Cybersecurity Governance and Career Opportunities

HIMSS Early Careerists Webinar Series

Kevin Deveau

Chair – Distance & Online Learning
Centennial College

Sem Ponnambalam

Co-founder and President
XAHIVE

HIMSS

Welcome

Kevin Deveau

Chair – Distance & Online Learning

Sem Ponnambalam

Co-founder and President - XAHIVE

Learning Objectives

- Distinguish global statistics on cybersecurity breaches & attacks aimed at healthcare sector
- Describe current cyber problems & gaps in healthcare
- Explain the tools needed to stay safe while at home
- Identify new career opportunities in cybersecurity
- Illustrate the type of education and skills needed to be successful in a career in the field

Centennial College

- Established in 1966 as Ontario's first community college
- Offer more than 260 programs (Business, Engineering Technology, Health Sciences, Transportation, Communication, Media Arts and Design)
- Diploma and degree-granting college located in Toronto, ON
- Recognized as most culturally diverse post-secondary institutions in Canada
- Ranked as one of the top 10 research colleges in 2016
- 22,000 FT students and 19,000 PT students

XAHIVE

Company:

- Cybersecurity company providing secure communication, online cybersecurity education and online privacy legislation compliance review for SMB & enterprise clients in Canada, US and the EU from healthcare, finance, legal & entertainment sectors
- xahive was established in 2013 by co-founders Sem Ponnambalam and David Mohajer
- Offices in Canada, NY, LA, London, UK.

Problem:

- xahive clients are professionals globally who need to transact valuable information without risking breaches and cyber attacks while remaining compliant with cybersecurity & privacy regulations in different regions globally

Solutions:

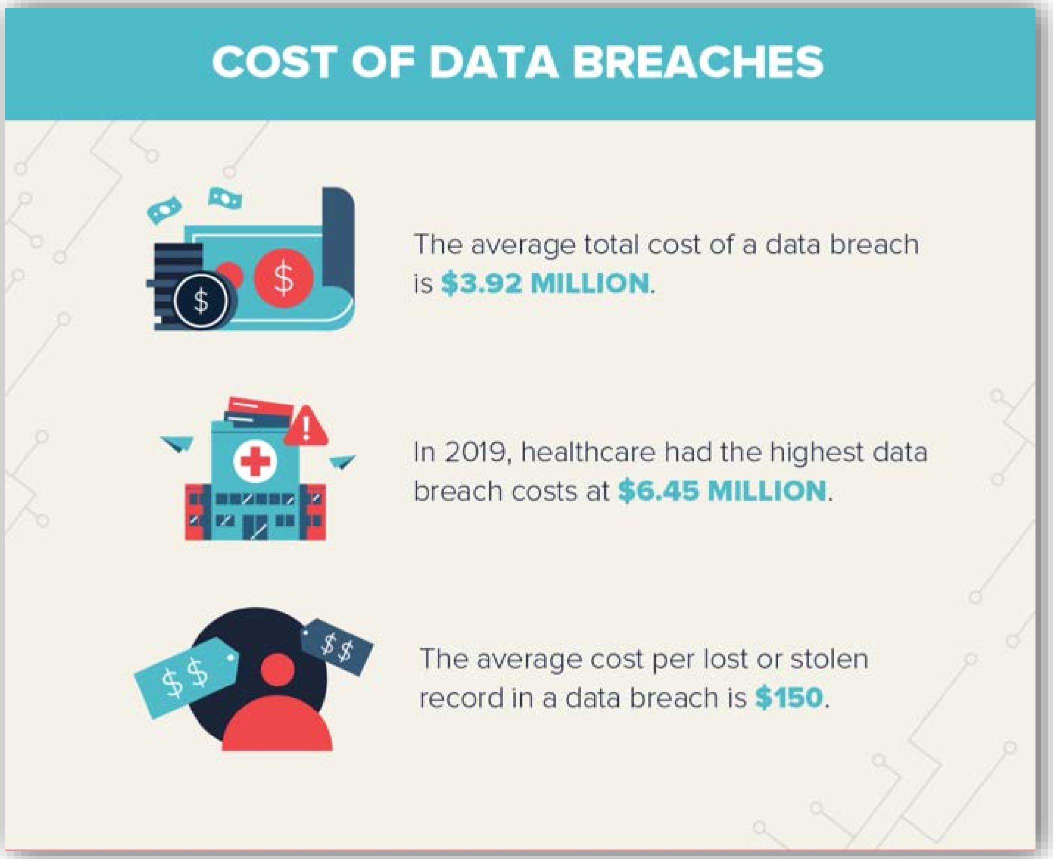
- xahive services: 1) secure communication SaaS 2) online cybersecurity education for non technical professionals (Centennial courses) and (3) online privacy compliance governance audits

Partners/Medical Journal Publications:

- Partnered with BlackBerry & Red Hat globally
- Panelists at the WEF, G20, co-authored in 2 different medical journal articles on cybersecurity

Centennial / XAHIVE Partnership

- Signed MOU to partner on development of flexible and accessible cybersecurity governance training
- Centennial offers a series of micro- and semester-based courses
- Current Offerings – Healthcare, IT, Finance, Internet, Legislation, Ethics
- Developing new courses to meet industry needs



