HIROC

Cyber Risk in Healthcare

AOHC, 3 June 2015

Kopiha Nathan, *Senior Healthcare Risk Management and Data Specialist*

James Penafiel, *Underwriting Supervisor, Insurance Operations*

CFPC Conflict of Interest - 1

Faculty/Presenter Disclosure

- **Presenters:**
  - Kopiha Nathan, Senior Healthcare Risk Management Specialist – Data Specialist
  - James Penafiel, Underwriting Supervisor, Insurance Operations

- **Relationships with commercial interests:**
  - **Grants/Research Support:** None
  - **Speakers Bureau/Honoraria:** None
  - **Consulting Fees:** None
  - **Other:** HIROC insures AOHC and few AOHC members

HIROC

CFPC Conflict of Interest - 2

Disclosure of Commercial Support

- **This program has received financial support from none in the form of none.**
- **This program has received in-kind support from none in the form of none.**
- **Potential for conflict(s) of interest:**
  - Speakers have not received any payments or funding from any organizations.
  - AOHC and some of its members are Healthcare Insurance Reciprocal of Canada subscribers. Although no products are being sold, we do offer Liability insurance coverage for not-for-profit healthcare organizations. Our expertise in the sector enables us to provide educational presentations and share our knowledge and experience related to the content covered in the presentation.

CFPC Conflict of Interest - 3

Mitigating Potential Bias

- We will not discuss details of any products sold by HIROC in this presentation.

Objectives

- Identify and understand cyber risks impacting healthcare environment
- Learn about strategies that can be employed by healthcare organizations to minimize cyber risk exposures
- Understand how an AOHC member organization manage cyber risk

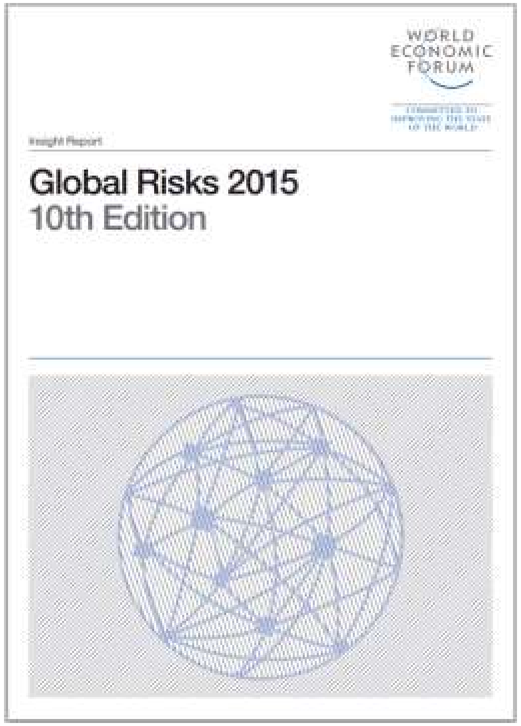
HIROC Disclosure

- We are owned and governed by you
  - Healthcare orgs.
  - Employees, volunteers, boards
  - Midwives
  - MDs in leadership
  - Regulatory colleges
  - National associations
- We are not-for-profit
- We are **passionate** about patient safety

What is cyber risk?

"…any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems. "

