SENG 460 / ECE 574
Practice of Information Security and Privacy

Week 11:

Building Security into the Organization

Gary Perkins, MBA, CISSP

garyperkins@uvic.ca

University of Victoria

ECE 574 – Security Film Festival

To open links, right click and open in new tab/window...

2021:

- Crucial Security Tips for Working from Home by NS
- Cyber Security Awareness by AJ & OFD
  Antivirus by AJ & OFD
- Cybersecurity for Kids by AM
- Data Privacy and why we should care by HA
- Malvertising by PM
- MITRE ATT&CK by VN
- Solarwinds Attack by AA
- Easy Passwords for Teenagers by AA
- Top 10 Types of Cyber Security Threats by NS
- Internet Safety 101 by CC
- Keyless Vehicle Crimes by LB
- Importance of Automation in Cybersecurity by RS
- Cyber Security and Cyber Attacks by SJB
- 7 tips to prevent major cyber attacks by MK
- Mobile Security by PP
- 10 Tips to be Safe Online for Families by RM
- Ransomware II by SH & QB
- Fake News by SC & CZ
- Password Security by IN & MB
- Remaining Anonymous - TOR and the Dark Web by HK & MS
- Cyber Security in Daily Life by SS & GSM
- Understanding Cyber Attacks by YW
- Security in Internet of Things by FR & EVE
- Data Breach in Digital World - Facebook-Cambridge Analytica Scandal by AD, BM, & AG
- The Five Tenets of Cybersecurity by SK, JD, & JS
- Waterholing - Malvertising - Piggyback-Tailgating by KT, MA & SM
- Ransomware by AD, NC, & GK
- What is Cybersecurity and how to Protect Yourself
- How Cybercrimes Affect our Daily Life Part 1 by EM, JW, & ET
- How Cybercrimes Affect our Daily Life Part 2 by EM, JW, & ET
- How Cybercrimes Affect our Daily Life Part 3 by EM, JW, & ET

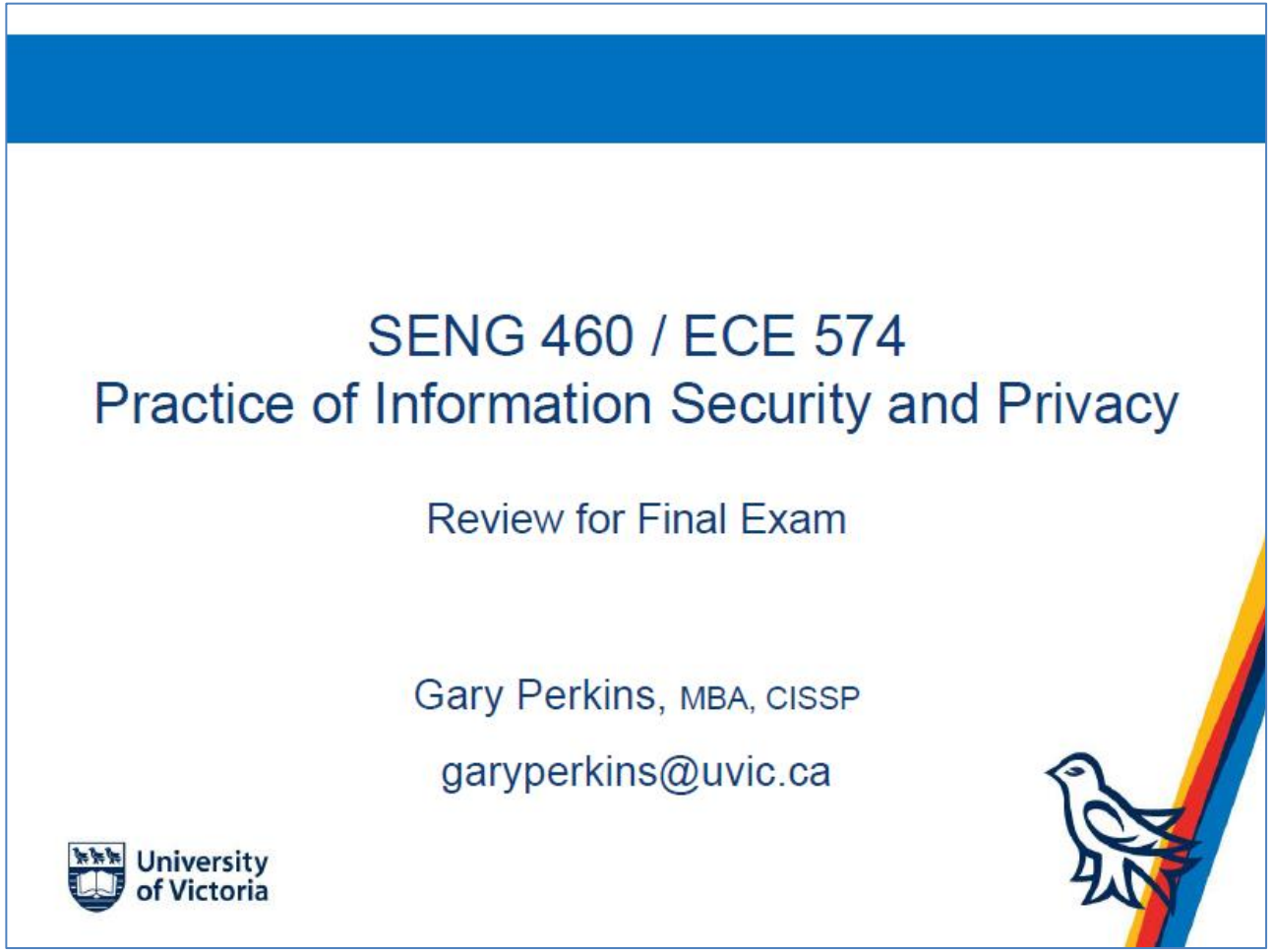
Final Exam

- 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

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, Physical Security Part II, BCP, DRP, Lab: MySQL
- Week 11: Building Security into the Organization and Responding to Incidents, 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