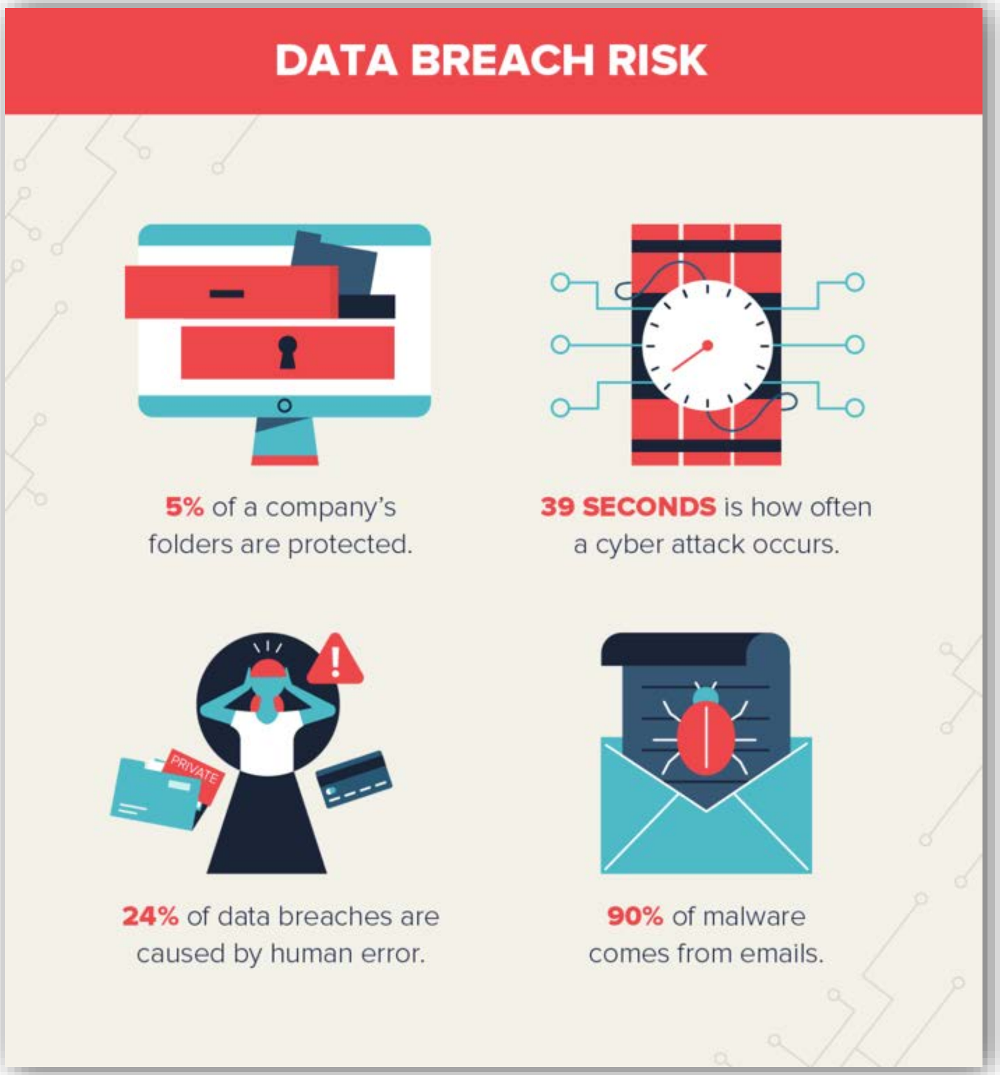
COST OF DATA BREACHES

The average total cost of a data breach is **$3.92 MILLION**.

In 2019, healthcare had the highest data breach costs at **$6.45 MILLION**.

The average cost per lost or stolen record in a data breach is **$150**.

- Attackers will zero in on biometric hacking and expose vulnerabilities in touch ID sensors, facial recognition and passcodes (Experian).