The Institute of Risk Management, 2014, p.8



WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Insight Report

Global Risks 2015
10th Edition

Table 1: The Ten Global Risks in Terms of Likelihood and Impact

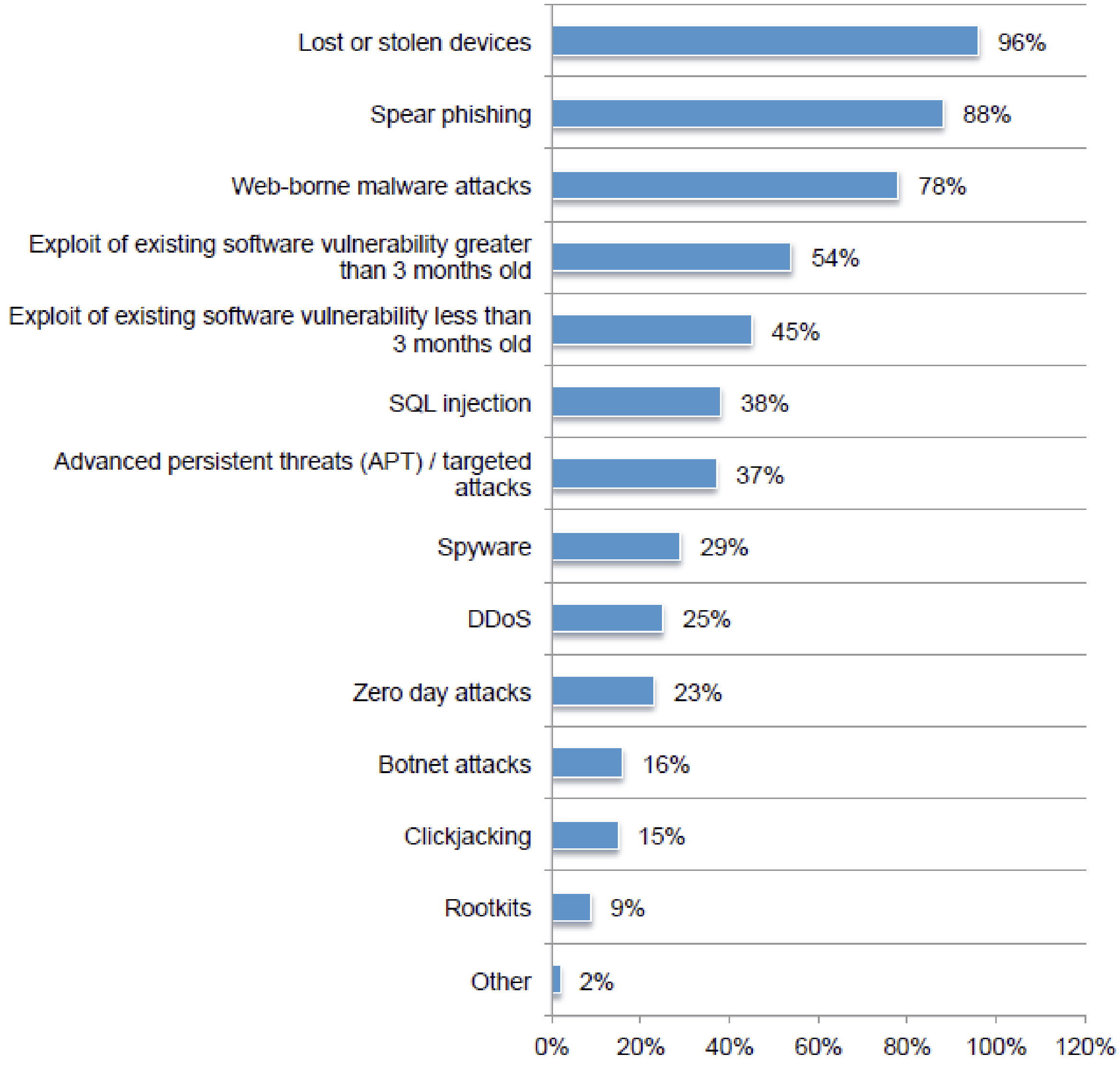
	Top 10 global risks in terms of **Likelihood**		Top 10 global risks in terms of **Impact**
1	Interstate conflict	1	Water crises
2	Extreme weather events	2	Spread of infectious diseases
3	Failure of national governance	3	Weapons of mass destruction
4	State collapse or crisis	4	Interstate conflict
5	Unemployment or underemployment	5	Failure of climate-change adaptation
6	Natural catastrophes	6	Energy price shock
7	Failure of climate-change adaptation	7	Critical information infrastructure breakdown
8	Water crises	8	Fiscal crises
9	Data fraud or theft	9	Unemployment or underemployment
10	Cyber attacks	10	Biodiversity loss and ecosystem collapse

Source: Global Risks Perception Survey 2014, World Economic Forum.

