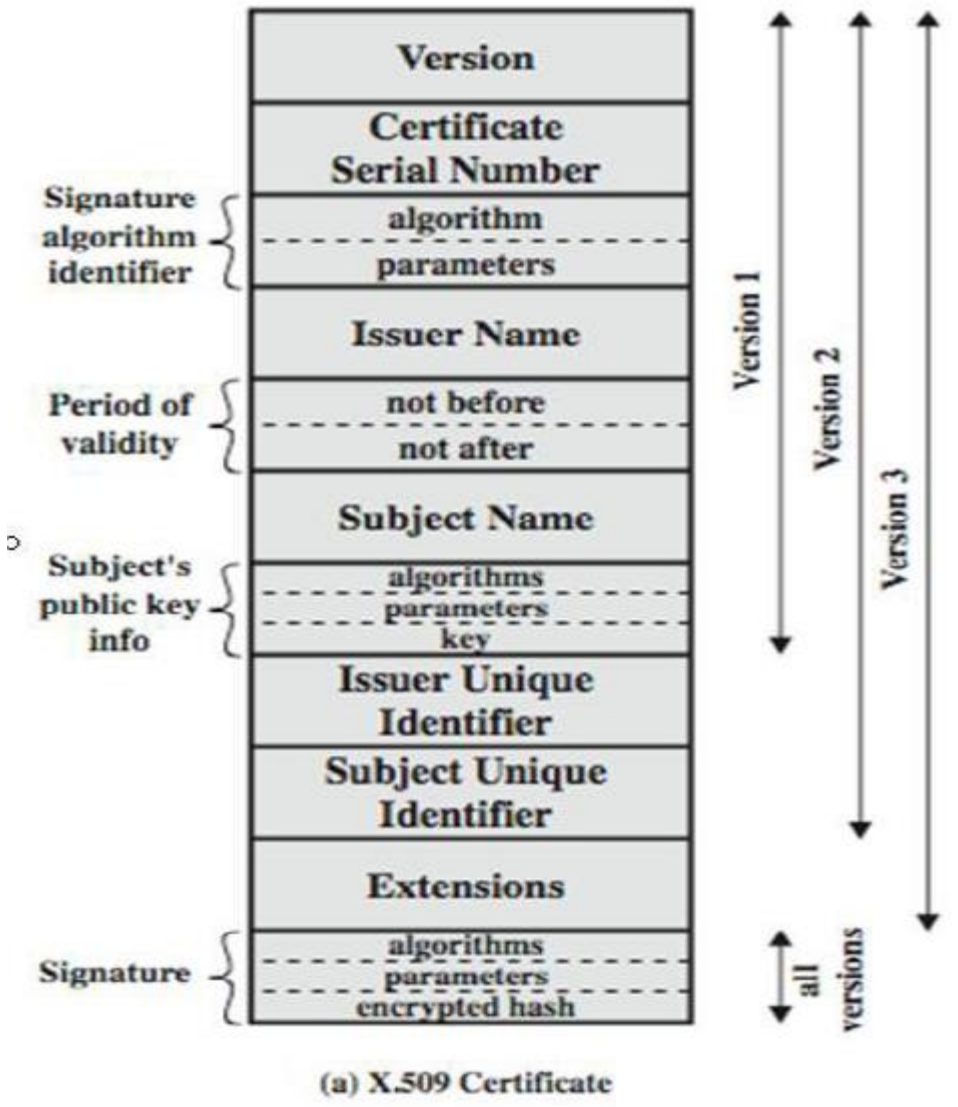
registration authorities (RA)



University of Victoria

Public Key Infrastructure (PKI)

- certificate associates public key with unique owner
- version, serial number, identifier
- validity period (start, end)
- public key info
- unique identifiers for issuer and subject
- signature

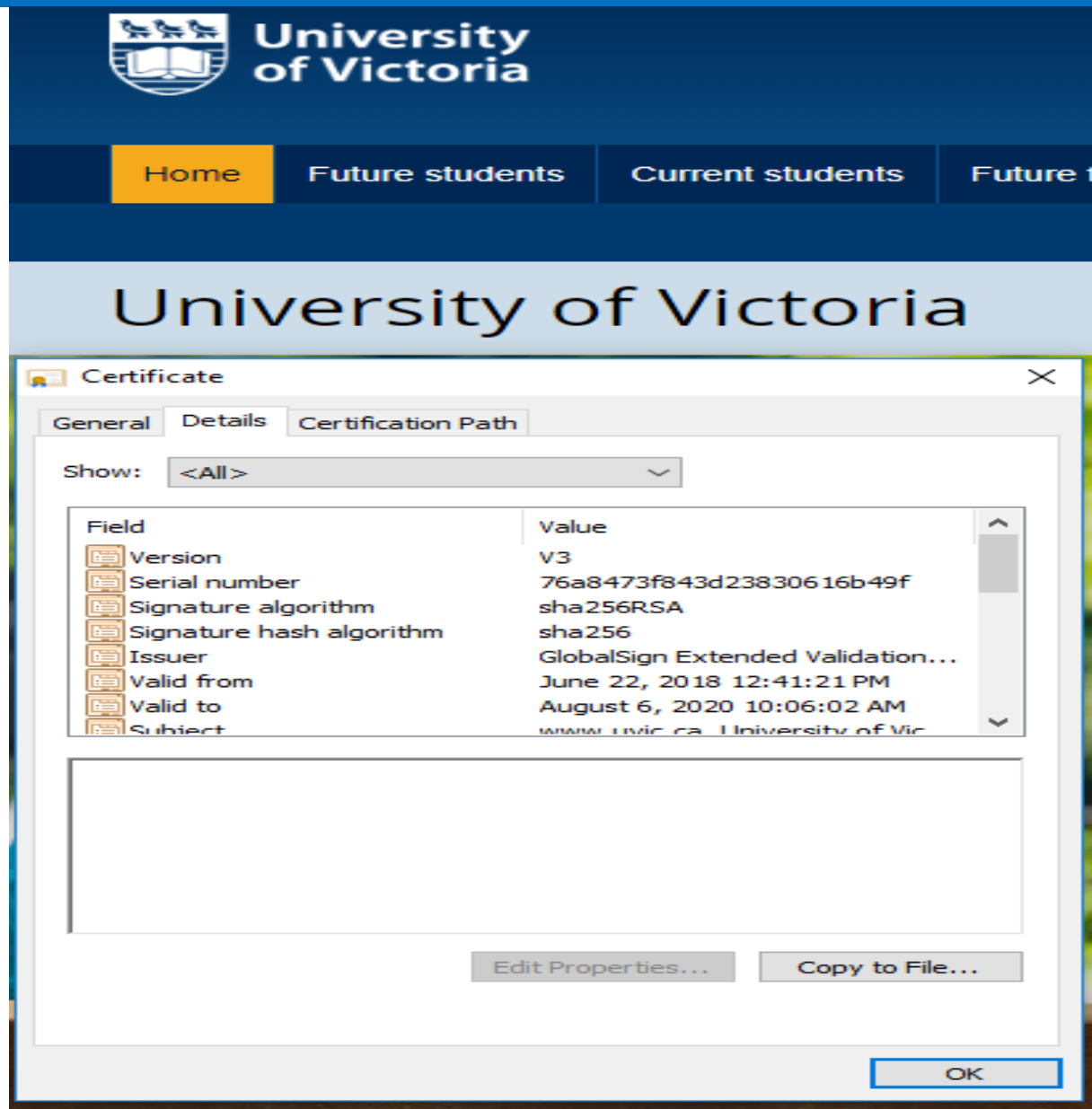


(a) X.509 Certificate

University of Victoria

Public Key Infrastructure (PKI)

- certificate associates public key with unique owner
- version, serial number, identifier
- validity period (start, end)
- public key info
- unique identifiers for issuer and subject
- signature



University of Victoria

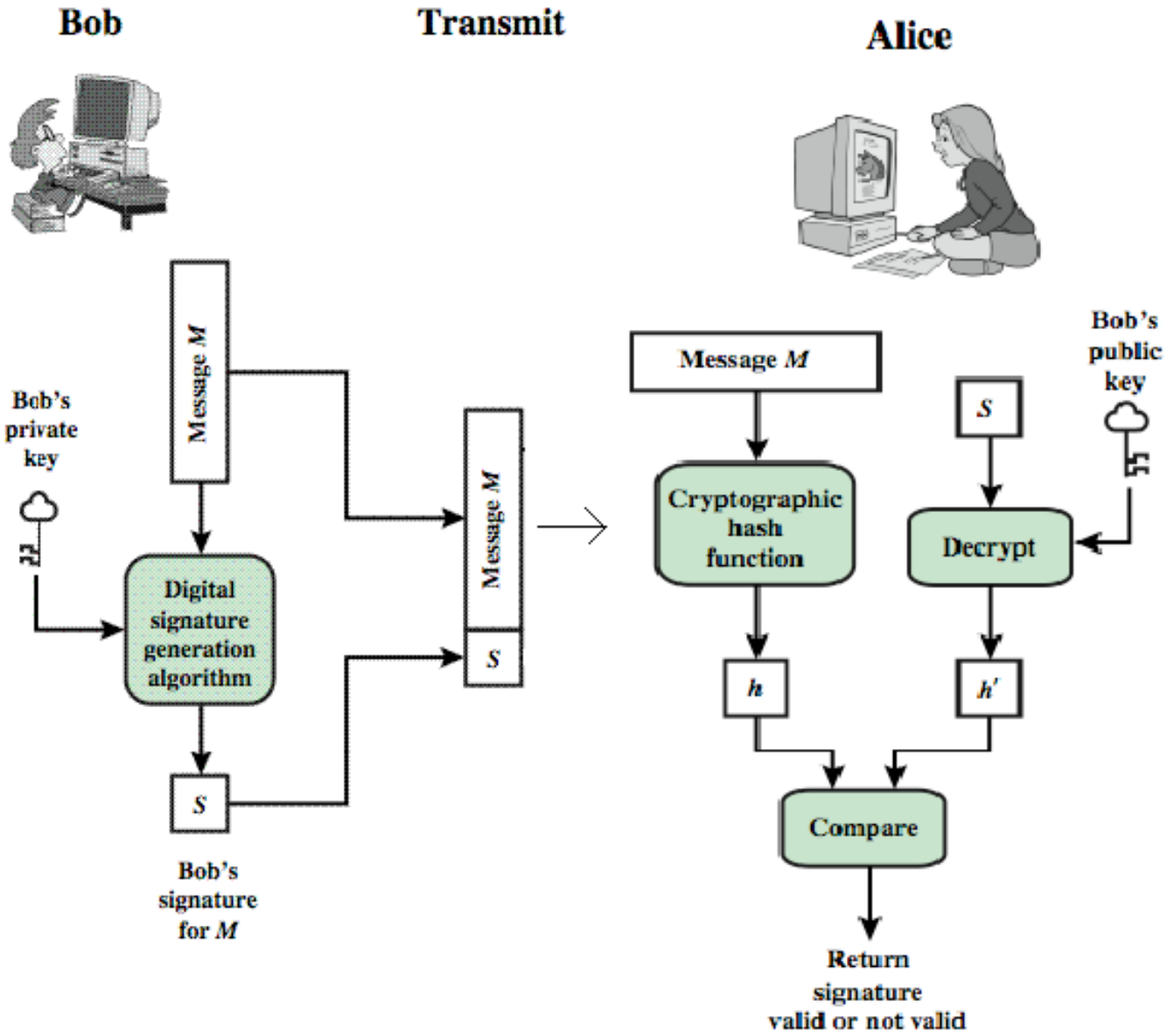
Public Key Infrastructure (PKI)

- **PKI provides confidentiality/encryption, message integrity, authentication, and non-repudiation**
- secure communication
  1) User1 requests User2's cert from User2 or repository
  2) User1 validates User2's cert by verifying signature
  3) User1 encrypts secret with User2's public key and sends encrypted secret to User2 with User1's certificate
  4) User2 decrypts secret using his private key, verifies User1's cert, generates his own secret, encrypts secret with User1's public key and sends encrypted secret to User1
  5) User1 decrypts User2's secret using own private key

Can now communicate securely
When should a user give out private key?

Public Key Infrastructure (PKI)

- digital signature
  - hash value encrypted with sender's private key
  - provides authentication, non-repudiation, and integrity



University of Victoria

Public Key Infrastructure (PKI)

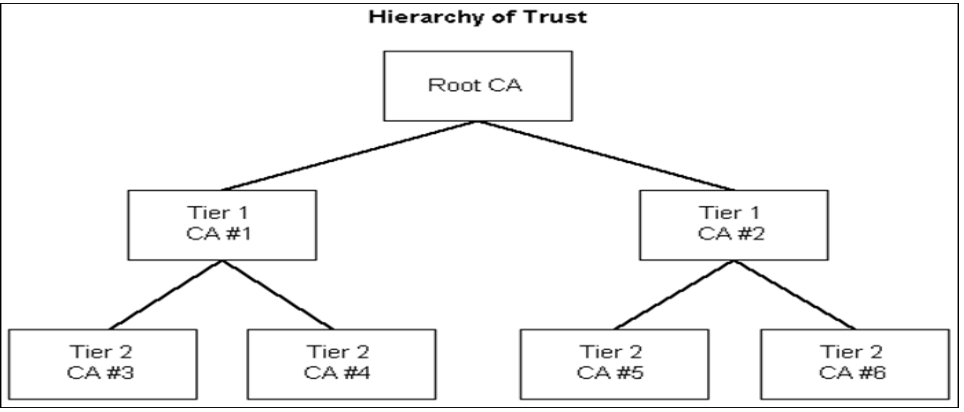
- where do you get the public key from?
- cross-certification
  - happens when two CAs issue certificates to each other
- all about trust
- consider assurance levels
- key management***
  - ensuring keys are protected during creation, distribution, transmission, storage, and destruction
- why should key recovery require more than one person?