DATA BREACH RISK

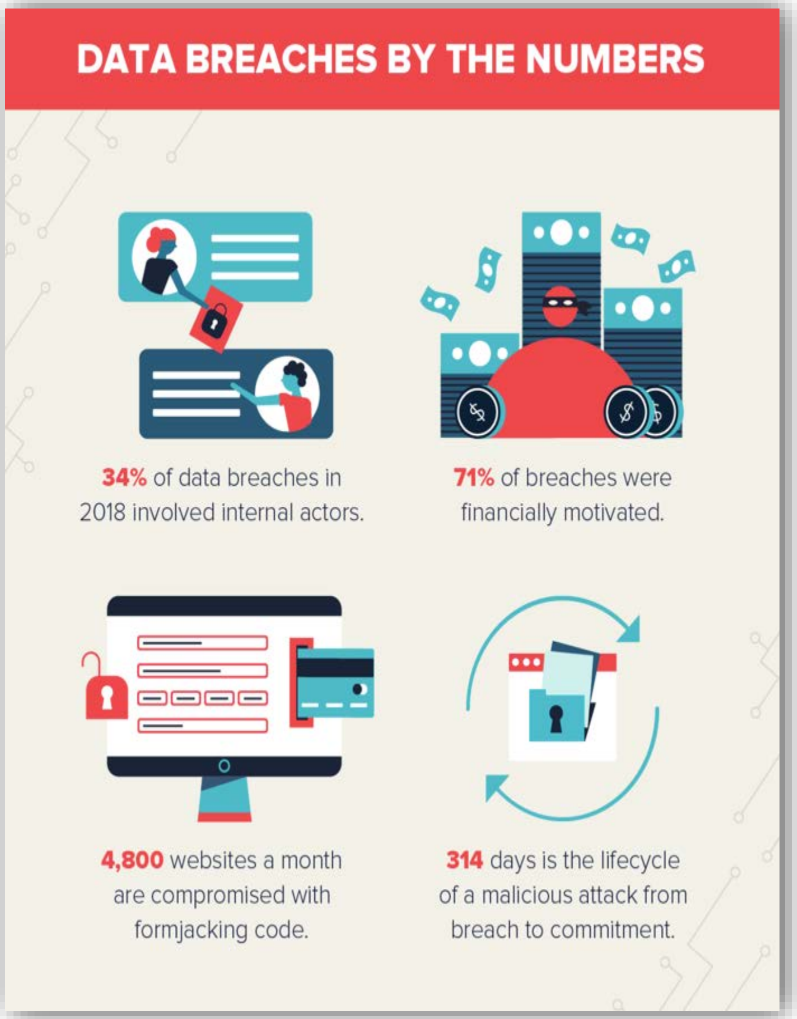
5% of a company's folders are protected.

39 SECONDS is how often a cyber attack occurs.

24% of data breaches are caused by human error.

90% of malware comes from emails.

- A major wireless carrier will be attacked with a simultaneous effect on both iPhones and Android, stealing personal information from millions of consumers and possibly disabling all wireless communications in the United States (Experian).



DATA BREACHES BY THE NUMBERS

34% of data breaches in 2018 involved internal actors.

71% of breaches were financially motivated.

4,800 websites a month are compromised with formjacking code.

314 days is the lifecycle of a malicious attack from breach to commitment.

- A cloud vendor will suffer a breach, compromising the sensitive information of hundreds of Fortune 1000 companies (Experian).

CYBERCRIME is estimated to cost the world **$6 TRILLION** annually by 2021.

Cybersecurity Ventures

- The online gaming community will be an emerging hacker surface, with cybercriminals posing as gamers and gaining access to the computers and personal data of trusting players (Experian).

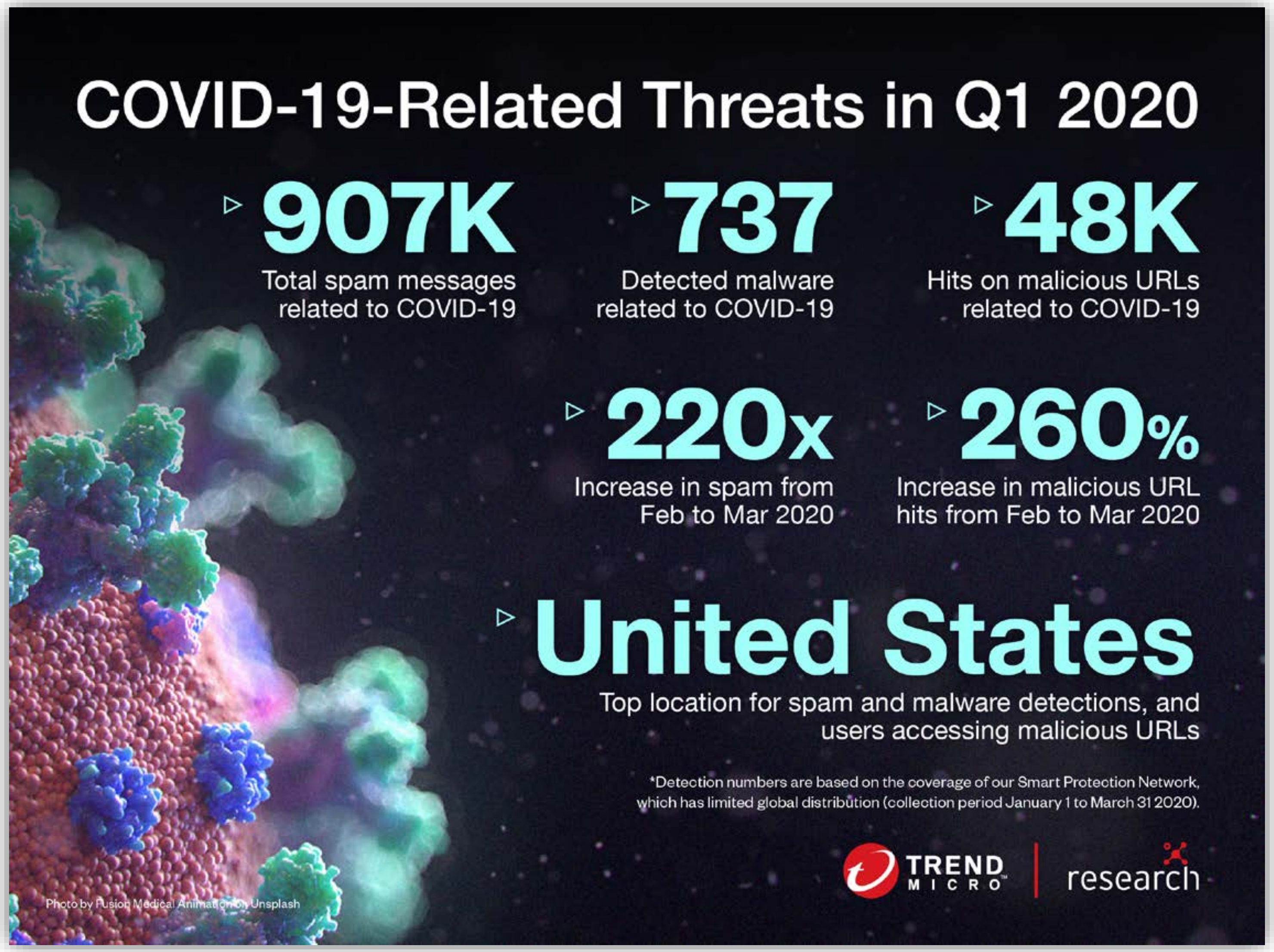
There was an **80% INCREASE** in the number of people affected by **HEALTH DATA BREACHES** from 2017 to 2019.