University of Victoria

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

University of Victoria

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

University of Victoria

Knowledge check

- viruses, worm, trojan, rootkit, keylogger, adware, spyware, bots, RAT, logic bomb, backdoor
- DoS, DDoS, man-in-the-middle, buffer overflow, SQL injection, cross-site scripting (XSS), privilege escalation
- amplification, reflection, ARP poisoning, BGP hijacking, DNS poisoning, domain hijacking
- hijacking (clickjacking, session hijacking, typo/squatting)

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

University of Victoria

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

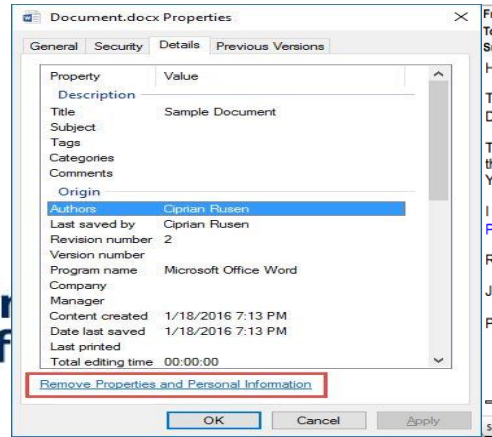
University of Victoria

Review

- identify your crown jewels, ensure they benefit from adequate protection otherwise end up as a headline

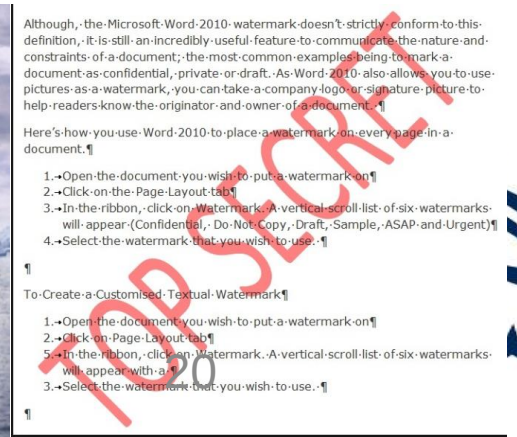
- techniques to mark files:

meta-tagging



beaconing,
email pixel tracking

watermarking

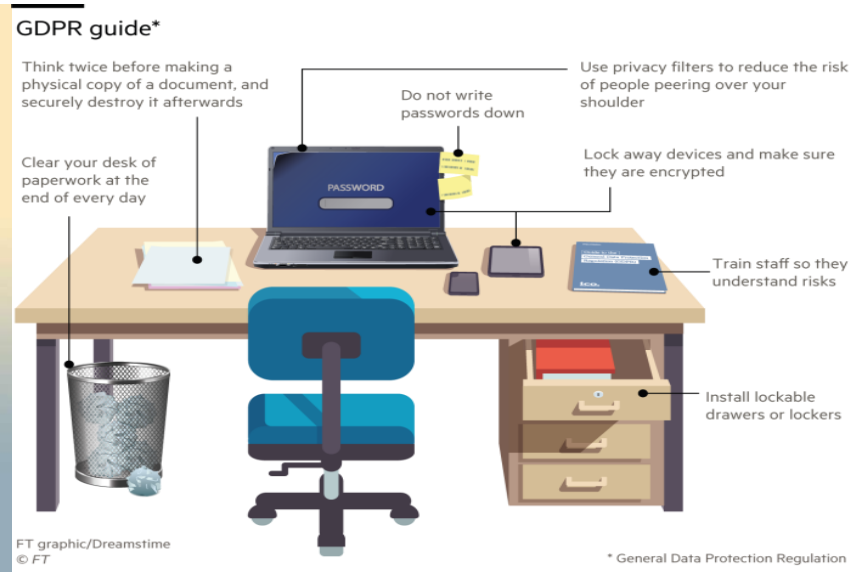


Review

- cyber is the number one national security threat to the US
- COMPLIANCE IS NOT EQUAL TO SECURITY
- approach to managing confidential info w/ employees:

  1. agree in advance, 2. remind during, 3. remind on exit

- clean desk policy (desk is free of sensitive material)