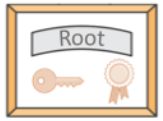
Cloud & BYOK

Certification: XKMS, X-KRSS, X-KISS

Public Key Infrastructure (PKI)

- root CA and chain of trust

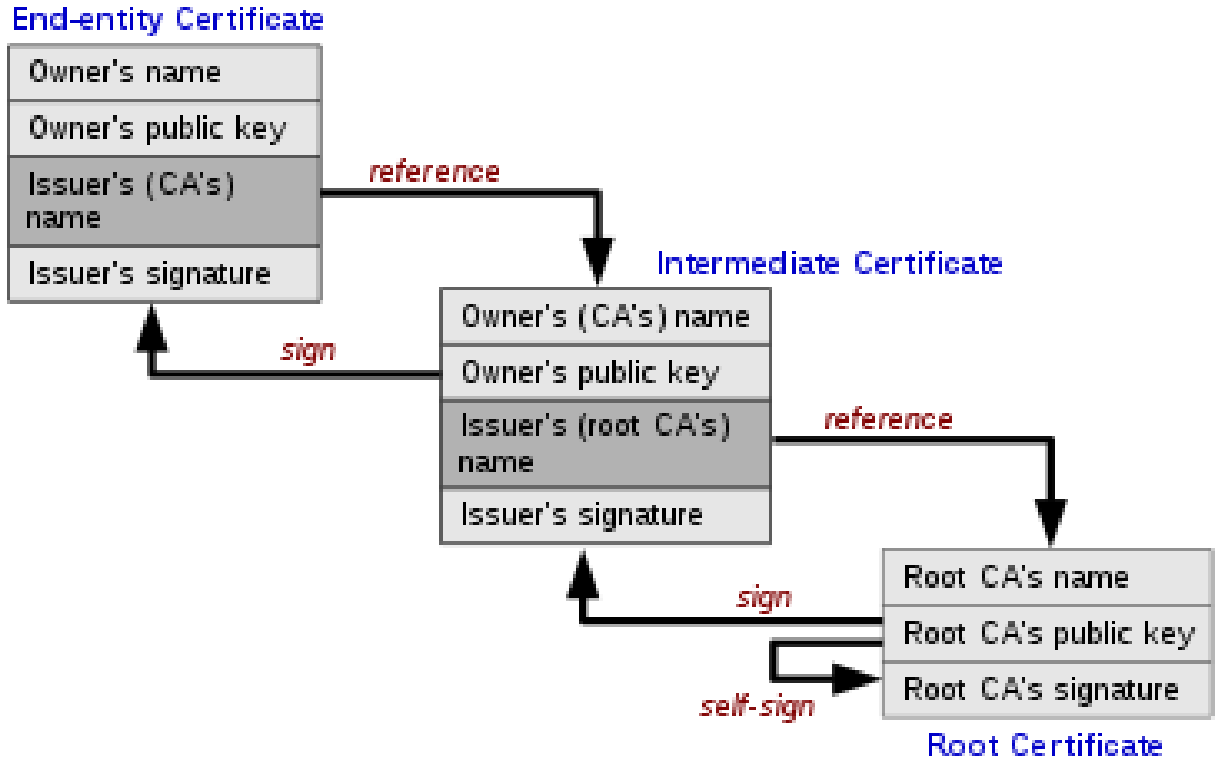




Root Certificate:
- Self-Signed, well known
- Has Root Certificate public key
- Signed by Root Certificate private key

Certificate 1:
- Has own public key
- Signed by Root Certificate private key
- Use Root Certificate public key to prove authenticity

Certificate 2:
- Has own public key
- Signed by Certificate 1 private key
- Use Certificate 1 public key to prove authenticity



- self-signing
- wildcard certs
- where to store certs?

Public Key Infrastructure (PKI)

- digital signature example
- email example
- encrypt file example

Demo?

- authentication example (encryption)
- SSL example (encryption)

University of Victoria

Public Key Infrastructure (PKI)

- certificate policies (CP) and rules
- key management lifecycle
- hardware storage of a key:
  - TPM trusted platform module
  - HSM hardware security module
- software storage of a key
- certificate revocation list (CRL)

University of Victoria

Cryptography

- 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
  - **differential cryptanalysis:** study of differences in input affects output
  - **side-channel attack**: uses info (timing/power consumption) gathered to determine processing functions
  - **replay attack**: valid transmission repeated to allow unauthorized access
  - **meet-in-the-middle**: uncover mathematical problem from two ends

Cryptography

- techniques
  - **frequency analysis**: study frequency of letters in ciphertext (effective to break classical ciphers)
  - **covert-channel attack**: gather outside info with goal of uncovering encryption key
  - **replay attack**: capture some data and resubmit to fool receiving device
  - **reverse engineering**: obtain cryptographic product and try to reverse the product to discover vulnerabilities

Review

- encryption
  - encryption is a big deal
  - most common way that comes to mind when protecting information at rest or in transit
  - tokenization and obfuscation are others
- common statement
  - with enough time [and compute] all existing cryptography will fail
  - consider quantum computers and what may be strong enough today is not strong enough ‘tomorrow’
  - consider - if someone accumulates encrypted materials now may decode in future and whether still relevant

Review

- Birthday Paradox
  - probability that two or more people in a group of 23 people share the same birthday is greater than 50.7%
- Birthday Attack
  - exploits the math behind the birthday paradox in probability theory
  - used to find collisions of hash functions

University of Victoria

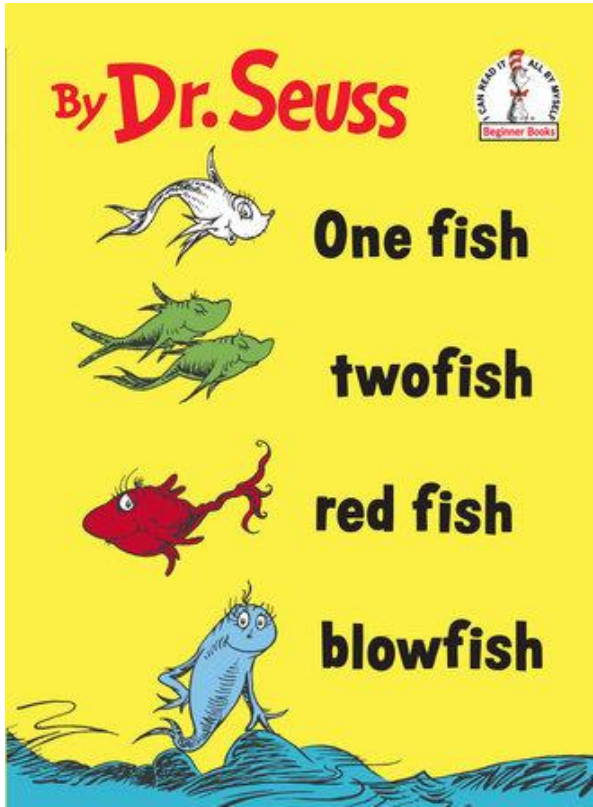
Certification

- Cryptographic life cycle (e.g., key management, algorithm selection)
- Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves)
- Public Key Infrastructure (PKI), Key management practices
- Digital signatures, Non-repudiation
- Integrity (e.g., hashing)
- Understand methods of cryptanalytic attacks
- Digital Rights Management (DRM)
- Describe the impact of certificates on security (includes PKI, public/private crossing the network, asymmetric/symmetric)
- Identify the certificate components in a given scenario
  - 2.11.a Cipher-suite
  - 2.11.b X.509 certificates
  - 2.11.c Key exchange
  - 2.11.d Protocol version
  - 2.11.e PKCS

Certification

- Understand fundamental concepts of cryptography
  - Hashing
  - Salting
  - Symmetric/asymmetric encryption/Elliptic Curve Cryptography (ECC)
  - Non-repudiation (e.g., digital signatures/certificates, HMAC, audit trail)
  - Encryption algorithms (e.g., AES, RSA)
  - Key strength (e.g., 256, 512, 1024, 2048 bit keys)
  - Cryptographic attacks, cryptanalysis, and counter measures

- Understand reasons and requirements for cryptography
  - Confidentiality
  - Integrity and authenticity
  - Data sensitivity (e.g., PII, intellectual property, PHI)
  - Regulatory



University of Victoria

Certification

- Understand and support secure protocols
  - Services and protocols (e.g., IPSec, TLS, S/MIME, DKIM)
  - Common use cases
  - Limitations and vulnerabilities

- Understand Public Key Infrastructure (PKI) systems
  - Fundamental key management concepts (e.g., key rotation, key composition, key creation, exchange, revocation, escrow)
  - Web of Trust (WOT) (e.g., PGP, GPG)

Business Continuity
&
Disaster Recovery

University of Victoria

Business Continuity Plan (BCP)

- plans and framework to ensure business can continue in an emergency
- minimize cost associated with disruptive event and mitigate risk
- 4 elements:
  1) scope and plan initiation
  2) business impact assessment (BIA)
  3) business continuity plan development
  4) plan approval and implementation

  …..maintenance

University of Victoria

Business Impact Assessment (BIA)

- identify the impact of a disruptive event on the business (quantitative – eg. financial or qualitative – eg. brand)

- 3 goals of BIA:
  1) criticality prioritization
  2) maximum tolerable downtime estimation
  3) resource requirements

- identify which business units are critical to maintaining operations

- catalog of important business processes and criticality

University of Victoria

Business Impact Assessment (BIA)

- loss impact analysis quantitative and qualitative

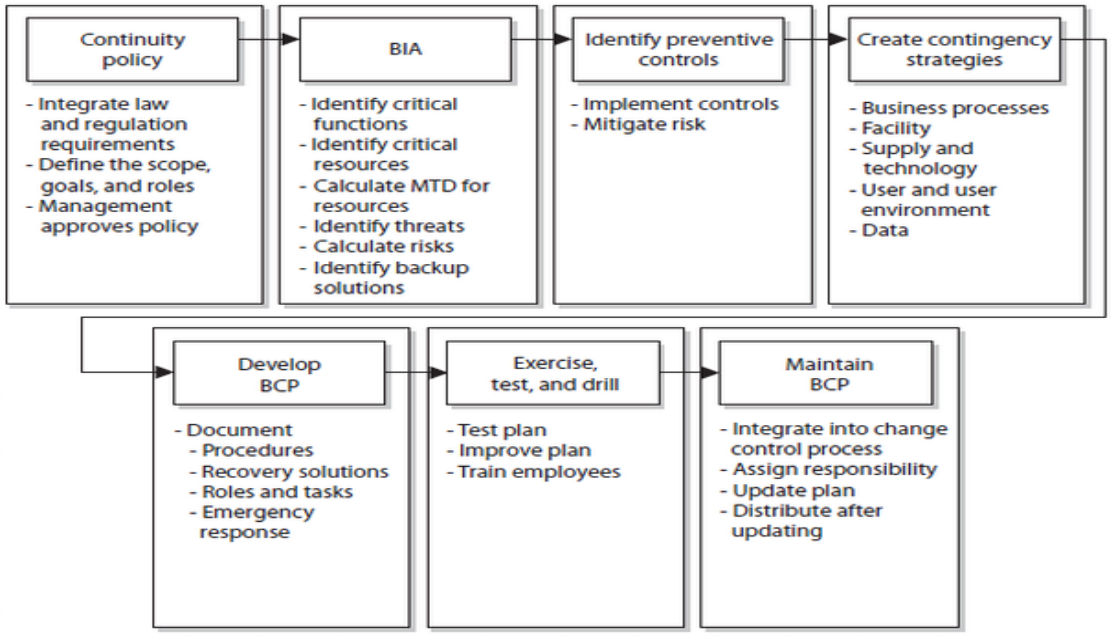
- Steps:
  1) information gathering
  2) risk analysis and threat assessment
  3) determine key metrics (maximum tolerable downtimes, recovery time objective, recovery point objective)
  4) develop impact statements

- ensure remember to establish criticality levels to assist with prioritization

Business Continuity Plan Development

1) identify the business areas
2) engage the stakeholders
3) develop and populate the plan
4) communicate and educate on the plan
5) test the plan
6) review and update on a regular basis

different approaches



1) Identify critical functions and priorities for restoration.
2) Identify support systems needed by critical functions.
3) Estimate potential outages and calculate the minimum resources needed to recover from the catastrophe.
4) Select recovery strategies and determine what vital personnel, systems, and equipment will be needed to accomplish the recovery.
5) Determine who will manage the restoration and testing process.
6) Calculate what type of funding and fiscal management is needed to accomplish these goals.

Business Continuity Plan (BCP)

- proactive
- provide procedures for sustaining essential business operations while recovering from a significant disruption
- continuation of critical business processes in an organization using different people, equipment, facilities
- long term planning of ensuing business can continue if emergency happens

University of Victoria

Differences between BCP & DRP

BCP	DRP
• activities required to ensure continuation of critical business processes in an organization	• assessment, salvage, repair, and restoration of damaged facilities and systems
• alternate personnel, equipment, and facilities	• often focuses on IT systems
• often includes non-IT aspects of business	

University of Victoria

Backup Strategies

- **Full**
  - all files are backed up modified or not (archive bit is reset)
- **Incremental**
  - archive data that has changed since the last full or incremental backup (archive bit is reset)
- **Differential**
  - archive data that changed since the last full backup only (archive bit isn’t reset)

Business Continuity Plan (BCP)

- **Business Impact Analysis**
  - A detailed and documented process designed to identify and prioritize business functions and workflow, including establishing Recovery Time Objectives by assessing impacts over time that might result if an organization was to experience a disruptive event.

- **Business Priority Service**
  - Business function or process that is not mission critical, but, should it not be performed, could lead to the loss of a major government service.

- **Critical Services**
  - General term that collectively refers to Business Priority and Mission Critical services.

University of Victoria

Business Continuity Plan (BCP)

- **Recovery Point Objectives (RPO)**
  - The point in time, relative to pre-disaster, at which available data from backup can be restored – max amount of data loss or work loss for a given process (eg. weekly backups RPO = 1 week)

- **Recovery Time Objectives (RTO)**
  - Amount of time that a business function can withstand an interruption before a negative or unacceptable consequence occurs.
  - Time allowed to recover systems – max amount of time process or system will be unavailable.

