Cyber Security

co-operators®

Presenters

Ben Anders, Financial Advisor

Anders Insurance Services

Ian Fraser, AVP, Cyber/Technology & Professional Lines

Sovereign Insurance

Sharon Kovacic, Financial Advisor

Sharon Kovacic Insurance Agency

Agenda

- Cyber as a Risk – State of The Market, Emerging Trends
- Cyber Coverages Explained
- Anatomy of a Cyber Event – By the Numbers
- Changes Privacy Legislation & Business Owner Responsibilities
- Key Exposures & Mitigative Risk Management Techniques
- Q&A

State of the Market & Emerging Trends

Emerging Trends

- Trend of Small-Medium-Enterprise being targeted beyond Large
- Convenience/function vs. security
- Attractive targets to gain consumer NPI – Healthcare/Health Services

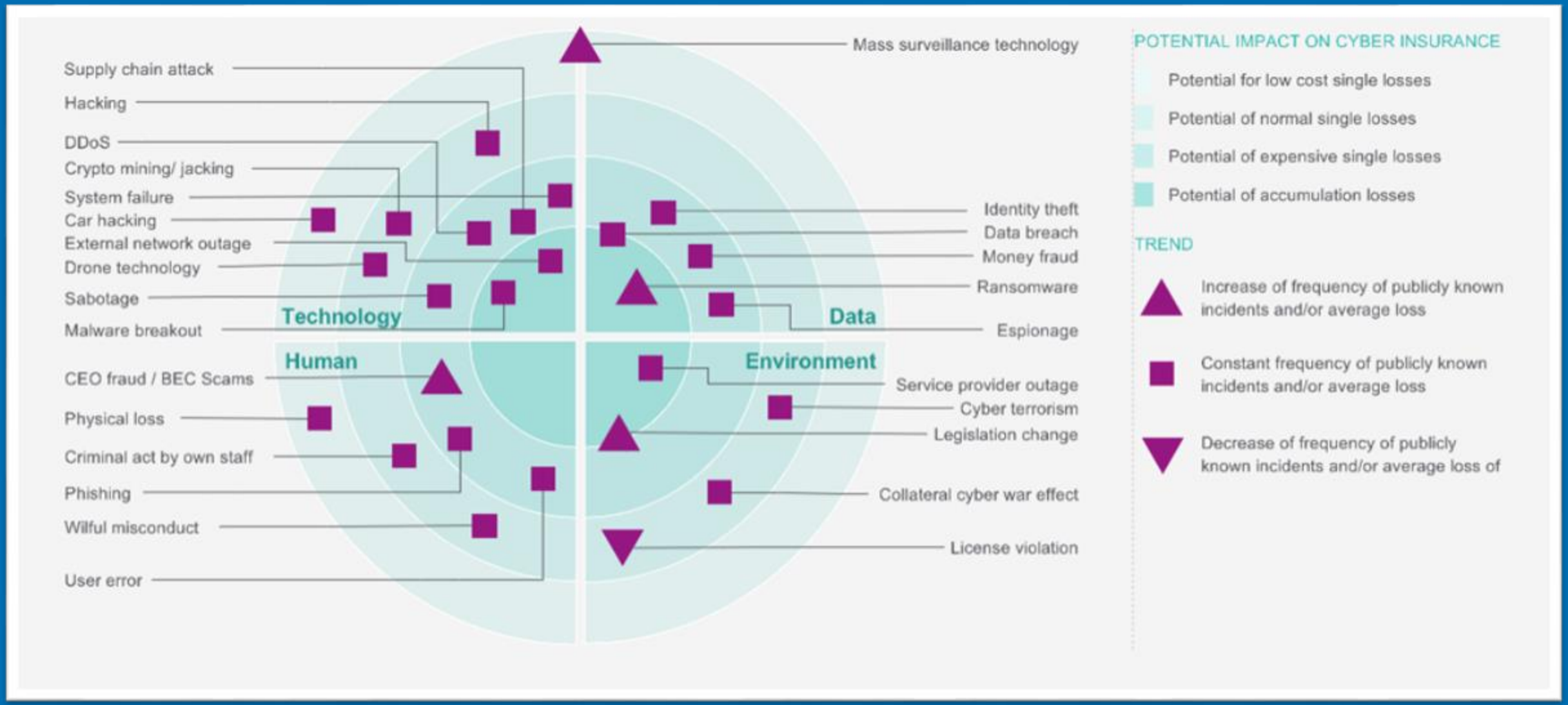
Trends

- Ransomware attacks increased 105% versus 2020—with more than 623 million attacks globally—and the number has tripled since 2019
- Sophistication of phishing campaigns has increased significantly
- OSFI Canadian Cyber results:

Domestic Carriers:	105% LR	(58 M GWP)	**2020**
Foreign Carriers:	469% LR	(164 M GWP)	**2020**
Domestic Carriers:	78% LR	(84 M GWP) +44%	**2021**
Foreign Carriers:	116% LR	(242 M GWP) +47%	**2021**

- Hard market: Rate injection 10%-25% on well priced accounts (shifting risk appetites & risk capacity)

Cyber Security Threat Radar



Cyber Insurance Coverages – Explained

3rd Party - Coverages

Privacy Liability and Network Security	• Protects the Insured against losses for the failure to protect a customer's personally identifiable information (credit card numbers, medical information, name, address, etc.) via theft, unauthorized access, viruses, or denial of service attack.
Electronic Media Liability	• Provides coverage against wrongful publication, defamation, libel, slander, product disparagement, invasion of privacy, misappropriation, copyright infringement, plagiarism, intentional torts and related liabilities.
Regulatory Proceedings Coverage	• Includes civil, administrative proceedings against an Insured brought by or conducted by a regulator. With payments of regulatory fines and penalties.

Cyber Insurance Coverages – Explained

1st Party - Coverages

Privacy Breach Expenses

- Will reimburse you for costs that you incur for expenses or losses as a result of a breach. This includes notification expenses, credit monitoring, data recovery, cyber investigation, and crisis management.

Cyber Extortion

- Triggered when in Insured receives a threat in which the extortionist threatens to either attack the Insured's computer system or to release confidential information in the Insured's possession for the purpose of demanding something of value, usually money.

Digital Assets

- Helps cover a business's costs following a data break or cyberattack. It can help pay for data recovery, restoration or recollection that have been altered, corrupted, destroyed, disrupted, deleted or damaged. This could include software or other information stored electronically.

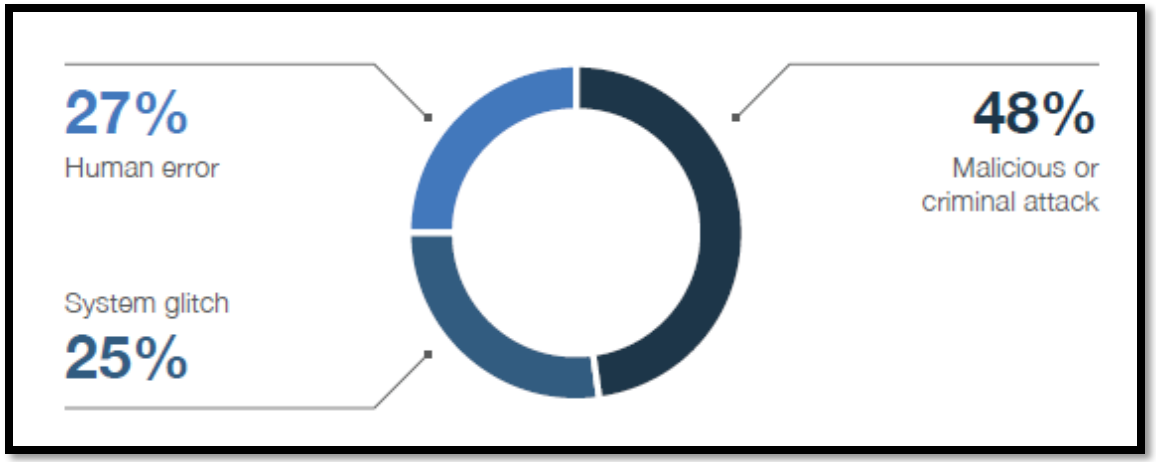
Business Interruption

- Occurs when a company has a loss of income as the direct results of a system failure or impairment due to a failure of network security. Covered losses include net profit before taxes and extra expenses arising out of the interruption of network service due to an attack on a company's network.