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

University of Victoria

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

Building Security Into the Organization

University of Victoria

Review

- 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

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

University of Victoria

Plan and EXECUTE

present state

gap analysis

plan & execute

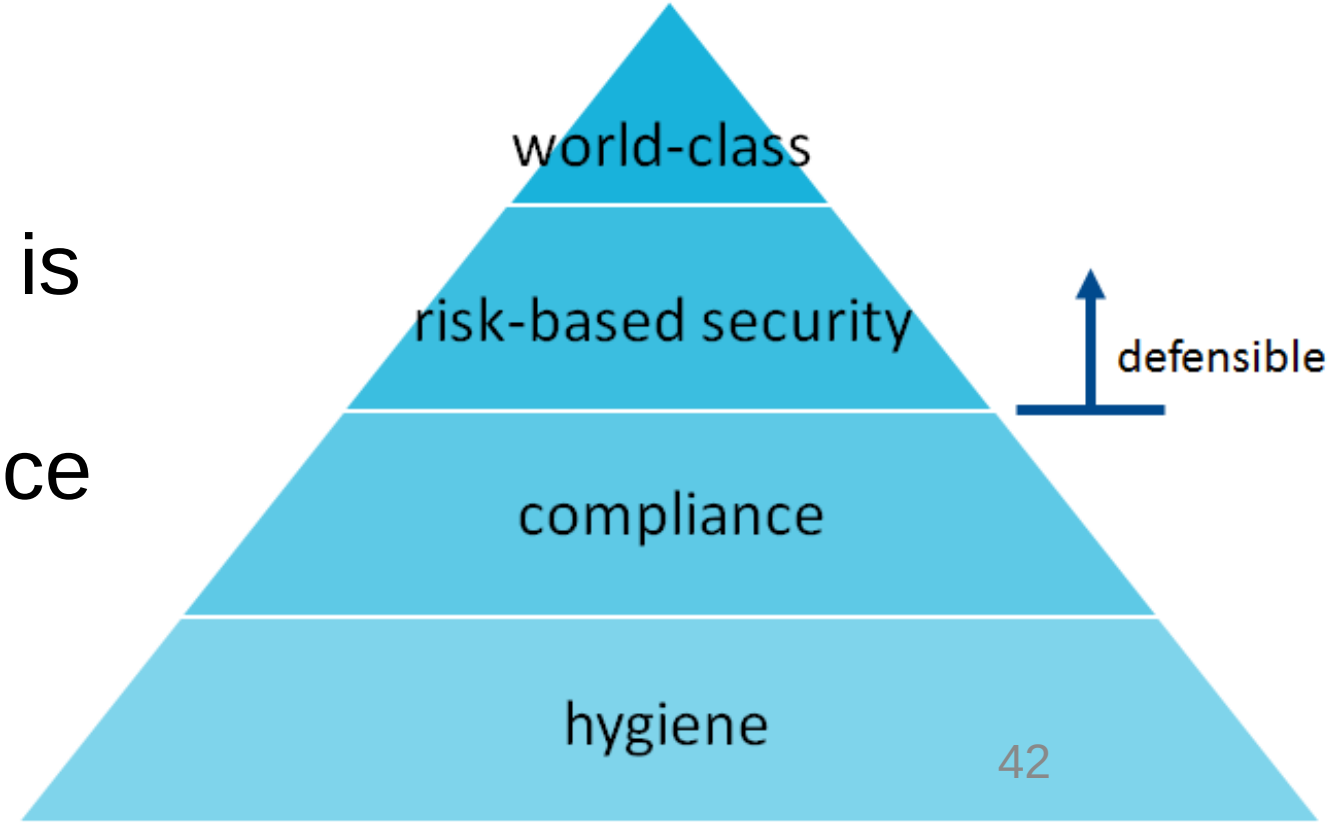
future state

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

University of Victoria

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

BRITISH COLUMBIA

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:

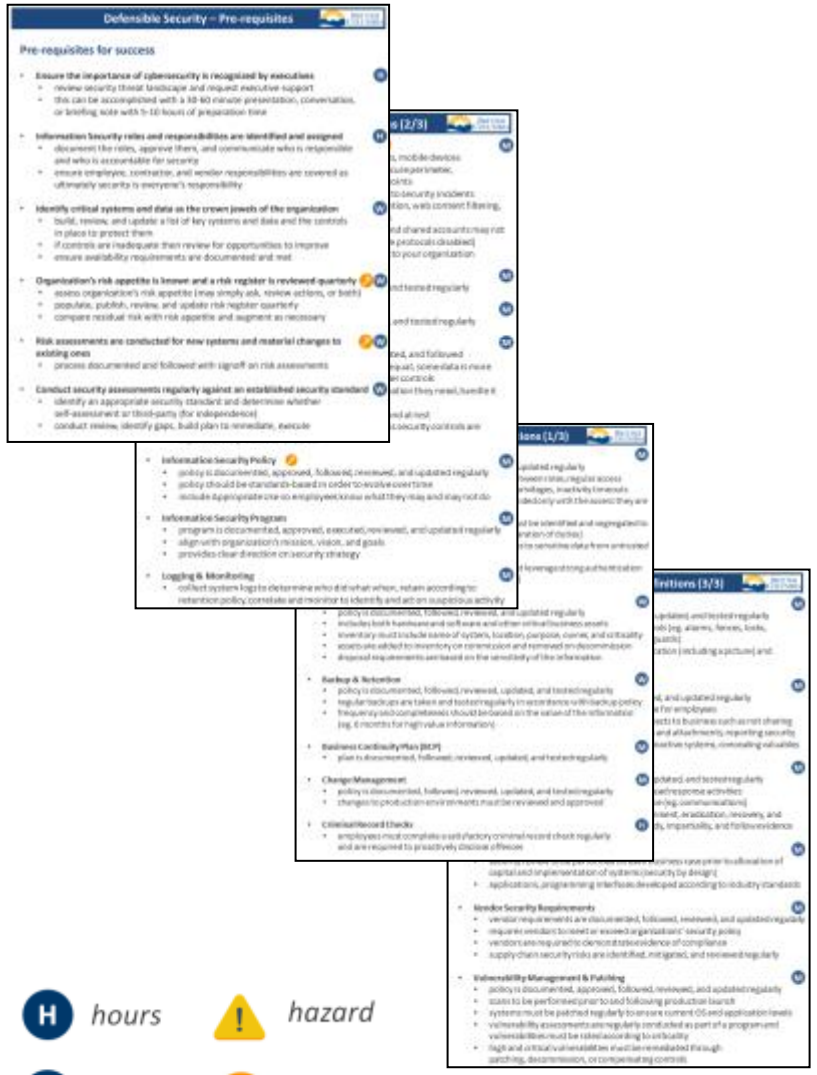
- ❑ Ensure the importance of cybersecurity is recognized by executives
- ❑ Information Security roles and responsibilities are identified and assigned
- ❑ Identify critical systems and data as the crown jewels of the organization
- ❑ Organization's risk appetite is known and a risk register is reviewed 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

