SENG 460 / ECE 574
Practice of Information Security and Privacy

Introduction to the Course

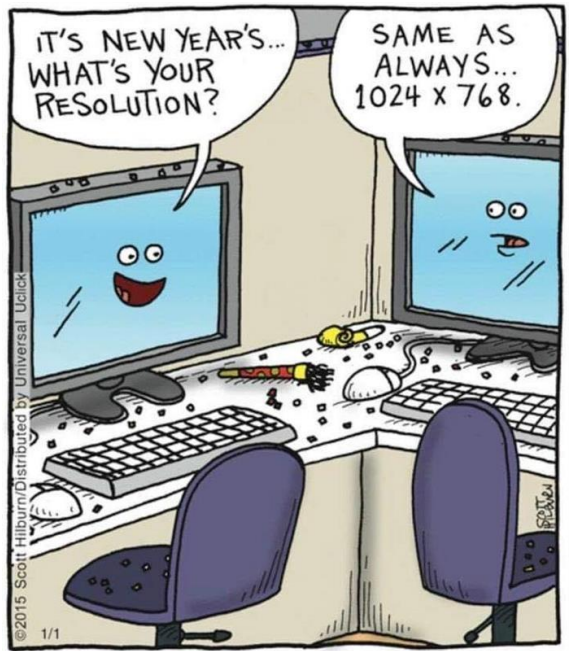
How to Get into a Career in Security

Cybersecurity Threat Landscape

Gary Perkins, MBA, CISSP

garyperkins@uvic.ca

University of Victoria



Introduction

- 20+ years' experience in IT operations, risk management, and security

- Chief Information Security Officer (CISO) for Province of British Columbia since Nov 2013

- prior to that worked at TELUS for ~18 years in Security Operations, Design/Build, Architecture, Incident Response

Why am I here

- two fastest ways to get my attention:
  1) threats to critical infrastructure
  2) developing the next generation of cybersecurity talent

University of Victoria

About the Course

- Class: SENG 460 – ECE 574
  - location: ELL 168 day/time: Friday 15:30 – 18:20
- Office hours:
  - location: ELL 168 day/time: on request
- TAs:
  - Mehrab Najafian
  - Araya Chaowalit
  - Sathvik Divilli
- Instructor:
  - Gary Perkins
    garyperkins@uvic.ca
- Discord:
  - Invite on BrightSpace

University of Victoria

About the Course

- Students will learn the common knowledge of the information security domains classified by major information security associations
- Students will understand information security requirements and practice in corporate environment
- Students will be able to apply information security theories, models and techniques in solving practical information security problems

University of Victoria

Topics (subject to change)

- Week 1 (Jan 13):
  - Introduction to Course, Careers in Cybersecurity, Cybersecurity Threat Landscape
  - Assignments: Lab 1, Read Chapters 1-6, 13-14

- Week 2 (Jan 20):
  - Attacks, Breaches, Best Practices, Prevention
  - Assignments: Lab 2, Read Chapters 34-39

- Week 3 (Jan 27):
  - Incident Handling/Incident Response, **Quiz**
  - Assignments: Lab 3, Read Chapters 7-12, 29, 30, 40, 41

- Week 4 (Feb 03):
  - Risk Management, Risk Assessment, Asset Security
  - Assignments: Lab 4, Read Chapters 15,19-23, 42-46

- Week 5 (Feb 10):
  - Midterm, Privacy, Security Awareness **Midterm**
  - Assignments: Lab 5, Read Chapters 24, 27, 28, 31, 33, Threats to the Democratic Process

University of Victoria

Topics (subject to change)

- Reading Break (Feb 17):

- Week 6 (Feb 24):
  - Investigations & Evidence, Open Source Intelligence, Threats to the Democratic Process
  - Assignments: Lab 6, Reading: Chapters 25, 26, 32

- Week 7 (Mar 3):
  - Security Architecture & Engineering, Security Operations, Network & Communications Security incl. IoT, Mobile Security
  - Assignments: Lab 7 (optional), Reading: Chapters 16-18

- Week 8 (Mar 10):
  - Identity & Access Management , Policies & Standards, Audits & Compliance, **Quiz**
  - Assignments: Lab 8 (optional), Reading: Chapters 15-19

- Week 9 (Mar 17):
  - Systems & Application Security, Software Development Security, Security Assessment & Testing
  - Assignments: Lab 9 (optional)

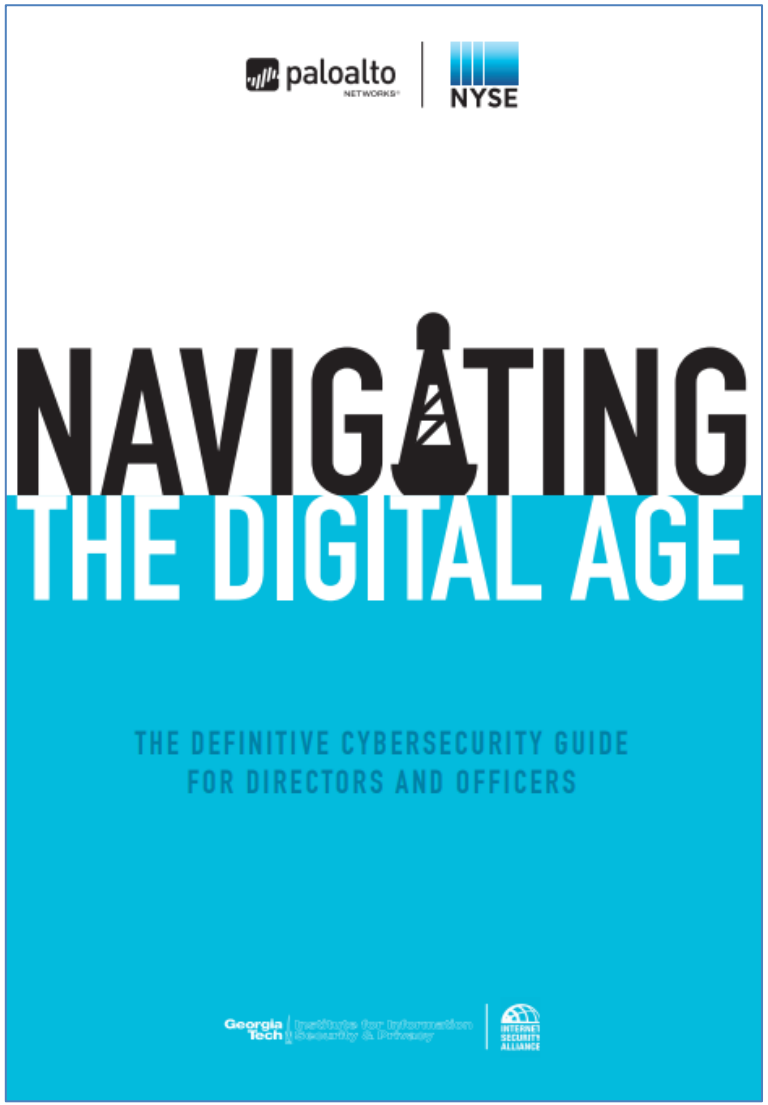
University of Victoria

Topics (subject to change)

- Week 10 (Mar 24):
  - Cryptography, Business Continuity Plans, Disaster Recovery Plans, Physical Security
  - Assignments: Lab 10 (optional) **ECE 574 Project DUE**
- Week 11 (Mar 31):
  - How to Build Security into the Organizations (Review), **Quiz**
  - Assignments: Lab 12 (optional)
- Final Exam (date TBD)

Textbook

- Navigating the Digital Age
- Posted on BrightSpace
- Links
  - https://www.securityroundtable.org/navigating-digital-age-second-edition/
  - https://www.securityroundtable.org/wp-content/uploads/2015/09/Cybersecurity-9780996498203-no_marks.pdf



University of Victoria

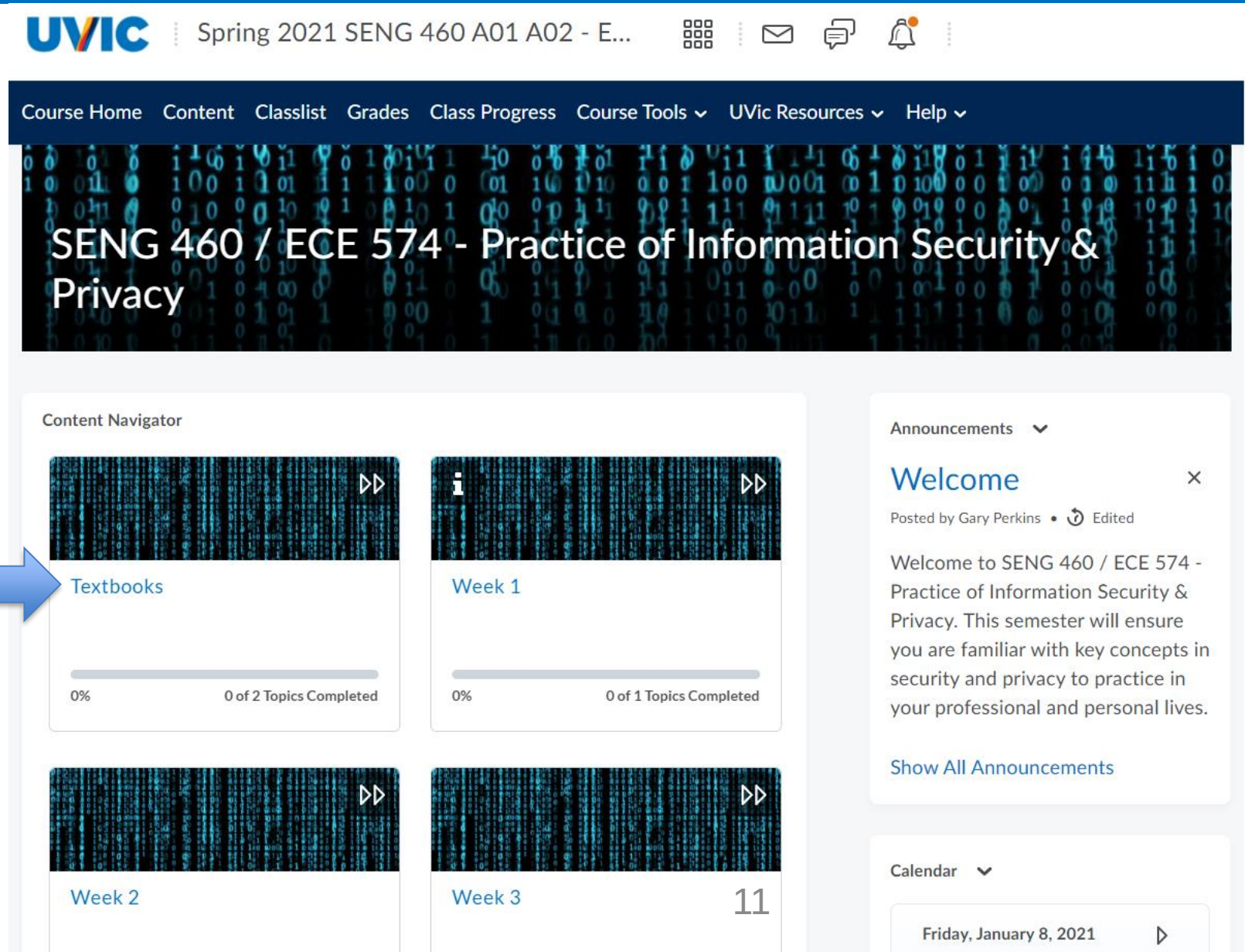
Textbook

- Cyber Threats to Canada's Democratic Process
- Posted on BrightSpace
- Link
  - https://cyber.gc.ca/sites/default/files/publications/cse-cyber-threat-assessment-e.pdf

University of Victoria

Website (on BrightSpace)

- course website is on BrightSpace



University of Victoria

Grading

- SENG 460
  - Quizzes 20% Jan 27, Mar 10, Mar 31
  - Midterm 40% Feb 10
  - Final 40% TBD

- ECE 574
  - Quizzes 20% Jan 27, Mar 10, Mar 31
  - Midterm 20% Feb 10
  - Project 20% Mar 24
  - Final 40% TBD

University of Victoria

Lab Assignment

- weekly self-guided labs are posted; many are quite short, a few are longer
- all are aimed at providing hands-on exposure to tools
- access https://labs.engr.uvic.ca, use SSH, or use your home linux instance
- labs are optional

ECE 574 Project Information

- ECE 574 students are also required to complete a project
- plan to benefit the industry by contributing to an online repository by producing a video to educate others on a security topic of your choice
- work either individually or in teams of two or three
- 4-5 minutes of content per student
- more details and examples available on the website

University of Victoria

ECE 574 Project Information

- it is challenging to get people to understand the importance of security and take the necessary steps to remain safe
- your video should provide practical advice
- submit the link to the project on BrightSpace and identify the topic(s), the intended audience, and group members
- video can be filmed using a smartphone or video camera

ECE 574 Project Information

- you can be in the video or not
  - video could be real life, acted out, story, presentation, interview, game show, how to, puppets, cartoons, animation, Claymation, or…?
  - use your imagination – could be the next Blair Witch Project
- you may use your voice(s) or not
  - there are many text to speech sites on the internet
- the video may have title screen, transitions, or credits but they do not count toward the 4-5 minutes of content

Public Service Announcement

- please don’t get scammed this semester (or ever)
- last time, students started coming forward…
- some had been scammed, some were being scammed
  - some knew it, some did not know it
- beware calls saying they are law enforcement or CRA
  - if anyone tells you to buy iTunes or Google Play cards….
- don’t click on suspicious links or attachments

University of Victoria

What is information security?