Statista

Data suggests that **CYBERCRIME** cost businesses over **$2 TRILLION** total in 2019.

Juniper

- Healthcare is the most expensive industry for a data breach at $6.45 million (IBM).



COVID-19-Related Threats in Q1 2020

▷ **907K** Total spam messages related to COVID-19

▷ **737** Detected malware related to COVID-19

▷ **48K** Hits on malicious URLs related to COVID-19

▷ **220x** Increase in spam from Feb to Mar 2020

▷ **260%** Increase in malicious URL hits from Feb to Mar 2020

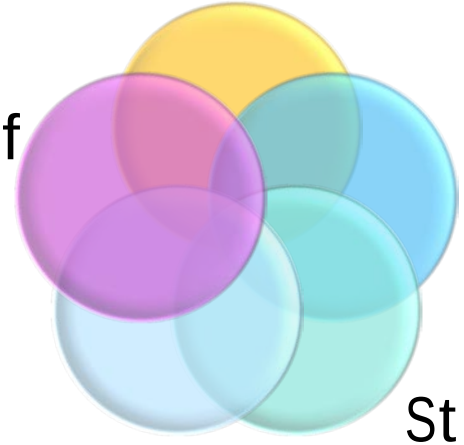
▷ **United States** Top location for spam and malware detections, and users accessing malicious URLs

*Detection numbers are based on the coverage of our Smart Protection Network, which has limited global distribution (collection period January 1 to March 31 2020).

TREND MICRO | research

Photo by Fusion Medical Animation on Unsplash

Who are the Threat Actors?



Hacktivists

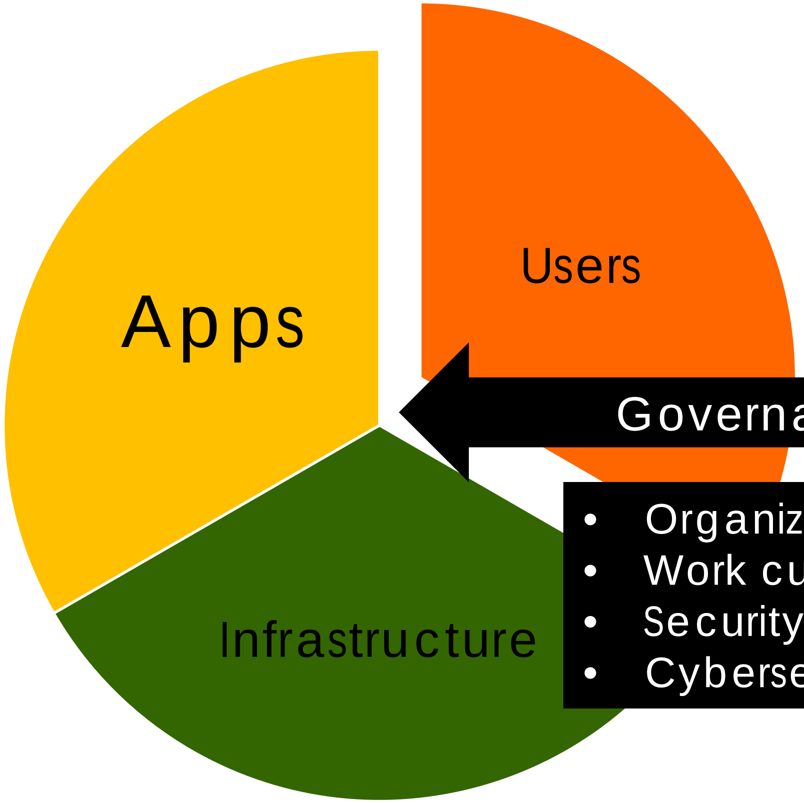
Cyber Criminals

State Sponsored

Hardware Failure

Accidents caused by staff

Cybersecurity Governance



Governance Framework:

- Organizational structure
- Work culture
- Security Awareness
- Cybersecurity governance

Managing how the people, the applications and infrastructure interact.