1 **Exec** awareness	2 **Roles** responsibilities	3 **Crown** jewels	Sample		4 **Risk** appetite	5 **Risk** assessments	6 **Security** assessments
7 **Asset** management	8 **Change** management	9 **Incid** management	10 **BCP**	11 **DRP**	12 **Backup** & retention	13 **Logging** & monitoring	14 **Physical** & visible ID
15 **Incid** response	16 **Policy** (security)	17 **Prog** (security)	18 **Info** classification		19 **Crim** record checks	20 **Aware** program/course	21 **Vendor** requirements
22 **Access** control	23 **DiD** for end-points & network					24 **Security** governance	25 **VM** & patching

- complete or substantially complete
- partially complete or in progress
- incomplete or substantially incomplete

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

1 **Exec** awareness	2 **Roles** responsibilities	3 **Crown** jewels			4 **Risk** appetite	5 **Risk** assessments	6 **Security** assessments
7 **Asset** management	8 **Change** management	9 **Incid** management	10 **BCP**	11 **DRP**	12 **Backup** & retention	13 **Logging** & monitoring	14 **Physical** & visible ID
15 **Incid** response	16 **Policy** (security)	17 **Prog** (security)	18 **Info** classification		19 **Crim** record checks	20 **Aware** program/course	21 **Vendor** requirements
22 **Access** control	23 **DiD** for end-points & network					24 **Security** governance	25 **VM** & patching

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

University of Victoria

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

Building the Plan

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

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

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

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

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

Building the Plan (extended version)

	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6	Month 7	Month 8	Month 9	Month 10	Month 11	Month 12	
Ensure the importance of cybersecurity is reco	■												
Information Security roles and responsibilities	■												
Identify critical systems and data as the crown	■												
Organization's risk appetite is known and a ris		■			■			■			■		quarterly
Risk assessments are conducted for new syste			■										ongoing
Conduct security assessments regularly again		■											annual
Asset Management & Disposal			■	■									annual
Change Management				■	■								weekly
Incident Management				■	■								daily/annu
Business Continuity Plan (BCP)						■	■						annual
Disaster Recovery Plan (DRP)						■	■						annual
Security Incident Response		■	■										annual
Information Security Policy				■	■								annual
Logging & Monitoring						■	■						ongoing
Backup & Retention							■	■					annual
Physical Security & Visible Identification						■	■						annual
Criminal Record Checks						■	■						ongoing
Security Awareness Program & Course				■	■	■							monthly/a
Access Control					■	■	■	■	■				ongoing &
Multifactor authenticatoin						■	■	■	■				
Defence in Depth for Endpoints and Networks				■	■	■	■	■	■	■	■	■	
Security Governance				■									on-deman
Vulnerability Management & Patching		■	■	■	■	■							annual
Information Security Classification								■	■	■	■	■	ongoing
Vendor Security Requirements								■	■	■			annual
Information Security Program				■	■	■							annual

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

University of Victoria

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

University of Victoria

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

Example using NIST

NIST

Microsoft Excel Worksheet

Instructions			
Quick Assessment: Fill out column C with 1 (low), 2 (medium), 3 (high)		Score:	1.00
Complete Assessment: Fill out column E with 1 (low), 2 (medium), 3 (high)			
You may prefer to adopt a maturity model and utilize 1-initial, 2-repeatable, 3-defined, 4-managed, 5-optimizing			

Function	Category	Quick Assessment	Subcategory	Individual Assessment
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	1.00	**ID.AM-1:** Physical devices and systems within the organization are inventoried	1
			ID.AM-2: Software platforms and applications within the organization are inventoried	1
			ID.AM-3: Organizational communication and data flows are mapped	1
			ID.AM-4: External information systems are catalogued	1
			ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	1
			ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers,	1
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	1.00	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	1
			ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	1
			ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	1
			ID.BE-4: Dependencies and critical functions for delivery of critical services are established	1
			ID.BE-5: Resilience requirements to support delivery of critical services are established	1
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	1.00	**ID.GV-1:** Organizational information security policy is established	1
			ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	1
			ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and	1
			ID.GV-4: Governance and risk management processes address cybersecurity risks	1
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	1.00	**ID.RA-1:** Asset vulnerabilities are identified and documented	1
			ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	1
			ID.RA-3: Threats, both internal and external, are identified and documented	1
			ID.RA-4: Potential business impacts and likelihoods are identified	1
			ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	1
			ID.RA-6: Risk responses are identified and prioritized	1
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	1.00	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	1
			ID.RM-2: Organizational risk tolerance is determined and clearly expressed	1
			ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	1