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

University of Victoria

Definitions

- **Information Security** – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
- **IT security** - "safeguards" to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information
- **Cybersecurity** – The ability to protect or defend the use of cyberspace from cyber attacks.
- **Cyber Attack** – An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
- **Cyberspace** – A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

University of Victoria

Sources: NIST and Government of Canada Policy

Security Domains

- often described as “a mile wide and inch deep”
- impossible to be an expert in all facets
- previous course content as CISSP prep course

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

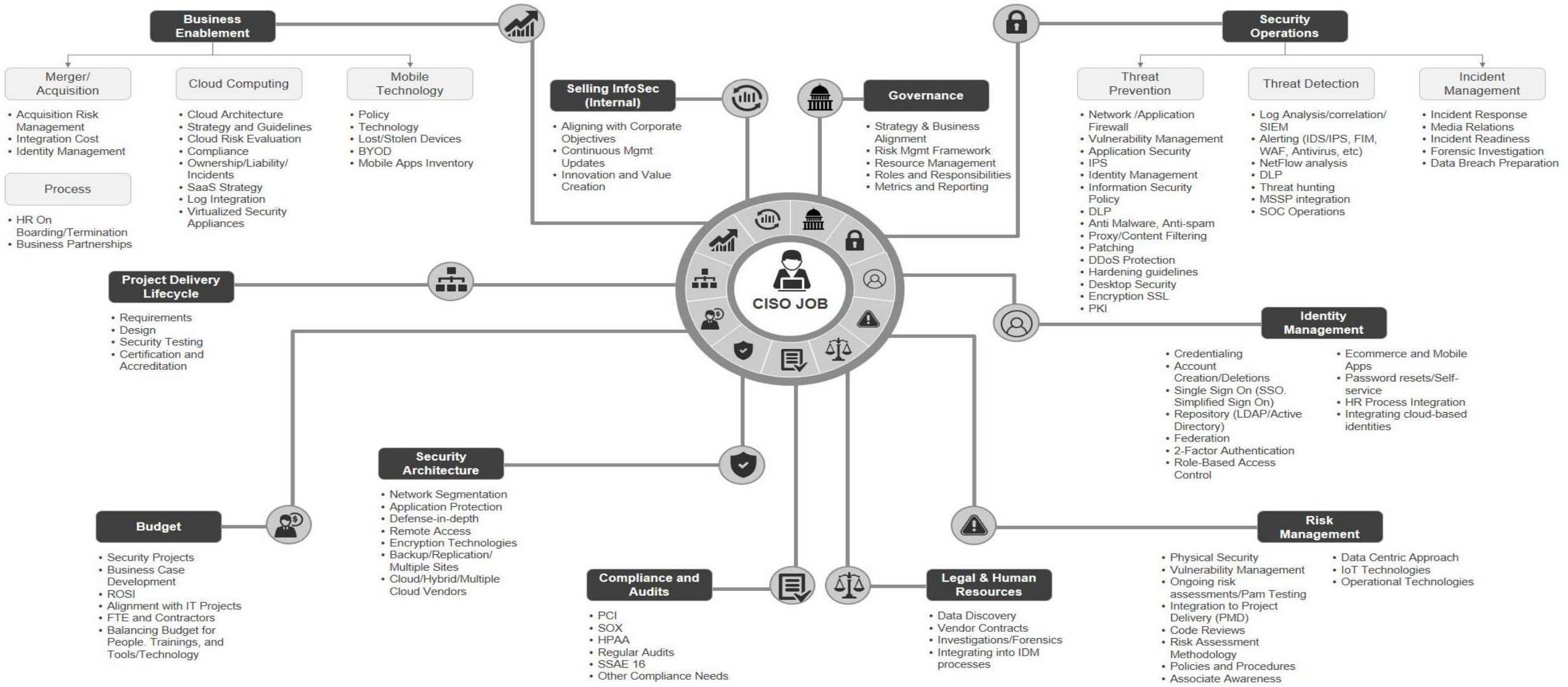
10 CISSP Domains (previous)
•Info. Security Governance and Risk Mgmt
•Access Control
•Cryptography
•Security Architecture and Design
•Telecommunications and Network Security
•Software Development Security
•Business Continuity and Disaster Recovery
•Legal, Regulations, Investigations, and Compliance
•Physical Security
•Operations Security

10 CISSP Domains (previous)
•Telecom. and network security
•Security management practices
•Applications and systems development
•Cryptography
•Security architecture and models
•Operations security
•Business continuity planning and disaster recovery planning
•Law, investigations and ethics
•Physical security

ISO 27002 Code of Practice
•security policy
•organization of information security
•asset management
•human resources security
•physical and environmental security
•communications and operations management
•access control
•information systems acquisition, dev and maintenance
•information security incident management
•business continuity management; and
•regulatory compliance

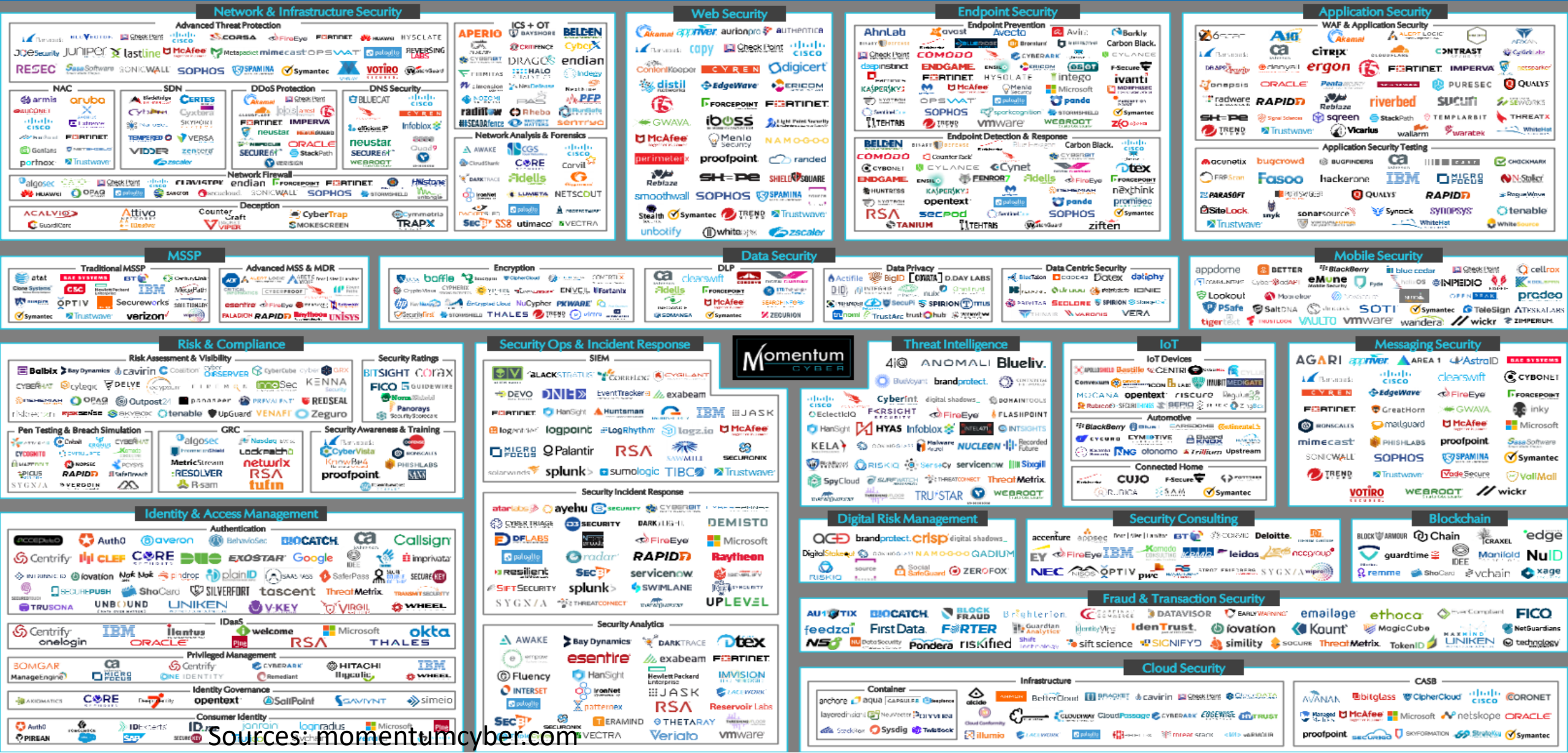
University of Victoria

CISO Mind Map: Overview of Responsibilities and ever-expanding role



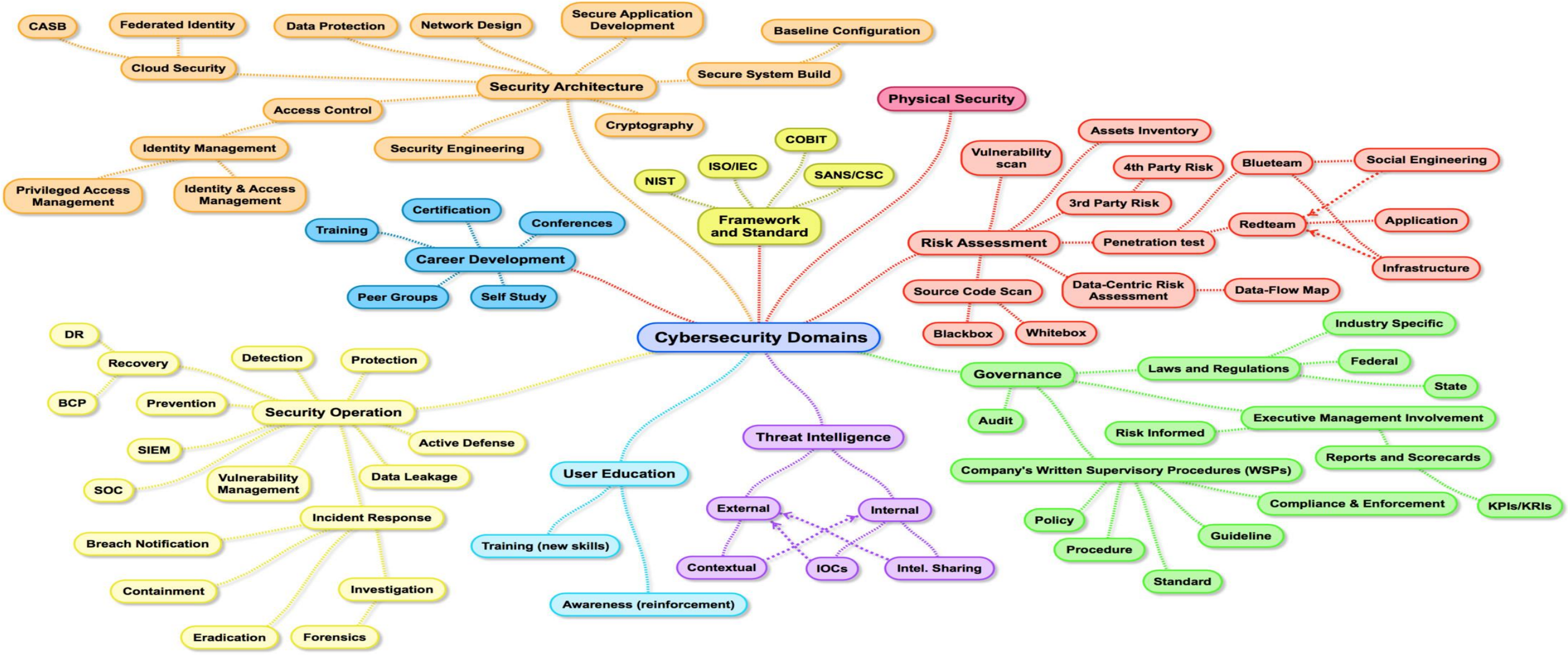
Source: http://rafeeqrehman.com/2015/05/17/the-latest-2015-ciso-mindmap-is-here/

Security Ecosystem



Sources: momentumcyber.com

Map of Cybersecurity Domains



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

SENG 460 / ECE 574
Practice of Information Security and Privacy

Introduction to the Course

How to Get into a Career in Security

Cybersecurity Threat Landscape

University of Victoria

0%**

cybersecurity

unemployment in BC

2016 Cybersecurity Skills Gap

Too Many Threats

$1 BILLION: PERSONALLY IDENTIFIABLE INFORMATION (PII) **RECORDS STOLEN IN 2014**[1]

97% BELIEVE APTs REPRESENT CREDIBLE THREAT TO **NATIONAL SECURITY AND ECONOMIC STABILITY**[2]

MORE THAN 1 IN 4 ORGANIZATIONS HAVE **EXPERIENCED AN APT ATTACK**[3]

$150 MILLION: AVERAGE COST OF A **DATA BREACH BY 2020**[4]

1 IN 2 BELIEVE THE IT DEPARTMENT IS UNAWARE OF ALL OF ORGANIZATION'S **INTERNET OF THINGS (IOT) DEVICES**[5]

74% BELIEVE LIKELIHOOD OF ORGANIZATION BEING **HACKED THROUGH IOT DEVICES IS HIGH OR MEDIUM**[6]

Too Few Professionals

2 MILLION: GLOBAL SHORTAGE OF CYBERSECURITY **PROFESSIONALS BY 2019**[7]

3X **RATE OF CYBERSECURITY JOB GROWTH** VS. IT JOBS OVERALL, 2010-14[8]

84% ORGANIZATIONS BELIEVE HALF OR FEWER OF APPLICANTS FOR **OPEN SECURITY JOBS ARE QUALIFIED**[9]

53% OF ORGANIZATIONS EXPERIENCE DELAYS AS LONG AS **6 MONTHS TO FIND QUALIFIED SECURITY CANDIDATES**[10]

77% **OF WOMEN** SAID THAT NO HIGH SCHOOL TEACHER OR GUIDANCE COUNSELOR MENTIONED CYBERSECURITY AS CAREER. **FOR MEN, IT IS 67%.**[11]

89% **OF U.S.** CONSUMERS BELIEVE IT IS IMPORTANT FOR ORGANIZATIONS TO **HAVE CYBERSECURITY-CERTIFIED EMPLOYEES.**[12**]

Cyberattacks are growing, but the talent pool of defenders is not keeping pace.

Although attacks are growing in frequency and sophistication, the availability of sufficiently skilled cybersecurity professionals is falling behind. Cybersecurity Nexus (CSX) is addressing this gap by creating a skilled global cybersecurity workforce. From the Cybersecurity Fundamentals Certificate for university students to CSXP, the first vendor-neutral, performance-based cybersecurity certification, CSX is attracting and enabling cybersecurity professionals at every stage of their careers.

SOURCES: 1. *2015 Cost of Data Breach Study: Global Analysis, IBM and Ponemon Institute, May 2015.* **2.** *ISACA 2015 APT Study, October 2015.* **3.** *ISACA 2015 APT Study.* **4.** *The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation, Juniper Research, May 2015.* **5.** *SACA 2015 IT Risk/Reward Barometer-Member Study, September 2015.* **6.** *ISACA 2015 IT Risk/Reward Barometer-Member Study.* **7.** *UK House of Lords Digital Skills Committee.* **8.** *Burning Glass Job Market Intelligence: Cybersecurity Jobs, 2015.* **9.** *State of Cybersecurity: Implications for 2015, ISACA and RSA Conference, April 2015.* **10.** *State of Cybersecurity: Implications for 2015.* **11.** *Securing Our Future: Closing the Cyber Talent Gap, Raytheon and NCSA, October 2015.* **12.** *2015 ISACA Risk/Reward Barometer-Consumer Study, September 2015.*

** "Employees" refers to data security professionals at organizations that potentially have access to survey respondent's personal information.

CSX CYBERSECURITY NEXUS

ISACA® Trust in, and value from, information systems

https://cybersecurity.isaca.org January 2016

NATIONAL SECURITY OCTOBER 7, 2016 6:05 PM

Want a sure-fire well-paid job? Train to fight computer hackers

BY TIM JOHNSON
tjohnson@mcclatchydc.com

WASHINGTON — Want a career with zero chances of going jobless?

Try the booming field of cybersecurity. Companies can't hire fast enough. In the United States, companies report 209,000 cybersecurity jobs that are in need of filling.

It'll only get worse. By 2019, according to the Cybersecurity Jobs Report, the workforce shortfall may reach 1.5 million. Globally, the shortage could hit 6 million, it added.

"The internet is growing faster than the growth of people to protect it," said Michael Kaiser, chief executive of the National Cyber Security Alliance.

