HOW TO BE A SECURITY OFFICER @WORK AND @HOME

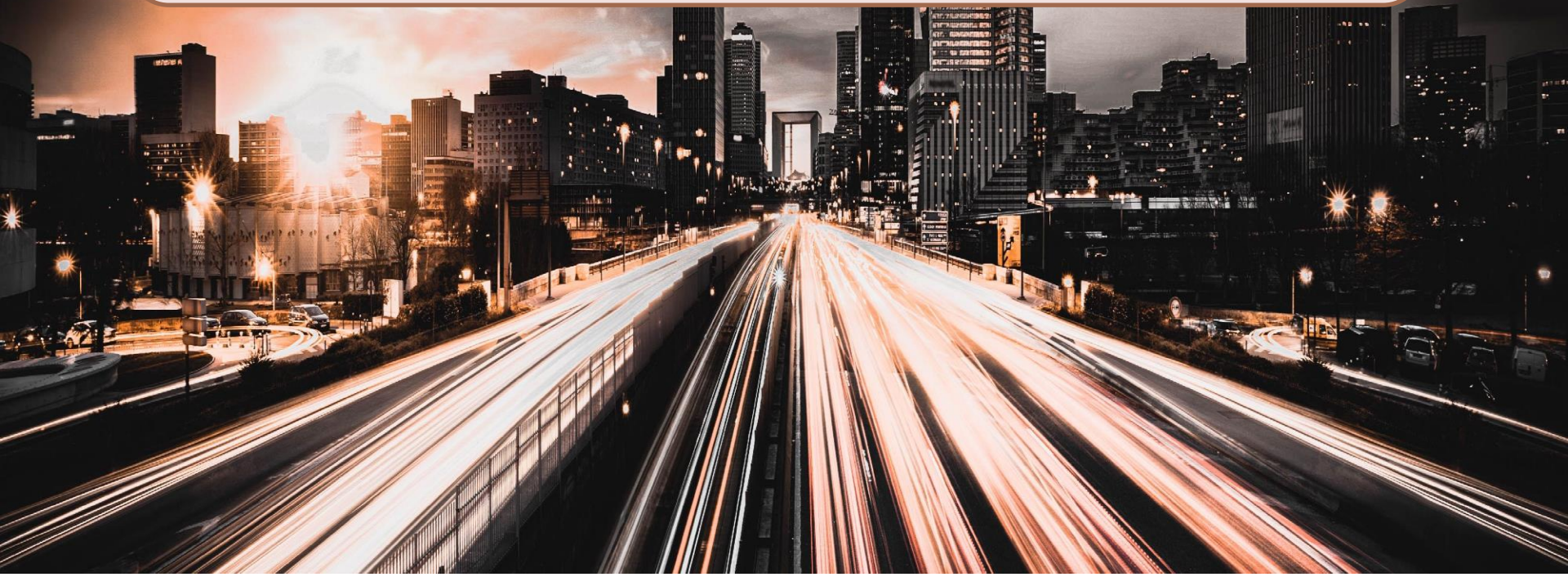
with

Michael Foltinek

Information Security Branch, OCIO

BRITISH COLUMBIA | Ministry of Citizens' Services

"The world's most valuable resource is no longer oil, but data"



The Economist: May 6th, 2017

What is Information Security?

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

~ NIST

@WORK

Information Security = Job Security

"The greatest virtual threat today is not state sponsored cyber-attacks; newfangled clandestine malware; or a hacker culture run amok…."

"**The most dangerous looming crisis in information security is instead a severe cybersecurity labor shortage.**"

- John Reed Stark, former Chief of the SEC's Office of Internet Enforcement


COME TO THE
DARK SIDE
WE HAVE COOKIES

BRITISH COLUMBIA | Ministry of Citizens' Services

THE REALITY OF DATA BREACHES

DATA RECORDS COMPROMISED IN FIRST HALF OF 2018

3,353,172,708

18,525,816 records lost or stolen every day	771,909 records every hour	12,865 records every minute	214 records every second

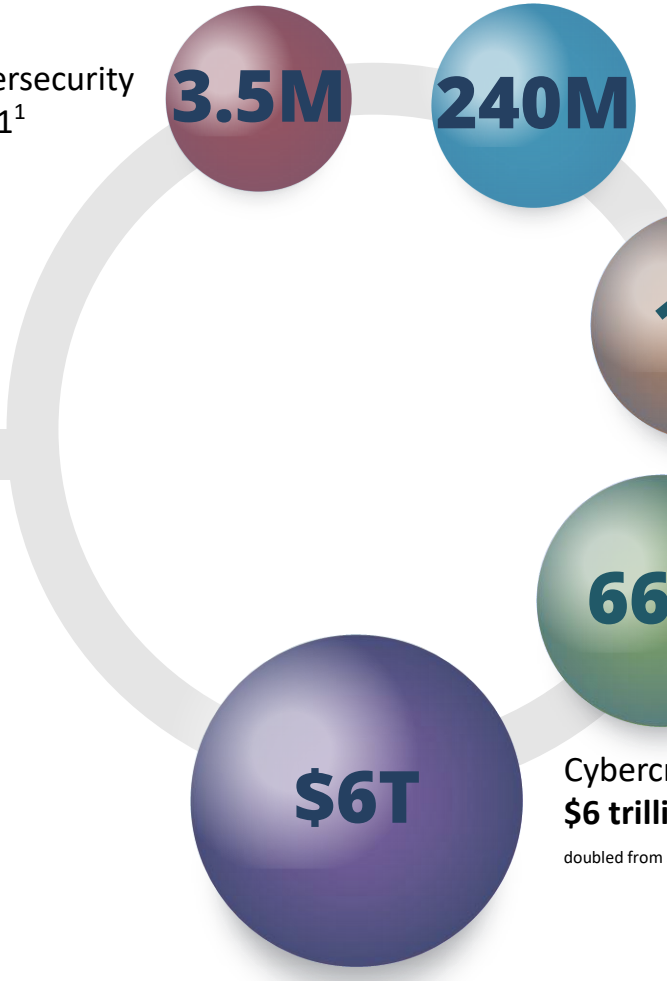
LESS THAN 3% of breaches were **"Secure Breaches"** where **encryption** rendered the stolen data useless

Source: https://safenet.gemalto.com/uploadedImages/resources/Infographics/Data_Protection/breach-level-index-infographic-h1-2018-v4.jpg

Global Context

BRITISH COLUMBIA | Ministry of Citizens' Services

Digital Security Landscape



3.5 million new cybersecurity job openings by 2021[1]

Almost **500 million** unauthorized access attempts to core government ministry systems are mitigated every day

Losses from cyber attacks estimated to cost **1%** of GDP per year[2]

Global cybersecurity industry forecasted to grow by **66%** by 2021[3]

Cybercrime to cost organizations **$6 trillion** by 2021[4]

doubled from $3 trillion in 2015

Sources:
[1] 2017 Global Information Security Workforce Study
[2] Australian Cyber Security Strategy 2016
[3] Research and Markets, "Cyber Security Market – Global Forecast to 2021", August 2016
[4] Cybersecurity Ventures

BRITISH COLUMBIA | Ministry of Citizens' Services

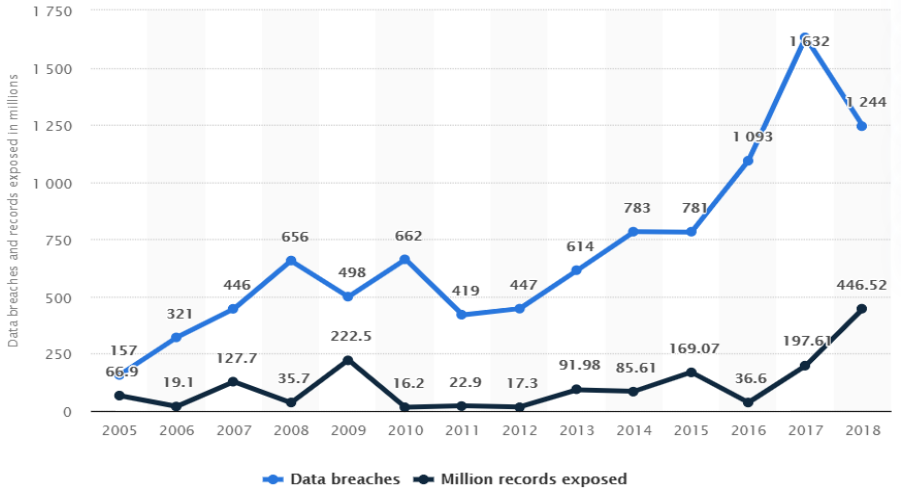
Cybersecurity has never been more imperative

Threat Landscape

Cyber attacks are more:

- frequent
- effective
- targeted
- profitable
- persistent
- elusive

Data Breaches & Exposed Records in the US (millions)



Business Impacts

- direct impact to citizens
- brand/reputation
- financial loss
- litigation, regulatory
- data breach and loss
- lost/stolen intellectual property

Why is Public Sector a Target?