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

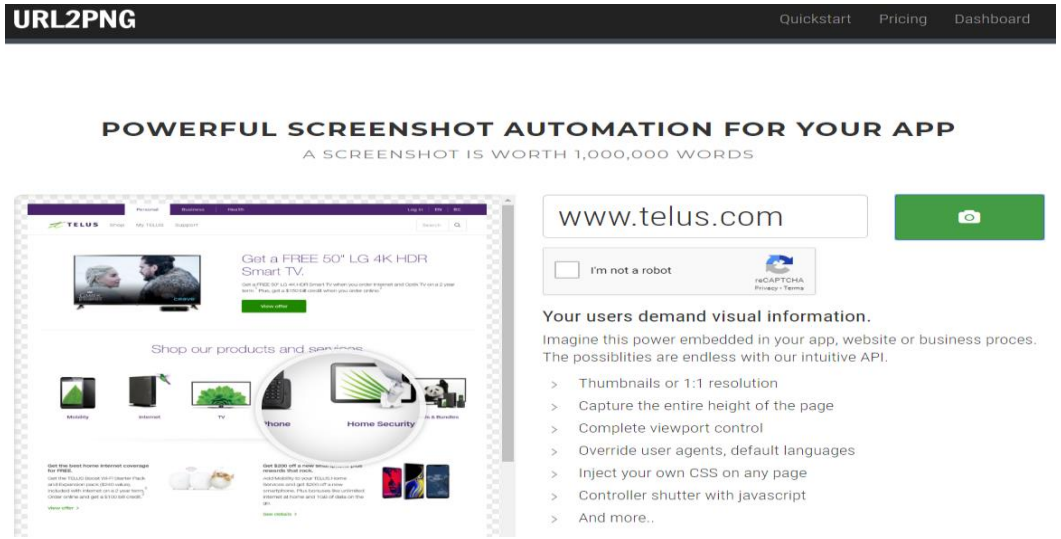
Review

- 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

University of Victoria

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?

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

University of Victoria

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	Automated Exfiltration	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	Exfiltration Over Alternative Protocol	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	Transfer Data to Cloud Account	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
		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							

= Has sub-techniques

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

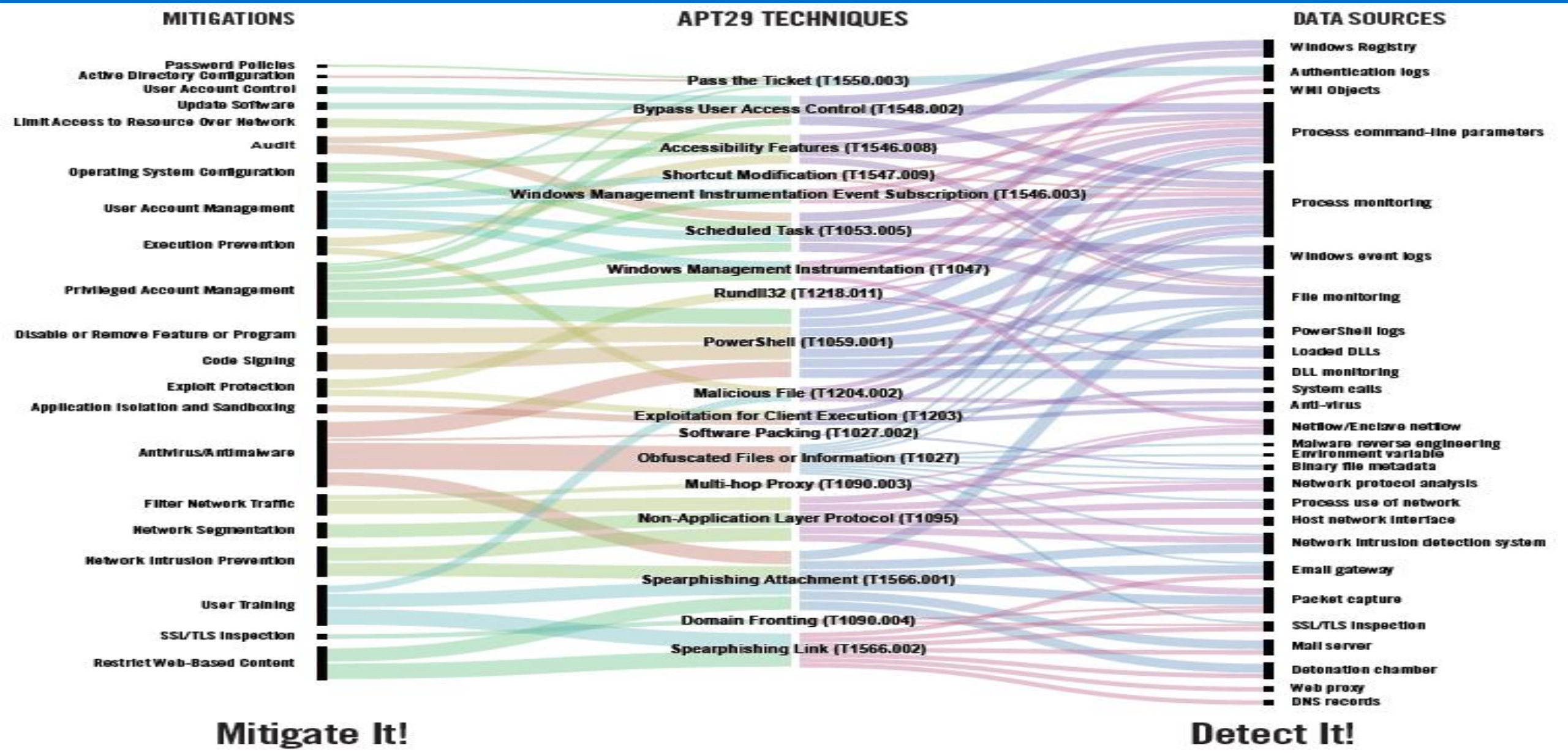
attack life cycle

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.