Business Continuity Plan (BCP)

- **Mean Time Between Failures (MTBF)**
  - how frequent are failures
- **Mean Time to Repair (MTTR)**
  - how long to repair equipment on average
- **Availability Formula**
  - MTBF / (MTBF + MTTR) = availability

Also:

- SLA — Service Level Agreement
- MTTF — Mean Time To Failure

525,600 – 6 = 525,594
525,594/525,600 * 100 = 99.99885%

University of Victoria

Business Continuity Plan (BCP)

Availability %	Downtime per year[note 1]	Downtime per month	Downtime per week	Downtime per day
55.5555555% ("nine fives")	162.33 days	13.53 days	74.92 hours	10.67 hours
90% ("one nine")	36.53 days	73.05 hours	16.80 hours	2.40 hours
95% ("one nine five")	18.26 days	36.53 hours	8.40 hours	1.20 hours
97%	10.96 days	21.92 hours	5.04 hours	43.20 minutes
98%	7.31 days	14.61 hours	3.36 hours	28.80 minutes
99% ("two nines")	3.65 days	7.31 hours	1.68 hours	14.40 minutes
99.5% ("two nines five")	1.83 days	3.65 hours	50.40 minutes	7.20 minutes
99.8%	17.53 hours	87.66 minutes	20.16 minutes	2.88 minutes
99.9% ("three nines")	8.77 hours	43.83 minutes	10.08 minutes	1.44 minutes
99.95% ("three nines five")	4.38 hours	21.92 minutes	5.04 minutes	43.20 seconds
99.99% ("four nines")	52.60 minutes	4.38 minutes	1.01 minutes	8.64 seconds
99.995% ("four nines five")	26.30 minutes	2.19 minutes	30.24 seconds	4.32 seconds
99.999% ("five nines")	5.26 minutes	26.30 seconds	6.05 seconds	864.00 milliseconds
99.9999% ("six nines")	31.56 seconds	2.63 seconds	604.80 milliseconds	86.40 milliseconds
99.99999% ("seven nines")	3.16 seconds	262.98 milliseconds	60.48 milliseconds	8.64 milliseconds
99.999999% ("eight nines")	315.58 milliseconds	26.30 milliseconds	6.05 milliseconds	864.00 microseconds
99.9999999% ("nine nines")	31.56 milliseconds	2.63 milliseconds	604.80 microseconds	86.40 microseconds

525600 minutes in a year

Wikipedia – High Availability

Business Continuity Plan (BCP)

- **Work Recovery Time (WRT)**
  - time required to configure systems

- **Minimum Operating Requirements (MOR)**

- **Maximum Tolerable Downtime (MTD) formula:**
  - MTD = RTO + WRT

- period of time after which the organization would suffer considerable pain if the process were unavailable

Disaster Recovery

- **Disaster Recovery**
  - refers to Information Technology (IT) recovery
  - Disaster Recovery Plans (DRPs) document process to recover and restore technology (computer processing, applications and data) needed to support critical business functions

- **Mission Critical Services**
  - functions and processes that, should they not be performed, could lead to loss of life or injury, personal hardship to citizens, major damage to the environment, or significant loss of revenue or assets

Disaster Recovery Plan (DRP)

- reactive – when an IT disaster strikes (DRP heavily IT focused)
- **management approved plan** that addresses operational processes for the recovery of a damaged facility
- what actions need to be taken to restore IT operations as quickly as possible
- assessment, salvage, repair, and eventual restoration of damaged facilities and systems
- **DRP is the effort to recover IT system and applications whereas BCP is effort to recover business processes**
- **detailed procedures** to facilitate recovery of capabilities at an alternate site

Disaster Recovery Plan (DRP)

- recover from emergency with minimum impact on business
- plan for before, during, and after the event
- objective is to move critical processes to an alternate site and return primary site and normal processing within a timeframe that minimizes loss
- **people are the number one priority**

Disaster Recovery Plan (DRP)

- **Hot site:**
  - fully configured computer facility with electrical power, heating, ventilation, and air conditioning (HVAC and **functioning** file/print servers and workstations – has all hardware and critical app data mirrored in real time (resume operations in < 1 hr)

- **Warm site:**
  - computer facility available with electrical power, heating, ventilation, and air conditioning (HVAC), limited file/print servers and workstations – data may not be in real time, backups may be required – MTD between 1 and 3 days with 24-48 hr recovery time

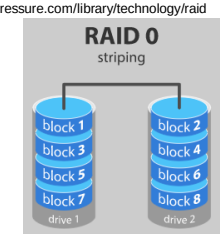
- **Cold site:**
  - computer facility available with electrical power, heating, ventilation and air conditioning (HVAC) – no computer hardware (long MTD required)

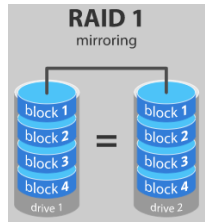
Disaster Recovery Plan (DRP)

- Data Centre alternatives
  - **Electronic Vaulting**
    - transfer of backup data to offsite location (transfer occurs over connectivity)
  - **Remote Journaling**
    - parallel processing of transactions to alternate site (transfer occurs live) – provide redundancy for transactions
  - **Database Shadowing**
    - uses live processing of remote journaling but creates more redundancy by duplicating database sets to multiple servers

Certification

https://www.prepressure.com/library/technology/raid



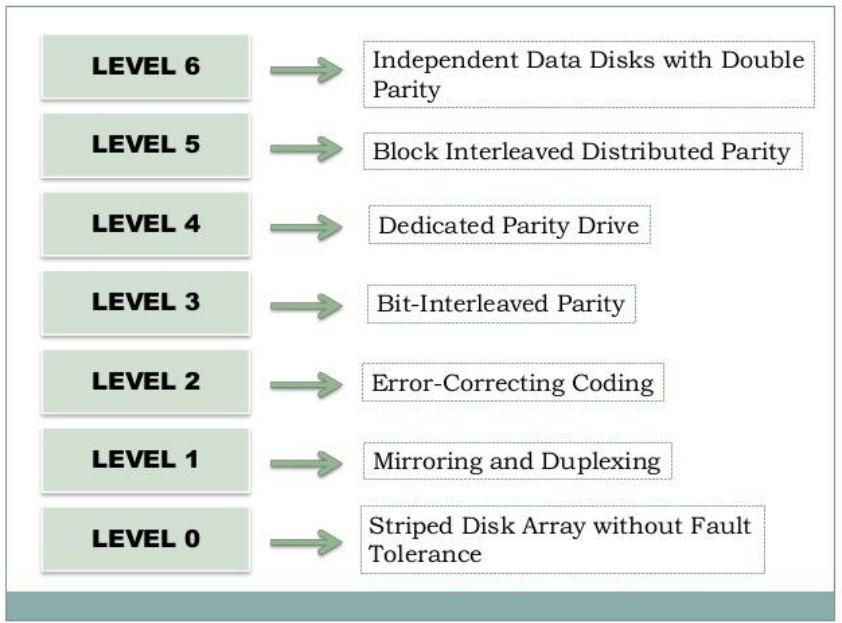


- RAID — RAID stands for Redundant Array of Independent Disk (or Inexpensive Disk)
  - RAID 0 — striping (improved performance but no fault tolerance)
  - RAID 1 — mirroring (redundancy only, not speed)
  - RAID 2 — not used commercially
  - RAID 3 — striped on byte level with extra parity drive (improved performance and fault tolerance)
  - RAID 4 — same as RAID3 but striped on block level
  - RAID 5 — (most popular) stripes the data and parity information – needs 3 or more drives
  - RAID 6 — dual parity – parity distributed over all drives
  - RAID 7 — same as RAID5 but all drives act as one single virtual disk

https://seniordba.wordpress.com/2018/04/09/raid-levels-explained/

RAID Level Comparison

Features	RAID 0	RAID 1	RAID 1E	RAID 5	RAID 5EE	RAID 6	RAID 10	RAID 50	RAID 60
Minimum # Drives	2	2	3	3	4	4	4	6	8
Data Protection	No Protection	Single-drive failure	Single-drive failure	Single-drive failure	Single-drive failure	Two-drive failure	Up to one disk failure in each sub-array	Up to one disk failure in each sub-array	Up to two disk failures in each sub-array
Read Performance	High	High	High	High	High	High	High	High	High
Write Performance	High	Medium	Medium	Low	Low	Low	Medium	Medium	Medium
Read Performance (degraded)	N/A	Medium	High	Low	Low	Low	High	Medium	Medium
Write Performance (degraded)	N/A	High	High	Low	Low	Low	High	Medium	Low
Capacity Utilization	100%	50%	50%	67% - 94%	50% - 88%	50% - 88%	50%	67% - 94%	50% - 88%
Typical Applications	High end workstations, data logging, real-time rendering, very transitory data	Operating system, transaction databases	Operating system, transaction databases	Data warehousing, web serving, archiving	Data warehousing, web serving, archiving	Data archive, backup to disk, high availability solutions, servers with large capacity requirements	Fast databases, application servers	Large databases, file servers, application servers	Data archive, backup to disk, high availability solutions, servers with large capacity requirements



Certification

- data centres
- media storage
- power
- avoid static electricity
- avoid water
- HVAC
- heating
- ventilation
- air-conditioning
- hot aisle
- cool aisle
- fire
- flood
- electromagnetic interference

- fire extinguishers
  - class A for typical fires caused by combustibles
  - class B for fires that get fuel from gasoline
  - class C electrical fires
  - class D heavy metal fires
  - class K kitchen fires with oils and fats

- fire suppression systems
  - water
  - wet-pipe
  - dry pipe systems (minimize risk of accidental discharge)
  - chemical suppression systems

Review

University of Victoria

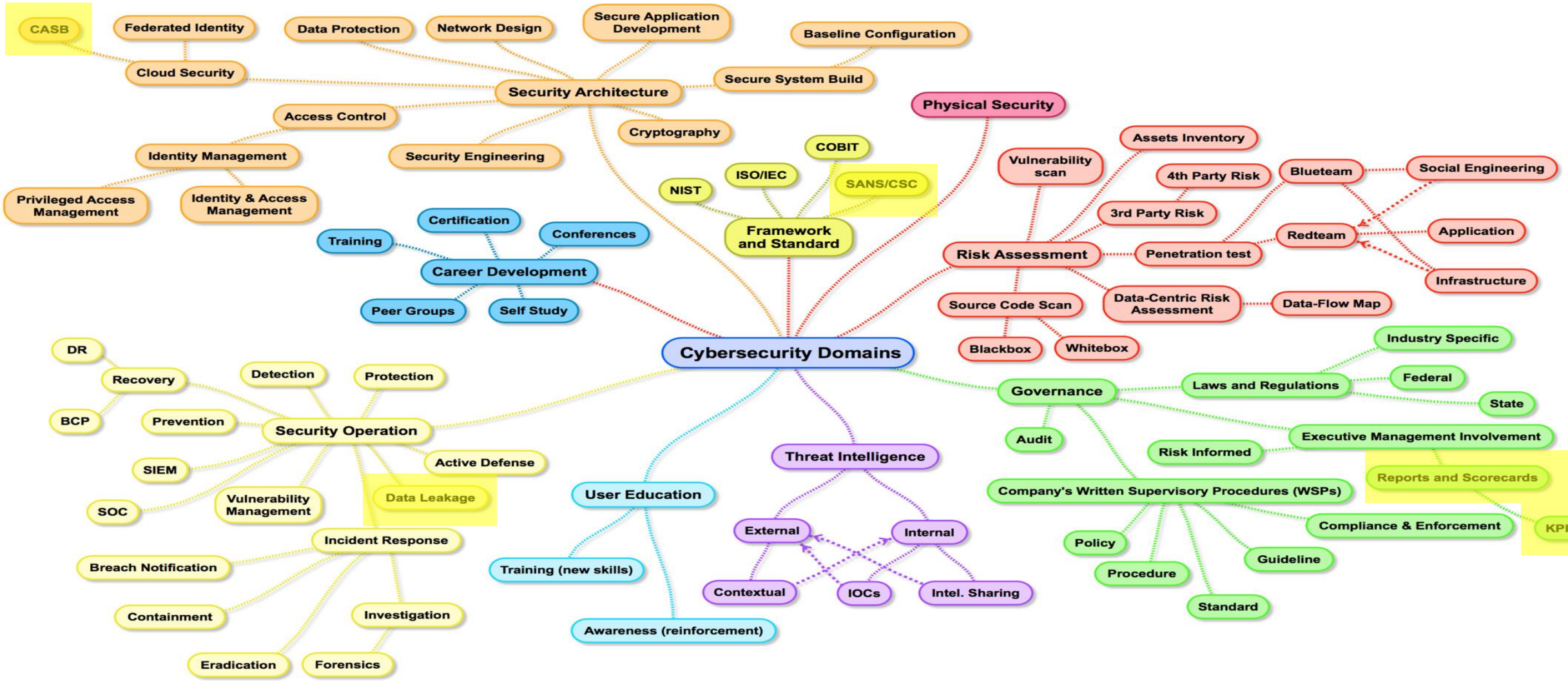
Review

8 CISSP Domains (2018)

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security

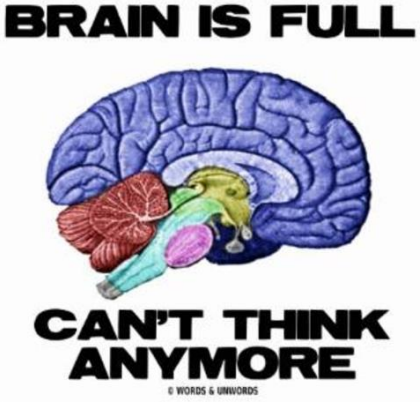
University of Victoria

Map of Cybersecurity Domains



https://www.linkedin.com/pulse/map-cybersecurity-domains-version-20-henry-jiang-ciso-cissp/

Review



- Week 1: Course Intro, Careers in Cybersecurity, Cybersecurity Threat Landscape, Lab: Linux
- Week 2: Attacks, Breaches, Best Practices, Prevention, Lab: VI
- Week 3: Incident Response and Recovery, Lab: Network Tools
- Week 4: Risk Management, Risk Assessment, Asset Security, Information Classification, Supply Chain, Third Parties, Cyber Insurance, Lab: whois, dig
- Week 5: Security Awareness, Privacy, Lab: Shell Scripting
- Week 6: Legal, Breaches, Investigations, Open Source Intelligence, Darknet, Foreign Threats to the Democratic Process, Lab: sed, awk, & friends
- Week 7: Architecture, Cloud, Mobile, IoT, Operations, Network Communications, Lab: RegEx
- Week 8: Identity, Access Management, Logging, Policies, Standards, Audits, Compliance, Lab: Nmap
- Week 9: Systems Application Security, Secure Development, Security Testing (Vulnerability Assessment, Penetration Testing), Physical Security Part I, Lab: HTML
- Week 10: Cryptography, PKI, BCP, DRP, Building Security into the Organization, Lab: MySQL
- Week 11: TBD, Lab: Packet Capture

University of Victoria

Review

- how much should you spend on security?
  - up to the organization but typically not more than the damage from incidents
- essential that you make employees aware of security expectations
- executives own the risk, may delegate to others
- cybersecurity must be driven from the top of the organization
- build security in from the ground up (security by design)
- can’t just focus on prevention, must do detection and response

Review

- security is not the “Office of No” or the team preventing you from doing something
  - should be the team helping decision makers understand the risks

- security teams should be a partner, an enabler to the business
  - helping the business to make informed decisions around risk
  - goal is to ensure business decisions are aligned with risk appetite
  - if business has a low risk appetite then decisions should typically be low risk as well