Cyber risks and related losses

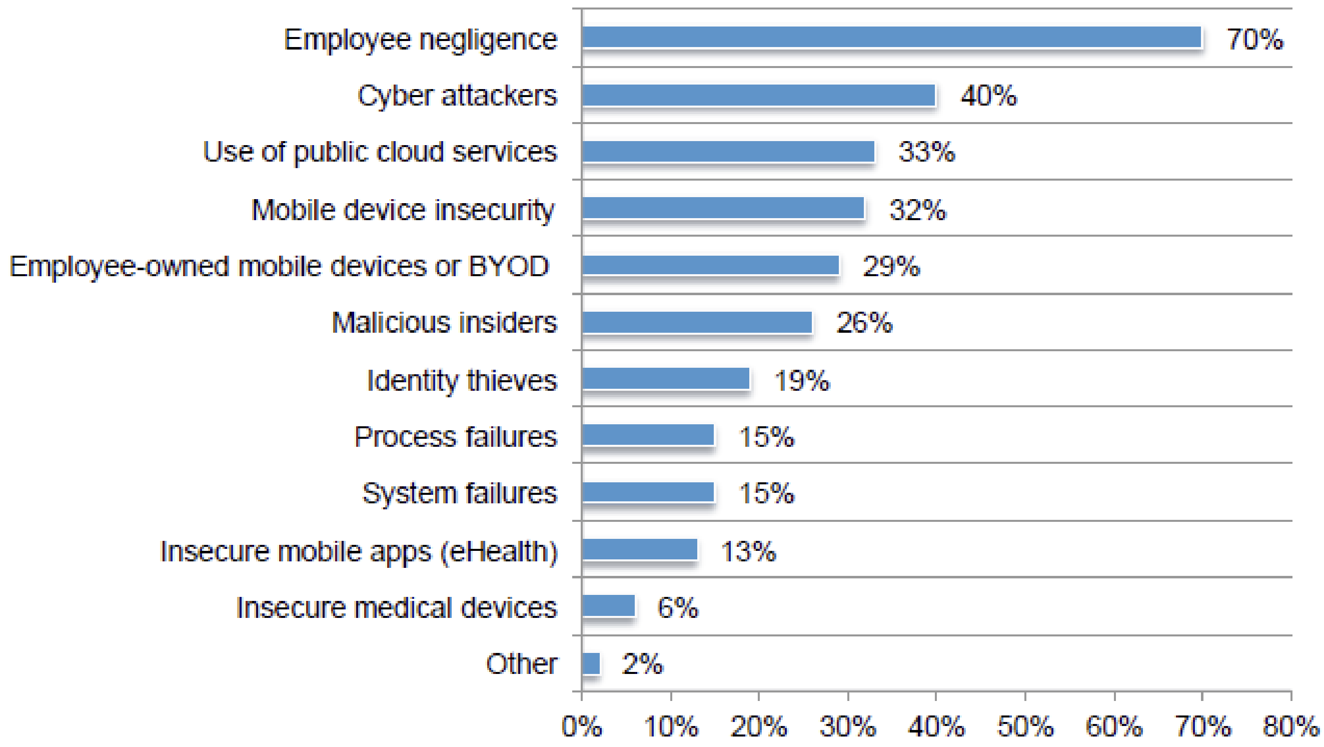
- **Privacy breach** – lost or stolen laptop, tablets or USB keys, inadequate encryption practices and access controls, inappropriate use of e-mails and social media, etc.
- **Fraud or theft** – social engineering scams(e.g. phishing emails, fraudulent calls, etc.), identity or information theft, etc.
- **Network breach or loss** – hacking or virus attacks resulting in loss of network connection, critical information system failure, poor system reliability, data integrity issues, etc.
- **Indirect financial losses –** cost of privacy breach notifications, look backs, recovery of systems or information, etc.
- **Compromised external relations** – loss of reputation or public trust, Information and Privacy Commissioner order, media attention, etc.

Security incidents experienced by healthcare organizations



* Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data
Ponemon Institute Research Report, May 2015 (US)

Security threats healthcare organizations worry about the most



* Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data
Ponemon Institute Research Report, May 2015 (US)

Existing skepticism:

“Could it happen to Canadian healthcare providers?”

Case Study 1

A phishing e-mail was sent to one of the finance staff members that had access to electronic banking. The e-mail contained banking details with a request for the staff member to perform certain activities online. The finance staff member acted on this by following the link in the e-mail to complete the activity.