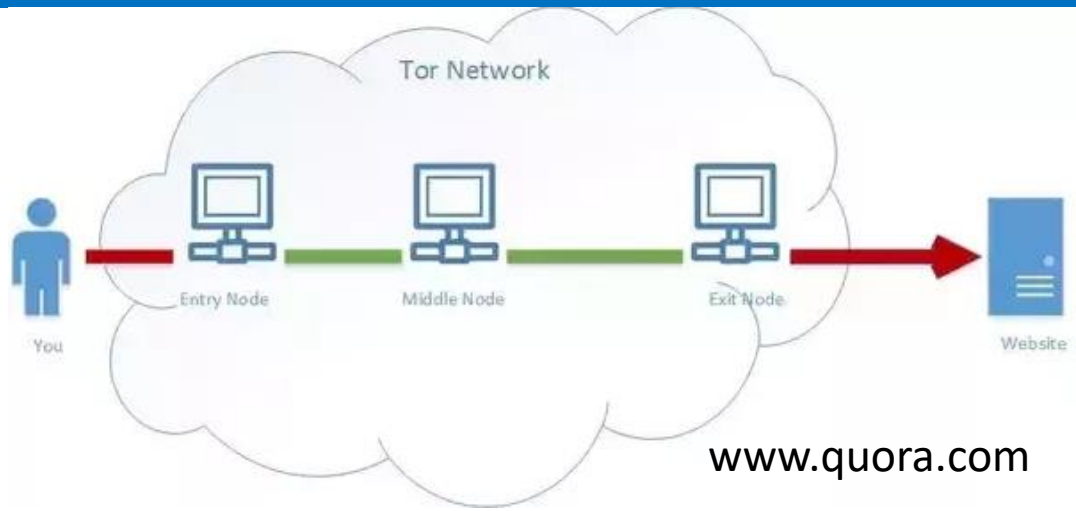
More recently, law enforcement's concern has been about Tor (which is slightly ironic, given that Tor was created and funded by the US government). The Snowden revelations have shown that, try as they might, the NSA has **not had much luck** in compromising Tor, and Snowden himself has noted that properly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

Review

- 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

University of Victoria

Review

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

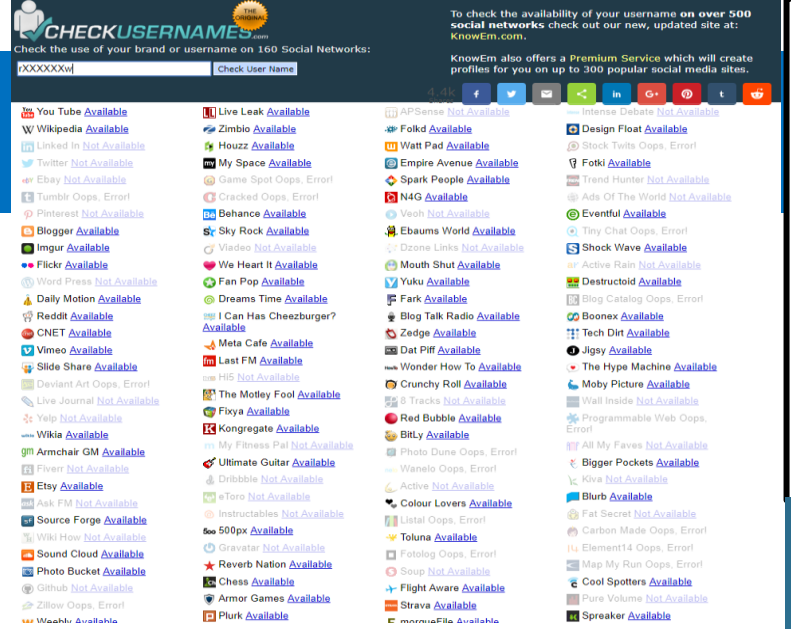
In those systems:
john.smith@org.com

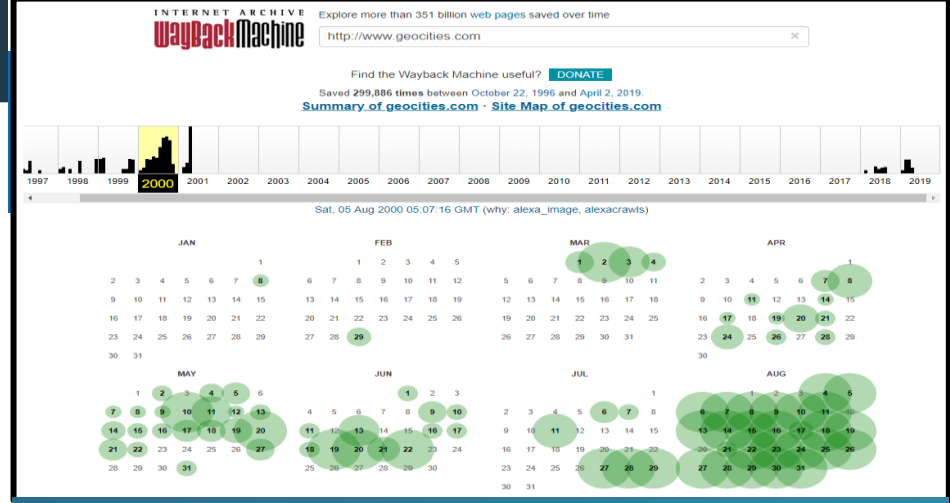
Review all available sources of information