Cyber Breach vs Cyber Attack

Definition:

- **Cyber attack** is someone attempting to gain unauthorized access to a system
- **cyber breach** is when a Cyber Attack is successful

Example:

- Someone sending you a scam email is an **attack** - if you click the link they provided it would be a **breach**

Who is affected by cyber -breaches?

- It isn’t a matter of “IF” but rather of “WHEN”
- PII, PHI, trade secrets or IP are high risk
- Education-- Legal – Financial – Healthcare – Insurance
- SMEs – Enterprises – Government

Who are you sharing your PII & PHI with?

- Customers
- Social Media
- Online Streaming
- Online Banking
- Online Shopping
- Gaming/Dating Apps
- Job Applications
- College/University Applications
- Medical Doctors Office
- Accounting/Legal Office
- Vendors & Value-Chain

Social Engineering & Business Email Compromise

- 90% of all email is spam and viruses
- 88% of reported phishing is from clicking links
- Average loss to businesses is $42,000 per account
- Average loss to individuals is $4,100 per victim
- 14% reply to malicious text, 60% click the links

How does this stuff work anyways?

PHISHING

- Online form of social engineering (advance pay aka “419” Scam)
- Can be targeted (Spear Phishing) or broad scoped
- Might even be automated via web service / malware

SOCIAL ENGINEERING
The clever manipulation of the natural human tendency to trust.

DEFENSIVE MEASURES

- Common sense rules – *You* are the target of Phishing
- Caveat Emptor – If it looks too good to be true. It’s too good to be true!
- Education is hard to come by without experiencing it yourself – www.419eater.com

How does this stuff work anyways?

People

- Training
- Skills and Qualifications

Technology

- Modern
- Support deployment

Process

- Management
- Governance
- IT Audits

Policies, Plans, Procedures

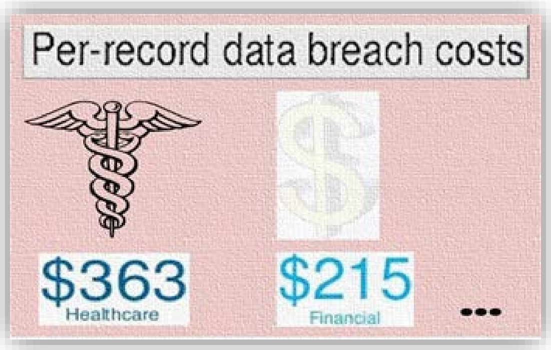
- Who is your Cyber/Privacy Security Official?
- Is there an information breach plan?
- What is your role?
- Practice Bi-Monthly!

Cybersecurity Education for Non IT Professionals

- All members of a covered entity who are likely to obtain access to PII & PHI
- Awareness of threats to PII & PHI
- Password management
- Encryption Communication
- Potential harm of viruses and malware

CENTENNIAL
COLLEGE

Why is Encryption Important



- Tech-savvy customers look for evidence that their businesses are keeping their data secure
- Data safety is quickly becoming a marketplace issue
- Encryption and other security measures are vital to your organization
- The bottom line is that using best practices like encryption to improve data security helps both your organization and entire value-chain be safe
- 84 % organizations are unrealistic & over confident about their cybersecurity skills
- Most organizations detect a cyber breach after 204 days on average once it has occurred

Cybersecurity Best Practices

- Patch management and or certification process.
- Anti-virus/malware/Trojan software installed .
- Host an intrusion prevention solution or a firewall.
- Periodically perform vulnerability scans.
- Use encryption solutions for every workstation.
- Employ a password management system.

Cybersecurity Best Practices

- Review wireless security.
- Use email filtering and Internet traffic filtering.
- Automated scans for malware on network.
- Review cloud storage security.
- Review your remote access for users.

Cybersecurity Best Practices

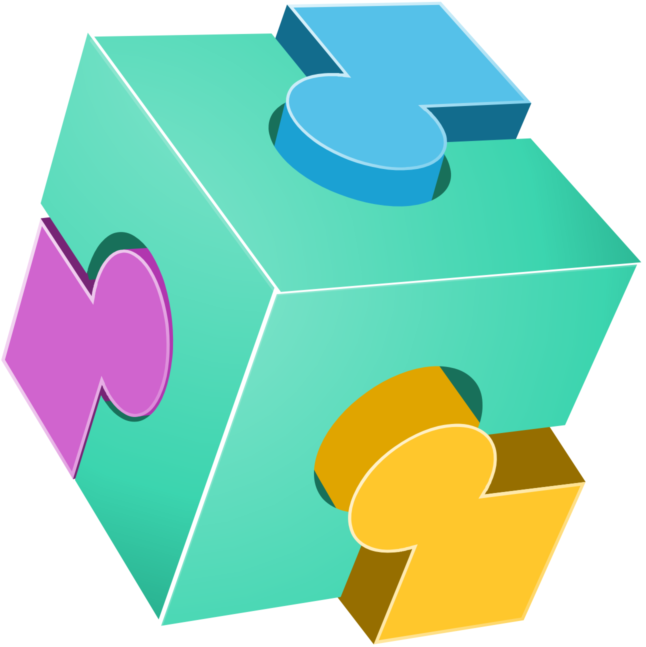
- Daily backups important business data/information
- Set up cyber liability insurance
- Ensure policy in place for regular behavioral reviews
- Ensure vendor information security policy in place
- Your vendors must demonstrate their security practices