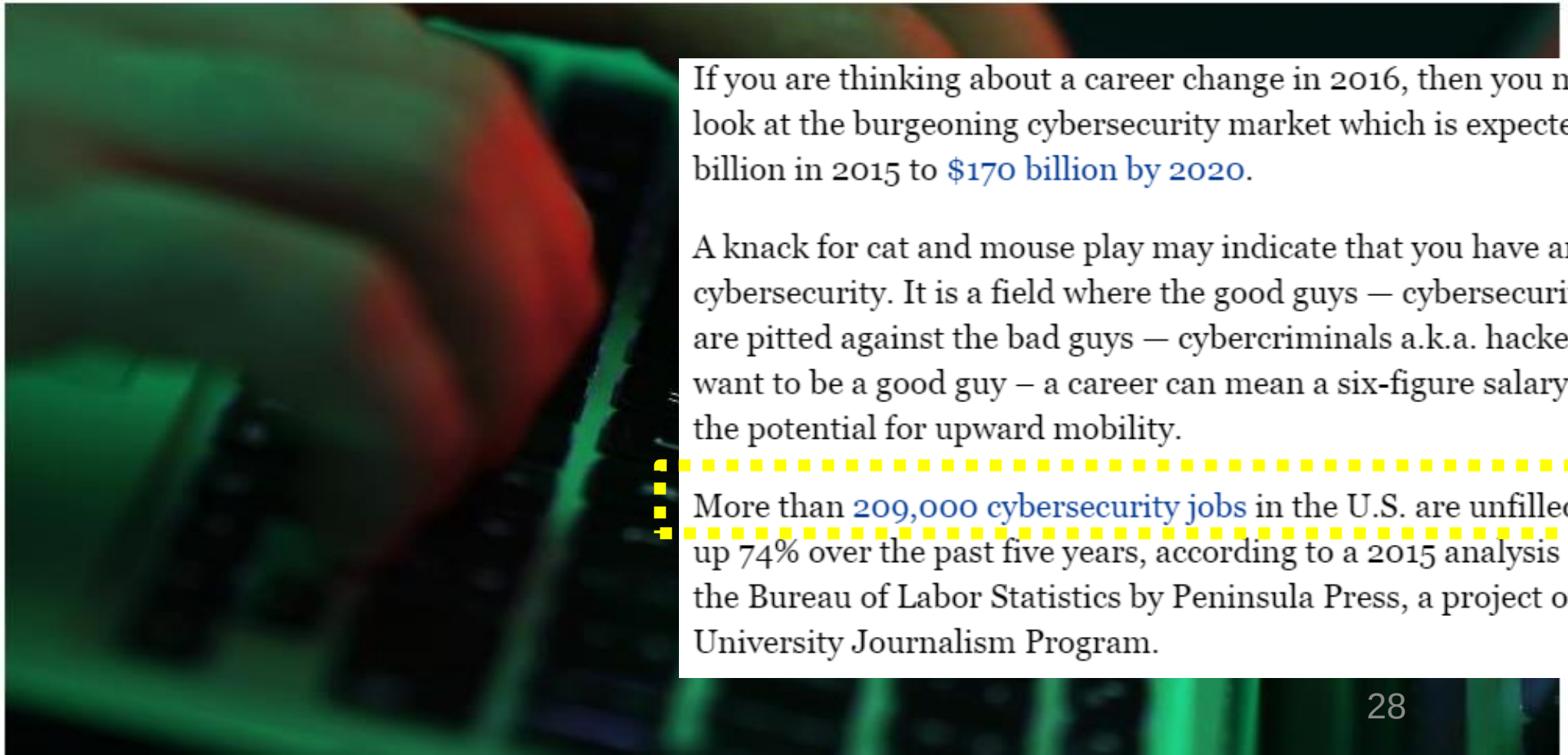
It is a problem with the full attention of the White House, which in July called for "immediate and broad-sweeping actions to address the growing workforce shortage and establish a pipeline of well-qualified cybersecurity talent."

One Million Cybersecurity Job Openings In 2016

Steve Morgan, CONTRIBUTOR

I write about the business of cybersecurity. **FULL BIO**

Opinions expressed by Forbes Contributors are their own.



If you are thinking about a career change in 2016, then you might want to have a look at the burgeoning cybersecurity market which is expected to grow from $75 billion in 2015 to $170 billion by 2020.

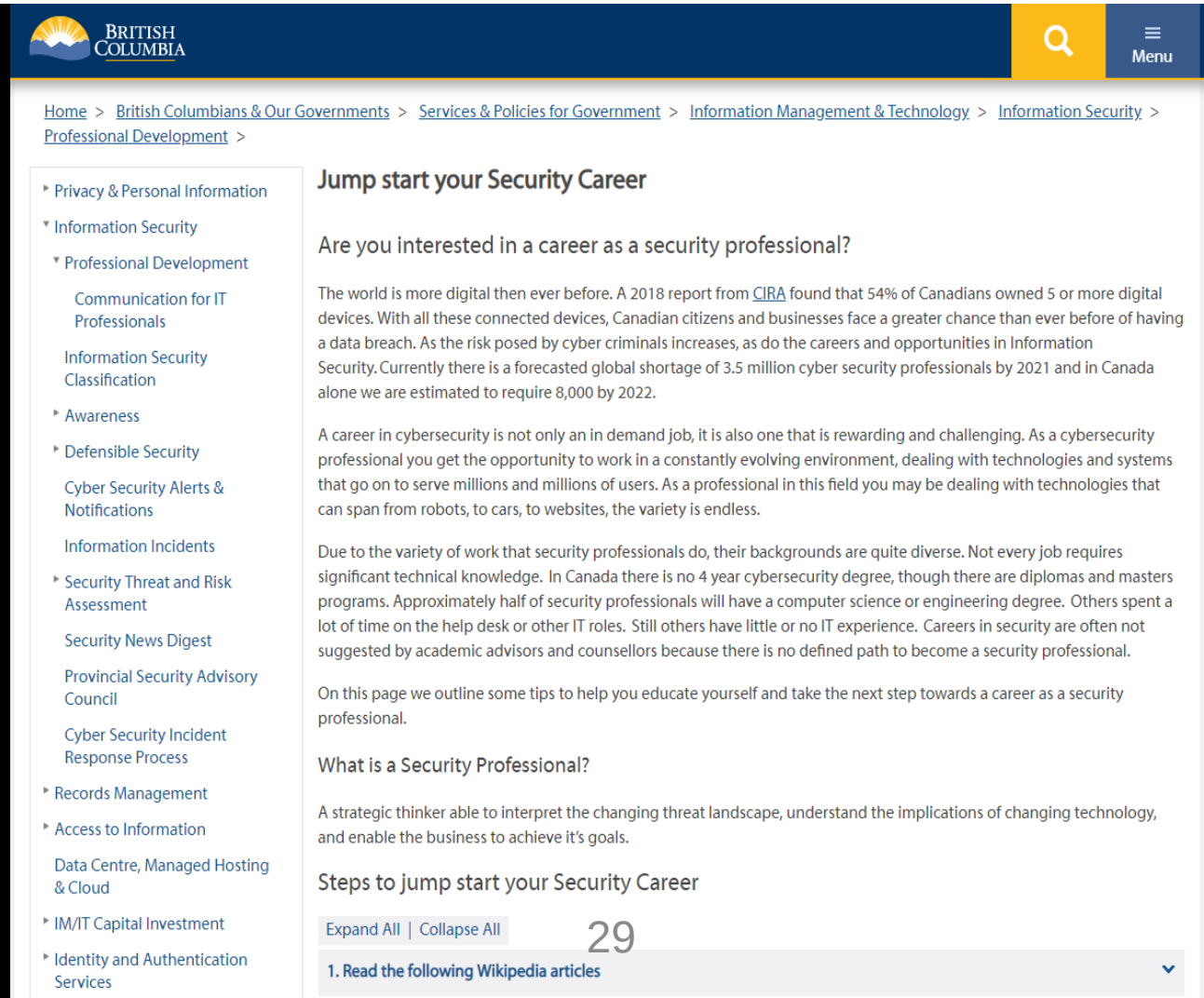
A knack for cat and mouse play may indicate that you have an aptitude for cybersecurity. It is a field where the good guys — cybersecurity professionals — are pitted against the bad guys — cybercriminals a.k.a. hackers. Assuming you'd want to be a good guy – a career can mean a six-figure salary, job security, and the potential for upward mobility.

More than 209,000 cybersecurity jobs in the U.S. are unfilled, and postings are up 74% over the past five years, according to a 2015 analysis of numbers from the Bureau of Labor Statistics by Peninsula Press, a project of the Stanford University Journalism Program.

How to get into security

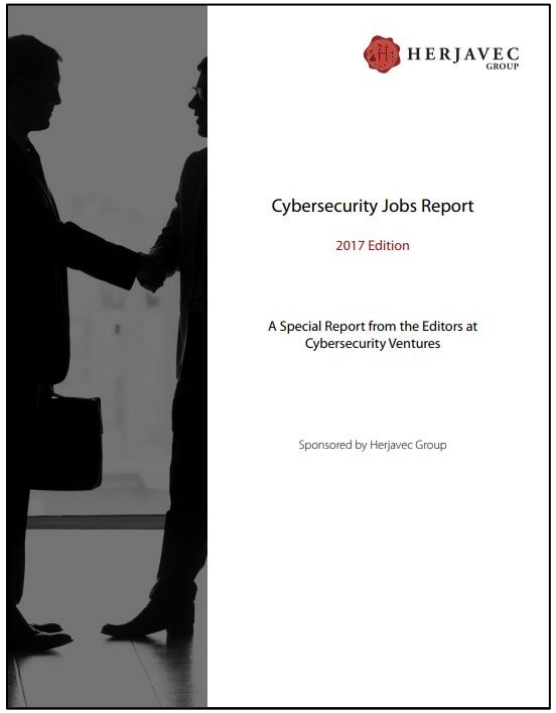
https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-security/information-security-awareness/careers_in_cybersecurity.pdf

https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/professional-development/jump-start-your-security-career



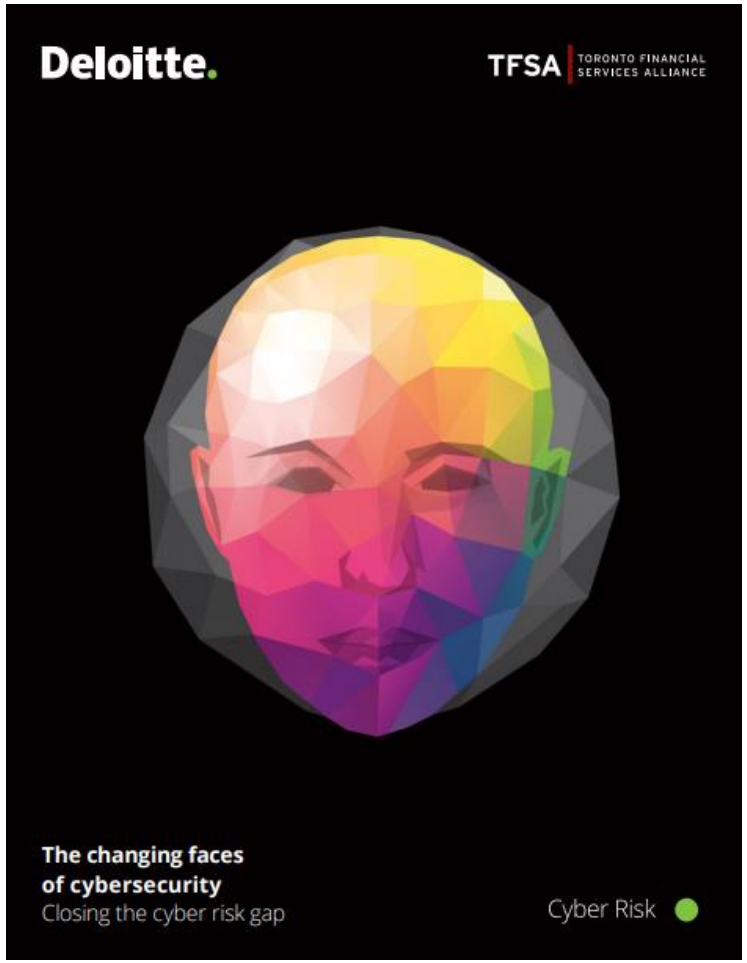
How to get into security

- careers in InfoSec are challenging and rewarding
- threats posed by cyber criminals not going away
- forecasted global shortage of 3.5 million professionals by 2021
- security professionals come from all walks of life
- not every job requires significant technology knowledge



University of Victoria

How to get into security



- 7 cybersecurity personas

Integration of cybersecurity concepts within broader computer science and engineering curricula remains relatively weak, with cybersecurity courses typically positioned as upper-year electives. When cybersecurity concepts are integrated, such as the concept of validation in computer science, they are not provided the import that the current situation warrants. In civil engineering, for example, safety is taught as a core design component.

University of Victoria

https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-cyber-talent-campaign-report-pov-aoda-en.PDF

What is a security professional?

- a strategic thinker able to interpret the changing threat landscape, understand the implications of changing technology, and enable the business to achieve it's goals

University of Victoria

[Review this article as it captures the main principles of security]

Information security

From Wikipedia, the free encyclopedia

Information security, sometimes shortened to **InfoSec**, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).[1]

Overview [edit]

IT security

Sometimes referred to as computer security, information technology security is information security applied to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smartphones and tablet computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber attacks that often attempt to breach into critical private information or gain control of the internal systems.

Information assurance

The act of providing trust of the information, that the Confidentiality, Integrity and Availability (CIA) of the information are not violated. E.g., ensuring that data is not lost when critical issues arise. These issues include, but are not limited to: natural disasters, computer/server malfunction or physical theft. Since most information is stored on computers in our modern era, information assurance is typically dealt with by IT security specialists. A common method of providing information assurance is to have an off-site backup of the data in case one of the mentioned issues arise.

Threats [edit]

Information security threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion. Most people have experienced software attacks of some sort. Viruses,[2] worms, phishing attacks, and Trojan horses are a few common examples of software attacks. The theft of intellectual property has also been an extensive issue for many businesses in the IT field. Identity theft is the attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information. Theft of equipment or information is becoming more prevalent today due to the fact that most devices today are mobile.[*citation needed*] Cell phones are prone to theft, and have also become far more desirable as the amount of data capacity increases.[*citation needed*] Sabotage usually consists of the destruction of an organization's website in an attempt to cause loss of confidence on the part of its customers. Information extortion consists of theft of a company's property or information as an attempt to receive a payment in exchange for returning the information or property back to its owner, as with ransomware. There are many ways to help protect yourself from some of these attacks but one of the most functional precautions is user carefulness.[*citation needed*]

How to get into security

- Find out more about different careers and what security professionals do:
  - https://resources.infosecinstitute.com/job-titles/
  - https://www.cs.seas.gwu.edu/cybersecurity-roles-and-job-titles
  - https://www.sans.org/cyber-security-careers/20-coolest
  - https://www.cyberseek.org/pathway.html
  - https://www.securitywizardry.com/index.php/home/cnd-ltd/recruitment/security-roles-defined.html

Sample job titles

- security administrator
- security analyst
- security consultant
- security specialist
- security operations, support, design, build
- security architect, engineer
- governance, risk, and compliance (GRC), vulnerability management, risk management
- network security, data security, application security, endpoint/device/mobile security
- security investigations, forensics, data recovery
- security tester, code reviewer, vulnerability assessment, **penetration testing, red team**
- incident handling, **incident response**
- threat intelligence, threat hunter
- SIEM analyst, big data analytics
- identity and access management
- encryption, cryptography, certificates
- security awareness, education, training, communications, marketing
- security auditor, project management, policy
- cloud security, vendor management, IOT, ICS, SCADA, hardware
- security manager/director/CISO
- security sales

How to get into security

- what do you want to do? eg. pentesting
- who do you want to do it for? eg. Amazon
- private sector, public sector, academia? eg. private sector
- what are your next 3 jobs? eg. jr -> intermed -> PT
- technical role or not? eg. technical

University of Victoria

How to get into security

- talk to security professionals and ask more questions
- join local MeetUp groups (eg. VicCyberSec)
  - in no other industry are people more willing to help you learn
  - find out what they do, how they do it, what they like, what they don't like
- join professional organizations like ISACA
  - Victoria, Vancouver, global
- find a mentor to recommend training, courses, identify gaps/ development opportunities, expand your network, provide career advice

Now on Discord!

