HLN HEALTH LAWYER NETWORK

Management of Cybersecurity Risk on a Shoestring

Community Health Advancement Conference

May 2018

Agenda

- What is Cybersecurity?
- Why it Matters to You
- Risk
- Management of Cybersecurity Risk on a Shoestring
- Questions
- Contact Information

Disclaimer

HLN is not providing legal advice on the subject matter of this session. For any particular legal problem, you should obtain the advice of a lawyer. HLN holds the exclusive copyright in these materials except when the materials have been provided by another party. It is requested that that you honour this copyright and not reproduce any portion of these materials without the prior written consent of HLN. Contact information is at the end of the materials.

What is Cybersecurity?

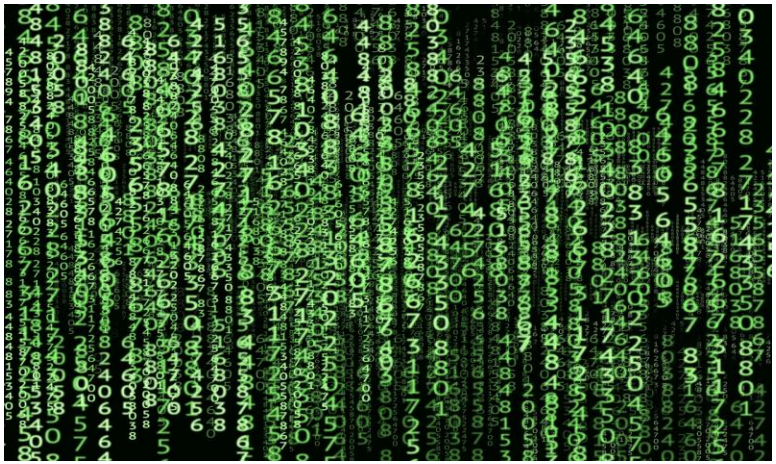
Definitions

- the ability to **protect or defend** an enterprise's use of cyberspace from an attack, conducted via 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***
- the **process of protecting information** by preventing, detecting, and responding to attacks**
- the **preservation of confidentiality, integrity and availability of information** in Cyberspace***

* Committee on National Security Systems (CNSS-4009), **National Institute of Standards and Technology quoted in the Cybersecurity Best Practices Guide For IIROC Dealer Members, ***Multiple sources

Cybersecurity is Not Solely …

- an information technology (IT) problem
- addressed by an IT solution
- the responsibility of your organization's security and/or IT departments



Understanding Cyber Threats*

There are various ways to gain access to information in cyberspace. Attackers can exploit **vulnerabilities in software and hardware**. They can exploit security vulnerabilities by **tricking people** into opening infected emails or visiting corrupted websites that infect their computers with malicious software. They can **take advantage of people** who fail to follow basic cyber security practices, such as changing their passwords frequently, updating their antivirus protection on a regular basis, and using only protected wireless networks.

* Canada's Cybersecurity Strategy: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-en.aspx

Why it Matters to You

Organizational Risk

- **Regulatory Compliance**
  - A health information custodian shall take **steps that are reasonable in the circumstances** to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal. [PHIPA, ss.12(1)]
  - IPC Orders/Decisions: HO-013, PHIPA Decisions 69 and 70
  - IPC Guidance:
    - *Protecting Against Ransomware*
    - *Detecting and Deterring Unauthorized Access to Personal Health Information*

Organizational Risk (2)