Review

- organizations are more connected than ever and more connected with each other than ever
- a very real risk to organizations is any other organization they are connected with
- organization can do a lot of things well but if they neglect connections with other organizations they are susceptible
- your organization inherits the risks of others you are connected with

University of Victoria

Review

- vendor contracts must have adequate security controls
- “securing the humans” is critical as they are often described as ‘the weakest link’
- humans can be the greatest liability but could be the greatest strength
- **people are the #1 most important part of security**

University of Victoria

Review

- technology is a core business enabler
- consider how cybersecurity can enable the business
- security can be a key differentiator
- consider the impacts of cyber risk
- know what needs to be protected (crown jewels)
- don’t blindly adopt standards and assume they will be sufficient
- do test your controls (trust and verify)

University of Victoria

Review

- APT – Advanced Persistent Threats

intended to refer to sophisticated threats
gain access
maintain persistence
go undetected for long periods of time
trickle out data

- TTP – **Tactics Techniques and Procedures**

how the bad guys
orchestrate and
manage attacks

~~Tools Tactics and Procedures~~

~~Tools Techniques and Procedures~~

- C&C or C2 – Command and Control

how the bad guys
control compromised
machines

We ❤ acronyms…

University of Victoria

Knowledge check

- make sure you can recognize attacks
- make sure you can recognize good behaviour
  - e.g. swift reporting, disclosure, security awareness
  - e.g. strong encryption, network segmentation
- what they did well, what they didn't do well,

  what could have prevented it

Knowledge check

- zero day vulnerability, zero day attack/exploit, replay, pass the hash
- scareware, ransomware, cryptomalware, cryptomining, cryptojacking
- social engineering (phishing, spearphishing, whaling, vishing, smishing)
- tailgating, dumpster diving, shoulder surfing
- waterholing, malvertising

Knowledge check

- **zombies**: computers controlled by cybercriminals
- **bots**: zombies with malware installed on them
- **botnets**: group of zombies with malware installed

Knowledge check

- policies, standards, guidelines, audits
  - build a policy aligned with a standard
  - auditors will audit you against a standard
  - you build a plan to remediate, execute
  - future audits …
- read through NIST and read through sample policy
  - https://www.nist.gov/cyberframework/framework
  - https://www.nist.gov/document/2018-04-16frameworkv11core1xlsx

University of Victoria

When your organization is attacked

University of Victoria

Review

- consider different threat actors and their motivation, access to resources, level of sophistication
  - threat actors: juveniles, insiders, hacktivists, organized crime, nation-states, cyber terrorists
  - motivation: curiosity, trophy/challenge/ego, revenge/retribution/punishment, profit/financial gain/money, fraud, leverage/blackmail/extortion/intimidation, espionage, surveillance, political, cause, bring awareness, maximum damage, fatalities, acts of terrorism…
  - resources: low, medium, high
  - sophistication: low, medium, high

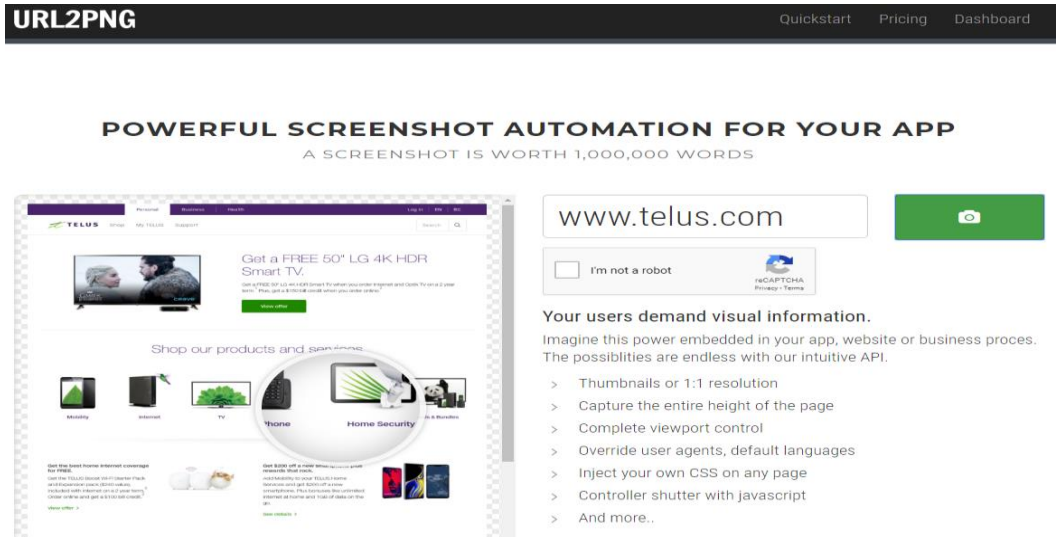
source: Recorded Future

Review

- do they do it themselves or do they hire someone else to do it
- if objective is to take offline then attack will be different than if objective is to make money
  - e.g. DDoS vs. credit card theft
- when accessing sites don't do it directly
  - use a third party* or if you access directly use a text browser like Lynx, wget, curl
- final option is to use a VM or a computer you don't care about and delete/reformat after – turn off images and scripts in browser

Don’t access links directly

“Screenshot as a Service”



wget or curl

```
$ wget www.telus.com
Will not apply HSTS. The HSTS database must be a regular and non-world-writable file.
ERROR: could not open HSTS store at '/home/gaperkin/.wget-hsts'. HSTS will be disabled.
--2019-04-03 18:45:26--  http://www.telus.com/
Resolving www.telus.com (www.telus.com)... 205.206.163.40
Connecting to www.telus.com (www.telus.com)|205.206.163.40|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.telus.com/ [following]
--2019-04-03 18:45:26--  https://www.telus.com/
Connecting to www.telus.com (www.telus.com)|205.206.163.40|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: /en/ [following]
--2019-04-03 18:45:27--  https://www.telus.com/en/
Reusing existing connection to www.telus.com:443.
HTTP request sent, awaiting response... 200 OK
Length: 286607 (280K) [text/html]
Saving to: ‘index.html’

index.html                  100%[=========================================>] 279.89K   803KB/s    in 0.3s

2019-04-03 18:45:28 (803 KB/s) - ‘index.html’ saved [286607/286607]

$ less index.html
```

Lynx

```
   Web History | Settings | Sign innx see the Lynx User's Guide, or the Lynx help files.

CreGoogle Images


   Google Search  I'm Feeling Lucky     Advanced search
      Language tools
   Lynx was originally developed by Lou Montulli, Michael Grobe, and Charles Rezac. Garrett Blythe
   Google offered in: Françaisoined the Lynx effort as well. Following the departures of Lou and Garrett
   for positions at Netscape in the summer of 1994, Craig Lavender provided support services for Lynx,
   Advertising Programs      Business Solutions      About Google      Google.com

   Lynx is maintained and supported by mem© 2019 - Privacy - Termsmunity coordinated via the lynx-dev

URL to open: www.suspiciousurl.com
```

```
$ curl www.telus.com
<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx</center>
</body>
</html>
$
```

Review

- know the difference between passive and active reconnaissance
- if you are touching the site with ping, nmap, Nessus, Metasploit, etc then it is active
- if you are accessing a third party for information like Shodan or WHOIS then it is passive
- consider different styles of attack

port scan?
vulnerability scan?
penetration test?

Shodan Developers Book View All...

SHODAN

Explore | Enterprise Access | Contact Us | New to Shodan? | Login or Register

The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account | Getting Started

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

56% of Fortune 100

1,000+ Universities

Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.

Cyber Kill Chain

https://www.novainfosec.com/2013/05/29/cyber-kill-chain-101/

MITRE ATT&CK Framework

Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 34 techniques	Credential Access 14 techniques	Discovery 24 techniques	Lateral Movement 9 techniques	Collection 16 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Valid Accounts	Scheduled Task/Job	Valid Accounts	Process Injection	Modify Authentication Process	Network Sniffing	System Service Discovery	Remote Services	Data from Local System	Data Obfuscation	Exfiltration Over Other Network Medium	Data Destruction
Replication Through Removable Media	Windows Management Instrumentation	Hijack Execution Flow	Access Token Manipulation	Direct Volume Access	OS Credential Dumping	Application Window Discovery	Software Deployment Tools	Data from Removable Media	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Trusted Relationship	Software Deployment Tools	Boot or Logon Initialization Scripts	Group Policy Modification	Rootkit	Input Capture	System Network Configuration Discovery	Replication Through Removable Media	Input Capture	Application Layer Protocol	Data Transfer Size Limits	Service Stop
Supply Chain Compromise	Shared Modules	Create or Modify System Process	Abuse Elevation Control Mechanism	Obfuscated Files or Information	Brute Force	System Owner/User Discovery	Internal Spearphishing	Data Staged	Proxy	Exfiltration Over C2 Channel	Inhibit System Recovery
Hardware Additions	User Execution	Event Triggered Execution	Exploitation for Privilege Escalation	Indicator Removal on Host	Two-Factor Authentication Interception	System Network Connections Discovery	Use Alternate Authentication Material	Screen Capture	Communication Through Removable Media	Exfiltration Over Physical Medium	Defacement
Exploit Public-Facing Application	Exploitation for Client Execution	Boot or Logon Autostart Execution		Modify Registry	Exploitation for Credential Access	Permission Groups Discovery	Lateral Tool Transfer	Email Collection	Web Service	Exfiltration Over Web Service	Firmware Corruption
Phishing	System Services	Account Manipulation		Trusted Developer Utilities Proxy Execution	Steal Web Session Cookie	File and Directory Discovery	Taint Shared Content	Clipboard Data	Multi-Stage Channels	Exfiltration Over Alternative Protocol	Resource Hijacking
External Remote Services	Command and Scripting Interpreter	External Remote Services		Traffic Signaling	Unsecured Credentials	Peripheral Device Discovery	Exploitation of Remote Services	Automated Collection	Ingress Tool Transfer	Transfer Data to Cloud Account	Network Denial of Service
Drive-by Compromise	Native API	Office Application Startup		Signed Script Proxy Execution	Credentials from Password Stores	Network Share Discovery	Remote Service Session Hijacking	Audio Capture	Data Encoding		Endpoint Denial of Service
	Inter-Process Communication	Create Account		Rogue Domain Controller	Steal or Forge Kerberos Tickets	Password Policy Discovery		Video Capture	Traffic Signaling		System Shutdown/Reboot
= Has sub-techniques		Browser Extensions		Indirect Command Execution	Forced Authentication	Browser Bookmark Discovery		Man in the Browser	Remote Access Software		Account Access Removal
		Traffic Signaling		BITS Jobs	Steal Application Access Token	Virtualization/Sandbox Evasion		Data from Information Repositories	Dynamic Resolution		Disk Wipe
		BITS Jobs		XSL Script Processing	Man-in-the-Middle	Cloud Service Dashboard		Man-in-the-Middle	Non-Standard Port		Data Manipulation
		Server Software Component		Template Injection		Software Discovery		Archive Collected Data	Protocol Tunneling		
		Pre-OS Boot		File and Directory Permissions Modification		Query Registry		Data from Network Shared Drive	Encrypted Channel		
		Compromise Client Software Binary		Virtualization/Sandbox Evasion		Remote System Discovery		Data from Cloud Storage Object	Non-Application Layer Protocol		
		Implant Container Image		Unused/Unsupported Cloud Regions		Network Service Scanning					
				Use Alternate Authentication Material		Process Discovery					
				Impair Defenses		System Information Discovery					
				Hide Artifacts		Account Discovery					
				Masquerading		System Time Discovery					
				Deobfuscate/Decode Files or Information		Domain Trust Discovery					
				Signed Binary Proxy Execution		Cloud Service Discovery					
				Exploitation for Defense Evasion							
				Execution Guardrails							
				Modify Cloud Compute Infrastructure							
				Pre-OS Boot							
				Subvert Trust Controls							

MITRE ATT&CK =
Adversarial Tactics, Techniques,
& Common Knowledge

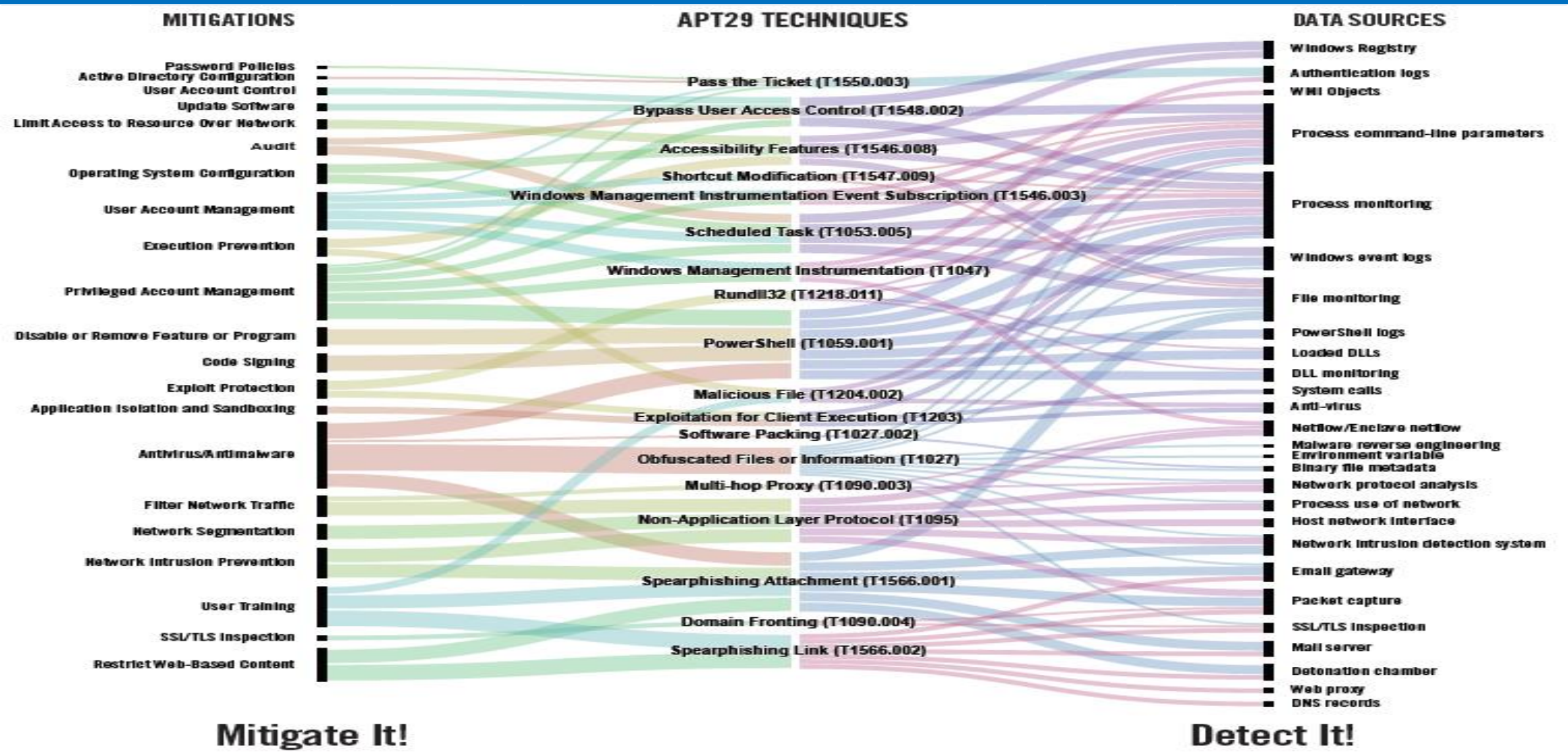
attack life cycle

common attack methods

MITRE ATT&CK®
Enterprise Framework
attack.mitre.org

https://attack.mitre.org

MITRE ATT&CK Framework



ToR

- is ToR infallible?