University of Victoria

How to get into security

- identify companies with 2 or more security professionals
- identify required education, experience, certifications, and skills
- review job profiles, job postings
- make a list of the requirements
- become familiar and gain experience with each skill

University of Victoria

How to get into security

- consider taking free online courses and learn the language/jargon
  - Cybrary
  - Coursera
  - Udemy (some)
  - SANS Cyber Aces
  - … many others including Fortinet…

University of Victoria

Take advantage of free materials

- articles (read something every day security-related and stay up to date on current trends)
  - KrebsonSecurity
  - DARKReading
  - Security Weekly
  - Naked Security Blog - Sophos
  - InfoSecurity Magazine
  - Schneier on Security
  - SC Magazine

University of Victoria

Take advantage of free materials

- Webinars
  - BrightTALK
  - Gartner
  - ISACA
  - Security Magazine
  - Canadian Security Mag
  - DARKReading
  - SANS

University of Victoria

Take advantage of free materials

- Forums and other security groups
  - ~~Peerlyst~~
  - LinkedIn
    - Information Security Community
    - Information Security Network
    - Information Security Careers Network
    - Advanced Persistent Threats (APT) & Cyber Security
    - Brian Krebs
    - Kevin Mitnick
  - Reddit
    - https://www.reddit.com/r/infosec
    - https://www.reddit.com/r/netsec

Take advantage of free materials

- Forums and other security groups (con't)
  - Twitter
    - Bruce Schneier,
    - Mikko Hypponen
    - Brian Krebs
    - Troy Hunt
    - US-CERT
    - Naked Security
    - NCSC UK
  - YouTube
    - Black Hat, Troy Hunt

University of Victoria

Take advantage of free materials

- Check out other sites online
  - ~~Norse~~ 

  - Digital Attack Map
  - Data is Beautiful
  - Shodan
  - Kaspersky
  - Fortiguard
  - FireEye
  - Check Point ThreatCloud
  - Security Wizardry

University of Victoria

Experiment at home

- familiarize with basic networking
- familiarize with firewalls and examine traffic inbound, outbound, and within your network
- familiarize with operating systems like Linux (Ubuntu, Kali)
- familiarize with different types of hardware
- familiarize with other topics based on interest (eg. risk, secure coding)
- familiarize with cloud (eg. spin up a VM on AWS)

How to get into security

- research and read a variety of material
  - Many good printed books, e-books, whitepapers, and other PDFs available online
  - Good deals on sites like HumbleBundle

- consider taking paid courses online or in classroom
  - Online: Udemy, SANS, Infosec Institute, ISACA
  - Instructor led: SANS, Global Knowledge, EC-Council, ISC2, ISACA
  - Post secondary: Individual Courses, Certificates, Diploma, Masters

How to get into security

- consider conferences
  - RSA Conference, BlackHat, DEF CON,
  - B-Sides Victoria, B-Sides Vancouver, BC Aware
  - CanSecWest, SecTor
  - SANS
  - Gartner Security and Risk Management Summit
  - FIRST Conference
  - IEEE
  - ISF
  - ISACA
  - Privacy & Security Conferences

University of Victoria

How to get into security

- consider pursuing relevant certifications
  - Self-study
    - if you are disciplined or already have experience you may be able to study and challenge the exam
  - Bootcamps
    - 5 days or less designed to ensure you are familiar with the exam material
  - Courses
    - greater commitments of time
  - Top certifications in-demand by employers
    - CISSP, CISM, CISA
  - If focused on penetration testing
    - CEH, LPT, GPEN, OSCP
  - If a beginner:
    - CompTia Security+, ISACA CSX, SSCP

How to get into security

- consider ways to get work experience
  - Co-op
  - Internship
  - Leadership Development Program
  - Volunteer
  - Mentoring
  - Job shadowing
  - On-loan
  - Temporary Assignment

University of Victoria

Employers are looking for

- passion
- demonstrated interest

  - informed on current events & trends

- practical experience

  - eg. developing security policy

  - eg. implementing and configuring security tools

- security certifications

University of Victoria

Certifications

CSX:F	Cybersecurity Fundamentals Certificate
CISSP	**Certified Information Security Professional**
CISA	**Certified Information Systems Auditor**
CISM	**Certified Information Security Manager**
PCI QSA	PCI Qualified Security Assessor
CCSP	Certified Cloud Security Professional
GSEC	GIAC Security Essentials
Security+	CompTIA Security+
C|EH	Certified Ethical Hacker
LPT	Licensed Penetration Tester

University of Victoria

... also GPEN, OSCP

SENG 460 / ECE 574
Practice of Information Security and Privacy

Introduction to the Course

How to Get into a Career in Security

Cybersecurity Threat Landscape

Gary Perkins, MBA, CISSP

garyperkins@uvic.ca

University of Victoria

Cybersecurity has never been more imperative

Previous Semesters

Studies of 30 of the highest profile breaches revealed they could have been prevented with one or more of the following:

1) security awareness
2) patching
3) offline backups
4) password management
5) supply chain security

University of Victoria

Global Context

- global annual cybercrime will cost the world in excess of $6 trillion annually by 2021
  - this is an increase from $400 billion in early 2015
- global spending on cybersecurity defence is projected to exceed $1 trillion over the next 5 years
- U.S. has declared a national emergency to deal with the cyber threat
- global shortage of cybersecurity professionals is expected to reach 2 million by 2019
  - now expected to be 3.5 million by 2021
  - half of this will be in North America

University of Victoria

* source: Herjavec 2016 Cybercrime Report

Global Context

- theft of intellectual property due to cybercrime is the single largest transfer of wealth in history
- according to the World Economic Forum (WEF), climate change and cyberattacks are the two greatest threats facing businesses today
- cybercrime is more profitable than the sale of all illegal drug sales combined

University of Victoria

* source: Cybersecurity Ventures

Key Messages

- incidents are increasing in frequency and are more sophisticated and targeted than ever
- no organization globally is immune to attack
- organizations will be judged not only on their ability to prevent but detect and respond
- doing the basics well will stop 80% of the problems
- security is not just an IT problem, it's business enterprise risk

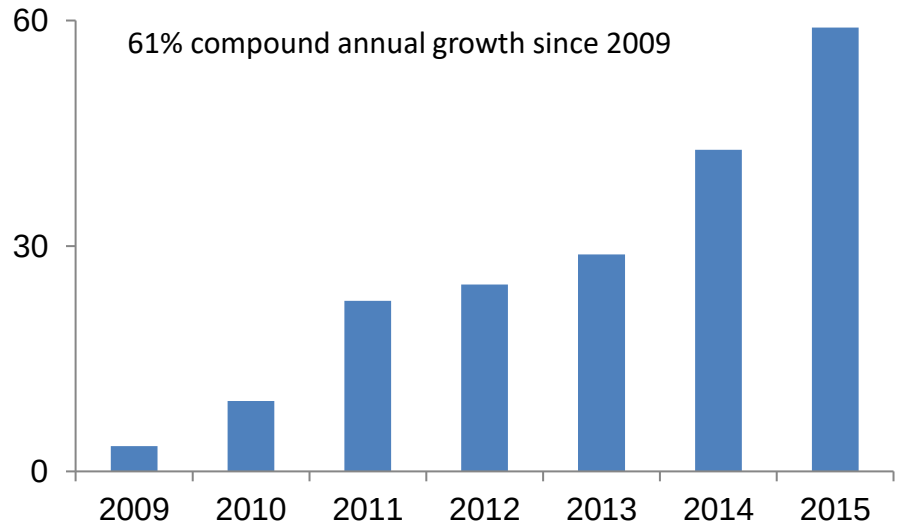
University of Victoria

Security Threat Landscape

Cyber attacks are more:

- frequent
- effective
- targeted
- sophisticated
- profitable
- elusive

Global Security Incidents (millions)



(based on reported incidents of sufficient size PWC 2016)

University of Victoria

Threat Actors***

- juveniles
- insiders
- hacktivists
- organized crime
- nation-states
- cyber terrorists

University of Victoria

Juveniles

Juveniles

Alias
Script Kiddies
Packet Warriors

Sophistication
LOW — HIGH

Resources
LOW — HIGH

Motivation
Curiosity
Trophy
Challenge

Insiders

Insiders

Alias Snowden

Sophistication

LOW — HIGH

Resources

LOW — HIGH

Motivation Profit
Espionage
Retribution

Hacktivists

Hacktivists

Alias Anonymous

Sophistication

LOW — HIGH

Resources

LOW — HIGH

Motivation Causes
Bring Awareness
Maximum Impact

Organized Crime

Organized Crime

Alias N/A

Sophistication

LOW — HIGH

Resources

LOW — HIGH

Motivation

Leverage
Fraud
Financial Gain

Nation States

Nation-states

Alias

PLA Unit 61398
Cozy / Fancy Bear

Sophistication

LOW — HIGH

Resources

LOW — HIGH

Motivation

Surveillance
Espionage
Political leverage

Cyber Terrorists

Cyber Terrorists

Alias N/A

Sophistication

LOW — HIGH

Resources

LOW — HIGH

Motivation Political
Acts of terrorism

Why Organizations are Targeted

- gain economic advantage
- access to financial or personal data (eg. health), for fraud/identity theft
- take over systems as launch point against others
- retribution or make a statement
- cause damage or distraction
- surveillance

University of Victoria

Business Impacts

- direct impact to clients, customers
- disruption of operations, lost productivity
- financial, value loss
- litigation, regulatory
- data breach and loss
- brand and reputation
- lost/stolen intellectual property

$6 trillion by 2021

In the news

Cyber attacks cost companies $400 billion every year

by Stephen Gandel @stephengandel JANUARY 23, 2015, 1:03 PM EST

Last year, the insurance industry took in $2.5 billion in premiums on policies to protect companies from losses resulting from hacks.

University of Victoria

Attack vectors/methods

- phishing, smishing, vishing, social engineering, spearphishing, whaling
- malware, cryptoware, ransomware, scareware, malvertising, waterholing, pharming
- weak/no passwords/brute force
- supply chain/vendors/partners
- distributed denial of service (DDoS)
- poor coding hygiene (SQL inject, buffer overflow)
- exploiting other vulnerabilities

Shodan Developers Book View All...

SHODAN

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

The search engine for the Internet of Things

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

Create a Free Account | Getting Started

Explore the Internet of Things

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

See the Big Picture

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

Monitor Network Security

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

Get a Competitive Advantage

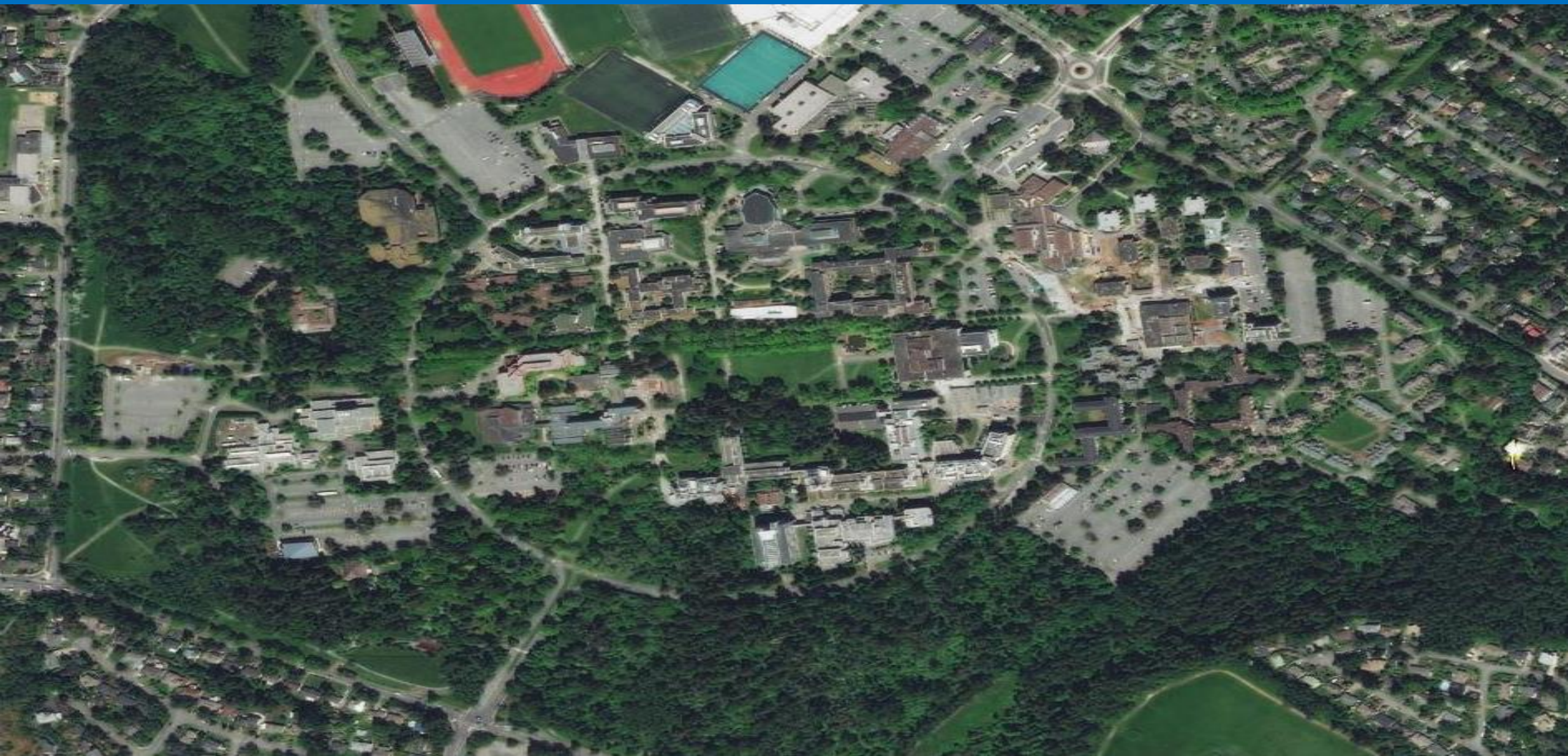
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