Cybersecurity Best Practices

- Your organization has a long-term cybersecurity plan
- Update your data analytics
- Conduct semi-annual audits

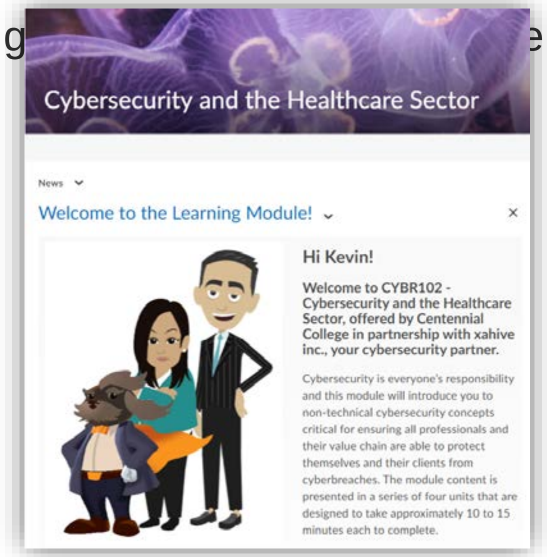
Cybersecurity Best Practices

- Daily review of CVEs
- Use encryption for sensitive business information
- Policy for disposing of old computers & media safely
- Plan for disasters and information security incidents
- Don’t get on conference calls while Alexa, Siri and other AI devices are on



Cybersecurity and the Healthcare Sector (CYBR102)

- Course Learning Outcomes:
- Identify statistics related to security breaches
- Explain the consequences of cybercrime events and their potential impact on an organization
- Outline five common pervasive cybersecurity threats and how to g em
- Describe the common features of data breach scenarios



Cybersecurity and the Healthcare Sector

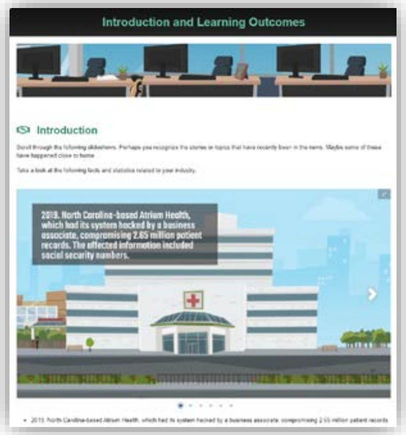
Welcome to the Learning Module!

Hi Kevin!

Welcome to CYBR102 - Cybersecurity and the Healthcare Sector, offered by Centennial College in partnership with xahive inc., your cybersecurity partner.

Cybersecurity is everyone's responsibility and this module will introduce you to non-technical cybersecurity concepts critical for ensuring all professionals and their value chain are able to protect themselves and their clients from cyberbreaches. The module content is presented in a series of four units that are designed to take approximately 10 to 15 minutes each to complete.

Cybersecurity and the Healthcare Sector



Introduction and Learning Outcomes

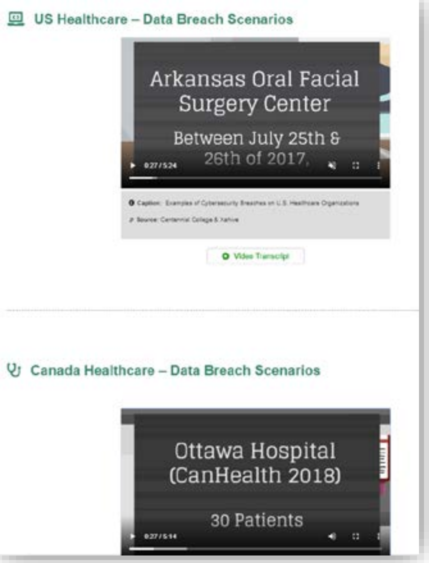
Introduction

Scroll through the following slideshows. Perhaps you recognize the stories or topics that have recently been in the news. Maybe some of these have happened close to home.

Take a look at the following facts and statistics related to your industry.

2019. North Carolina-based Atrium Health, which had its system hacked by a business associate, compromising 2.65 million patient records. The affected information included social security numbers.

- 2019. North Carolina-based Atrium Health, which had its system hacked by a business associate, compromising 2.65 million patient records



US Healthcare – Data Breach Scenarios

Arkansas Oral Facial Surgery Center

Between July 25th & 26th of 2017.