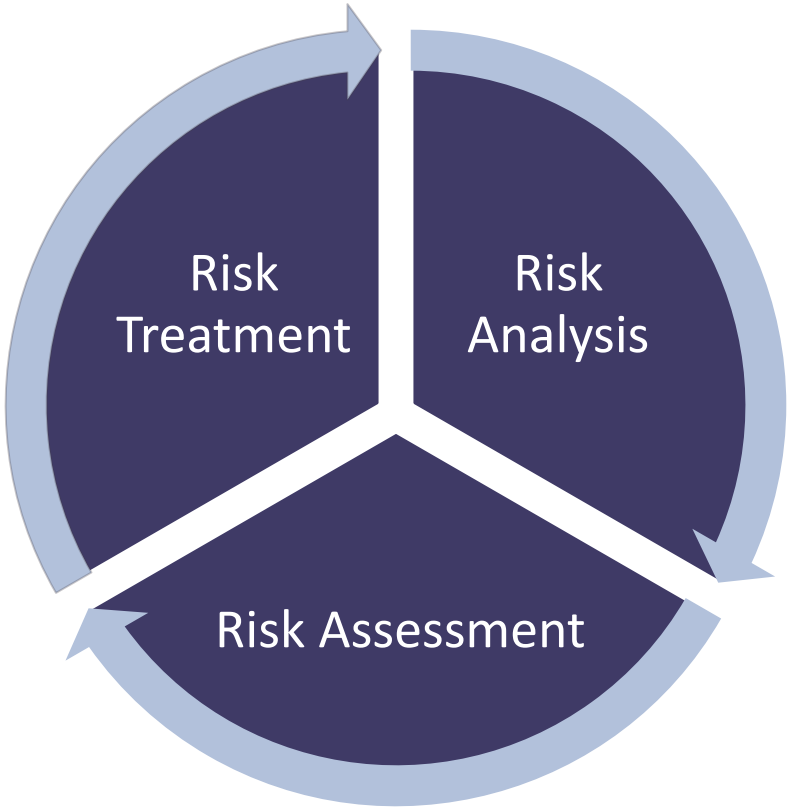
- **Client Trust**
  - your organizations are custodians of some of the most sensitive types of PHI: mental health and addictions
  - clients need assurances that their privacy will be protected and their PHI maintained in a confidential and secure manner
  - client trust in their healthcare providers is necessary in order for them to provide complete and accurate information for diagnosis and treatment

Organizational Risk (3)

- **Legal liability in the event of a breach**
  - client class action lawsuits
    - *Rowlands v. Durham Region Health*, 2012 ONSC 3948
    - *Hopkins v. Kay*, 2015 ONCA 112
  - penalties for convictions of offences under PHIPA
    - $100,000 maximum for individuals
    - $500,000 maximum for corporations
  - potential claims against directors and officers
    - currently no decisions of Canadian courts
    - evolving risk to watch