56% of Fortune 100

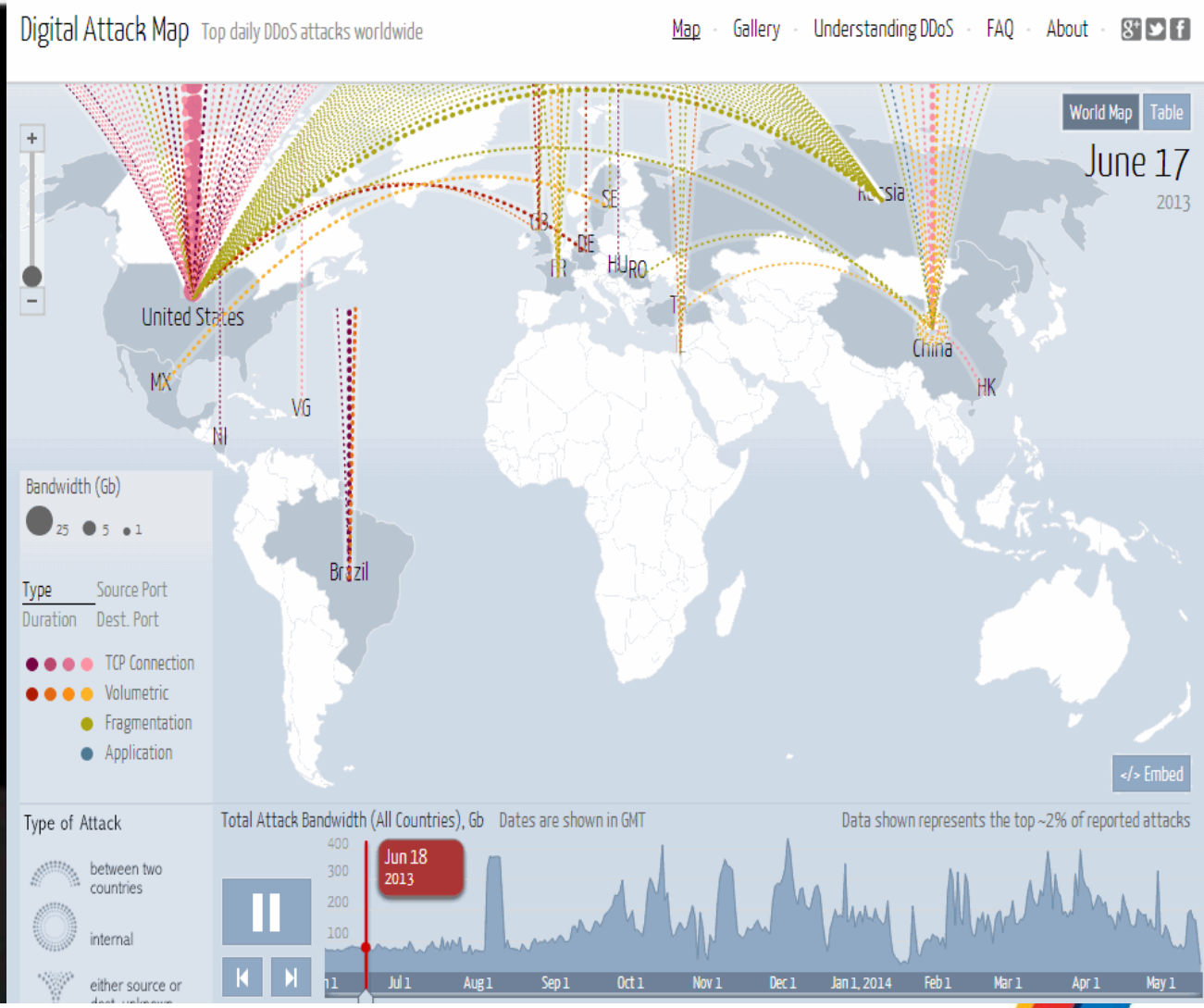
1,000+ Universities

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

Thingful



Global Context



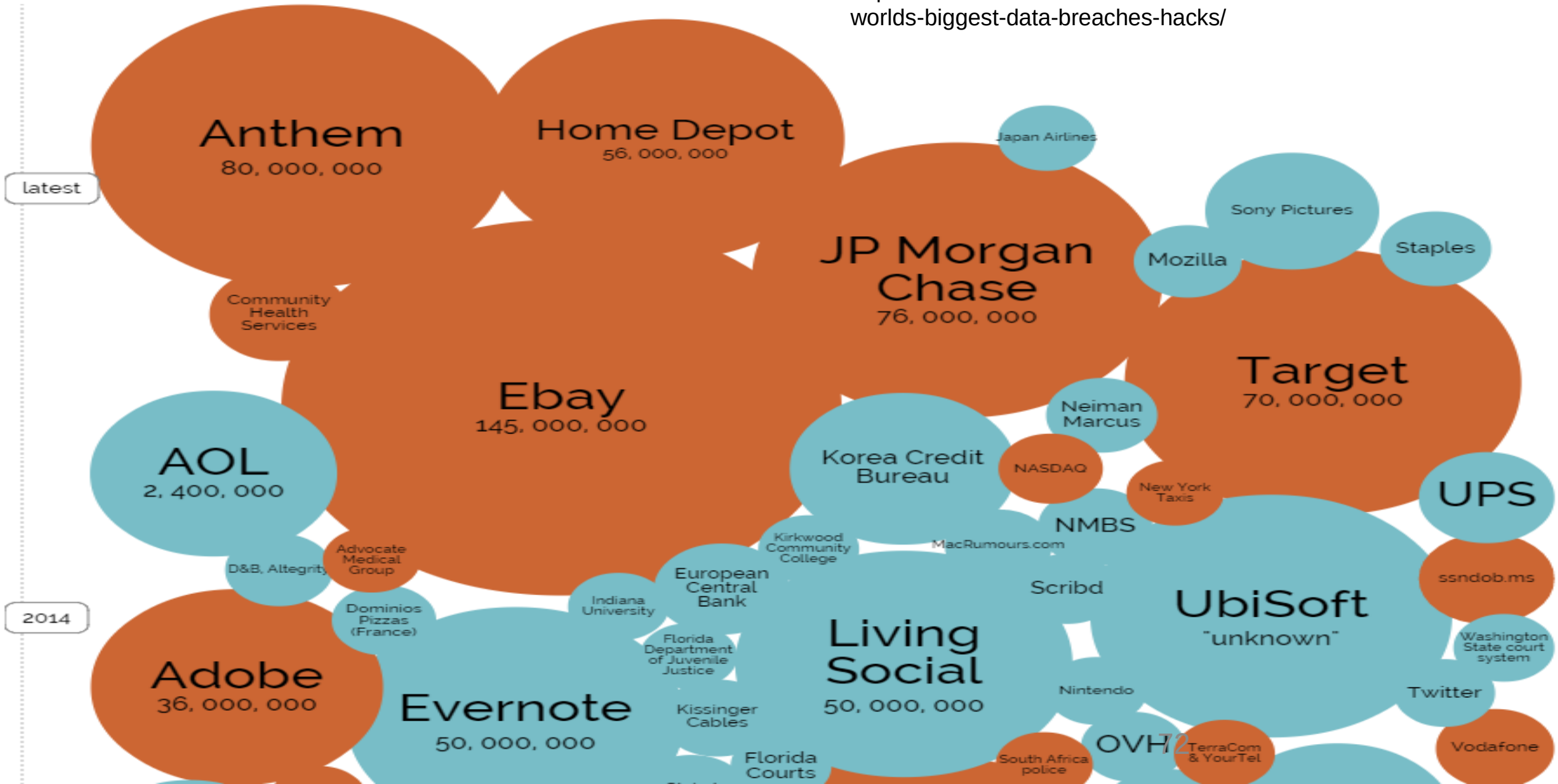
University of Victoria

World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 5th Feb 2015)

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



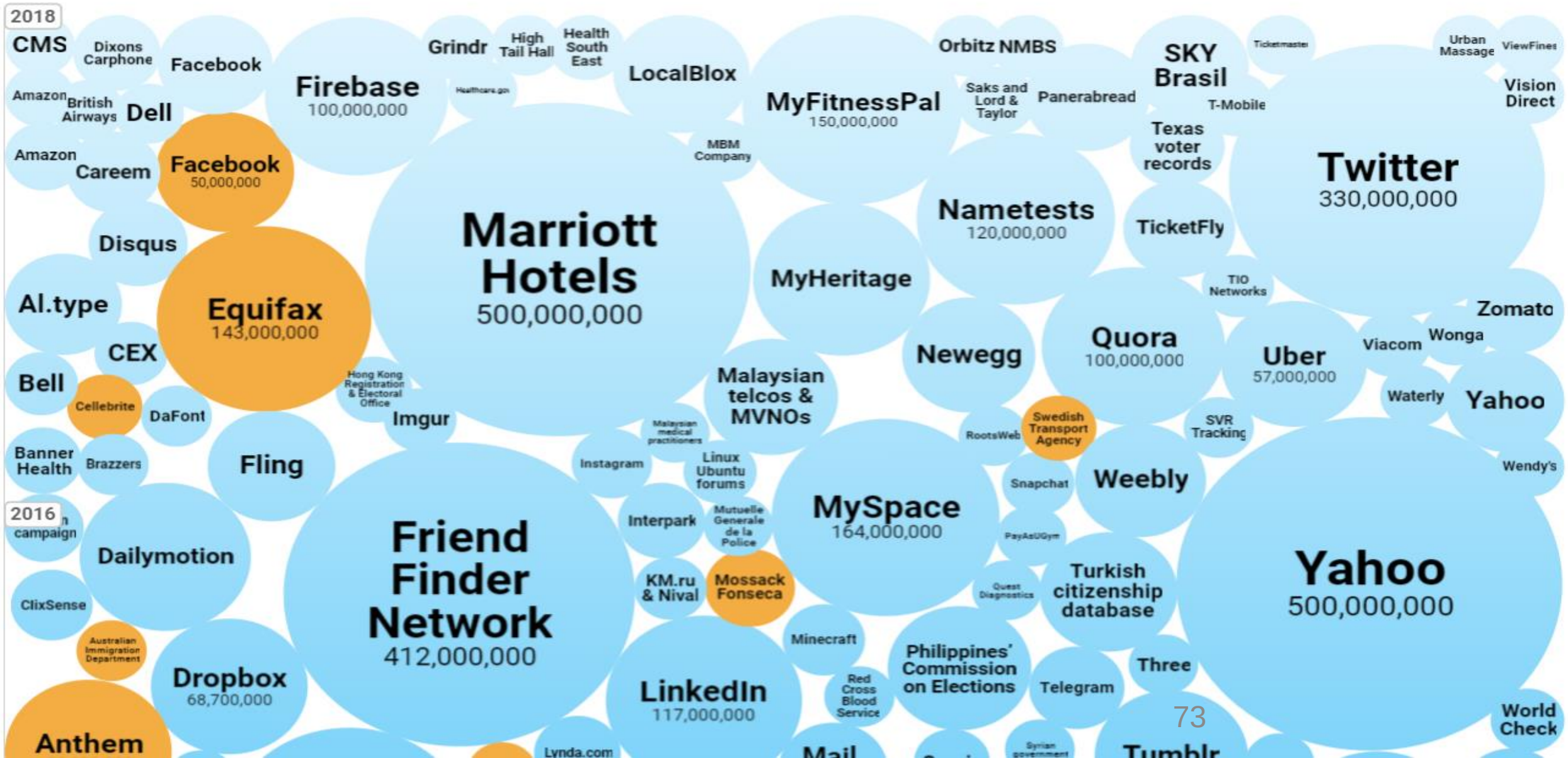
World's Biggest Data Breaches & Hacks

Select losses greater than 30,000 records
(updated Dec 5th 2018)

Interesting Story

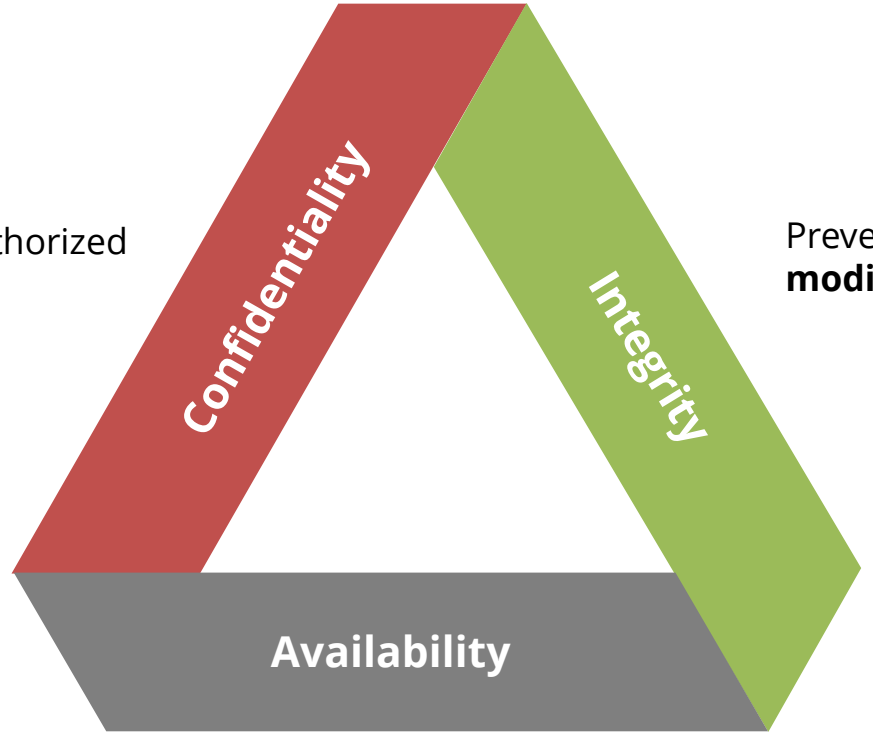
Colour | YEAR | DATA SENSITIVITY | Filter

Search...



Goals of Information Security

"CIA Triad"



Prevent unauthorized **disclosure**

Prevent unauthorized **modification**

Prevent **disruption** of service and productivity.