- gain economic advantage
- access to personal data (e.g. health), fraud
- trusted launch point against others
- law enforcement, justice/courts
- surveillance

Why is Information Security Important?

- After surveying 790 IT executives Radware stated that the average estimated cost of a cyberattack for an enterprise was $1.1 million in 2018—**up 52% from the year before**. That number is expected to rise to $1.7 million in 2019.

https://blog.sucuri.net/2019/10/cost-of-cyber-attacks.html

Why is Information Security Important?

- 60 per cent of small and medium-sized businesses (SMBs) hit by ransomware attacks close within six months.
- Only 32 per cent have the tools to monitor their networks for malicious activity 24 hours a day, seven days a week.
- It's a paradox: Canadian business owners underestimate the threat of cyberattack while simultaneously overestimating how prepared they are to face one.
- "What's happening out there is that all the hackers are targeting small and medium-sized businesses because they know that their skill set and the technology they're using is very basic." Martin Bélanger, Telus.

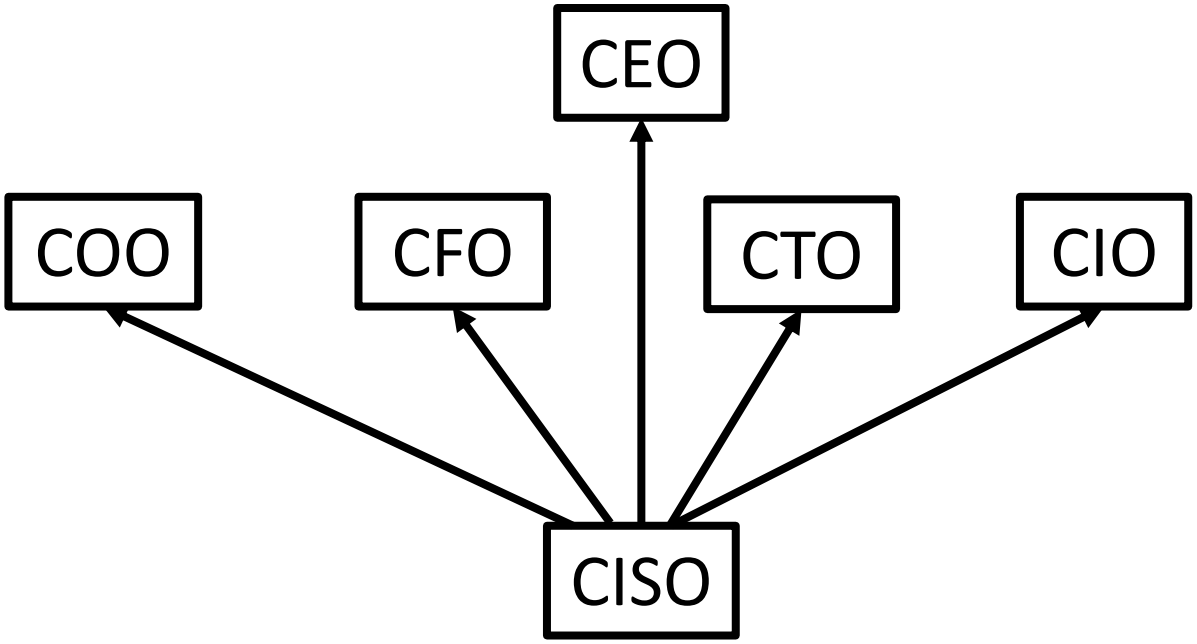
- https://www.theglobeandmail.com/business/adv/article-are-you-protecting-your-business-from-cyber-attack/ *(January 14, 2020)*

Why is Information Security Important?

- 97 of the world's 100 largest airports had massive cybersecurity risks
- Just three airports received an A+ and only 15 managed to score an A
- 97% of the websites are deploying outdated web software, 24% had known and exploitable vulnerabilities
- For the 36 airport mobile apps that researchers examined, more than 500 security and privacy issues were found as well as 288 mobile security flaws, with an average of 15 per application.
- Nearly 90% of the airports had data leaks on public code repositories and 503 of the 3,184 leaks are of a critical or high risk that could potentially lead to a breach. Three percent of airports studied had unprotected public clouds with sensitive data available.