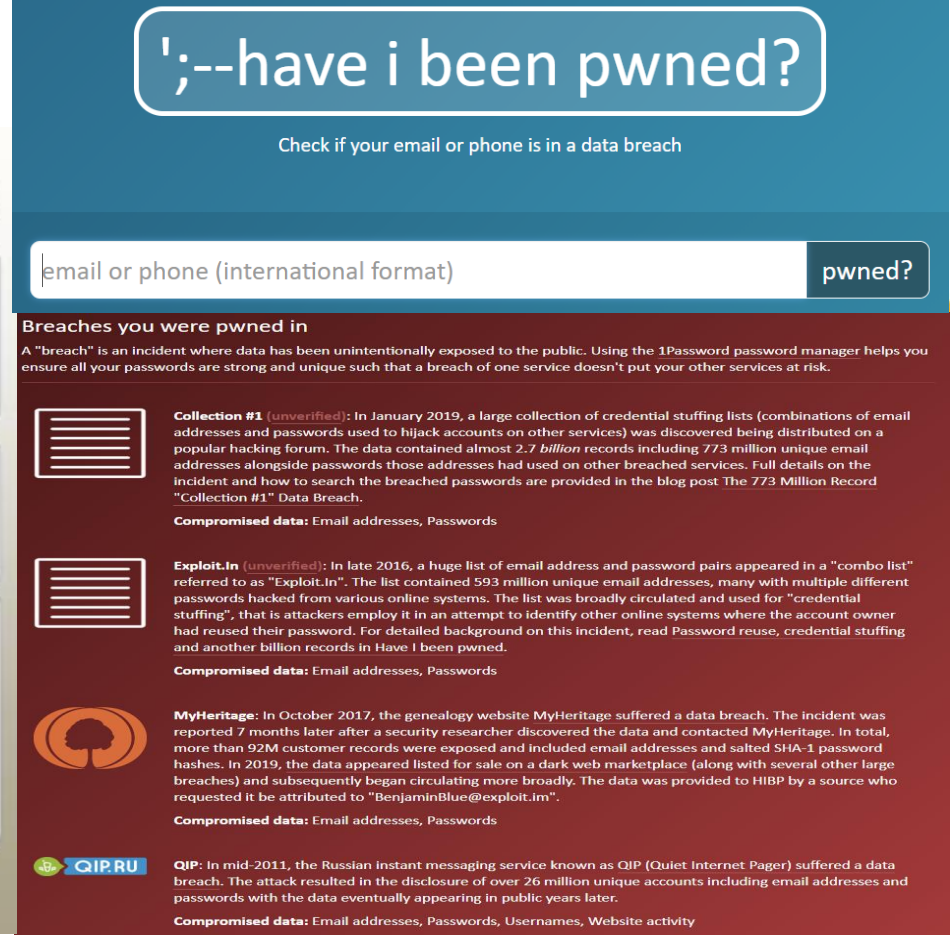
University of Victoria

Reconnaissance

- so many websites
  so little time



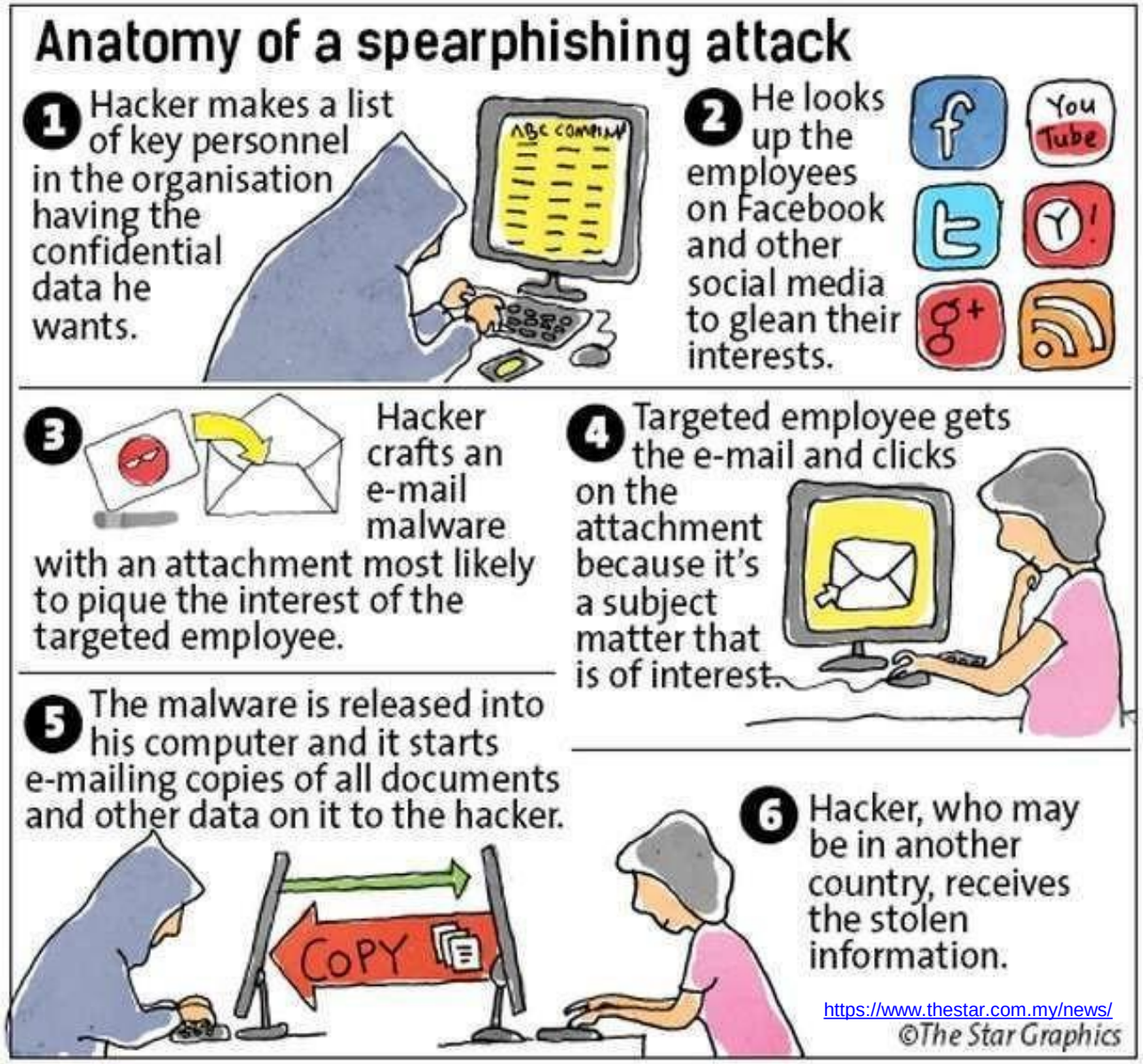




Weaponization

- “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/



https://www.thestar.com.my/news/

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

University of Victoria

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

University of Victoria

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

Epilogue

University of Victoria

Summary

- cyberattacks are a significant global problem
  - threatens democracy, economy
- significant shortage of security professionals
  - security professionals come from all backgrounds
- security is not just the role of security professionals
  - security is everyone's responsibility
  - security is not solely an IT problem
- all crimes are cyber crimes
  - cybercrimes are not victimless crimes
  - no-one knows what the future damage will be
  - we are all victims

University of Victoria

Key messages

- incidents are increasing in frequency and are more sophisticated and targeted than ever
- no organization globally is immune to attack and
- organizations can no longer ignore the risk that security threats pose
- doing the basics well will stop 80% of the problems
- security is not just an IT problem, it’s business enterprise risk
- security is a top issue of concern for executives and Boards of Directors globally

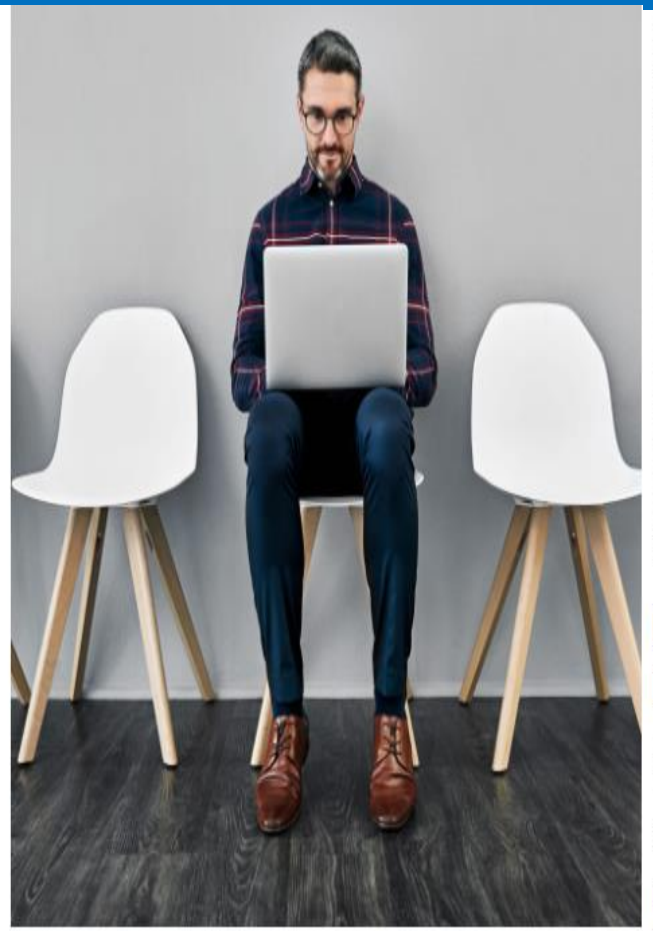
University of Victoria

Next Generation of Cyber Talent

Start → News & Media → Insights → The cybersecurity skills gap

The cybersecurity skills gap: 4 million professionals needed worldwide