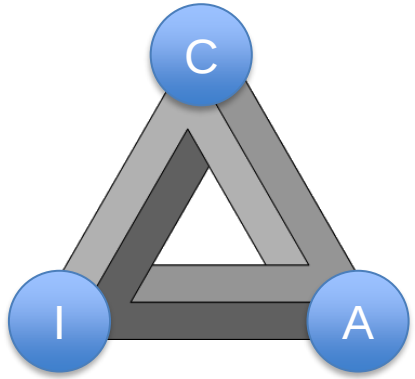
University of Victoria

CIA Triad *

- confidentiality

  the property that information is not made available or disclosed

  to unauthorized individuals, entities, or processes



- integrity

  maintaining and assuring the accuracy and completeness of data over its entire life-cycle

- availability

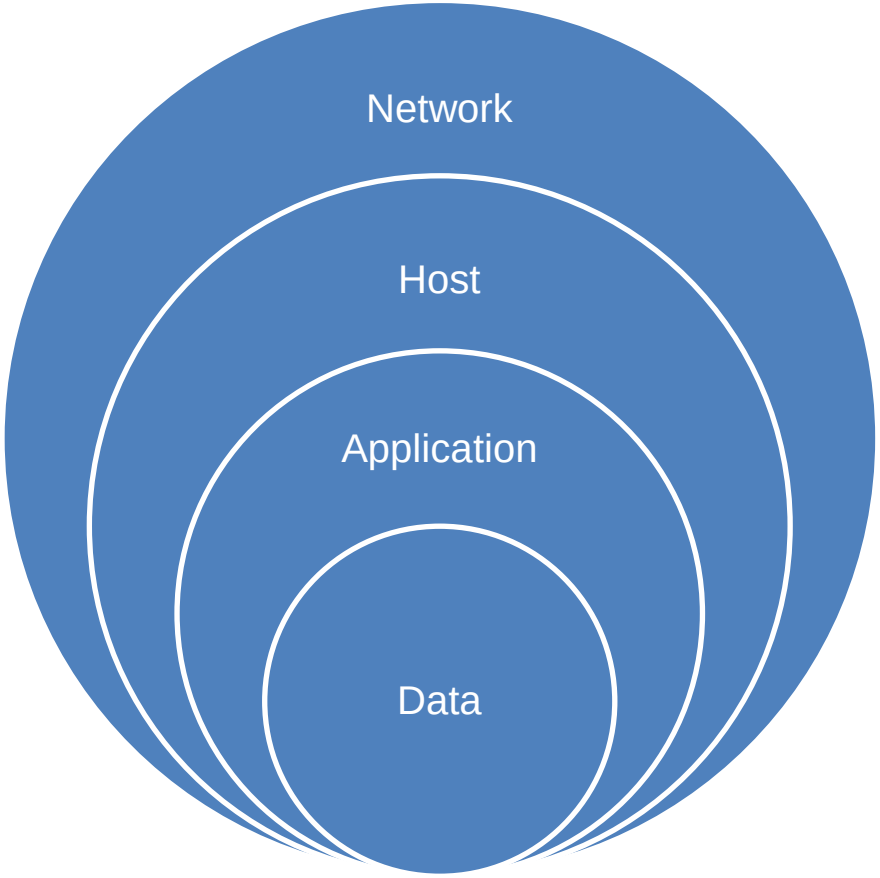
  preventing service disruptions due to power outages, hardware failures, and system

  upgrades; also preventing denial-of-service attacks

University of Victoria

Five tenets of security

1) strong authentication
2) least privilege
3) non-repudiation
4) separation of duties
5) defence in depth



University of Victoria

Five tenets

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

Strong Authentication

- single-factor authentication
  - difficult to guess
    - passphrase
  - composition rules
    - minimum length
    - lowercase, uppercase, numbers, punctuation
  - password aging
  - password history
  - lockout after unsuccessful attempts

susceptible to attack
dictionary
brute force
rainbow tables

University of Victoria

Strong Authentication

- two-factor / multi-factor authentication
  - **something you know**
    eg. password
  - **something you have**
    eg. token
  - **something you are**
    eg. biometrics

strong authentication

- AAA or “triple A”
  - authentication: grants access
  - authorization: determines permissions
  - accounting: ensures logging

University of Victoria

Least Privilege

- “The principle of least privilege has been described as important for meeting integrity objectives. The principle of least privilege requires that a user be given no more privilege than necessary to perform a job. Ensuring least privilege requires identifying what the user's job is, determining the minimum set of privileges required to perform that job, and restricting the user to a domain with those privileges and nothing more. By denying to subjects transactions that are not necessary for the performance of their duties, those denied privileges cannot be used to circumvent the organizational security policy.” (source: unknown)

- user, program, or system not granted any more access than required to do the job

- **need to know**: gives access rights and information to a person to perform their job function

Non-Repudiation

- “the assurance that someone cannot deny the validity of something” (source: https://www.cryptomathic.com/
- one party cannot deny having received a transaction nor can the other party deny having sent a transaction
- proof of origin of data and integrity of data
- ability to ensure that the document or communications could only have originated with a specific individual
- eg. shared user account vs. multi-factor authentication or digital certificates

University of Victoria

Separation of Duties

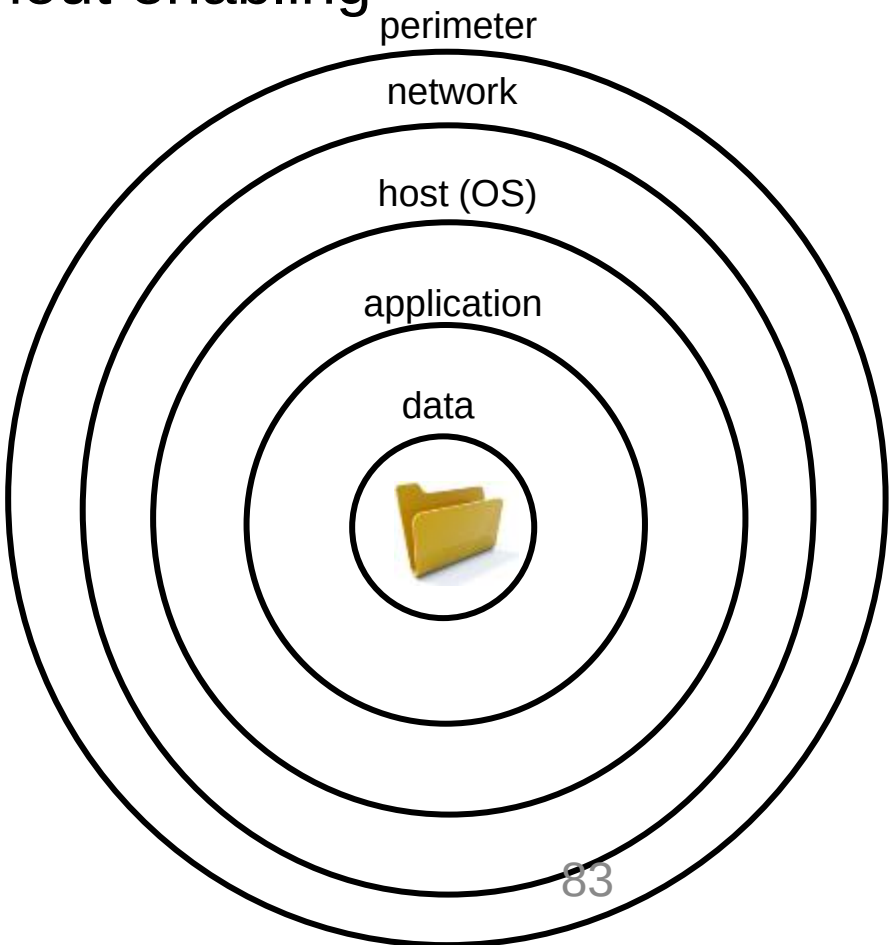
- “internal control to prevent error and fraud by ensuring that at least two individuals are responsible for the separate parts of any one task” (source: https://whatis.techtarget.com)
- require more than one person to accomplish a task
- key concept of internal controls
- establishes system of checks and balances
- increased protection from fraud and errors
- eg. an employee who submits a request for reimbursement should not also be able to authorize payment or print the cheque

University of Victoria

* mandatory vacations

Defence in Depth

- having more than one layer of defence
- any one layer alone may be defeated without enabling compromise
- combining multiple layers to make it more difficult to compromise asset
- failure of any one layer should not cause failure of the system



University of Victoria

Types of Security Controls

- **administrative**: written policies, procedures, standards and guidelines
- **logical**: (technical controls) use data, software, and hardware to control access to information and computing systems
- **physical**: monitor and control the environment of the work place and computing facilities

Security Technology

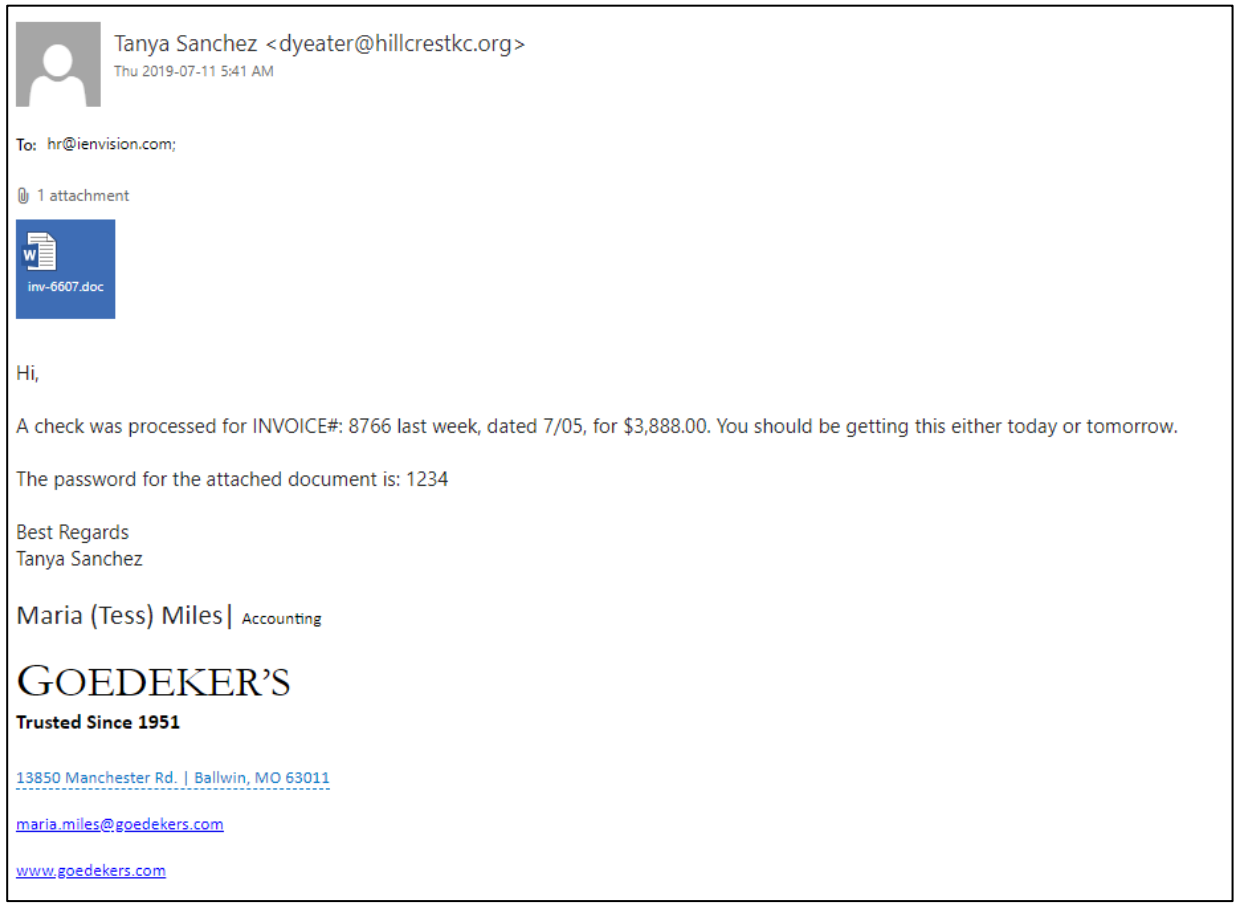
- firewalls, VPN
- intrusion detection/prevention
- web content filtering
- email content filtering
- DDoS prevention
- Security Information and Event Management (SIEM)
- … and more

University of Victoria

Challenges

- more connected and dependent on networks, systems, and data than ever
- despite awareness efforts, devices released with little to no security
- not getting through to users effectively
- broad misunderstanding of the impacts of not taking security seriously
- belief that security is an IT problem
- significant shortage of talent

Phishing



Tanya Sanchez <dyeater@hillcrestkc.org>
Thu 2019-07-11 5:41 AM

To: hr@ienvision.com;

1 attachment

inv-6607.doc

Hi,

A check was processed for INVOICE#: 8766 last week, dated 7/05, for $3,888.00. You should be getting this either today or tomorrow.

The password for the attached document is: 1234

Best Regards
Tanya Sanchez

Maria (Tess) Miles | Accounting

GOEDEKER'S
Trusted Since 1951

13850 Manchester Rd. | Ballwin, MO 63011

maria.miles@goedekers.com

www.goedekers.com

- phishing is effective
  - create a sense of urgency
  - play on people's emotions
- consider
  - look at the from address
  - look at the subject
  - look at the to address
  - beware attachments including PDF, doc, and docx
  - beware links – hover over
  - what are they asking you to do?

It can happen to anyone…

University of Victoria

Phishing

Received: from tailor.uvic.ca (142.104.225.130) by lyretail.uvic.ca (142.104.225.129) with Microsoft SMTP Server (TLS) id 15.0.1473.3 via Mailbox Transport; Thu, 11 Jul 2019 05:41:34 -0700
Received: from boxfish.uvic.ca (142.104.224.1) by tailor.uvic.ca (142.104.225.130) with Microsoft SMTP Server (TLS) id 15.0.1473.3; Thu, 11 Jul 2019 05:41:28 -0700
Received: from mako.comp.uvic.ca (142.104.177.234) by boxfish.uvic.ca (142.104.224.1) with Microsoft SMTP Server (TLS) id 15.0.1473.3 via Frontend Transport; Thu, 11 Jul 2019 05:41:28 -0700
Received: from gateway9.unifiedlayer.com (gateway9.unifiedlayer.com [70.40.200.246]) by mako.comp.uvic.ca (8.14.4/8.14.4) with ESMTP id x6BCfKOQ014861
(version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-GCM-SHA384 bits=256 verify=NO) for <garyperkins@uvic.ca>; Thu, 11 Jul 2019 05:41:21 -0700
Received: from cm6.websitewelcome.com (cm6.websitewelcome.com [108.167.139.19]) by gateway9.unifiedlayer.com (Postfix) with ESMTP id 0323E200BB7B7
for <garyperkins@uvic.ca>; Thu, 11 Jul 2019 07:19:05 -0500 (CDT)
Received: from mail.ivy.arvixe.com ([23.91.70.105]) by cmsmtp with SMTP id lY2MhTLZo7MgvlY2Mhh3eV; Thu, 11 Jul 2019 07:19:05 -0500
Received: from [127.0.0.1] (Unknown [216.1.95.222]) by mail.ivy.arvixe.com with ESMTPA; Thu, 11 Jul 2019 07:18:57 -0500
X-AuthUser: dyeater@hillcrestkc.org
Reply-To: <christopherrpacker@cock.li>
Date: Thu, 11 Jul 2019 06:18:55 -0600
Subject: Payment Invoice - #4981
Message-ID: <ekjjko7b97ul5adcak34s108.1052209470004@hillcrestkc.org>
From: Tanya Sanchez <dyeater@hillcrestkc.org>
To: <hr@ienvision.com>
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="--_com.android.email_5349471126272"
X-Source-IP: **216.1.95.222**
X-Source-Sender: (Unknown) [216.1.95.222]:
X-UVic-Virus-Scanned: OK - Passed virus scan by ClamAV (clamd) on mako
X-UVic-Virus-Scanned: TEMPFAIL - Could not virus scan by Sophos (sophie) on mako

Phishing

warning: From info@HelpDesk

REPLY REPLY ALL FORWARD ...

Mark as unread

Khin Thanda Lat <ThandaL@pttep.com>
Wed 2019-03-20 3:26 PM
Junk Email

This message was sent with high importance.

Your mailbox is about to exceed it's storage limit.

4.5 GB 5 GB

At 5 GB, you will not be able to send or receive messages till you increase your mailbox quota.

Visit our >MAILBOX QUOTA PAGE< and Sign In to increase your Mailbox Quota.