0:27 / 5:24

Caption: Examples of Cybersecurity Breaches on U.S. Healthcare Organizations

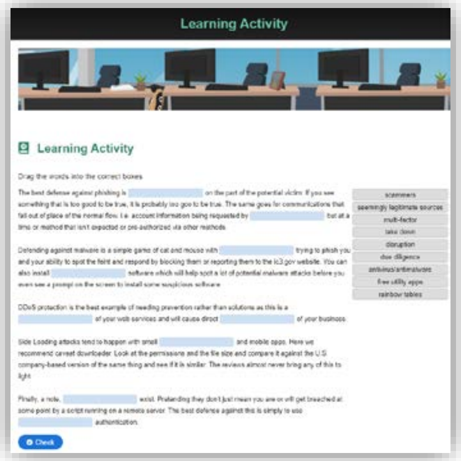
Source: Centennial College & Xahive

Canada Healthcare – Data Breach Scenarios

Ottawa Hospital (CanHealth 2018)

30 Patients

0:27 / 5:14



Learning Activity

Learning Activity

Drag the words into the correct boxes

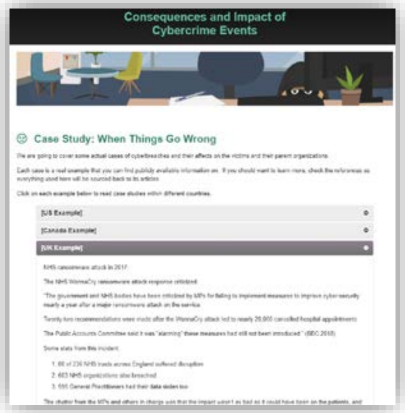
The best defense against phishing is ________ on the part of the potential victim. If you see something that is too good to be true, it is probably too goo to be true. The same goes for communications that fall out of place of the normal flow. i.e. account information being requested by ________ but at a time or method that isn't expected or pre-authorized via other methods.

Defending against malware is a simple game of cat and mouse with ________ trying to phish you and your ability to spot the feint and respond by blocking them or reporting them to the ic3.gov website. You can also install ________ software which will help spot a lot of potential malware attacks before you even see a prompt on the screen to install some suspicious software.

DDoS protection is the best example of needing prevention rather than solutions as this is a ________ of your web services and will cause direct ________ of your business.

Side Loading attacks tend to happen with small ________ and mobile apps. Here we recommend caveat downloader. Look at the permissions and the file size and compare it against the U.S. company-based version of the same thing and see if it is similar. The reviews almost never bring any of this to light.

Finally, a note, ________ exist. Pretending they don't just mean you are or will get breached at some point by a script running on a remote server. The best defense against this is simply to use ________ authentication.



Consequences and Impact of Cybercrime Events

Case Study: When Things Go Wrong

We are going to cover some actual cases of cyberbreaches and their affects on the victims and their parent organizations.

Each case is a real example that you can find publicly available information on. If you should want to learn more, check the references as everything used here will be sourced back to its articles.

Click on each example below to read case studies within different countries.

[US Example]

[Canada Example]

[UK Example]

NHS ransomware attack in 2017

The NHS WannaCry ransomware attack response criticised

"The government and NHS bodies have been criticised by MPs for failing to implement measures to improve cyber-security nearly a year after a major ransomware attack on the service.

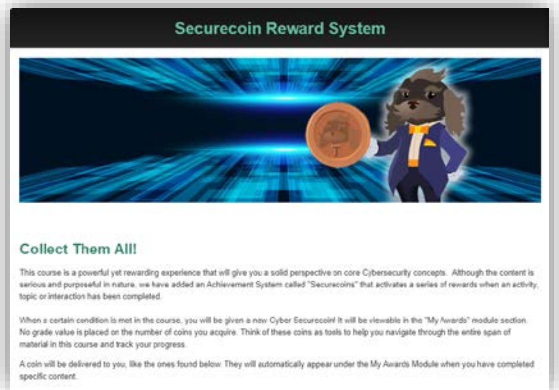
Twenty-two recommendations were made after the WannaCry attack led to nearly 20,000 cancelled hospital appointments.

The Public Accounts Committee said it was "alarming" these measures had still not been introduced." (BBC 2018)

Some stats from this incident:

1. 80 of 236 NHS trusts across England suffered disruption
2. 603 NHS organizations also breached
3. 595 General Practitioners had their data stolen too

The chatter from the MPs and others in charge was that the impact wasn't as bad as it could have been on the patients, and



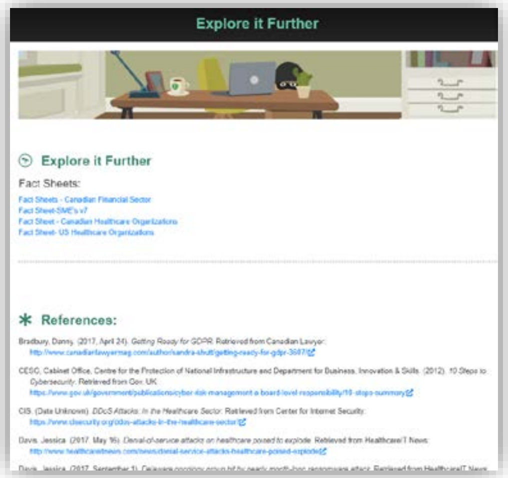
Securecoin Reward System

Collect Them All!

This course is a powerful yet rewarding experience that will give you a solid perspective on core Cybersecurity concepts. Although the content is serious and purposeful in nature, we have added an Achievement System called "Securecoins" that activates a series of rewards when an activity, topic or interaction has been completed.

When a certain condition is met in the course, you will be given a new Cyber Securecoin! It will be viewable in the "My Awards" module section. No grade value is placed on the number of coins you acquire. Think of these coins as tools to help you navigate through the entire span of material in this course and track your progress.