A month later, finance staff noticed a few questionable payroll transactions processed over the weekend. The staff immediately contacted the bank and confirmed that the account had been compromised.

- **‘Phishing’ – social engineering**
- **Internal education and staff awareness is key to preventing such losses**
- **Segregation of duty in financial area is very important (2 stage banking authorization, by 2 individuals)**

Case Study 2

A methadone clinic had a surveillance camera in the washroom to ensure urine samples provided were not tampered with. They had a simple wireless camera/receiver system installed that had three wireless cameras. Their receivers were connected to a single monitor with no recording devices attached. The images could only be monitored in real time by clinic staff. The system was not connected to a computer or internet.

An individual pulled into the parking lot of the clinic and activated the back up camera in his vehicle and saw the images transmitted from the washroom.

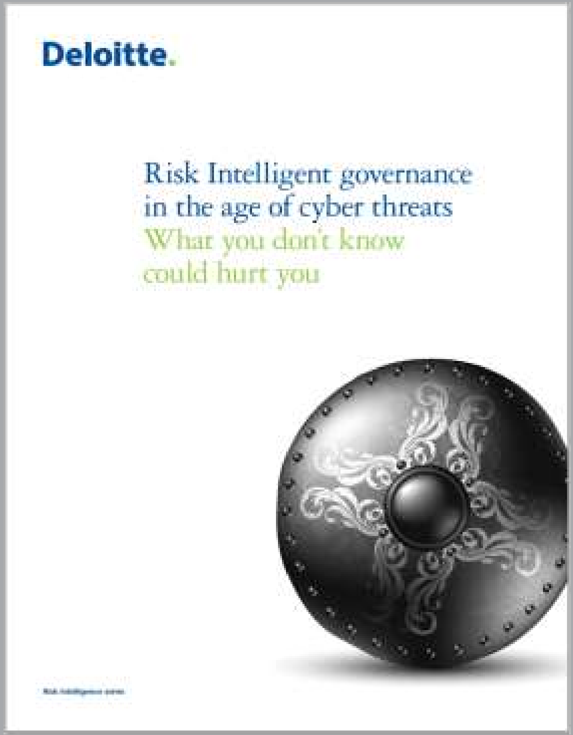
- **IPC order was issued**
- **The methadone Clinic disabled the system immediately and installed a closed circuit television cameras (CCTV)**
- **College of Physicians of Ontario (CPSO) was notified about the breach**
- **CPSO sent a memo to all clinics requesting them to dismantle the wireless surveillance camera**

Case Study 3

An employee lost a USB key while walking from the main office building to the car. The employee reported the incident immediately and took a number of immediate steps to locate the missing memory stick. The USB key contained unencrypted confidential personal information of close to 85,000 patients who had received flu shots.

In addition, it contained user IDs, passwords and security levels of the staff members who had access to a particular Data Collection System.

- **IPC order was issued: PHIPA Order HO-007**
- **Class Action: Rowlands v. Durham Region Health 2012 ONSC 3948**
- **Court approved a settlement whereby each class member would be compensated for demonstrable economic harm as determined by an adjudicator**
- **Class counsel were awarded $500,000 for costs & disbursements**



Deloitte.

Risk Intelligent governance
in the age of cyber threats
What you don't know
could hurt you

[illegible]

"… cyber threats are both a relatively new and constantly evolving source of risk, many organizations may not be as effective at managing cyber threat risk"