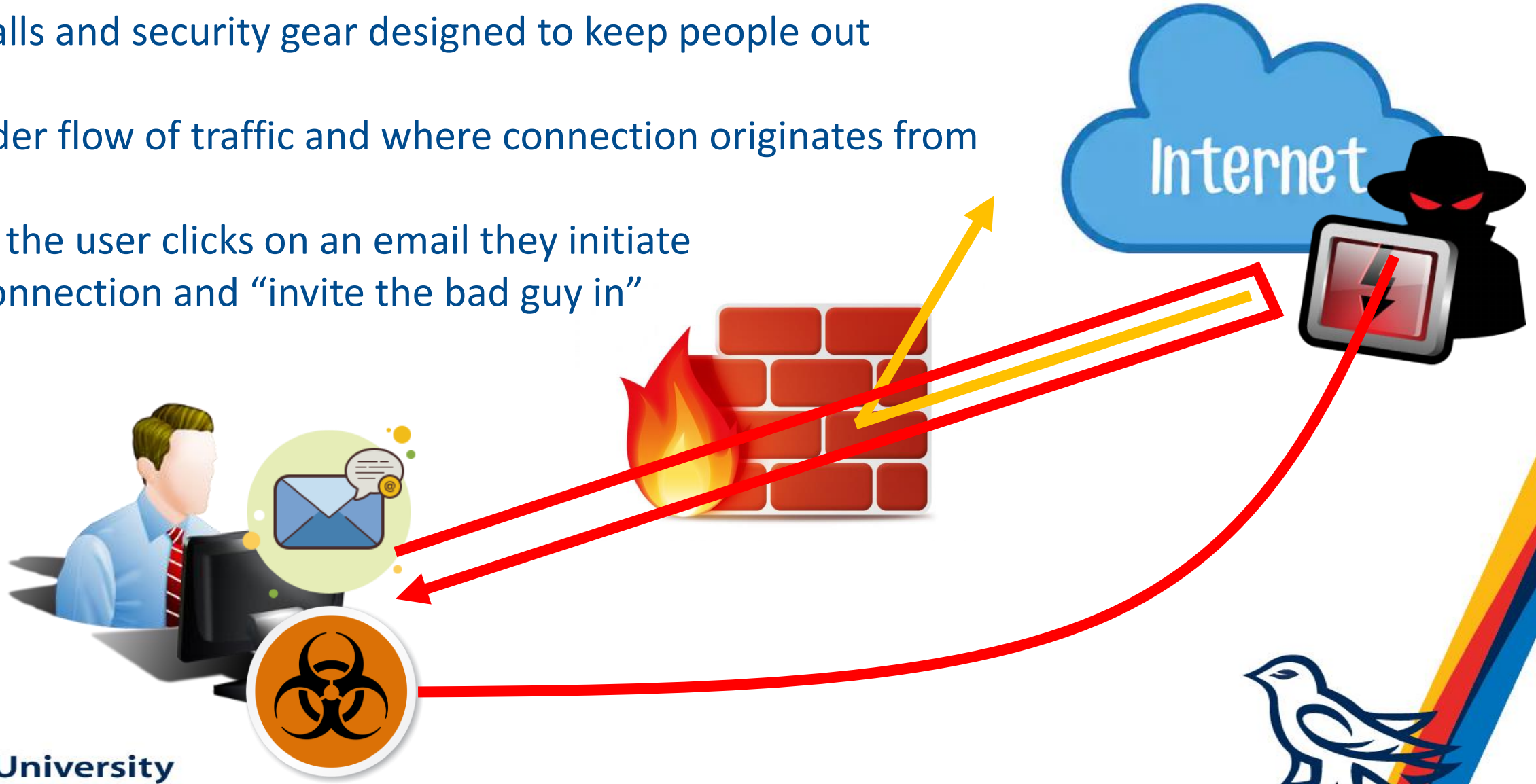
© 2019 IT Help Desk

Phishing

Received: from lyretail.uvic.ca (142.104.225.129) by lyretail.uvic.ca (142.104.225.129) with Microsoft SMTP Server (TLS) id 15.0.1473.3 via Mailbox Transport; Wed, 20 Mar 2019 15:26:56 -0700
Received: from boxfish.uvic.ca (142.104.224.1) by lyretail.uvic.ca (142.104.225.129) with Microsoft SMTP Server (TLS) id 15.0.1473.3; Wed, 20 Mar 2019 15:26:56 -0700
Received: from angelshark.comp.uvic.ca (142.104.42.104) by boxfish.uvic.ca (142.104.224.1) with Microsoft SMTP Server (TLS) id 15.0.1473.3 via Frontend Transport; Wed, 20 Mar 2019 15:26:56 -0700
Received: from ironport-ext.pttep.com (mailgw1.pttep.com [175.176.220.228]) by angelshark.comp.uvic.ca (8.14.4/8.14.4) with ESMTP id x2KMQaku108134; Wed, 20 Mar 2019 15:26:46 -0700
Received: from unknown (HELO HQ-HC02.pttep.com) ([10.1.0.18]) by ironport-int.pttep.com with ESMTP; 21 Mar 2019 05:26:46 +0700
Received: from RGN-HUB01.pttep.com (10.15.1.36) by HQ-HC02.pttep.com (10.1.3.216) with Microsoft SMTP Server (TLS) id 14.3.389.1; Thu, 21 Mar 2019 05:27:03 +0700
Received: from RGN-MB01.pttep.com ([169.254.1.8]) by RGN-HUB01.pttep.com ([10.15.1.36]) with mapi id 14.03.0389.001; Thu, 21 Mar 2019 04:57:01 +0630
From: Khin Thanda Lat <ThandaL@pttep.com>
Subject: warning: From info@HelpDesk
Thread-Topic: warning: From info@HelpDesk
Thread-Index: AdTa7UK7DBHcOTLDRHSXYrMzzFNamQ==
Importance: high
X-Priority: 1
Date: Wed, 20 Mar 2019 22:27:01 +0000
Message-ID: <6283909ECB0BDC48BC5F478CA95BD7FC03BEAEF3@RGN-MB01.pttep.com>
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach:
X-MS-TNEF-Correlator:
x-originating-ip: [10.1.3.219]
X-TM-AS-Product-Ver: SMEX-12.5.0.1300-8.5.1010-24502.003
X-TM-AS-Result: Yes-8.893400-5.000000-11
X-TM-AS-User-Approved-Sender: No
X-TM-AS-User-Blocked-Sender: No
X-UVic-Virus-Scanned: OK - Passed virus scan by ClamAV (clamd) on angelshark
X-UVic-Virus-Scanned: OK - Passed virus scan by Sophos (sophie) on angelshark

How phishing works

- firewalls and security gear designed to keep people out
- consider flow of traffic and where connection originates from
- when the user clicks on an email they initiate the connection and “invite the bad guy in”



University of Victoria

Ransomware

- common type of cyber attack is ransomware
- data is encrypted by malware contained in websites and email attachments
- attacker demands payment to provide keys to decrypt data
- organizations with backups can restore files and avoid paying

Nunavut reels after 'ransomware' attack knocks out government services

Food vouchers replace cheques in Nunavut as government struggles with cyber attack aftermath

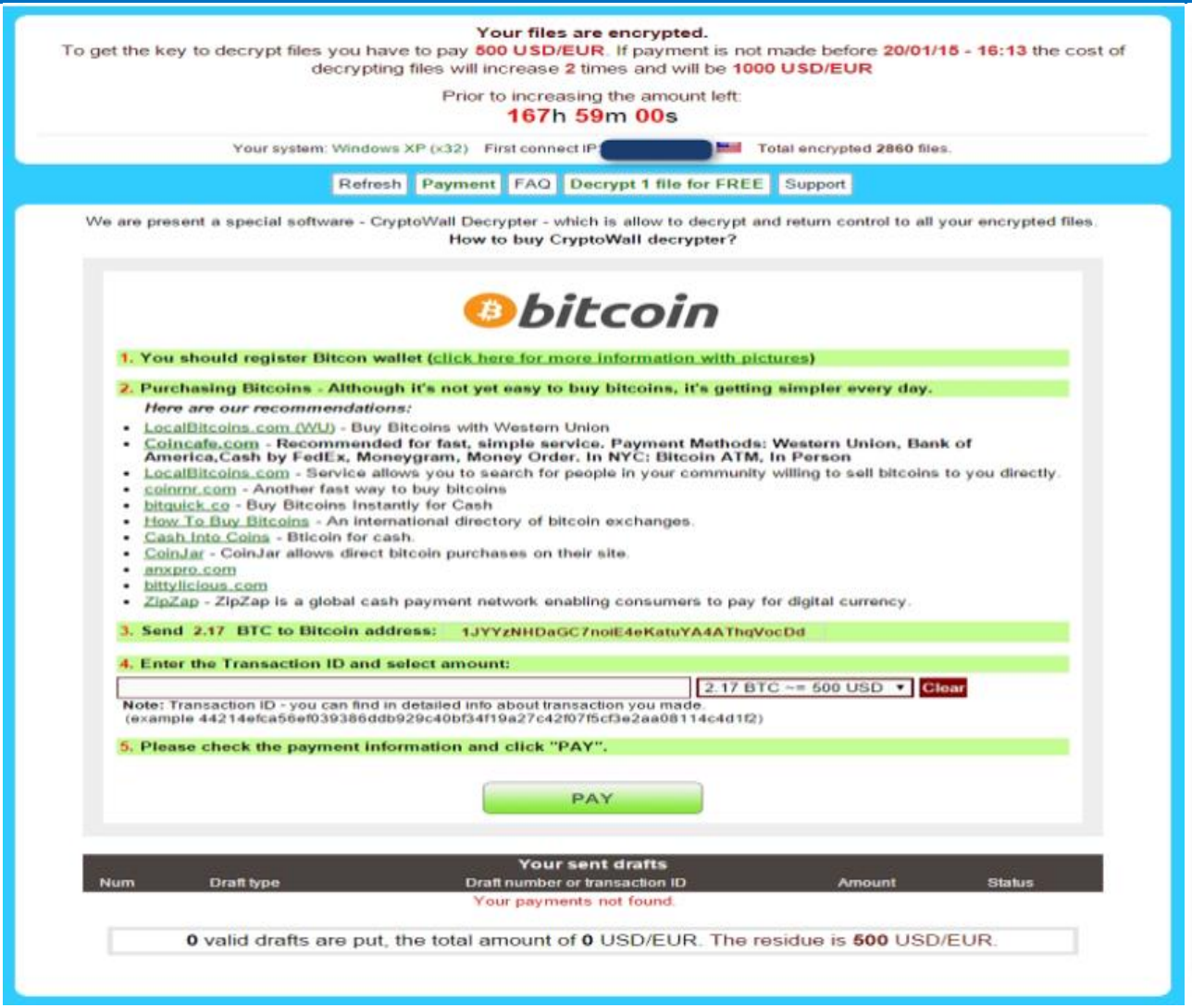
University of Victoria

Extortionware

- attackers realized if organizations have backups they are unlikely to pay
- new malware encrypts the data but sends a copy of the data to the attacker first (breach)
- attacker threatens to post data online if organization doesn't pay
- backups are insufficient and organization may need to pay

University of Victoria

Ransomware Examples



University of Victoria

Headlines - Ransomware

Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating

Doctors reverted to pens and paper after hospital taken offline by a ransomware attack

By Lauren O'Neil, CBC News Posted: Feb 16, 2016 10:59 PM ET | Last Updated: Feb 17, 2016 10:03 PM ET

The Hollywood Presbyterian Medical Center hack may be part of a larger trend predicted for this year, in which ransomware is used to target the medical sector – potentially leading hackers to threaten victims with their own lives if they don't pay up. (Hollywood Presbyterian Medical Center/Facebook)

124 shares

Facebook

Twitter

A Los Angeles hospital paid a ransom in bitcoins equivalent to about $17,000 US to hackers who infiltrated and disabled its computer network, the medical centre's chief executive said Wednesday.

It was in the best interest of Hollywood Presbyterian Medical Center to pay the ransom of 40 bitcoins — currently worth $16,664 — after the

University Of Calgary Paid $20,000 In Ransom To Hackers

The Huffington Post Alberta | By Sarah Rieger

Posted: 06/07/2016 5:53 pm EDT | Updated: 06/07/2016 5:59 pm EDT

The University of Calgary paid $20,000 in ransom after a malware attack on the school's computers last week.

The university announced the payment in a release Tuesday, 10 days after a cyberattack that left students and staff unable to access university-issued computers, email or Skype.

"A ransomware attack involves an unknown cyberattacker locking or encrypting computers or computer networks until a ransom is paid, and when it is, keys, or methods of decryption, are provided," wrote Linda Dalgetty, vice-president of finances and services at the university, in a release.

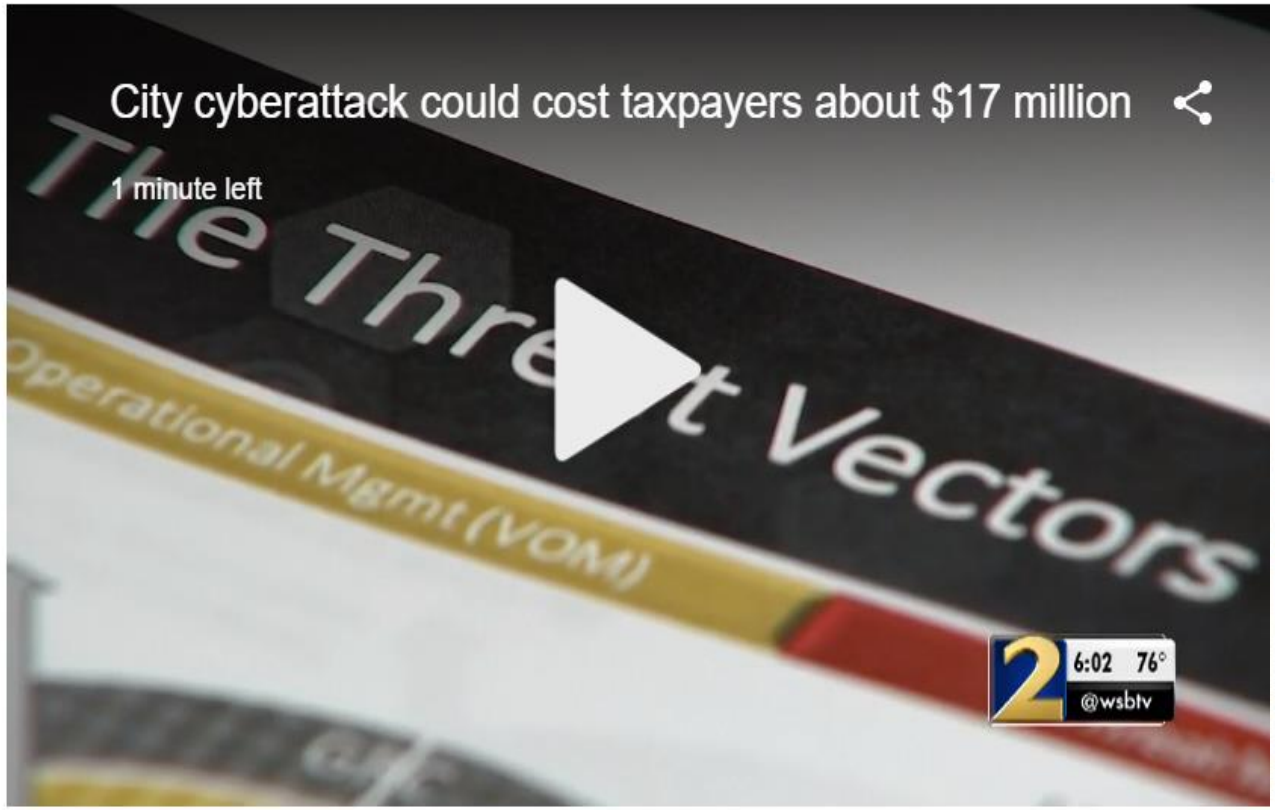
University of Victoria

SFU urges password changes after ransomware attack breaches personal info

The data breach occurred on Feb. 27; the issue was detected and fixed on Feb. 28. No SFU systems or data are currently exposed.