16 DECEMBER 2020



Cybersecurity is facing an unprecedented challenge: finding and training enough professionals to answer the growing needs of global businesses, which are facing an ever-growing threat of cyberattacks.

Cybersecurity Jobs. PHOTO: Cybercrime Magazine.

Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021

350 percent growth in open cybersecurity positions from 2013 to 2021

The 2019/2020 Official Annual Cybersecurity Jobs Report is sponsored by Herjavec Group, a leading global cybersecurity advisory firm and Managed Security Services Provider (MSSP) with offices across the United States, Canada, and the United Kingdom.

– *Steve Morgan, Editor-in-Chief*

Sausalito, Calif. – Oct. 24, 2019

The New York Times reports that a stunning statistic is reverberating in cybersecurity: Cybersecurity Ventures' prediction that there will be 3.5 million unfilled cybersecurity jobs globally by 2021, up from one million positions in 2014.

Next Generation of Cyber Talent

- 3.5 million global shortage of security professionals forecasted by 2021

- 3 million global shortage estimated now

Summary

- whether you are a citizen, student, teacher, employee, manager, executive, or security professional
  - ➢ build in security by design

- throughout the course I hope you gained a better appreciation for privacy and security and….
  - consider privacy and security more in the future
  - consider privacy and security as a career

- share your thoughts on the course survey and with other students who should take the course

University of Victoria

Thank you for listening…

University of Victoria


University
of Victoria