https://www.immuniweb.com/blog/state-of-cybersecurity-top-100-airports.html

Information Security in the Organisation

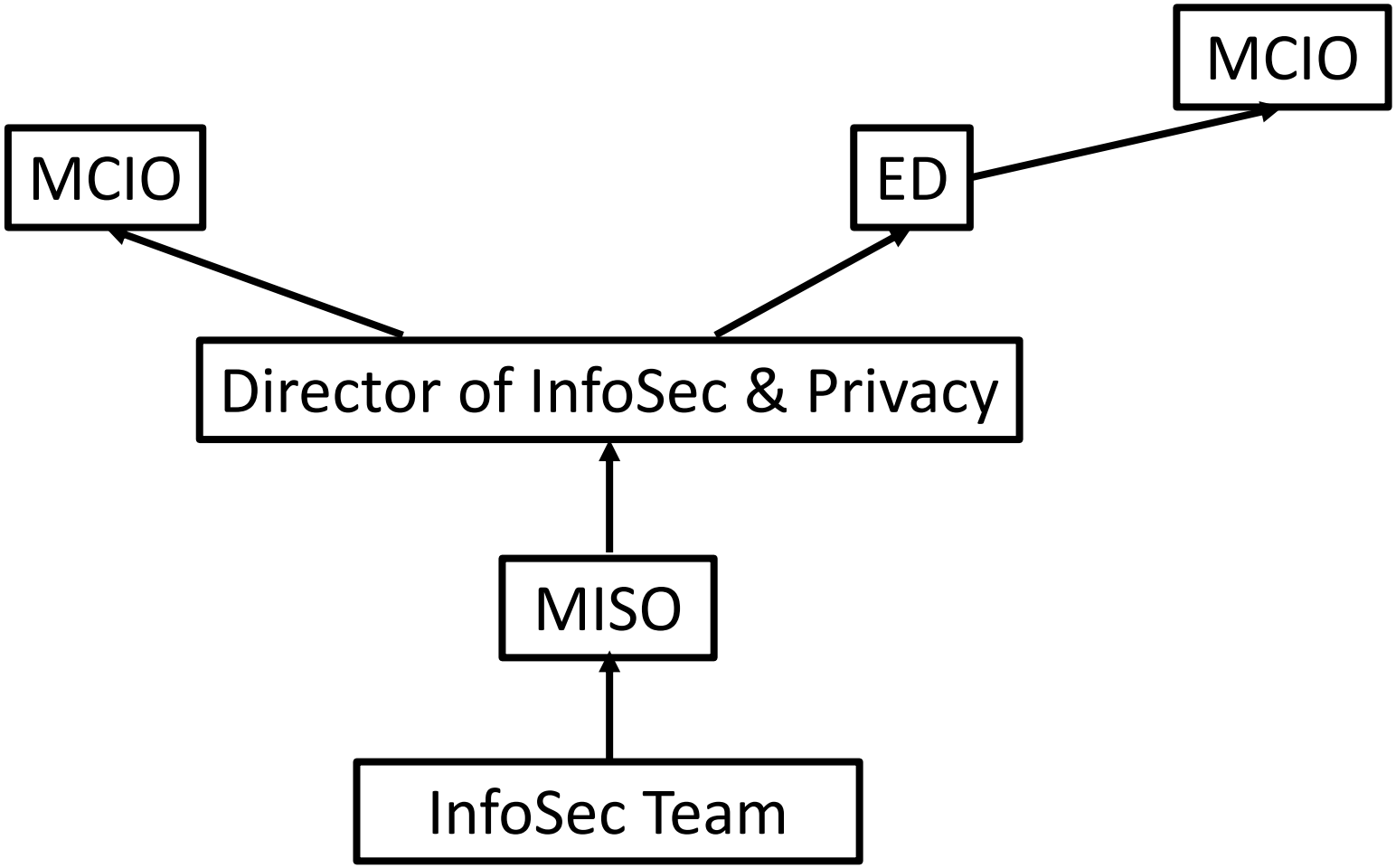


Information Security in the Organisation

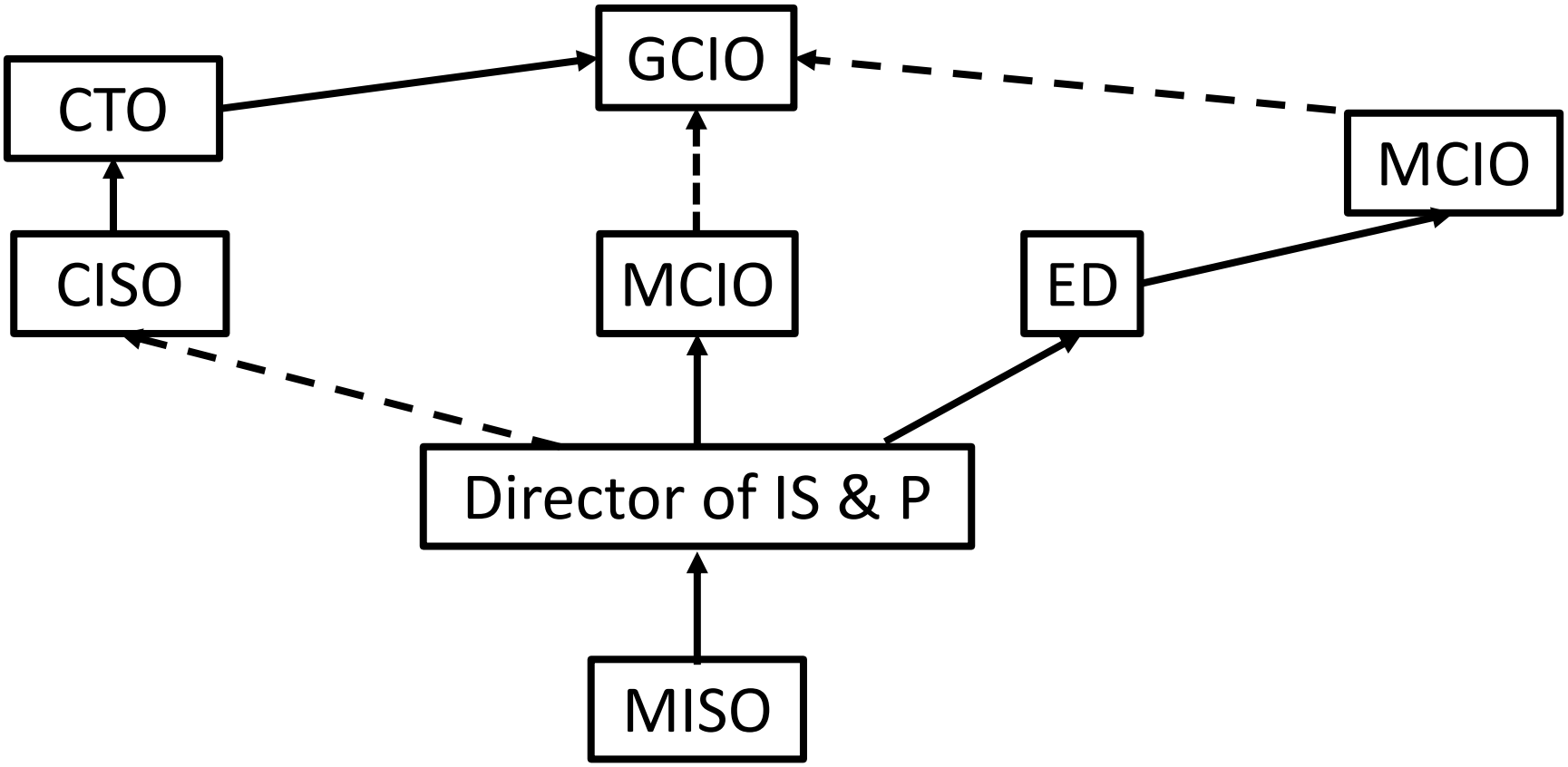
Responsibilities of a CISO
(rafeeqrehman.com)

Business Enablement
Project Delivery Lifecycle
Budget
Compliance and Audits
Legal and Human Resources
Risk Management
Governance
Identity Management
Security Architecture
Security Operations
Selling Information Security internally

Information Security in the BC Government



Information Security in the BC Government



According to a study by (ISC)2

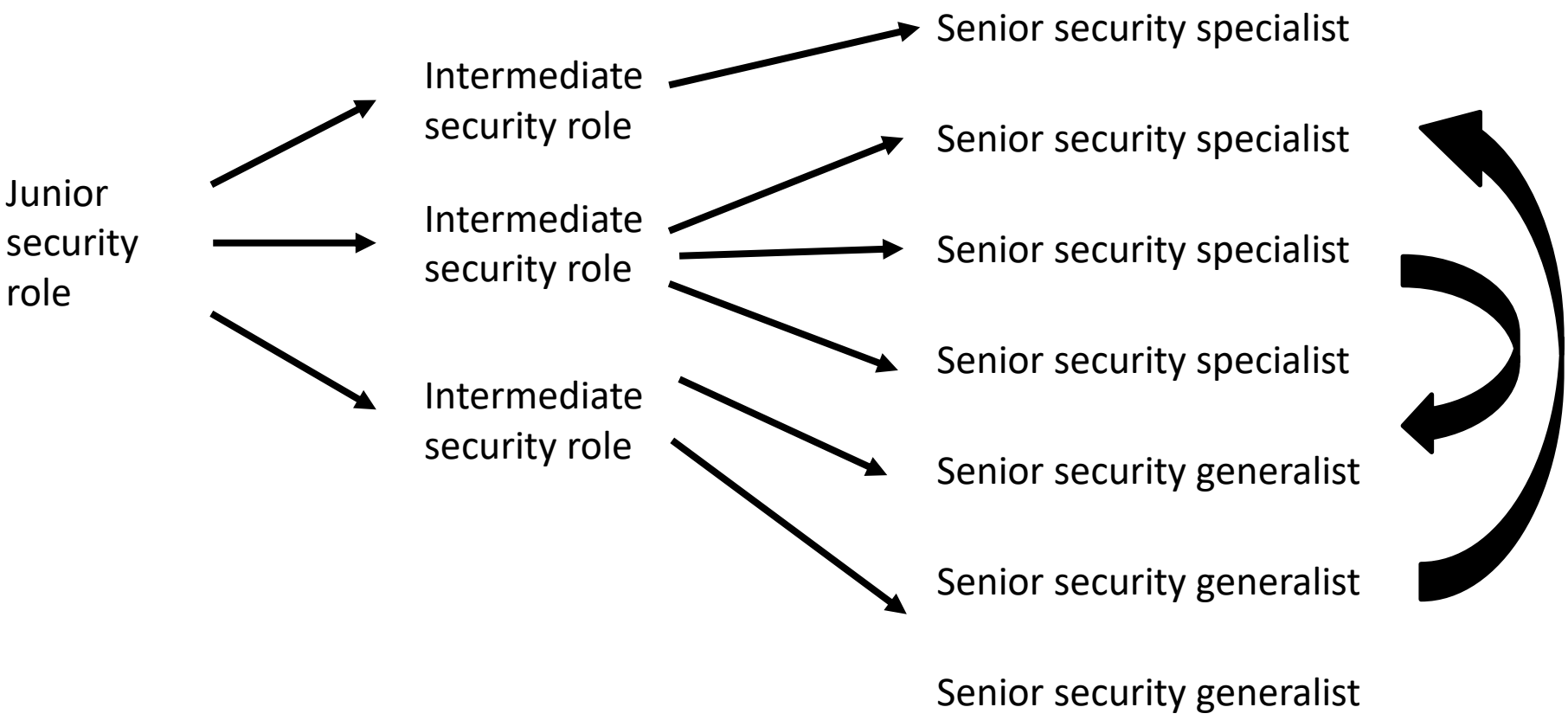
- Just 42% of respondents indicate that they started their careers in cybersecurity; meaning 58% moved into the field from other disciplines
- 30% of survey respondents are women; 23% of whom have security-specific job titles
- 37% are below the age of 35, and 5% are categorized as Generation Z, under 25 years old

- *https://www.helpnetsecurity.com/2019/11/08/cybersecurity-workforce-skills-gap/*

Getting into Security

- IT operations:
  - IT ops -> security ops, security analyst
- Other parts of the organisation:
  - Auditor -> security
  - Privacy -> security
  - Risk Management -> security
  - Physical security -> security

Getting into Security



Getting into Security

- What do you want to do?
- Who do you want to do it for?
  - *Private Sector, Public Sector, Academia?*
- What are your next 3 jobs?
  - *Technical roles or not?*

Steps to jump start your Security career

- Read Wikipedia articles, tech sites, security blogs
- Find out more about different careers and what security professionals do
- Decide if you're still interested
- Talk to security professionals you know, and ask more questions
- Join a local Meetup group focused on security and ask questions

Steps to jump start your Security career

- Join a professional organisation like ISACA
  - Events are great places to volunteer, network, learn, and get involved
- Consider finding a mentor
- Identify the required education, experience, skills, certifications
- Consider taking free online courses and learn the jargon

Steps to jump start your Security career

- Take advantage of free materials
- Experiment at home
- Research and read a variety of material
- Consider taking paid courses online or in classroom
- Consider attending conferences
- Consider pursuing relevant certifications
- Consider ways to get work experience

Jump start your Security Career

Are you interested in a career as a security professional?

The world is more digital then ever before. A 2018 report from CIRA found that 54% of Canadians owned more digital devices. With all these connected devices, Canadian citizens and businesses face a greater c than ever before of having a data breach. As the risk posed by cyber criminals increases, as do the career opportunities in Information Security. Currently there is a forecasted global shortage of 3.5 million cyber professionals by 2021 and in Canada alone we are estimated to require 8,000 by 2022.