Yes, Federal Agents Can Identify Anonymous Tor Users, Because Most People Don't Know How To Be Anonymous

Privacy

from the *well,-duh* dept
Thu, Apr 3rd 2014 10:51am — **Mike Masnick**

For many, many years now, we keep hearing law enforcement whine about the "threats" of anonymity and how people would be able to get away with all sorts of criminal activity if they weren't given the ability to track, monitor and tap pretty much every communications technology that has come along. A decade ago the fear was that free and open WiFi was going to be a **major boon to criminals** who could use it "with no trace." As we pointed out, however, nothing about using an anonymous connection like that means you won't get caught, because criminals have to do a lot of things, many of which will expose them in other ways, without having to tap and track every technological interaction. What's known as good old-fashioned detective work can often track down criminals who used tools to be anonymous -- and for years, we've pointed out **many**, **many**, **many** examples of this.

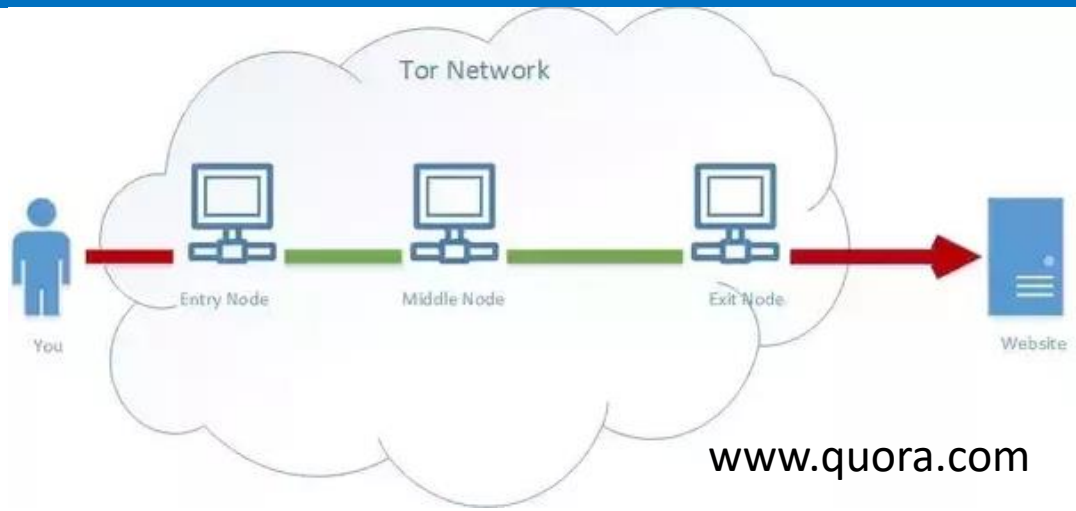
More recently, law enforcement's concern has been about Tor (which is slightly ironic, given that Tor was created and funded by the US government). The Snowden revelations have shown that, try as they might, the NSA has **not had much luck** in compromising Tor, and Snowden himself has noted that properly used encryption **mostly works**.

A recent Wall Street Journal article notes that law enforcement is slowly realizing that perhaps Tor isn't a parade of horribles that must be encumbered with backdoors for wiretapping... after **realizing that most criminals more or less reveal themselves** by doing something stupid along the way anyway.

> *But officials are becoming more confident that Tor's shield of anonymity isn't impenetrable.*
>
> *"There's not a magic way to trace people [through Tor], so we typically capitalize on human error, looking for whatever clues people leave in their wake," said James Kilpatrick, one of the HSI agents who is part of Operation Round Table, a continuing investigation into a Tor-based child-pornography site that has so far resulted in 25 arrests and the identification of more than 250 victims, all children.*

This is a good thing. We should want law enforcement to be able to track down criminals -- and it's good to see that they're figuring out ways to do so. But it's important that they should need to do so *via basic detective work*, rather than by compromising important technology, creating security flaws and opening up all sorts of dangerous unintended consequences.

As with all kinds of new technologies, anonymizing technologies seem to create something of a moral panic among law enforcement types, who then insist those technologies need to be "broken" and backdoored or else criminals could somehow get away with everything. But that's silly. Sooner or later most criminals do other things that reveal who they are, opening them up to investigation and potential indictment, arrest, trial etc.



www.quora.com

- scripts enabled?
- identifying features?
- network traffic?
- VPN first?
- who owns the node?

Reconnaissance

- consider sources attackers will use to gather info
  - job postings
  - procurements to buy things

- provide information about
  - people, contacts, access, organization
  - policies, procedures, processes
  - tools, technology, systems including versions!

- remember that attackers will use this info to improve the chances that phishing emails will be successful

Reconnaissance

Active vs Passive

- direct vs indirect sources
  - websites
    - org charts
    - who are we / about us / board / executive
    - contact us
  - phone systems
    - switchboard
    - voicemail systems
    - social engineering opportunities (eg. intentional mistakes)
  - LinkedIn
    - present employees
    - past employees (look at their experience)
  - records
    - ARIN
    - WHOIS
    - DNS

Most companies have:
- web
- email (in / out)
- webmail
- DNS
- VPN
- others?

Common formats eg.
vpn.acme.org
mail.acme.org

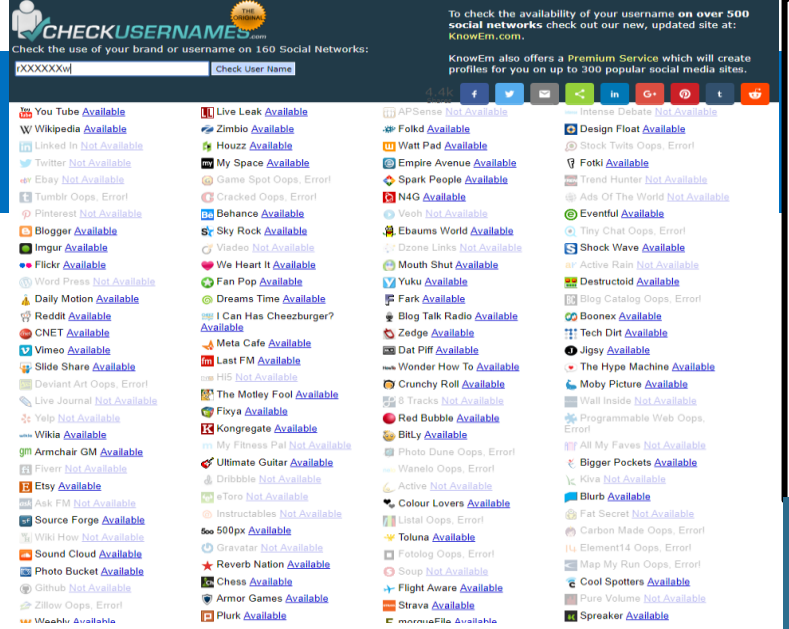
In those systems:
john.smith@org.com

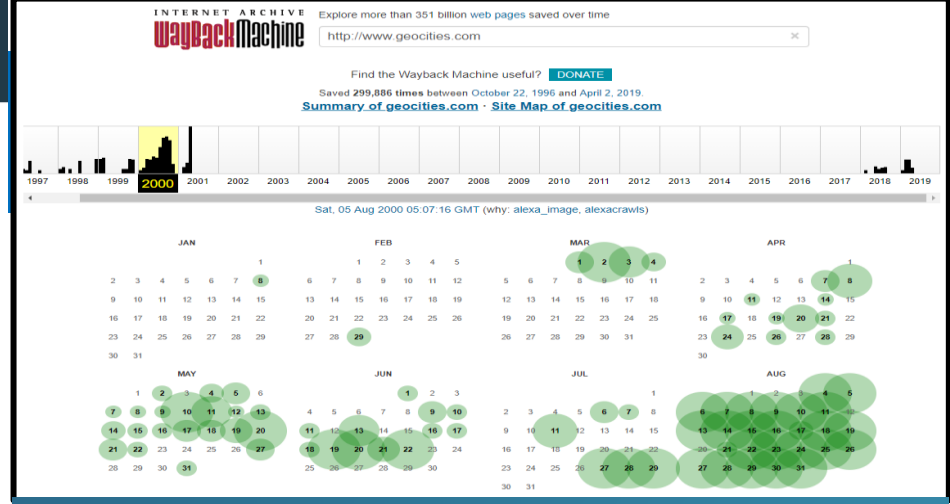
Review all available sources of information

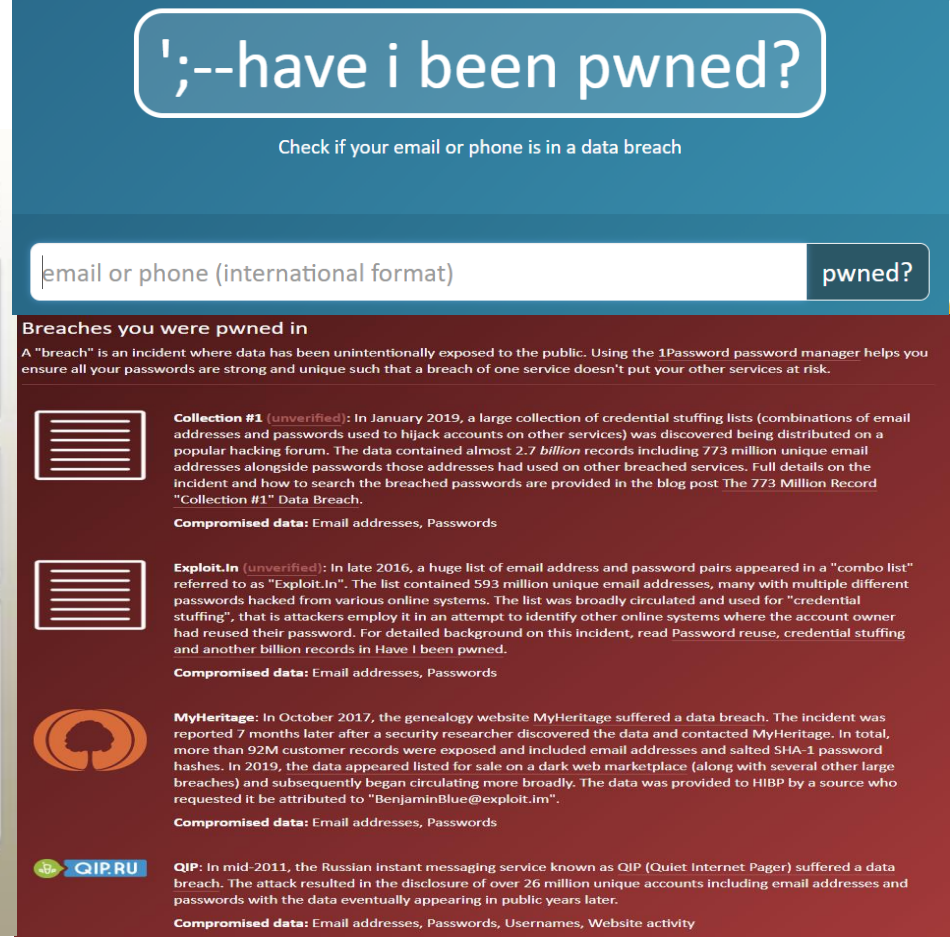
University of Victoria

Reconnaissance

- so many websites
  so little time







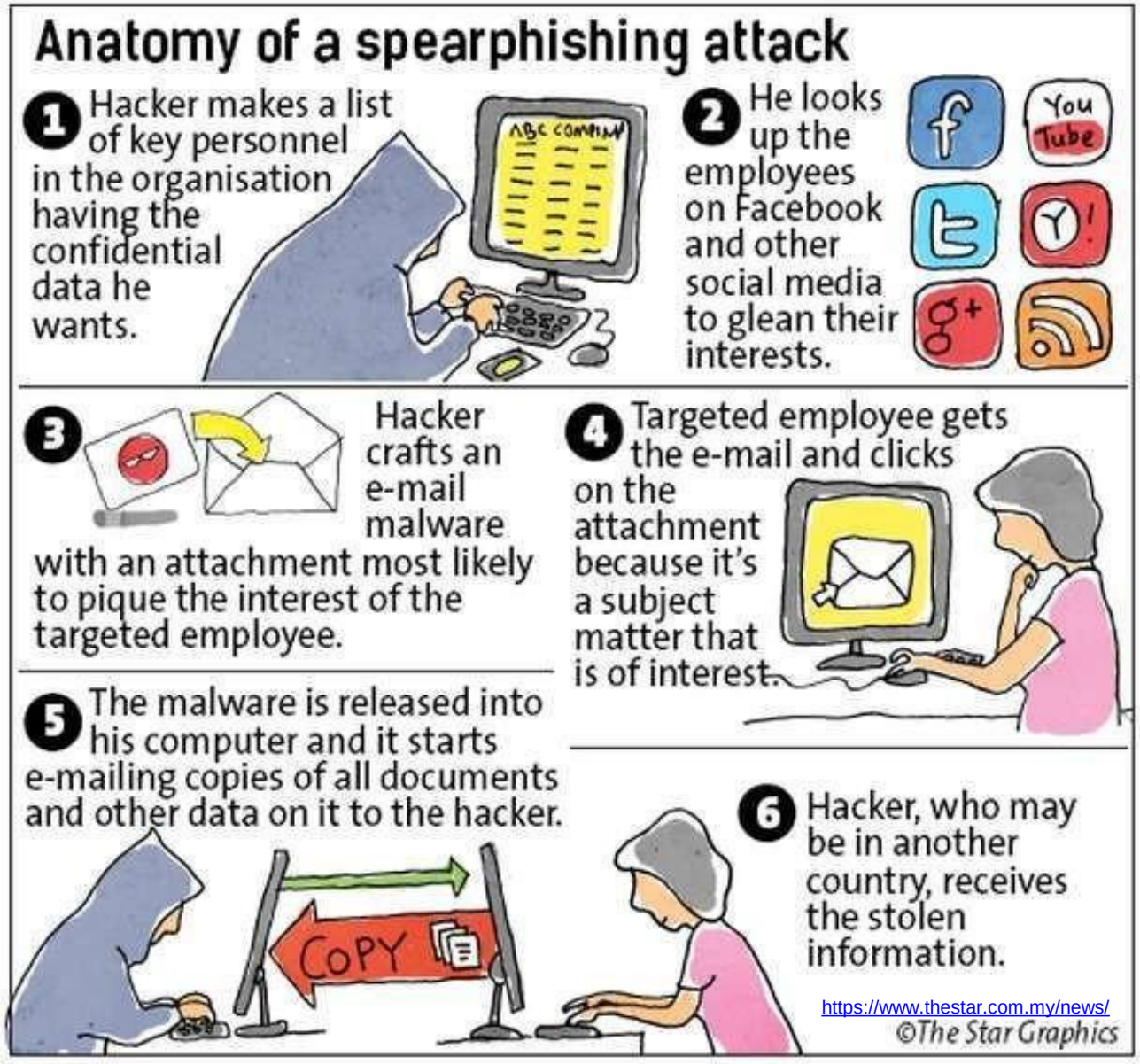
Weaponization

- “forging something sinister out of the average or commonplace… taking a harmless looking PDF or Microsoft Word/Excel files and manipulating built-in features to execute malicious code on assets within the target organization is a common example of such weaponry”

https://www.psoltech.com/cyber-kill-chain-ii-weaponization/

University of Victoria

s/Hacker/Cybercriminal



Exploitation

- APT malware is triggered, executes on target network to exploit vulnerability
- take advantage of vulnerabilities to escalate privileges
- execute code or harvest credentials
- move lateral to infect another host
- conduct activities from that host
  - eg. port scan example and shovel back shell