Risk

Risk Management

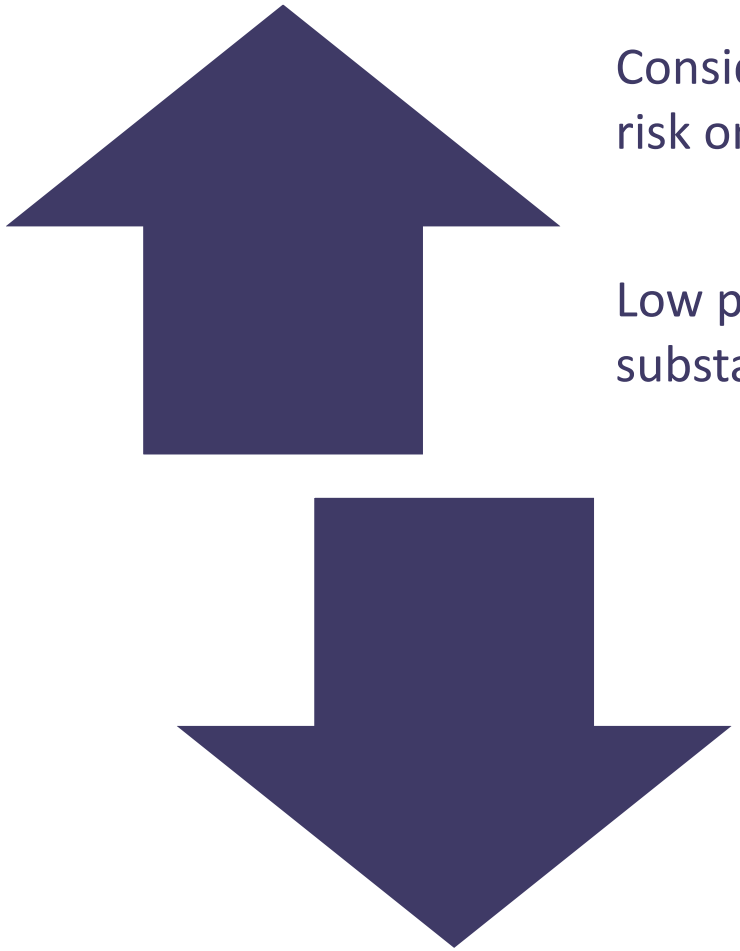


- Adopt a *what if* mentality
- Integral to process

Risk Analysis

- Analysis
  - identify all the potential items that can go wrong
  - estimate the probability of occurrence
  - process
    - simple listing of risk
    - more formal process
      - protocols and procedures
      - more people involved
      - …

Risk Assessment



Considerations of the likely impact of a risk on an organization

Low probability risks may have a substantial impact

High probability risks may have a low impact

Risk Treatment

Risk Treatment	Example
Avoid/Eliminate	Probably impossible
Mitigate/Reduce	Controls
Transfer	Cybersecurity insurance
Accept	Residual risk that remains after all other reasonable steps have been taken

BUT
You cannot begin to treat risk if you are unaware of your risk environment

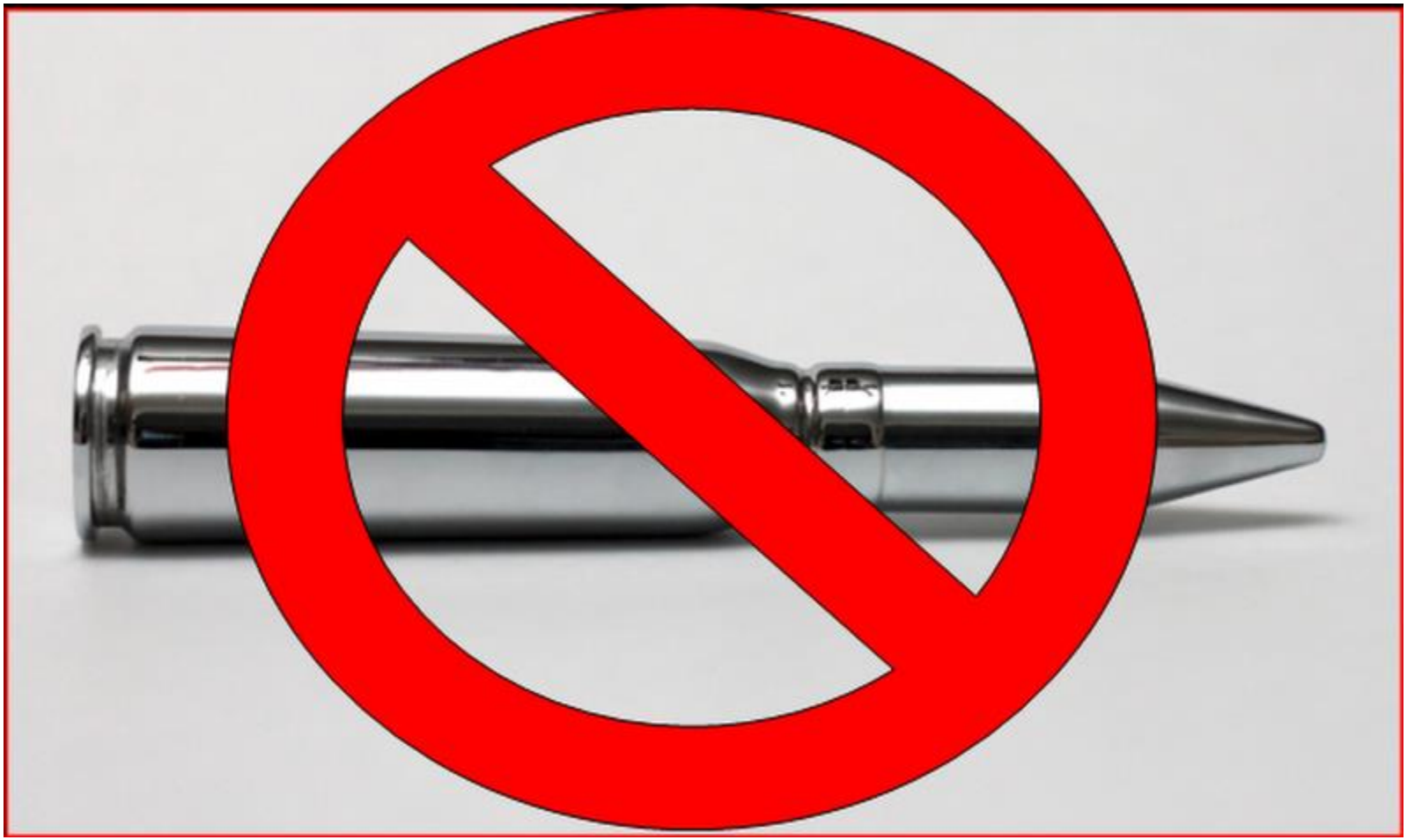
WHAT YOU DON'T KNOW *CAN* HURT YOU!
ANY CYBER RISK TREATMENT MUST BEGIN WITH IDENTIFICATION OF THE RISKS TO WHICH THE ORGANIZATION IS EXPOSED