A career in cybersecurity is not only an in demand job, it is also one that is rewarding and challenging. As cybersecurity professional you get the opportunity to work in a constantly evolving environment, dealing technologies and systems that go on to serve millions and millions of users. As a professional in this field be dealing with technologies that can span from robots, to cars, to websites, the variety is endless.

Due to the variety of work that security professionals do, their backgrounds are quite diverse. Not every requires significant technical knowledge. In Canada there is no 4 year cybersecurity degree, though ther diplomas and masters programs. Approximately half of security professionals will have a computer scien engineering degree. Others spent a lot of time on the help desk or other IT roles. Still others have little experience. Careers in security are often not suggested by academic advisors and counsellors because t no defined path to become a security professional.

On this page we outline some tips to help you educate yourself and take the next step towards a career a security professional.

BC Government values:

Teamwork

Curiosity

Passion

Courage

Accountability

Service

Soft Skills and Success Factors

- Empathy
- Humility
- Integrity
- Confidence
- Pragmatism
- Flexibility
- "Agile"

DON'T:

Righteousness
Arrogance
Hysteria
"Chicken Little" thinking

Deloitte.

TFSA | TORONTO FINANCIAL SERVICES ALLIANCE

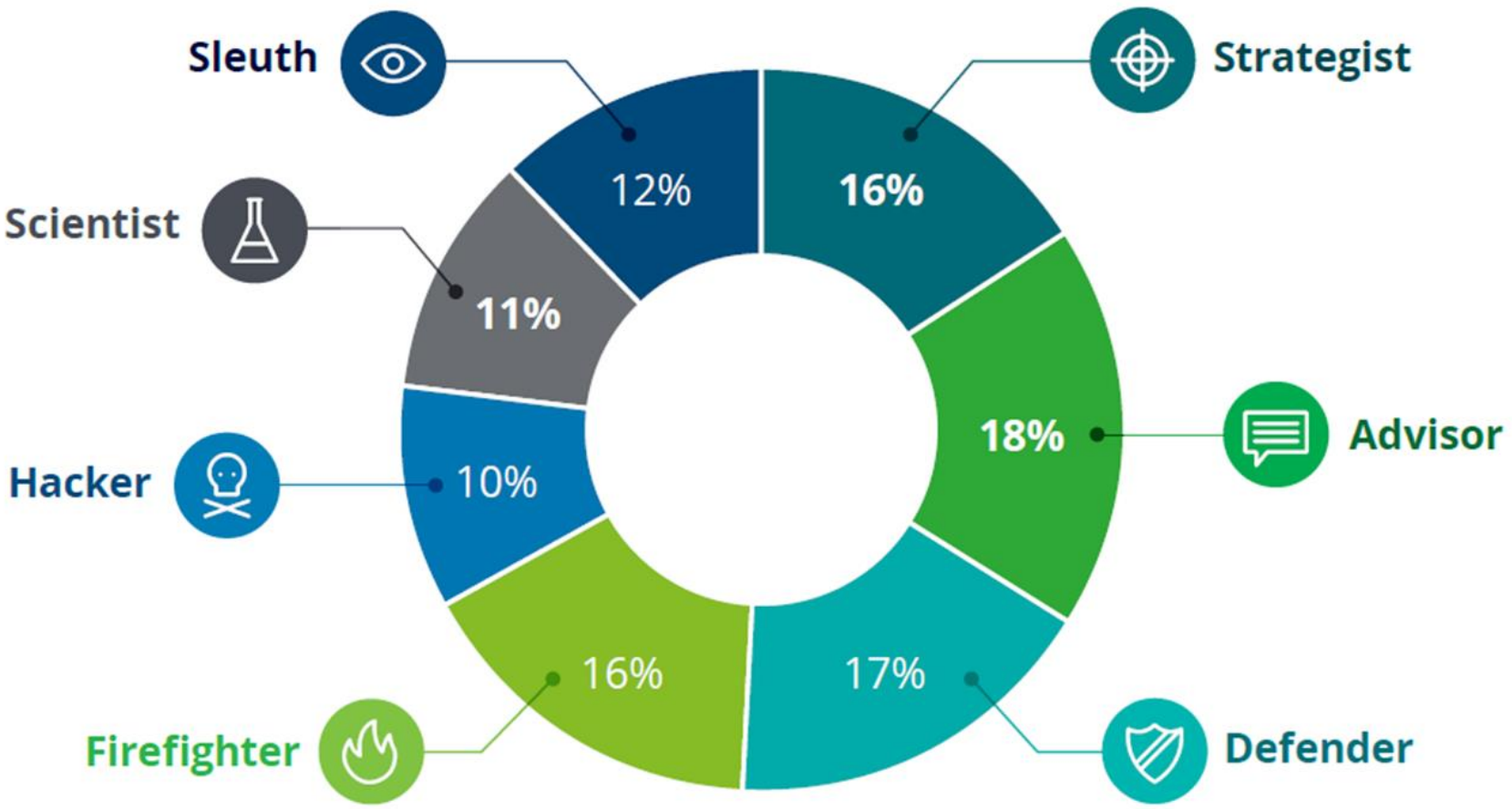
The changing faces of cybersecurity

Closing the cyber risk gap

Cyber Risk


Defender
Scientist
Sleuth
Hacker
Firefighter
Strategist
Advisor

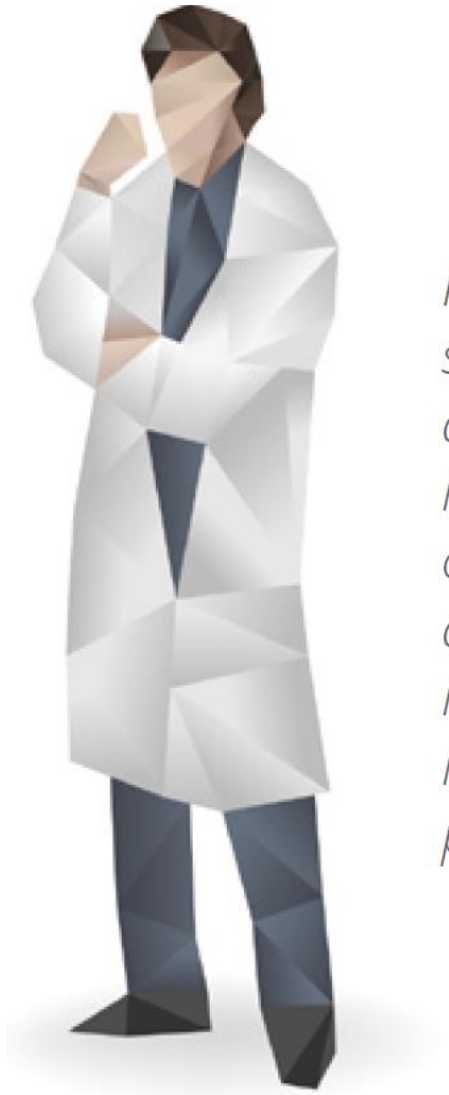
Figure 12: The composition of Canada's cyber workforce



Hardest to find today: Strategist, Scientist

Expected to grow the most in importance: Strategist, Scientist, Advisor

Scientist



Performs specialized analysis of threat intelligence, and cryptographic and security information to improve security posture

Capabilities

- Critical thinking
- Quantitative
- Threat mindset

Knowledge and skills

1. Intelligence analysis
2. Data science
3. Cryptography

Common roles

- Threat intelligence analyst
- Cyber analytics manager

Strategist

Capabilities

- Influence
- Communication
- Leadership
- Ethical impact

Knowledge and skills

1. Business acumen
2. Policy, legal, regulatory
3. Security architecture
4. Security risk management

Common roles

- Chief information security officer
- Cyber strategy analyst
- Cyber policy analyst
- Cyber communications analyst
- Cyber program/product manager