Deloitte, 2013

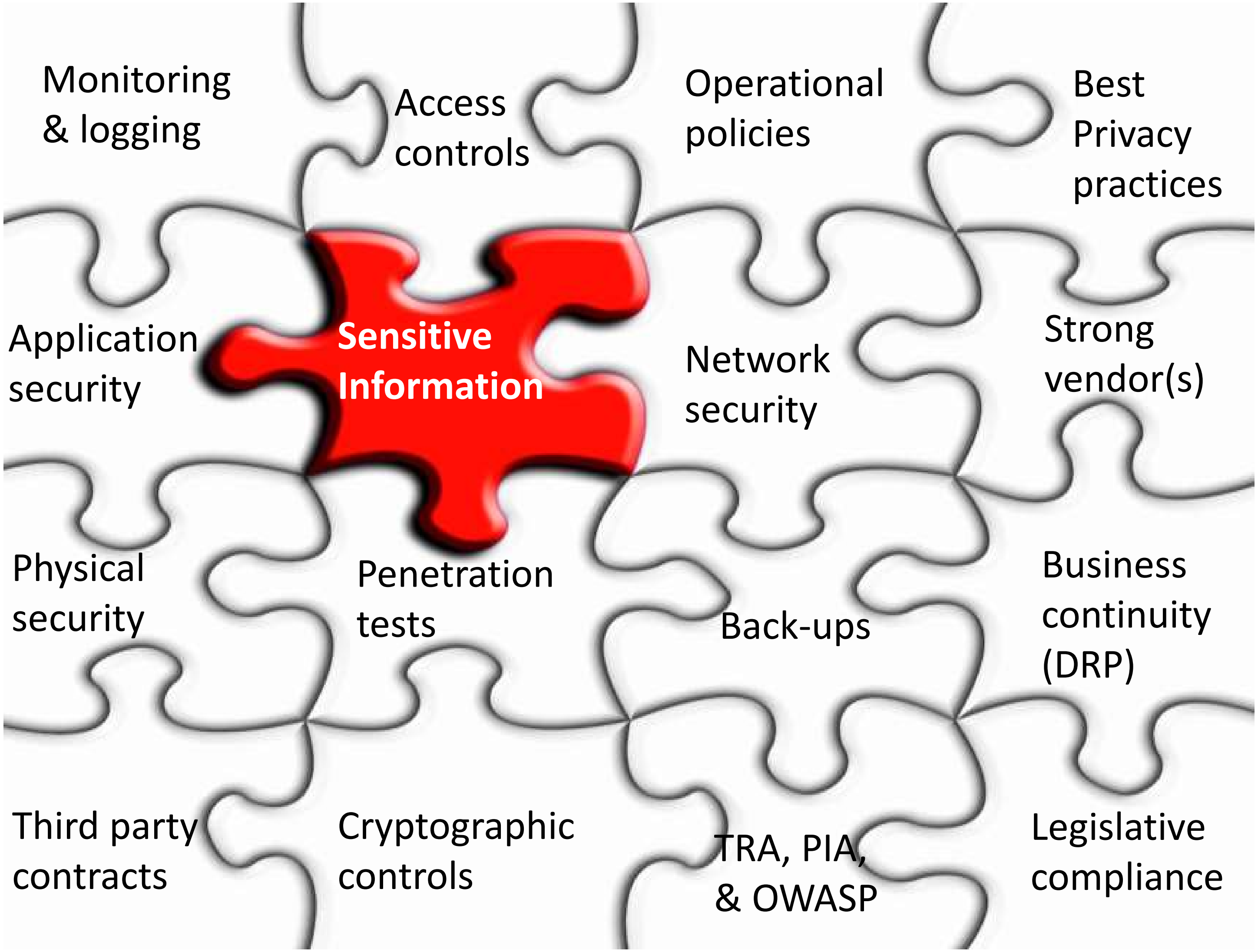
Risk management strategies - *Governance*

- Security starts at the top – cyber risk should be part of the Integrated Risk Management (IRM) program
- Build in accountability for information security across the organization from frontline to executive staff
- Ensure the information security function is visible (Senior management accountability and board engagement)
- Employ *Privacy by design (PbD)** strategies when deploying new strategic projects, processes, systems and information technology solutions

*Information and Privacy Commissioner of Ontario

HIROC

Information Security Strategies



Monitoring & logging

Access controls

Operational policies

Best Privacy practices

Application security

Sensitive Information

Network security

Strong vendor(s)

Physical security

Penetration tests

Back-ups

Business continuity (DRP)

Third party contracts

Cryptographic controls

TRA, PIA, & OWASP

Legislative compliance

Risk controls

- at minimum

- Deploy appropriate anti-virus and firewall(s) solutions – monitor virus and threat notifications
- Monitor and deploy security patches and upgrades in a timely manner
- Design and implement user access controls based on individual's roles/duties
- Enforce strong password policy (e.g. minimum 9 characters long with one symbol, letter and number, avoid vulnerable words in the password, etc.)

