*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
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
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
Attackers will zero in on biometric hacking and expose vulnerabilities in touch ID sensors, facial recognition and passcodes (Experian).
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).
A cloud vendor will suffer a breach, compromising the sensitive information of hundreds of Fortune 1000 companies (Experian).
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%** \textbf{INCREASE} in the number of people affected by \textbf{HEALTH DATA BREACHES} from 2017 to 2019. 

Statista

Data suggests that \textbf{CYBERCRIME} cost businesses over $2 \textbf{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).
Who are the Threat Actors?

- Hacktivists
- Accidents caused by staff
- Hardware Failure
- Cyber Criminals
- State Sponsored
Cybersecurity Governance

Managing how the people, the applications and infrastructure interact.

Governance Framework:
- Organizational structure
- Work culture
- Security Awareness
- Cybersecurity governance
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
- 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

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?

**Technology**
- Modem
- Support deployment

**People**
- Training
- Skills and Qualifications

**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
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 guard against them
  - Describe the common features of data breach scenarios
Cybersecurity and the Healthcare Sector
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 programming/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
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

HIMSS