Provides cybersecurity management, direction, and advocacy

Advisor

Advises on the concept, design, and/or building of secure systems and networks

Capabilities

- Critical thinking
- Quantitative
- Communication
- Influence

Knowledge and skills

1. Security risk management
2. Security architecture
3. Policy, legal, regulatory
4. Business acumen

Common roles

- Security architect
- Security risk analyst
- Application security analyst

Defender

Capabilities

- Judgment
- Collaboration
- Threat mindset

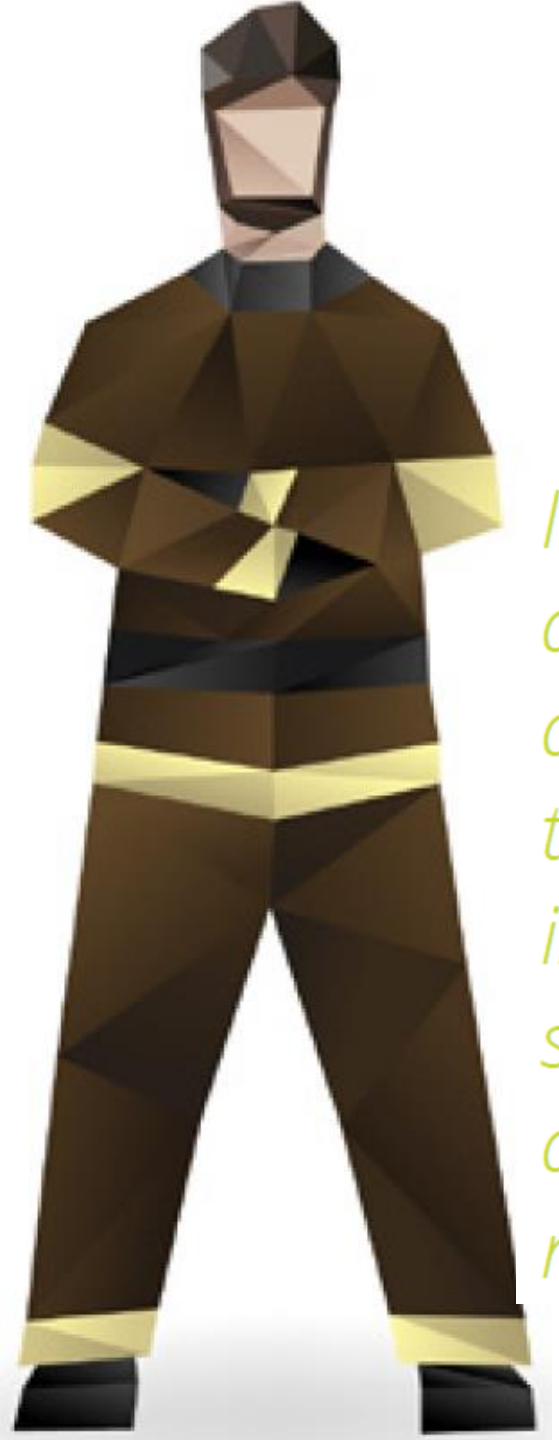
Knowledge and skills

1. Infrastructure security
2. Security tools administration
3. Security risk management
4. Security architecture

Common roles

- Systems security analyst
- Security administrator

Supports, administers, and maintains the security of systems, data, and networks



Firefighter

Identifies, analyzes, and mitigates threats to internal systems, data, and networks

Capabilities

- Agility
- Judgment
- Critical thinking
- Threat mindset

Knowledge and skills

1. Security incident management
2. Security tools administration
3. Infrastructure security
4. IT administration

Common roles

- Cyber analyst
- Security engineer
- Cyber incident responder
- Vulnerability analyst
- Security operations centre manager

Hacker

Conducts specialized threat detection and deception activities to identify and mitigate cybersecurity risks

Capabilities

- Threat mindset
- Critical thinking
- Creativity
- Ethical impact

Knowledge and skills

1. Penetration testing
2. Computer forensics
3. Infrastructure security
4. Threat modelling

Common roles

- Cyber operator
- Threat hunter

Sleuth

Investigates cybersecurity events or crimes related to systems, networks, and digital evidence

Capabilities

- Threat mindset
- Critical thinking
- Social awareness
- Ethical impact

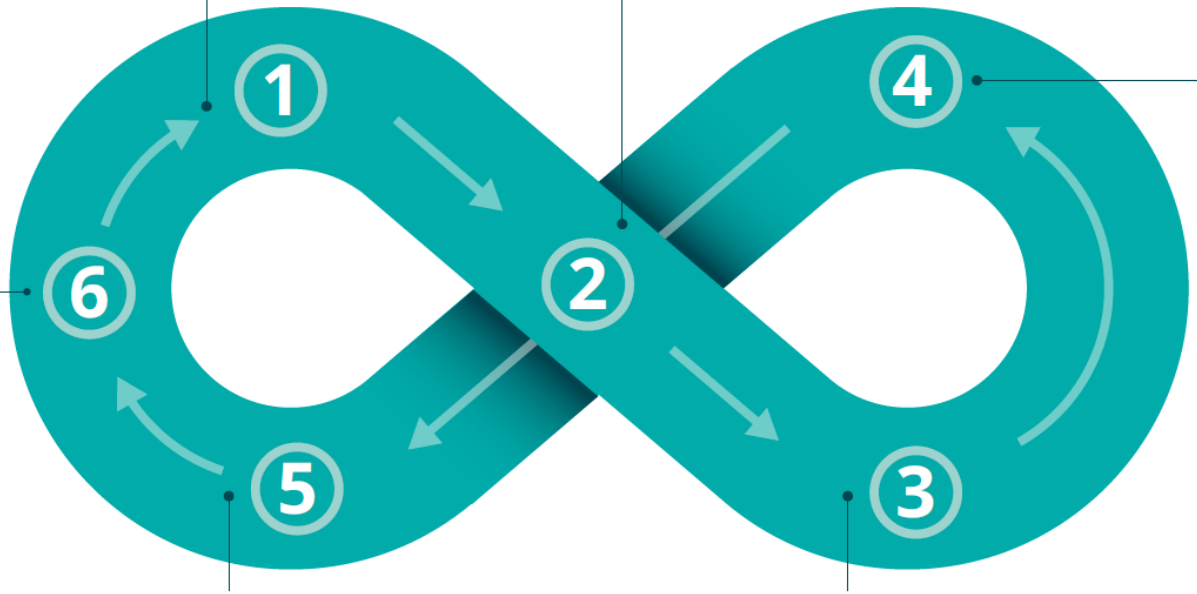
Knowledge and skills

1. Computer forensics
2. Security incident management

Common roles

- Cyber forensics analyst

Figure 13: The talent life cycle model



Grow

- Find innovative ways to expand the pool of cyber talent.

Recruit

- Raise your visibility in the cyber talent marketplace.
- Broaden the tent.
- Tap into non-traditional talent sources.
- Innovate.

Develop

- Promote continuous learning.
- Avoid plateaus and roadblocks.
- Make cybersecurity training a priority for the entire enterprise.

Offboard

- Don't burn bridges.

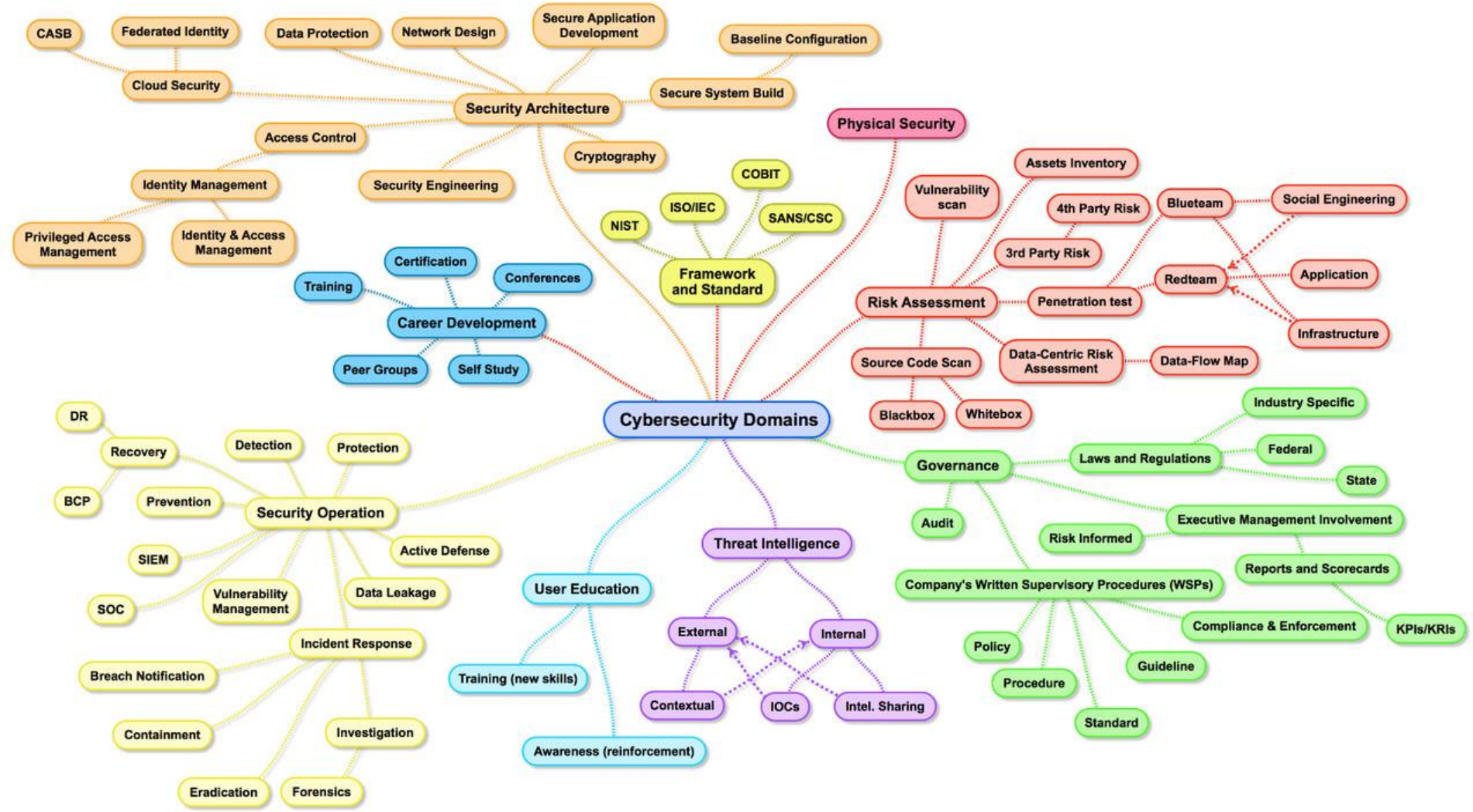
Retain

- Make retention a priority. But prioritize the priorities.
- Focus on millennials.
- Pay to play.