University of Victoria

Installation

- APT malware installed on target system – establishes backdoor usable by intruder
- download additional instructions or malware
- initial delivery payload can be small
- called the “dropper”
- then reaches out to C2 host for further instructions
- download additional components to have better control and gain more access

Command & Control

- management and communication APT malware on target network
- attacker can move further into network
- can exfiltrate data, do harm, DoS, or…?

University of Victoria

Actions on Objectives

- dependent on the specific mission
  - exfiltration, denial of service, destruction

- take action to achieve goals

Example

- malware executes on target
- it's a "dropper" used to bypass anti-virus/anti-malware and once on the system will download instructions from external host (command and control or "C2")
- could exploit vulnerabilities on local system or harvest credentials
- could target remote systems and move laterally to infect another host
- actions on objectives will depend on what the original goal was – do damage or exfiltrate data or…

University of Victoria

Building Security Into the Organization

Concepts

- passwords should be long **OR** strong – if they are long enough then can be harder to crack than shorter more complex passwords
- ransomware – should you pay? it's really up to the business…
- use the term cybercriminal rather than hacker when referring to committing cyber crimes

University of Victoria

Approach

- make sure you have the basics done
- these are the ‘hygiene’ level controls similar to washing your hands or brushing your teeth
- if you don’t at least have these you’re going to be in trouble
- they’re not all technical

University of Victoria

Hygiene Procedural Controls

Security Controls	
Information Security Policy	Identify what employees may and may not do that will impact risk to systems and data
Risk Register	Conscious identification and treatment of physical and logical risks to systems and data
Risk Assessments	Review risk each time a new system is introduced or upon material change to an existing system
Incident Response Plan	Respond to inevitable security incidents in a consistent and scalable way
Incident Response Team	Team that is dedicated, virtual, or on retainer with third party provider to respond to security incidents
Security Education and Awareness	Humans represent the easiest method for attackers to gain unauthorized access to systems and data

Hygiene Technical Controls

Security Controls	
Firewall	Modern version designed to prevent illegitimate network traffic
Intrusion Prevention	Sensors to prevent unauthorized access to networks and data
Website Content Filtering	System to detect employee access to inappropriate and infected websites
Email Content Filtering	System to detect infected email and spam messages
Anti-virus/Malware	Software to detect malware and viruses on workstations and servers

Approach

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/report

University of Victoria

Approach

- for this example we will use the “Defensible Security for Public Sector Organizations” framework developed in government but you can just as easily use ISO or NIST as long as you have access to the list of controls

- remember – you look at each one, determine if an organization is doing it and whether there is evidence and, if not, put it on the plan to do

- determine present state, future state where you want to be, the difference between them is the gap analysis, and then you prioritize, plan, and execute

University of Victoria

I don’t know about you but I find the best plans are the ones that are executed on.

Plan and EXECUTE

present state

gap analysis

plan & execute

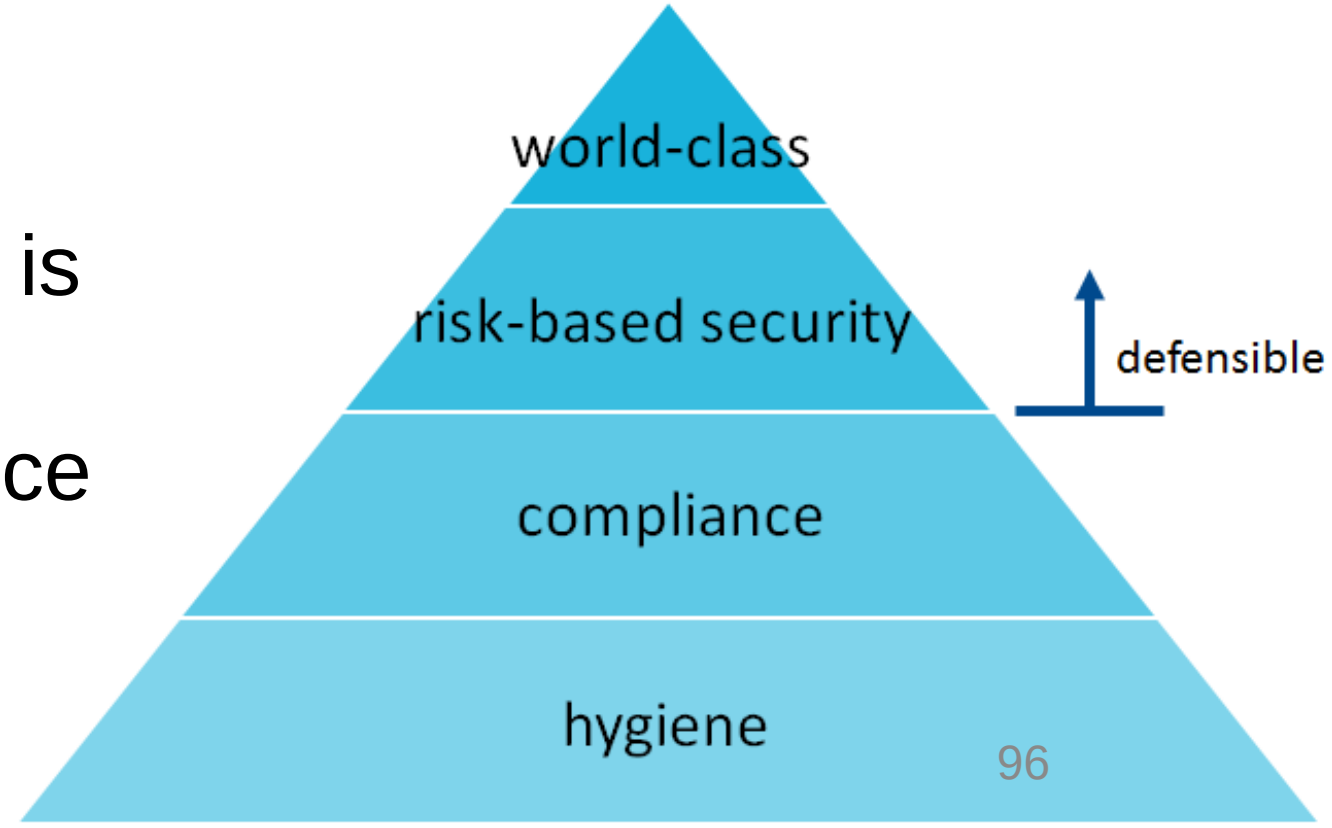
future state

University of Victoria

Defensible Security

Cybersecurity has never been as imperative as it is today. Most organizations have failed to invest at a rate that has sustained previously achieved capability levels. Others have never reached a level of security maturity adequate to mitigate risks to an acceptable level. Organizations must target a level at or above risk-based security. It is critical to ensure hygiene and compliance level controls are in effect. Organizations have a responsibility to apply appropriate safeguards and maintain a defensible level of security.

Defensible security is
<u>at or above</u>
hygiene + compliance



University of Victoria

Pre-requisites for Success

The following are pre-requisites to success for security:

- ❑ Ensure the importance of cybersecurity is recognized by executives
- ❑ Information Security roles and responsibilities are identified and assigned
- ❑ Identify critical systems and data as the crown jewels of the organization
- ❑ Organization’s risk appetite is known and a risk register is reviewed quarterly
- ❑ Risk assessments are conducted for new systems and material changes to existing
- ❑ Conduct security assessments regularly against an established security standard

Defensible Security

Organizations must have documented, followed, reviewed, updated, and tested:

- ❑ Asset Management & Disposal
- ❑ Change Management
- ❑ Incident Management
- ❑ Business Continuity Plan (BCP)
- ❑ Disaster Recovery Plan (DRP)
- ❑ **Backup & Retention**
- ❑ Logging & Monitoring
- ❑ Physical Security & Visible Identification
- ❑ Security Incident Response
- ❑ Information Security Policy
- ❑ Information Security Program
- ❑ Information Security Classification
- ❑ Criminal Record Checks
- ❑ **Security Awareness Program & Course**
- ❑ Vendor Security Requirements

The following practices must be in effect:

- ❑ Access Control
- ❑ Defence in Depth for Endpoints and Networks
- ❑ Security Governance
- ❑ **Vulnerability Management & Patching**

University of Victoria

Bolded are the ones that would prevent or recover from ransomware.

Defensible Security

Durations are based on an average-sized organization and intended as a guide. Whether an organization must invest more or less time will depend on scope, volume, and maturity.

- **H** *hours*
- **W** *week(s)*
- **M** *month+*
- *hazard*
- *hygiene*

In this framework tried to give organizations an idea of the amount of time or resources they'll need to invest.

University of Victoria

Defensible Security Framework

Defensible Security for Organizations

Cybersecurity has never been as imperative as it is today. Most organizations have failed to invest at a rate that has sustained previously achieved capability levels. Others have never reached a level of security maturity adequate to mitigate risks to an acceptable level. Organizations must target a level at or above risk-based security. It is critical to ensure hygiene and compliance level controls are effective. Organizations have a duty and responsibility to apply appropriate safeguards and maintain a defensible level of security.

Defensible security is at or above hygiene + compliance:

The following are prerequisites to success for security:

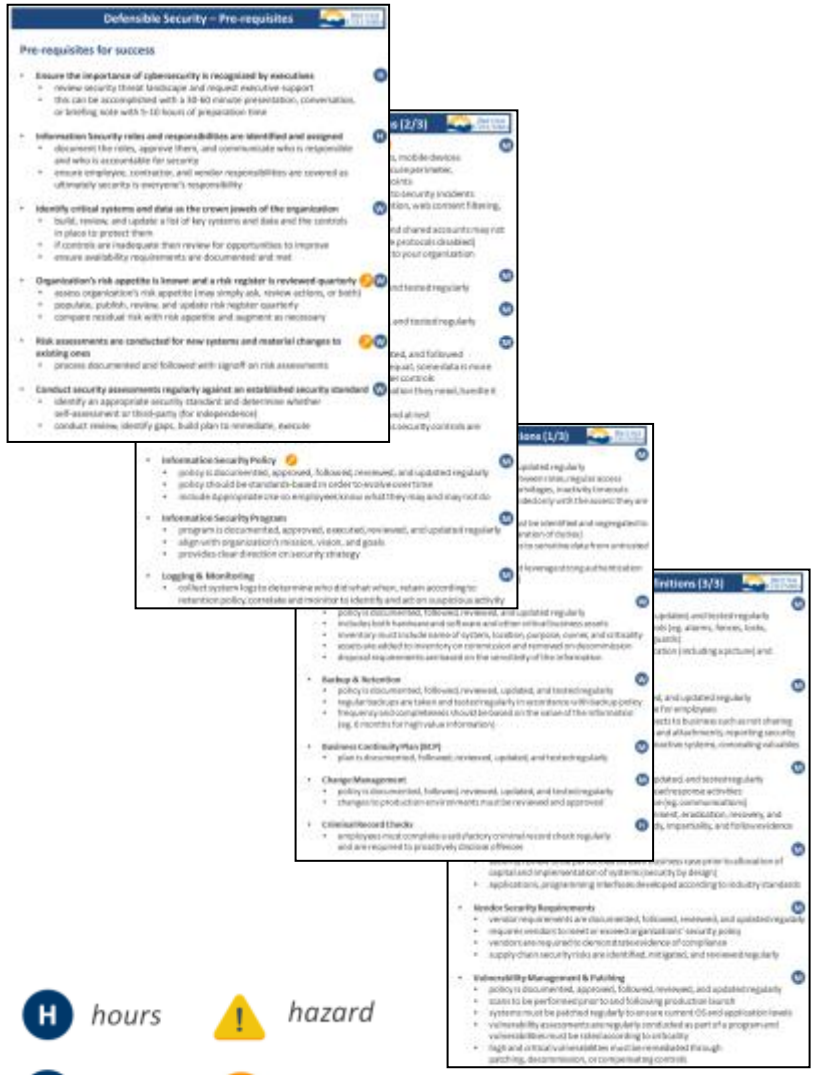
- ❑ Ensure the importance of cybersecurity is recognized by executives
- ❑ Information Security roles and responsibilities are identified and assigned
- ❑ Identify critical systems and data as the crown jewels of the organization
- ❑ Organization's risk appetite is known and a risk register is reviewed quarterly
- ❑ Risk assessments are conducted for new systems and material changes to existing ones
- ❑ Conduct security assessments regularly against an established security standard

Organizations must have documented, followed, reviewed, updated, and tested:

- ❑ Asset Management & Disposal
- ❑ Change Management
- ❑ Incident Management
- ❑ Business Continuity Plan (BCP)
- ❑ Disaster Recovery Plan (DRP)
- ❑ Backup & Retention
- ❑ Logging & Monitoring
- ❑ Physical Security & Visible Identification
- ❑ Security Incident Response
- ❑ Information Security Policy
- ❑ Information Security Program
- ❑ Information Security Classification
- ❑ Background Checks
- ❑ Security Awareness Program & Course
- ❑ Vendor Security Requirements
- ❑ Application Security

The following practices must be in effect:

- ❑ Access Control
- ❑ Defence in Depth for Endpoints and Networks
- ❑ Security Governance
- ❑ Vulnerability & Patch Management



H hours hazard

W week(s) hygiene

M month+

Defensible Security

Pre-requisites for success

- **Ensure the importance of cybersecurity is recognized by executives** H
  - review security threat landscape and request executive support
  - this can be accomplished with a 30-60 minute presentation, conversation, or briefing note with 5-10 hours of preparation time
- **Information Security roles and responsibilities are identified and assigned** H
  - document the roles, approve them, and communicate who is responsible and who is accountable for security
  - ensure employee, contractor, and vendor responsibilities are covered as ultimately security is everyone's responsibility
- **Identify critical systems and data as the crown jewels of the organization** W
  - build, review, and update a list of key systems and data and the controls in place to protect them
  - if controls are inadequate then review for opportunities to improve
  - ensure availability requirements are documented and met
- **Organization's risk appetite is known and a risk register is reviewed quarterly** W
  - assess organization's risk appetite (may simply ask, review actions, or both)
  - populate, publish, review, and update risk register quarterly
  - compare residual risk with risk appetite and augment as necessary
- **Risk assessments are conducted for new systems and material changes to existing ones** W
  - process documented and followed with signoff on risk assessments
- **Conduct security assessments regularly against an established security standard** W
  - identify an appropriate security standard and determine whether self-assessment or third-party (for independence)
  - conduct review, identify gaps, build plan to remediate, execute

Common pre-requisites to success

Definitions

Defensible Security – Definitions (1/3)

- **Access Control** (M)
  - policy is documented, followed, reviewed, and updated regularly
  - address onboarding, off-boarding, transition between roles, regular access reviews, limit and control use of administrator privileges, inactivity timeouts
  - employees/contractors/vendors should be provided only with the access they are authorized to use
  - conflicting duties and areas of responsibility must be identified and segregated to reduce incidents of fraud and other abuse (separation of duties)
  - multi-factor authentication is required for access to sensitive data from untrusted networks
  - system accounts unable to use multi-factor must leverage strong authentication (eg. password aging, length/complexity, history)
- **Asset Management & Disposal** (W)
  - policy is documented, followed, reviewed, and updated regularly
  - includes both hardware and software and other critical business assets
  - inventory must include name of system, location, purpose, owner, and criticality
  - assets are added to inventory on commission and removed on decommission
  - disposal requirements are based on the sensitivity of the information
- **Backup & Retention** (W)
  - policy is documented, followed, reviewed, updated, and tested regularly
  - regular backups are taken and tested regularly in accordance with backup policy
  - frequency and completeness should be based on the value of the information (eg. 6 months for high value information)
- **Business Continuity Plan (BCP)** (M)
  - plan is documented, followed, reviewed, updated, and tested regularly
- **Change Management** (M)
  - policy is documented, followed, reviewed, updated, and tested regularly
  - changes to production environments must be reviewed and approved
- **Criminal Record Checks** (H)
  - employees must complete a satisfactory criminal record check regularly and are required to proactively disclose offences

Defensible Security – Definitions (2/3)

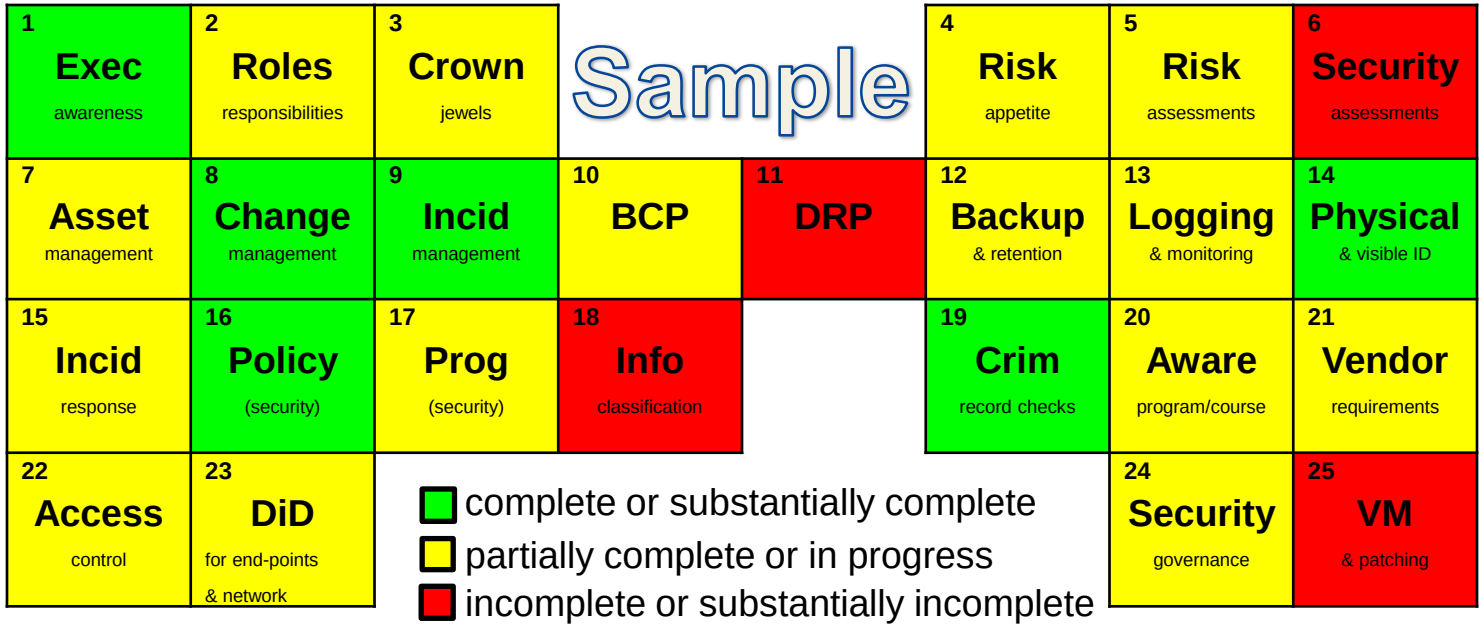
- **Defence in Depth for Endpoints and Networks** (M)
  - endpoints include servers, desktops, laptops, tablets, mobile devices
  - networks include wired and wireless and require secure perimeter, network segmentation, and known ingress/egress points
  - controls must exist to prevent, detect, and respond to security incidents
  - technologies must include firewall, intrusion prevention, web content filtering, email content filtering, and anti-virus at a minimum
  - systems must be hardened (eg. default passwords and shared accounts may not be used, unnecessary services are disabled, insecure protocols disabled)
  - additional controls may be required to mitigate risk to your organization
- **Disaster Recovery Plan (DRP)** (M)
  - plan is documented, followed, reviewed, updated, and tested regularly
- **Incident Management** (M)
  - policy is documented, followed, reviewed, updated, and tested regularly
- **Information Security Classification** (M)
  - classification is documented, approved, communicated, and followed
  - employees must understand not all data is created equal, some data is more sensitive than others and should benefit from greater controls
  - employees should possess only the sensitive information they need, handle it carefully, and label it as appropriate
  - sensitive information must be encrypted in-transit and at rest
  - prohibit production data in test environments unless security controls are equivalent to production or better
- **Information Security Policy** (M)
  - policy is documented, approved, followed, reviewed, and updated regularly
  - policy should be standards-based in order to evolve over time
  - include Appropriate Use so employees know what they may and may not do
- **Information Security Program** (M)
  - program is documented, approved, executed, reviewed, and updated regularly
  - align with organization's mission, vision, and goals
  - provides clear direction on security strategy
- **Logging & Monitoring** (M)
  - collect system logs to determine who did what when, retain according to retention policy, correlate and monitor to identify and act on suspicious activity

Defensible Security – Definitions (3/3)

- **Physical Security & Visible Identification** (M)
  - policy is documented, followed, reviewed, updated, and tested regularly
  - facilities must benefit from adequate controls (eg. alarms, fences, locks, lighting, access control systems, cameras, guards)
  - staff and visitors must wear visible identification (including a picture) and challenge those who do not
- **Security Awareness Program and Course** (M)
  - program is documented, followed, reviewed, and updated regularly
  - includes annual information security course for employees
  - educate users on common threats and impacts to business such as not sharing credentials, not clicking on suspicious links and attachments, reporting security incidents, maintaining clean desk, locking inactive systems, concealing valuables
- **Security Incident Response** (M)
  - plan is documented, followed, reviewed, updated, and tested regularly
  - dedicated, virtual, or on-retainer team to lead response activities
  - identify roles and responsibilities in advance (eg. communications)
  - address preparation, identification, containment, eradication, recovery, and lessons learned and ensure chain of custody, impartiality, and follow evidence
- **Security Reviews** (M)
  - security review to be performed on each business case prior to allocation of capital and implementation of systems (security by design)
  - applications, programming interfaces developed according to industry standards
- **Vendor Security Requirements** (M)
  - vendor requirements are documented, followed, reviewed, and updated regularly
  - requires vendors to meet or exceed organizations' security policy
  - vendors are required to demonstrate evidence of compliance
  - supply chain security risks are identified, mitigated, and reviewed regularly
- **Vulnerability Management & Patching** (M)
  - policy is documented, approved, followed, reviewed, and updated regularly
  - scans to be performed prior to and following production launch
  - systems must be patched regularly to ensure current OS and application levels
  - vulnerability assessments are regularly conducted as part of a program and vulnerabilities must be rated according to criticality
  - high and critical vulnerabilities must be remediated through patching, decommission, or compensating controls

University of Victoria

Present State Example

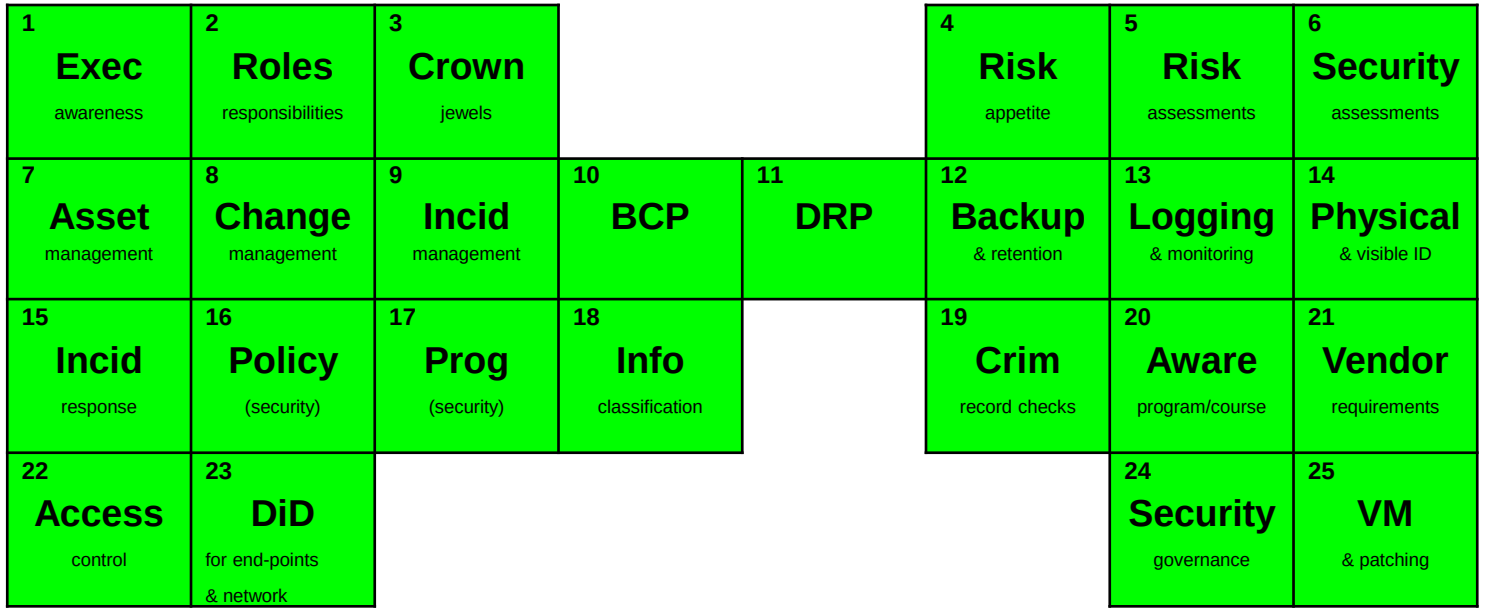


Notes:

- self assessments are notorious for being too generous
- third party assessment provides independence
- may use third party as a baseline to show improvement
- otherwise may prefer to remediate self-assessed gaps first

University of Victoria

Future State Example



Notes:

- self assessments are notorious for being too generous
- third party assessment provides independence
- may use third party as a baseline to show improvement
- otherwise may prefer to remediate self-assessed gaps first

University of Victoria

Eating the Elephant: Bites 1-6

The following are pre-requisites to success for security:

- ❑ Ensure the importance of cybersecurity is recognized by executives
- ❑ Information Security roles and responsibilities are identified and assigned
- ❑ Identify critical systems and data as the crown jewels of the organization
- ❑ Organization's risk appetite is known and a risk register is reviewed quarterly
- ❑ Risk assessments are conducted for new systems and material changes to existing
- ❑ Conduct security assessments regularly against an established security standard

- culture and support for security comes from the top
- ensure common understanding of the threat

- how do you find out if you have support?