Management of Cybersecurity Risk on a Shoestring

On a Shoestring

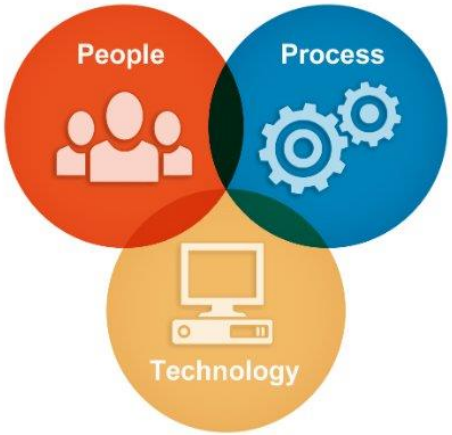
- Balancing act
  - limited resources vs. other requirements
  - cybersecurity can be addressed with limited $
    - not an all or nothing approach
    - prioritize risks
    - consider developing an incremental approach
    - a silo approach will not likely be effective

Technology is Not a Silver Bullet



People, Processes and Technology

- popularised in the late 90s by American cryptographer, computer security & privacy specialist and writer, Bruce Schneier
- the “golden triangle”:
  - the 3 keys to successful project implementations and organisational change
  - back-to-basics approach to solving complex business problems.



Cybersecurity Risk Management Checklist

- People
  - buy in from the Board and senior management buy-in
  - assigned roles
- Processes
  - implement policy through procedures
  - train, train, train
- Technology
  - access controls
  - logging, auditing and monitoring

If Cyber Risk Materializes …

- Be ready to implement your privacy breach protocol
- Management of the breach is just as, if not more important than management of the risk

What to do When faced with a Privacy Breach: Guidelines for the Health Sector

Reporting a Privacy Breach to the Commissioner

Information and Privacy Commissioner of Ontario

Questions?

Contact Information

Phone: 416.576.1154
Email: afineberg@finebergprivacy.ca
debby@shaperopropp.ca
sbirenbaum@sympatico.ca

Website: www.healthlawyernetwork.ca