POSTMEDIA NEWS Updated: March 3, 2020

CONFIDENTIAL REPORT: Atlanta's cyber attack could cost taxpayers $17 million



A cyber expert says the report shows the city was forced to make drastic changes

Ransomware Cyberattacks Knock Baltimore's City Services Offline

May 21, 2019 · 5:02 AM ET

Heard on Morning Edition

Cyberattack Hobbles Baltimore for Two Weeks and Counting

City faces second ransomware attack in 15 months; water bills, home sales face delays

Hit by Ransomware Attack, Florida City Agrees to Pay Hackers $600,000

The city council in Riviera Beach, Fla., voted quietly to authorize a nearly $600,000 ransom payment after hackers paralyzed the city's computer systems. Wilfredo Lee/Associated Press

University of Victoria

Example: Ransomware

Ransomware attack knocks Nunavut government services offline

All Word documents and PDF files the virus had access to are encrypted and unreadable by the government, according to Martin Joy, Nunavut's director of information, communications and technology.

According to their investigation, Joy said it looks like the ransomware began acting on the government's network around 4 a.m. Saturday morning. By 6:30 a.m. information technology (IT) staff had confirmed the attack.

The virus was likely downloaded to Nunavut's network when an employee, working late on Friday night clicked on a web advertisement or email link, said Joy.

Joy said security systems in place didn't detect the virus. The email sent by the ransomware looks like the DoppelPaymer, a newer ransomware that the government of Nunavut's security systems weren't yet trained to detect, Joy said.

Nunavut government rebuilding network after ransomware attack

Canadian Nunavut government systems crippled by ransomware

The lockdown has impacted medical, legal, and social services.

Nunavut government checking computers for ransomware virus, fixing network

The territory's Premier says the network will hopefully be running again within a week or two

Nunavut government officials still locked out of electronic accounts after weekend ransomware attack

Nunavut ransomware attack impacting 'all government services'

Nunavut government trying to get back online after weekend ransomware attack

Ransomware attack knocks Nunavut government services offline

Government of Nunavut falls victim to ransomware attack

Ransomware Remedies

Assigned Reading

- sign up to “Reserve your Digital Copy”
  - https://www.securityroundtable.org/navigating-digital-age-second-edition/
- or Google the title and filetype:pdf and download directly:
  - https://www.securityroundtable.org/wp-content/uploads/2015/09/Cybersecurity-9780996498203-no_marks.pdf
- always check where you’re clicking
- read Foreword, Intro, & Chapters 1-6, 13-14
- consider the labs

University of Victoria


University
of Victoria

Best Practices

- Remember different kinds of controls
  - administrative, procedural
  - technical, logical
  - physical
- COBIT (good practice framework)
- ITIL (IT Service Management)
- NIST (cybersecurity framework)
- ISO/IEC 27001 (information security standard)
- ISO/IEC 27002 (information security standard)

University of Victoria

Best Practices

- CIS (Center for Internet Security; best practices)
- SOX (Sarbanes Oxley)
- SAS70/SSAE16 (Statement on Standards for Attestation)
- PCI DSS (payment card industry data security standard; set of controls)
- FOIPPA (freedom of information and protection of privacy act)
- requires personal information be stored, accessed, and disclosed only in Canada

*** exceptions, amendments (processing, routing)

University of Victoria

Best Practices

Framework Altitudes

Governance Objective

Stakeholder Needs: Value Creation

- Benefits Realization
- Resource Optimization
- Risk Optimization

Governance Drivers

Performance (*Business Goals*)

Conformance (*Legal, Regulatory*)

Enterprise Governance

- Balanced Scorecard
- COSO

Governance of Enterprise IT

COBIT

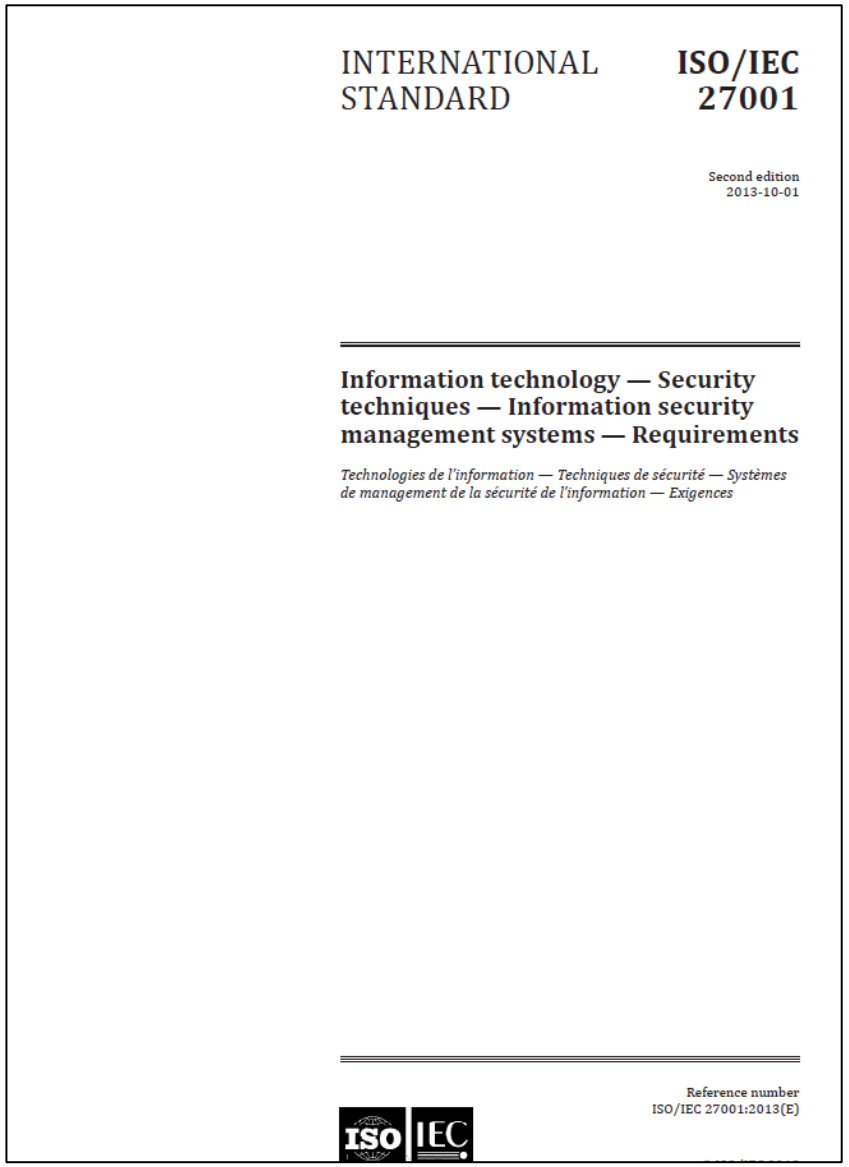
Standards

ISO, NIST, etc.

Good Practices

ITIL, TOGAF, BOKs, etc.

ISO/IEC 27001



INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

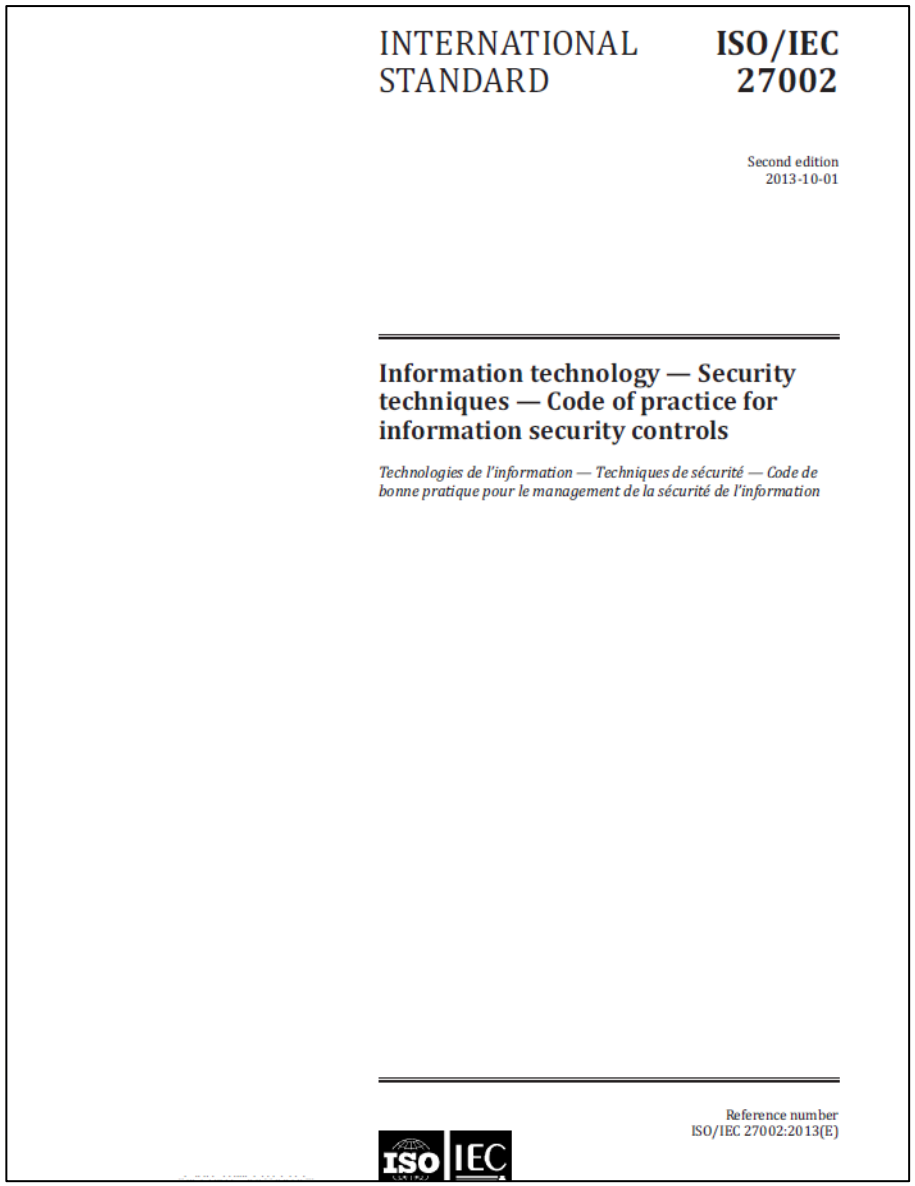
Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)

ISO IEC

Contents

ISO/IEC 27002



INTERNATIONAL STANDARD

ISO/IEC 27002

Second edition
2013-10-01

Information technology — Security techniques — Code of practice for information security controls

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information

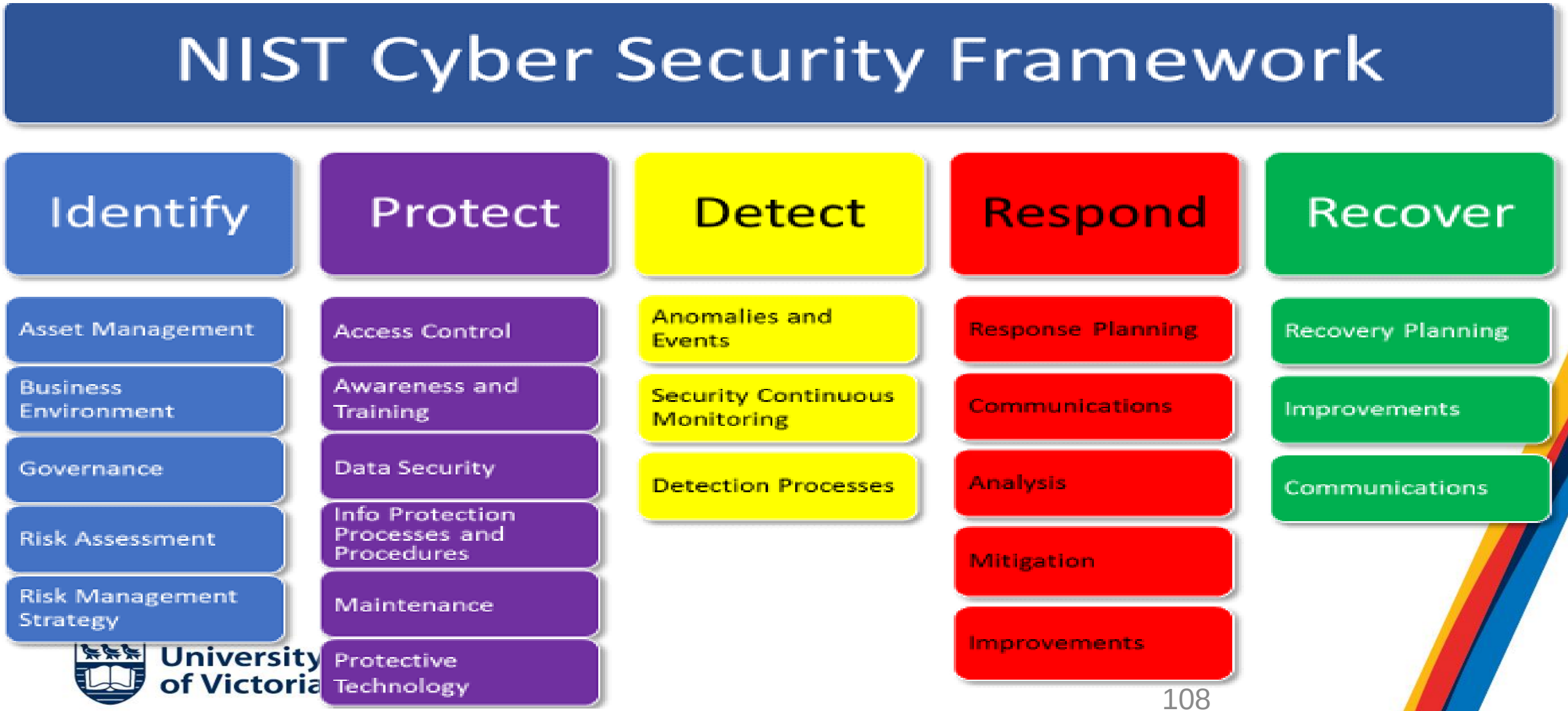
Reference number
ISO/IEC 27002:2013(E)

ISO IEC

Contents

ISO/IEC 27002:2013

NIST



https://securityaffairs.co/wordpress/58163/laws-and-regulations/nist-cybersecurity-framework-2.html

NIST

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.
	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.
	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.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
PROTECT (PR)	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

University of Victoria

NIST

DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

Hygiene Controls (procedural)

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 Controls (technical)

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