Onboard

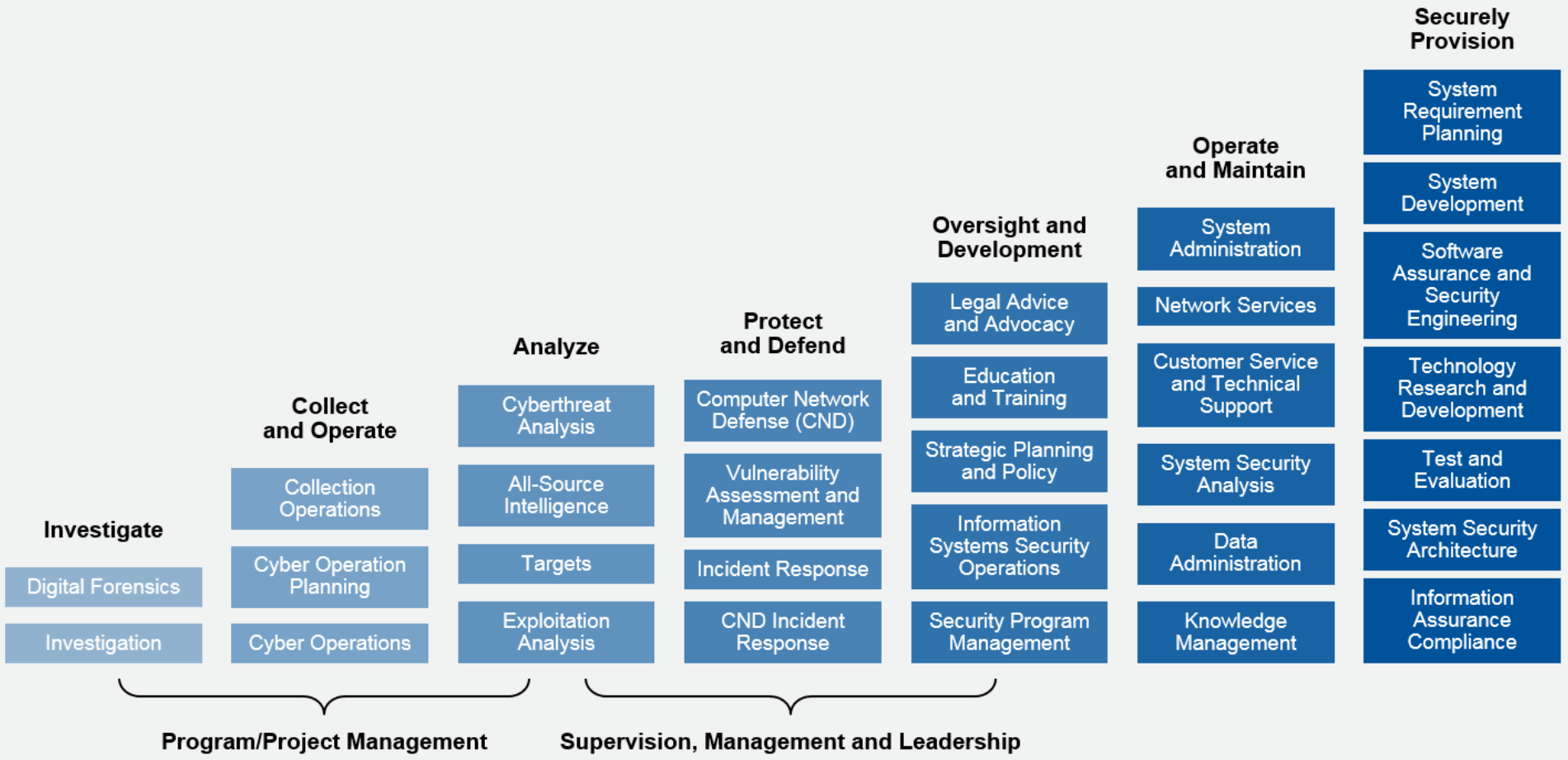
- Jumpstart the process of becoming part of the organization.
- Emphasize development from day one.
- Capitalize on fresh perspectives and insights.

BRITISH COLUMBIA | Ministry of Citizens' Services



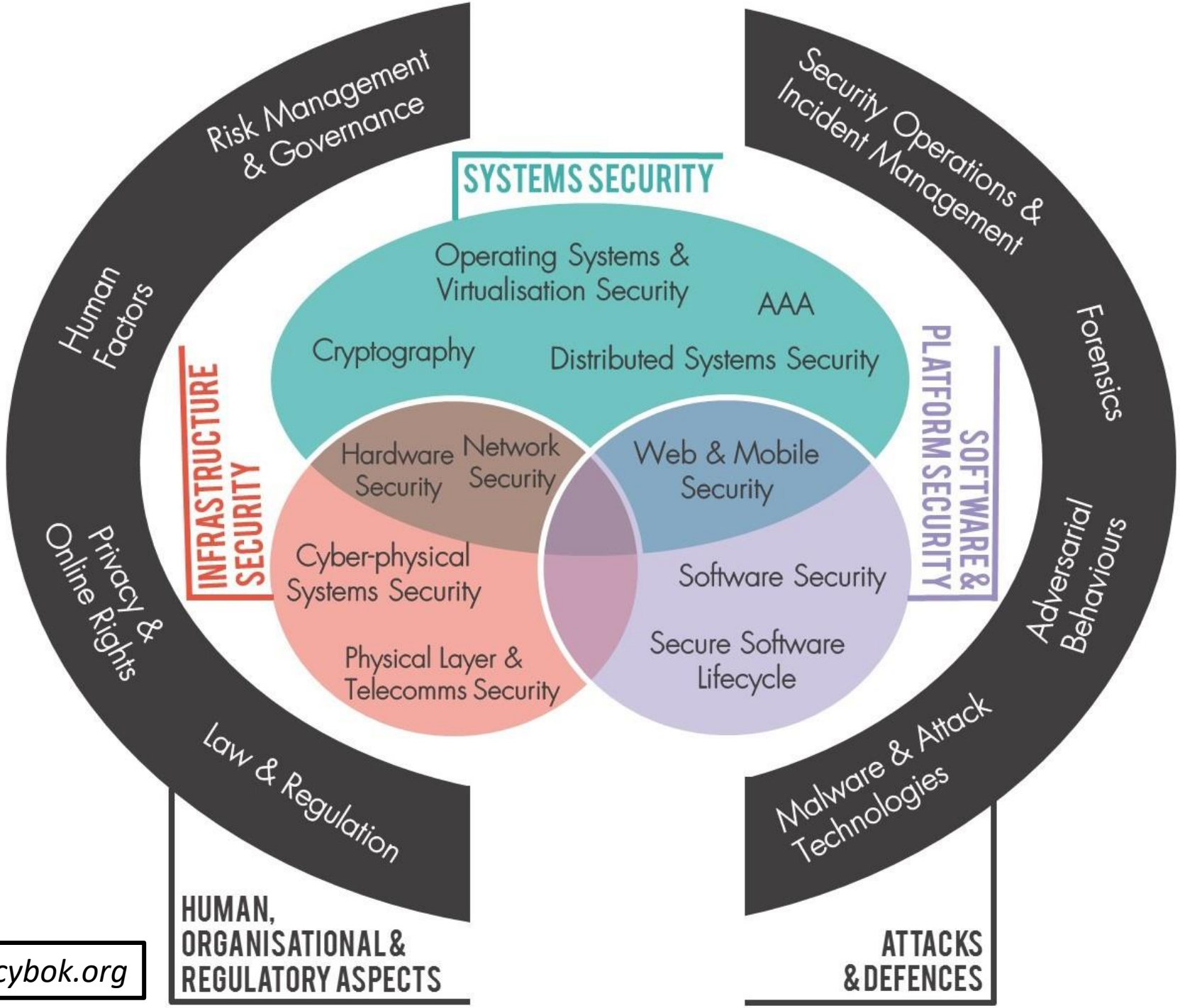
BRITISH COLUMBIA | Ministry of Citizens' Services

Cybersecurity Roles Spectrum



ID: 345806

Source: Gartner (February 2018)



www.cybok.org

- Are there work streams that might be better handled through alternative sourcing or managed services?
- Can cognitive technologies and automation (e.g., automated detection of threats) be used to reduce human involvement?
- Can skills be combined in new ways to solve difficult problems and drive innovation?