University of Victoria

Example: Risk Register

Version 1.0

Identify risks, rate inherent risk and trend
Identify key risk mitigation strategies and residual risk
Review quarterly

Risk	Definition	Inherent risk	Risk trend	Key risk mitigation strategies	Residual risk	Owner
Network Security	Insufficiently proactive approach on identification of threats and vulnerabilities in network infrastructure and timely mitigation may result in network outages and exposure	H	↑	•		
Data Security	Insufficient application of adequate security controls, heightened by increased risks from ransomware and profit-driven cyber criminals results in an inability to identify and mitigate unauthorized access, disclosure, modification, deletion of sensitive data	H	↑	•		

* network security, data security, cyber security, physical security, identity, fraud

Eating the Elephant: Bites 7-13

Organizations must have documented, followed, reviewed, updated, and tested:

- ❑ Asset Management & Disposal
- ❑ Change Management
- ❑ Incident Management
- ❑ Business Continuity Plan (BCP)
- ❑ Disaster Recovery Plan (DRP)
- ❑ Security Incident Response
- ❑ Information Security Policy

Example: Asset Management

Version 1.0

Identify scope
Asset inventory
Process to add assets when purchased and commissioned
Process to remove assets when decommissioned and disposed of

Asset name	Purpose	IP address	Owner	Location	Criticality
luke	web server	12.34.56.78	Jane Doe	768 Seymour	med
leia	web server	12.34.56.79	Jane Doe	768 Seymour	med
darth	dns server	12.34.57.12	John Smith	768 Seymour	high
yoda	dns server	12.34.57.13	John Smith	768 Seymour	high
tatooine	database	12.34.58.1	Bob Jones	768 Seymour	med
alderaan	database	12.34.58.2	Bob Jones	768 Seymour	med

Eating the Elephant: Bites 14-18

Organizations must have documented, followed, reviewed, updated, and tested:

- ❑ Backup & Retention
- ❑ Logging & Monitoring
- ❑ Physical Security & Visible Identification
- ❑ Criminal Record Checks
- ❑ Security Awareness Program & Course

University of Victoria

Eating the Elephant: Bites 19-26

The following practices must be in effect:

- ❑ Access Control ⚠
- ❑ Defence in Depth for Endpoints and Networks ⚠
- ❑ Security Governance
- ❑ Vulnerability Management & Patching
- ❑ Application Security

Mature organizations have:

⚠

- ❑ Information Security Classification
- ❑ Vendor Security Requirements
- ❑ Information Security Program

University of Victoria

Summary

Security programs will be successful when they are:

- supported by executive
- aligned with government and ministry goals
- risk-based, aligned with business and risk appetite
- standards-based, evolve over time
- capture present and target state accurately
- plans are realistic and actionable
- resourced effectively
- focused on building security in from the ground up
- measured/monitored - continuous improvement
- communicated appropriately
- executed on

Ensure the importance of cybersecurity is recognized by executives

H PR

- review security threat landscape and request executive support
- this can be accomplished with a 30-60 minute presentation, conversation, or briefing note with 5-10 hours of preparation time

Deliverable:

- presentation to executive and/or agreement

University of Victoria

Information Security roles and responsibilities are identified and assigned

H PR

- document key roles, approve them, and communicate who is responsible and who is accountable for security
- add to security policy when complete
- ensure employee, contractor, and vendor responsibilities are covered as ultimately security is everyone's responsibility

Deliverable:

- 1+ pages documenting key security roles and who occupies them (RACI is optional)
- roles may include executives, CIO, directors, managers, employees, contractor, vendors

University of Victoria

Identify critical systems and data as the crown jewels of the organization

PR

- build, review, and update a list of key systems and data and the controls in place to protect them
- if controls are inadequate then review for opportunities to improve
- ensure availability requirements are documented and met

Deliverable:

- list of key systems and data and what security controls exist
- template in Excel of the systems, whether they hold sensitive data to include criticality
- process to keep it current (eg. annually)

University of Victoria

Organization's risk appetite is known and a risk register is reviewed quarterly

PR

- assess organization's risk appetite (may simply ask, review actions, or both)
- populate, publish, review, and update risk register quarterly
- compare residual risk with risk appetite and augment as necessary (eg. build action plan to address)

Deliverable:

- risk appetite (low/med/high)
- risk register (template already exists)
- schedule review quarterly in calendar with signoff

University of Victoria

Risk assessments are conducted for new systems and material changes to existing ones

PR

- process documented and followed with signoff on risk assessments
- for new systems or material changes to existing ones
- documented, stored on file

Deliverable:

- risk assessment process
- policy that states to conduct risk assessment for new systems and material changes to existing ones
- documented and stored in a repository

University of Victoria

Conduct security assessments regularly against an established security standard

PR

- identify an appropriate security standard and determine whether self-assessment or third-party (for independence)
- conduct review, identify gaps
- build plan to remediate, execute

Deliverable:

- assess against standard
- build/document and execute the plan

University of Victoria

Asset Management & Disposal

S1

- policy is documented, followed
- reviewed, and updated regularly
- includes both hardware and software and other critical business assets (scope)
- inventory must include name of system, purpose, location, owner, and criticality at a minimum (could include commission date, last updated date and name)
- assets are added to inventory on commission and removed on decommission
- disposal requirements are based on the sensitivity of the information

Deliverable:

- asset management policy (must follow the commission/decommission process)
- commission/decommission process says you must add/remove from inventory
- asset management inventory
- schedule review at least annually

University of Victoria

Incident Management

S1

- policy is documented, followed, reviewed, updated, and tested regularly

Deliverable:

- incident management policy
- schedule review annually

University of Victoria

Change Management

S1

- policy is documented, followed, reviewed, updated, and tested regularly
- changes to production environments must be reviewed and approved

Deliverable:

- change management policy
- schedule review annually

University of Victoria

Business Continuity Plan (BCP)

S1

- plan is documented, followed, reviewed, updated, and tested regularly

Deliverable:

- Business Continuity Plan (BCP)
- schedule test and review annually

University of Victoria

Disaster Recovery Plan (DRP)

S1

- plan is documented, followed, reviewed, updated, and tested regularly

Deliverable:

- Disaster Recovery Plan (DRP)
- schedule test and review annually

University of Victoria

Security Incident Response

S1

- plan is documented, followed, reviewed, updated, and tested regularly
- dedicated, virtual, or on-retainer team to lead response activities
- identify roles and responsibilities in advance (eg. communications)
- address preparation, identification, containment, eradication, recovery, and lessons learned and ensure chain of custody, impartiality, and follow evidence

Deliverable:

- Incident Response Plan
- schedule test and review annually
- template for an IR retainer RFP

University of Victoria

Information Security Policy

S1

- policy is documented, approved, followed, reviewed, and updated regularly
- policy should be standards-based in order to evolve over time
- include Appropriate Use so employees know what they may and may not do

Deliverable:

- Information Security Policy & Appropriate Use
- schedule review annually

University of Victoria

Logging & Monitoring

S2

- collect system logs to determine who did what when, retain according to retention policy, correlate and monitor to identify and act on suspicious activity

Deliverable:

- Logging & Monitoring Policy
- deploy logging system
- configure systems to log to logging system
- set up correlation and alerts
- respond to alerts

Backup & Retention

S2

- policy is documented, followed, reviewed, updated, and tested regularly
- scope and define as necessary
- regular backups are taken and tested regularly in accordance with backup policy
- frequency and completeness should be based on the criticality of the information

Deliverable:

- Backup Policy & Retention Schedule
- schedule test and review annually

University of Victoria

Physical Security & Visible Identification

S2

- policy is documented, followed, reviewed, updated, and tested regularly
- facilities must benefit from adequate controls (eg. alarms, fences, locks, lighting, access control systems, cameras, guards)
- staff and visitors must wear visible identification (including a picture) and challenge those who do not

Deliverable:

- Physical Security Policy
- schedule test and review annually

University of Victoria

Criminal Record Checks

S2

- employees must complete a satisfactory criminal record check *regularly (eg. every 5 years)* and are required to proactively disclose offences

Deliverable:

- Criminal Record Check process to conduct criminal record checks on employees
- policy that requires you to follow the process

University of Victoria

Security Awareness Program and Course

S2

- program is documented, followed, reviewed, and updated regularly
- includes annual information security course for employees
- educate users on common threats and impacts to business such as not sharing credentials, not clicking on suspicious links and attachments, reporting security incidents, maintaining clean desk, locking inactive systems, concealing valuables
- should be tailored for the employee roles
- annual security course with signoff

Deliverable:

- security awareness plan (and promotional materials)
- security awareness course
- schedule review annually

University of Victoria

Access Control

S3

- policy is documented, followed, reviewed, and updated regularly
- address onboarding, off-boarding, transition between roles, regular access reviews, limit and control use of administrator privileges, inactivity timeouts
- employees/contractors/vendors should only have access they are authorized to use
- conflicting duties and areas of responsibility must be identified and segregated to reduce incidents of fraud and other abuse (separation of duties)
- multi-factor auth is required for access to sensitive data from untrusted networks
- system accounts unable to use multi-factor must leverage strong authentication (eg. password aging, length/complexity, history)

Deliverable:

- Access Control Policy
- processes and systems in support of policy (including MFA)
- schedule review annually

University of Victoria

Defence in Depth for Endpoints/Networks

S3

- endpoints include servers, desktops, laptops, tablets, mobile devices
- networks include wired and wireless and require secure perimeter, network segmentation, and known ingress/egress points
- controls must exist to prevent, detect, and respond to security incidents
- technologies must include firewall, intrusion prevention, web content filtering, email content filtering, and anti-virus at a minimum
- systems must be hardened (eg. default passwords and shared accounts may not be used, unnecessary services are disabled, insecure protocols disabled)
- additional controls may be required to mitigate risk to your organization

Deliverable:

- firewall, intrusion prevention, web content filtering, email content filtering, and next generation anti-malware on network and endpoints
- configure devices according to best practices

University of Victoria

Security Governance

S3

- security review to be performed on each business case prior to allocation of capital and implementation of systems (security by design) with business signoff
- applications, programming interfaces developed according to industry standards

Deliverable:

- guidance on security requirements for projects (exists)
- insert security review/signoff in IM/IT capital investment process
- secure development standard

University of Victoria

Vulnerability Management & Patching

S3

- policy is documented, approved, followed, reviewed, and updated regularly
- scans to be performed prior to & following production launch
- systems must be patched regularly to ensure current OS and application levels
- vulnerability assessments are regularly conducted as part of a program and vulnerabilities must be rated according to criticality
- high and critical vulnerabilities must be remediated through patching, decommission, or compensating controls

Deliverable:

- VM program to identify, notify, follow up, and report on high/critical vulnerabilities
- patching policy
- recurring vulnerability scans

University of Victoria

Application Security

S3

- applications, programming interfaces developed according to industry standards
- web application vulnerability scans are performed prior to and following production launch and vulnerabilities are addressed
- code is reviewed in accordance with industry best practices

Deliverable:

- application security policy, standards
- recurring web app vulnerability scans (& static code analysis)

University of Victoria

Information Security Classification

S4

- classification is documented, approved, communicated, and followed
- employees must understand not all data is created equal, some data is more sensitive than others and should benefit from greater controls
- employees should possess only the sensitive information they need, handle it carefully, and label it as appropriate
- sensitive information must be encrypted in-transit and at rest
- prohibit production data in test environments unless security controls are equivalent to production or better

Deliverable:

- Information Classification Standard
- employees are aware of what to do and how to do it (systems may be needed to support)

University of Victoria

Vendor Security Requirements

S4

- vendor requirements are documented, followed, reviewed, and updated regularly
- requires vendors to meet or exceed organizations' security policy
- vendors are required to demonstrate evidence of compliance
- supply chain security risks are identified, mitigated, and reviewed regularly

Deliverable:

- vendor security schedule to be included in contracts
- schedule review annually
- audit or other evidence of compliance

University of Victoria

Information Security Program

S4

- program is documented, approved, executed, reviewed, and updated regularly
- align with organization's mission, vision, and goals
- provides clear direction on security strategy

Deliverable:

- Information Security Program
- schedule review annually

University of Victoria


University
of Victoria

Summary of Cybersecurity Panel

University of Victoria

Panel

- the following slides are a summary of a cybersecurity panel that occurred at the 2019 Privacy & Security Conference in Victoria, BC
- security is not an IT problem, it is a business enterprise risk
- impacts of security are much more than a computer getting a virus
- security is everyone's responsibility, not just the responsibility of the security team
  - it is everyone in this room and everyone at your organization's responsibility

University of Victoria

Panel

- security professionals come from all walks of life, not just technical fields
- significant talent shortage previously estimated at 2 million by 2019 now 3.5 million by 2021 and presently assessed at 3 million globally
- AI is not expected to solve the talent shortage
- referenced changing faces of cyber security document by Deloitte and personas

University of Victoria

Panel

- panel members recommended audience members reach out to the business and connect with them, show empathy
- other panel members recommended using tabletop exercises to educate executive
- critical to get board visibility and sponsorship for cyber initiatives

University of Victoria

Panel

- how to get board member support?
  - know your audience
  - communicate in business terms
  - find out what they value, what keeps them up at night (to ensure relevance)

- cloud can be very secure
  - still need to ensure appropriate security controls are applied
  - most cloud breaches are because organizations have failed to take advantage of the controls the cloud providers have made available

University of Victoria

Panel

- critical to have visibility on your network to know when you are having an incident and when it has been remediated
- DevOps or DevSecOps can allow security to be built in at every level
- similar to cloud, if you don’t build the security in then it may not be any more secure

University of Victoria

Panel

- security should be built in from the ground up
  - “security by design”
- security built in from the beginning is easier, faster, cheaper, and more effective
- security bolted on after the fact is more difficult, slower, more expensive, and less effective

Panel

- global impact of cyber crime is forecasted to hit $6 trillion and organizations will be willing to spend $1 trillion to combat the threat
- depending on who you ask Canada could be well positioned to be a leader in cybersecurity
- Canada has a long way to go but has many attractive precursors to success

University of Victoria

Panel

- security is not a destination, it’s a journey
  - what you did last year may not be enough, need to continue evolving
- cloud will happen to you – you don’t have a choice
- MVP meaning could go from “minimum viable product” to “minimum viable prototype”

University of Victoria

Panel

- concept of “trust but verify” or “trust and verify” means you make sure to doublecheck
- make sure there are checks and balances
- maintain a layered security approach
- sit down with people and listen
- empathize with victims of cybercrime, cyber bullying

University of Victoria

Panel

- raising a generation that are having a hard time with empathy
  - practice empathy, some small way
  - ask them how they're doing, don't just email them
- every single person should do that
- world would be a greater place, better at security

University of Victoria

Panel

- tabletop simulations, red-team exercises are useful
- can talk about scorecards, risk assessments and other theoretical things – vulnerabilities in applications
- nothing will grip the executive more than hearing “the team got through, they are holding the data”
  - can be moments of truth from the board and executive

University of Victoria

Panel

- people are part of cybersecurity… and can be challenging
  - technology can be easy
- people should talk to “other side of the organization” – if on the IT side talk to business and if on business talk to IT
- if not having discussion going back and forth neither side will be successful
  - “create and understand the blueprint of your environments and invest in simplicity”

University of Victoria