A coin will be delivered to you, like the ones found below. They will automatically appear under the My Awards Module when you have completed specific content.



Explore it Further

Explore it Further

Fact Sheets:

Fact Sheets - Canadian Financial Sector
Fact Sheet-SME's v7
Fact Sheet - Canadian Healthcare Organizations
Fact Sheet- US Healthcare Organizations

References:

Bradbury, Danny. (2017, April 24). *Getting Ready for GDPR*. Retrieved from Canadian Lawyer: http://www.canadianlawyermag.com/author/sandra-shutt/getting-ready-for-gdpr-3687/

CESG, Cabinet Office, Centre for the Protection of National Infrastructure and Department for Business, Innovation & Skills. (2012). *10 Steps to Cybersecurity*. Retrieved from Gov. UK: https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary

CIS. (Date Unknown). *DDoS Attacks: In the Healthcare Sector*. Retrieved from Center for Internet Security: https://www.cisecurity.org/ddos-attacks-in-the-healthcare-sector/

Davis, Jessica. (2017, May 16). *Denial-of-service attacks on healthcare poised to explode*. Retrieved from HealthcareIT News: http://www.healthcareitnews.com/news/denial-service-attacks-healthcare-poised-explode

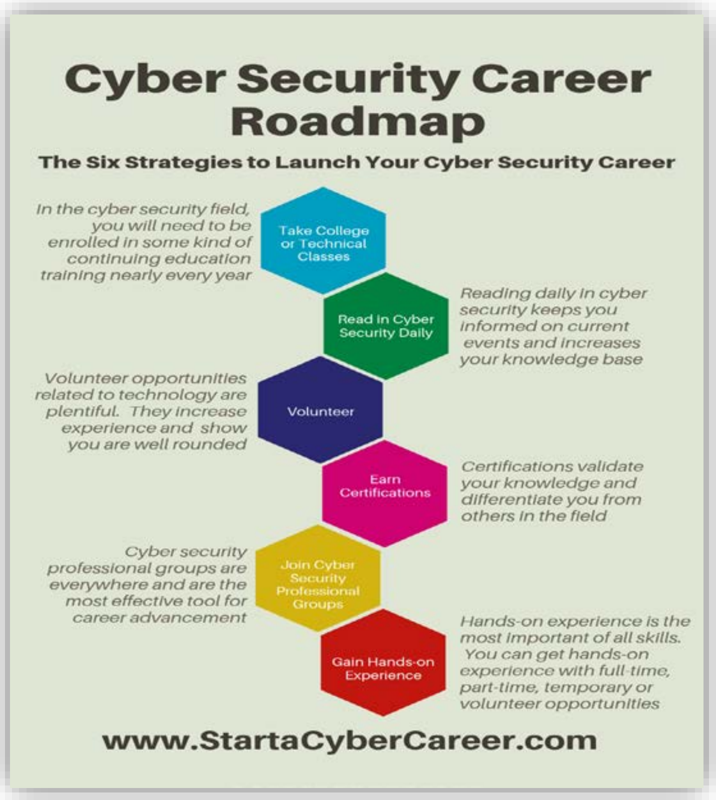
Davis, Jessica. (2017, September 1). *Delaware oncology group hit by nearly month-long ransomware attack*. Retrieved from HealthcareIT News

Cybersecurity Careers

- Cyber Cryptographer
- Cyber white-hacker
- Legal/Privacy Officer
- Compliance Officer
- Cyber Financial Auditor
- Cyber Crimes Official
- Cyber Governance & Educator

Cybersecurity Career Roadmap

- Take programing/legal/auditing courses
- Read about cybersecurity news daily
- Volunteer with an organization
- Obtain cybersecurity certifications
- Find a cybersecurity mentor at a College
- Gain direct hands-on experience either technical or governance



Cyber Security Career Roadmap

The Six Strategies to Launch Your Cyber Security Career

Take College or Technical Classes

In the cyber security field, you will need to be enrolled in some kind of continuing education training nearly every year

Read in Cyber Security Daily

Reading daily in cyber security keeps you informed on current events and increases your knowledge base

Volunteer

Volunteer opportunities related to technology are plentiful. They increase experience and show you are well rounded

Earn Certifications

Certifications validate your knowledge and differentiate you from others in the field

Join Cyber Security Professional Groups

Cyber security professional groups are everywhere and are the most effective tool for career advancement

Gain Hands-on Experience

Hands-on experience is the most important of all skills. You can get hands-on experience with full-time, part-time, temporary or volunteer opportunities

www.StartaCyberCareer.com

Thank You!

CENTENNIAL COLLEGE

1-416-289-5000 ext. 2555
1-800-268-4419

kdeveau@centennialcollege.ca
https://www.centennialcollege.ca/programs-courses/part-time/cybersecurity/

Toronto, ON, Canada

xahive
Your Cybersecurity Partner

1-613-286-6484
1-646-205-2246
1-323-428-9537

sem@xahive.com
www.xahive.com

Canada
Ottawa, ON
US
NYC, NY
LA, CA
UK
London

Certified WEConnect INTERNATIONAL Women's Business Enterprise