MISO Responsibilities

MISO Responsibilities

Knowing the information security policy and standard requirements and communicating them within their ministries

MISO Responsibilities

Assisting business areas to understand and comply with information security policies and standards

MISO Responsibilities

Ensuring that procedures to support day-to-day security activities are per the Information Security Standard

MISO Responsibilities

Co-ordinating information security awareness and education activities and resources for their ministry

MISO Responsibilities

Providing up-to-date information on issues related to information security

MISO Responsibilities

Facilitating business areas with conducting Security Threat and Risk Assessments

MISO Responsibilities

Providing advice on security requirements for information systems development and enhancements

MISO Responsibilities

Co-ordinating ministry information security initiatives with cross-government information security initiatives

MISO Responsibilities

Providing advice on emerging information security standards relating to ministry specific lines of business

MISO Responsibilities

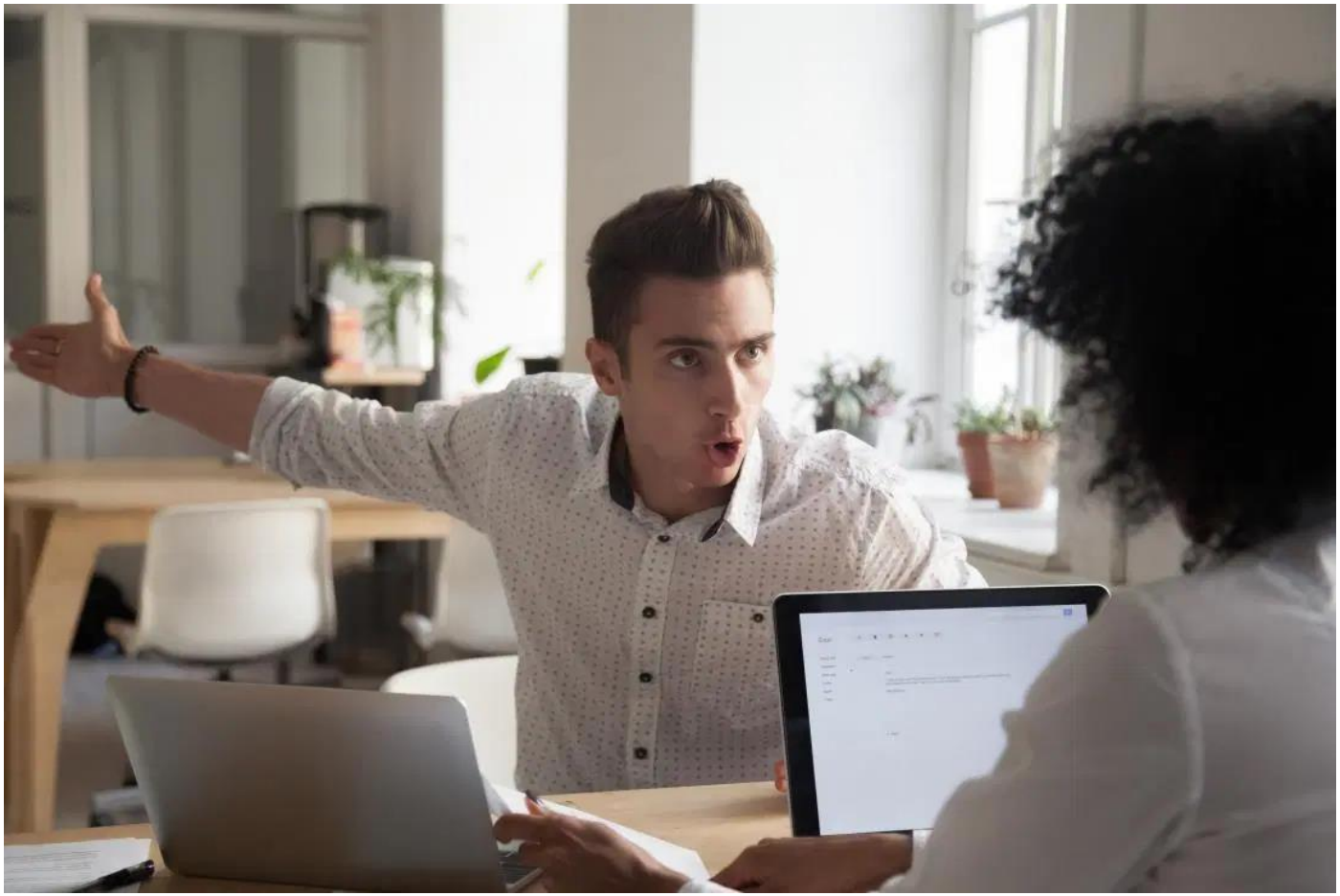
Raising ministry security issues to the cross-government information security forums

MISO Responsibilities

Investigate reported information security events to determine if further investigation is warranted

MISO Responsibilities

Address IT Security related audits



MISO Responsibilities

Assessing and Addressing Information Security Vulnerabilities

MISO Responsibilities

Perform Ministry Security Assessments Using Defensible Security Framework

@HOME

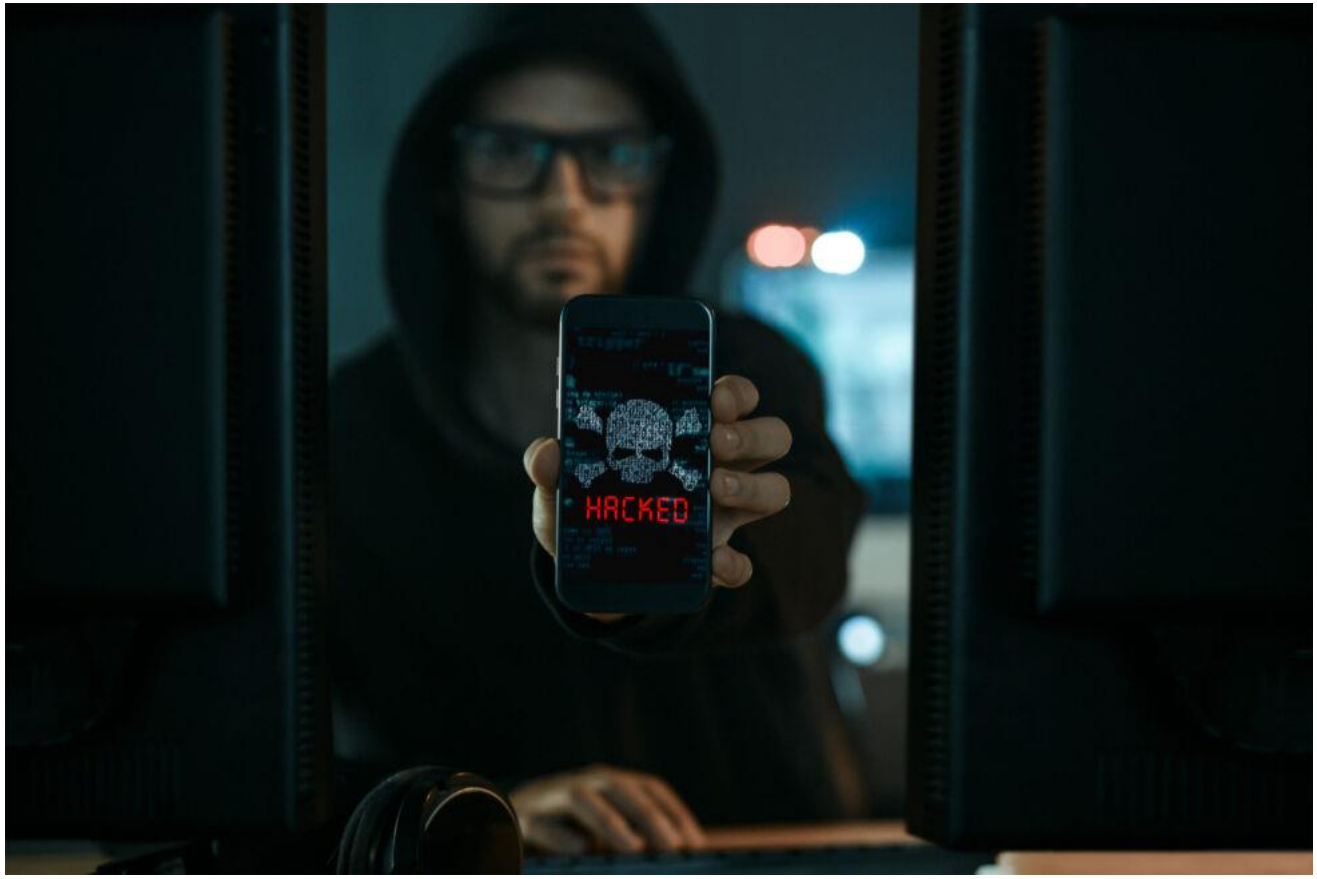
Secure your "smart" devices

Check for software updates

Scammers Are Using Fake Job Ads to Steal People's Identities

https://www.nextgov.com/cybersecurity/2021/10/scammers-are-using-fake-job-ads-steal-peoples-identities/186381/