Risk controls
- at minimum

- Minimize the use of portable storage devices and adopt encryption practices
- Methodically clear out the data storage when donating, replacing, distributing and disposing owned and leased electronic devices
- Turn on audit functions for all applications, servers, etc. and review/audit user access rights, audit logs of systems containing sensitive information and network access logs regularly
- Proper physical security (i.e. authorized access to server room – access cards) should be in place

Risk management strategies

- Embed best information security practices into the organization's culture and monitor compliance (i.e. policy/procedures/protocols and training)
- Execute strong privacy, confidentiality and data sharing agreements with vendors, partners, third party service providers, etc.
- Conduct Threat and Risk Assessment and Privacy Impact Assessment – on new systems as well as existing systems

HIROC

Risk management strategies

- Ensure appropriate protocols are in place to comply with provincial and federal legislations and regulations
- Implement a disaster recovery plan and test data recovery procedures
- Put in place a security incident response plan (e.g. privacy breach response plan)
- Review current property, general liability and crime insurance coverage to assess if appropriate and adequate insurance is in place to cover Information Technology related losses. Traditional coverage may fall short of covering these losses

Cyber Risk Insurance

Basic insurance program includes Commercial General Liability and Property Insurance. There are potential gaps in coverage from Cyber Risk:

- Breach of privacy due to hacking;
- Damage to others’ intangible property (data is not tangible);
- Web sites that include editorial content (e.g. medical advice,, blogs) that fall outside of the definition of “advertisement”;
- Damage to your own data (not tangible);
- Property coverage requires “direct” physical loss.

Cyber Risk Insurance

Cyber Risk Insurance policies would cover the following:

Liability

- Privacy Injury Liability
- Network Security Liability
- Media or Content Liability

Cyber Risk Insurance

Expenses

- Notification costs;
- Privacy regulatory proceedings;
- Crisis management expenses;
- Cyber extortion expenses.

Property

- Network business interruption;
- Loss or damage to your network.

Additional resources

- Information and Privacy Commissioner of Ontario, https://www.ipc.on.ca/english/Home-Page/
- Office of the Privacy Commissioner of Canada, https://www.priv.gc.ca/index_e.asp
- Canadian Anti-Fraud Centre, http://www.antifraudcentre-centreantifraude.ca/english/index.html
- Canadian Cyber Incident Response Centre (CCIRC), Public Safety Canada, http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-eng.aspx
- RCMP, http://www.rcmp-grc.gc.ca/scams-fraudes/index-eng.htm

Managing Cyber Risk -
The Anne Johnston Health Station
(Community Experience)

Brenda McNeill
Executive Director
AOHC, 3 June 2015

HIROC

CFPC Conflict of Interest

Disclosure of Commercial Support

Presenter Disclosure

Presenter: Brenda McNeill, Executive Director, The Anne Johnston Health Station

Relationships with commercial interests:

- **Grants/Research Support:** None
- **Speakers Bureau/Honoraria:** None
- **Consulting Fees:** None
- **Other:** None

Personal Side of Cyber Risk

- Anne Johnston Health Station
  - Who we are
    - Youth
    - Seniors
    - People with Physical Disabilities
- Personal Health Information (PHI)
- Risk

CYBER Profile

- Electronic Medical Record
  - ASP
- Privacy Impact Assessment (PIA)
  - Policy
- Threat Risk Assessment (TRA)
  - Technology
- Passwords and Fobs + PIN
- Business Intelligence Reporting Tool – BIRT
- Data Sharing Agreements – Circle of Care

Risk Assessment

- Home Visits – iPads
- USB – Encrypted Laptops
- Family and staff
- Need to know - Audits
- Staff Education
- Social Engineering

Kopiha Nathan
Senior Healthcare Risk Management Specialist – Data Specialist, HIROC
knathan@hiroc.com

James Penafiel
Underwriting Supervisor,
Insurance Operations, HIROC
jpenafiel@hiroc.com

Brenda McNeill
Executive Director,
The Anne Johnston Health Station
brendam@ajhs.ca