Please have a password



BRITISH COLUMBIA | Ministry of Citizens' Services

8 Social Media Safety Tips

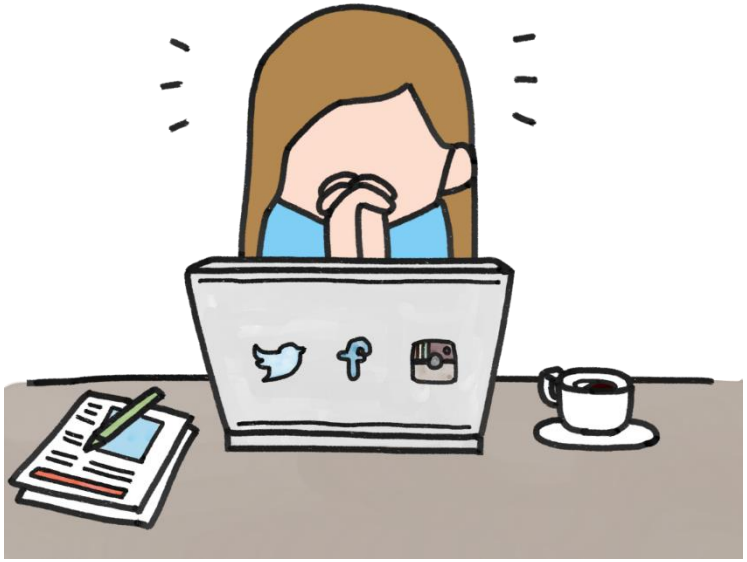
Defensible Security: @ Work, @ Home and @ Play

November 3, 2021

ADJUST YOUR PRIVACY SETTINGS

- Almost all social networking sites have pre-set or default privacy settings.
- Adjusting your privacy settings manually.

CONSIDER WHAT TO POST BEFORE YOU POST

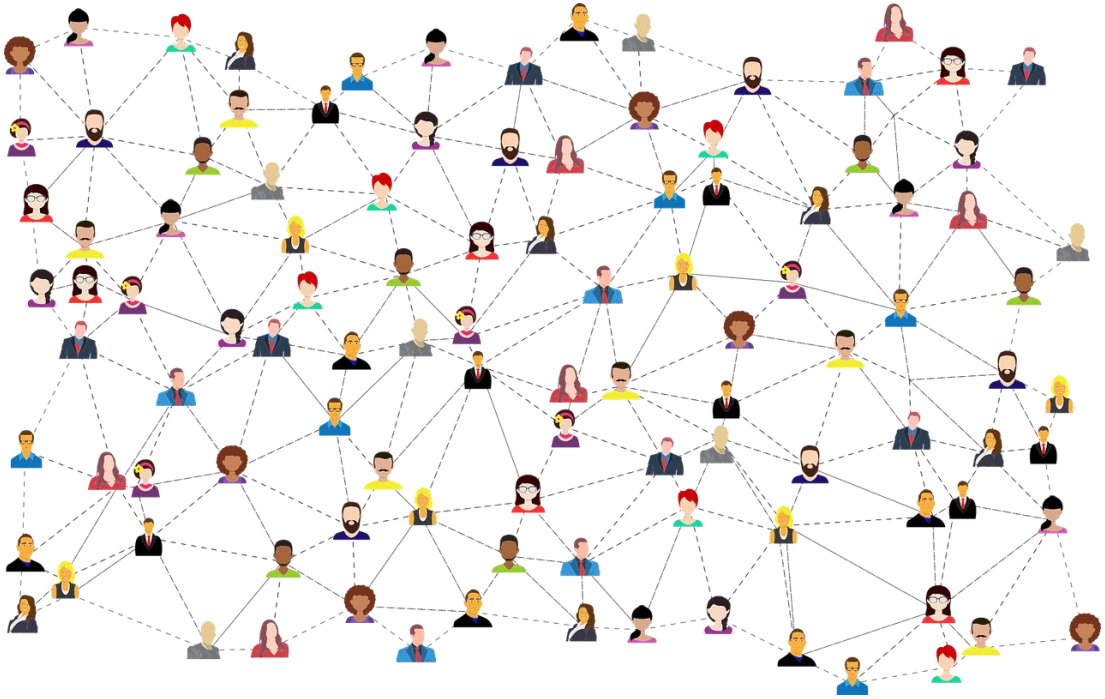


- Posting is permanent

TURN OFF GEOTAGGING

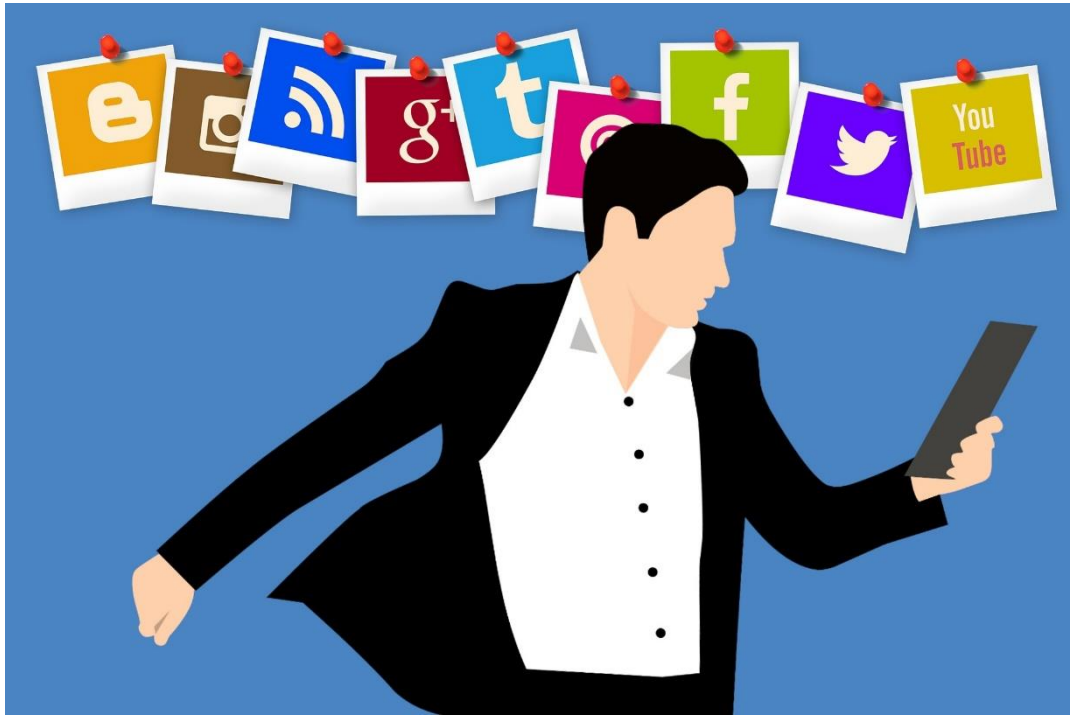
- Do not post your location – locally or away from home.

THINK BEFORE CONNECTING



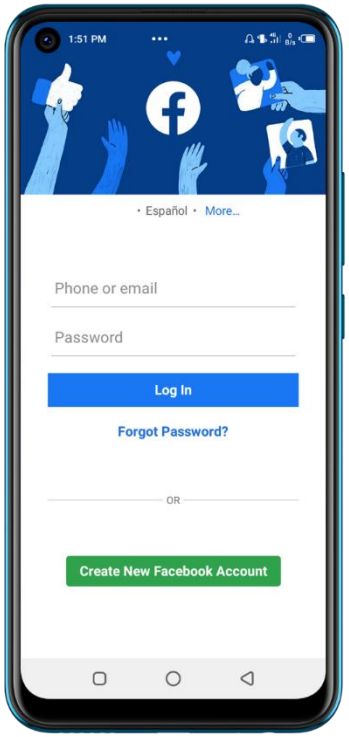
- Only connect online with people you know in real life.

RESTRICT WHAT YOU SHARE



- Decrease your security and privacy risks by not sharing too much information, like your birthday and vacation details.

LOG OFF AFTER YOU ARE FINISHED



- Mitigate security and privacy risks by logging off once you're finished.

CHECK AND ADJUST ACCOUNT SETTINGS REGULARLY

- Check your social media account settings every few months as social media platform updates cause account settings to go back to default.

DON'T SHARE PERSONAL DETAILS

- Don't publish details that offer personal information, like your birthday, or where you will be at a certain time.

THANK YOU!