Anatomy of a Cyber Event

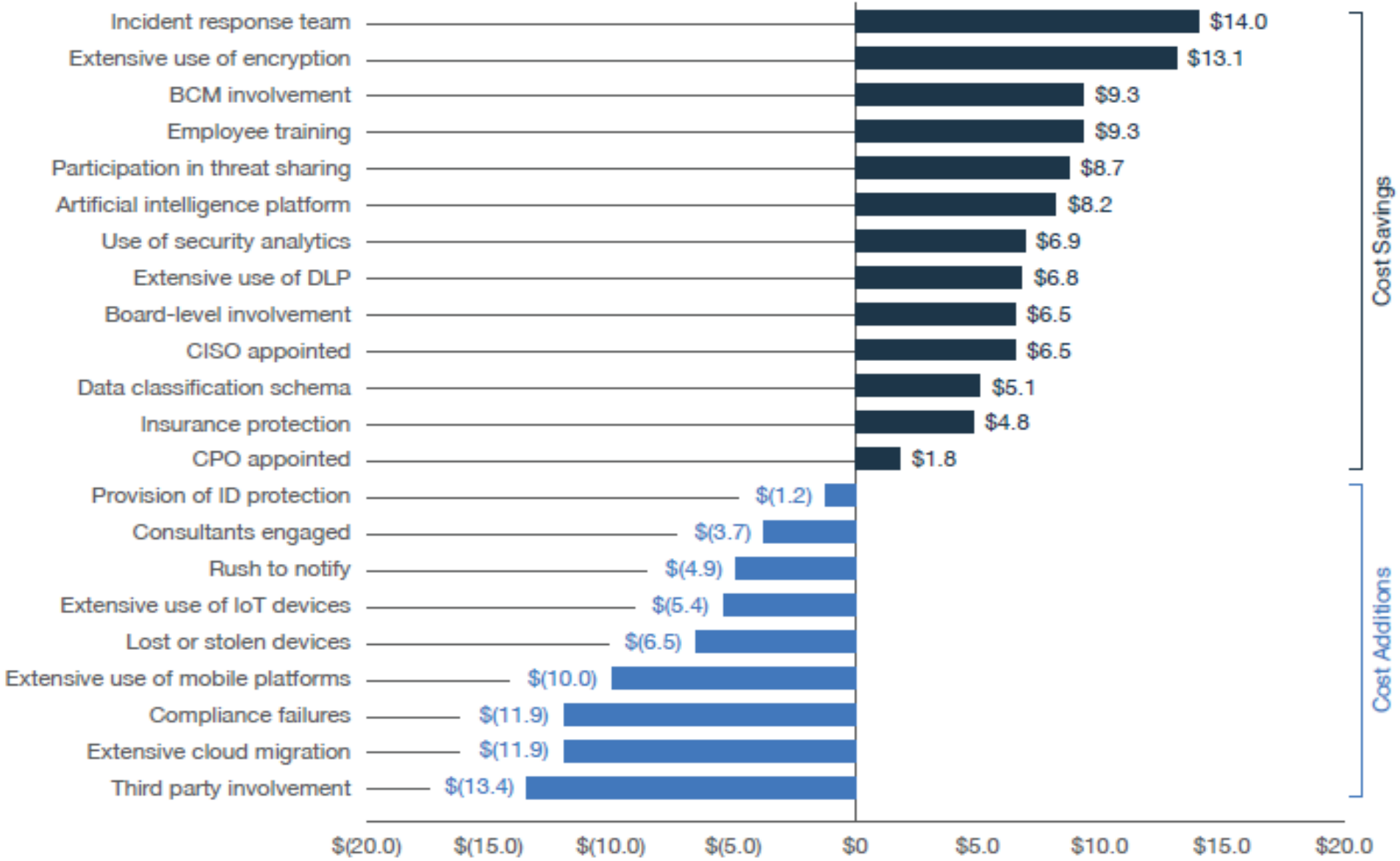
Ponemon Study: survey includes 477 companies of which 28 are Canadian

- Privacy Breach/Loss or Theft of Data total average cost of a breach in Canada is $4.74M
- ~50% of all breaches were caused by malicious or criminal attacks
  - Cyber Extortion/Ransomware/Hacking
- Mean time to identify a breach was 181 days
- Mean time to contain a breach is 69 days
- $202 average cost per record lost or stolen - $86 is direct and $116 is indirect
- 22,275 records breached on average



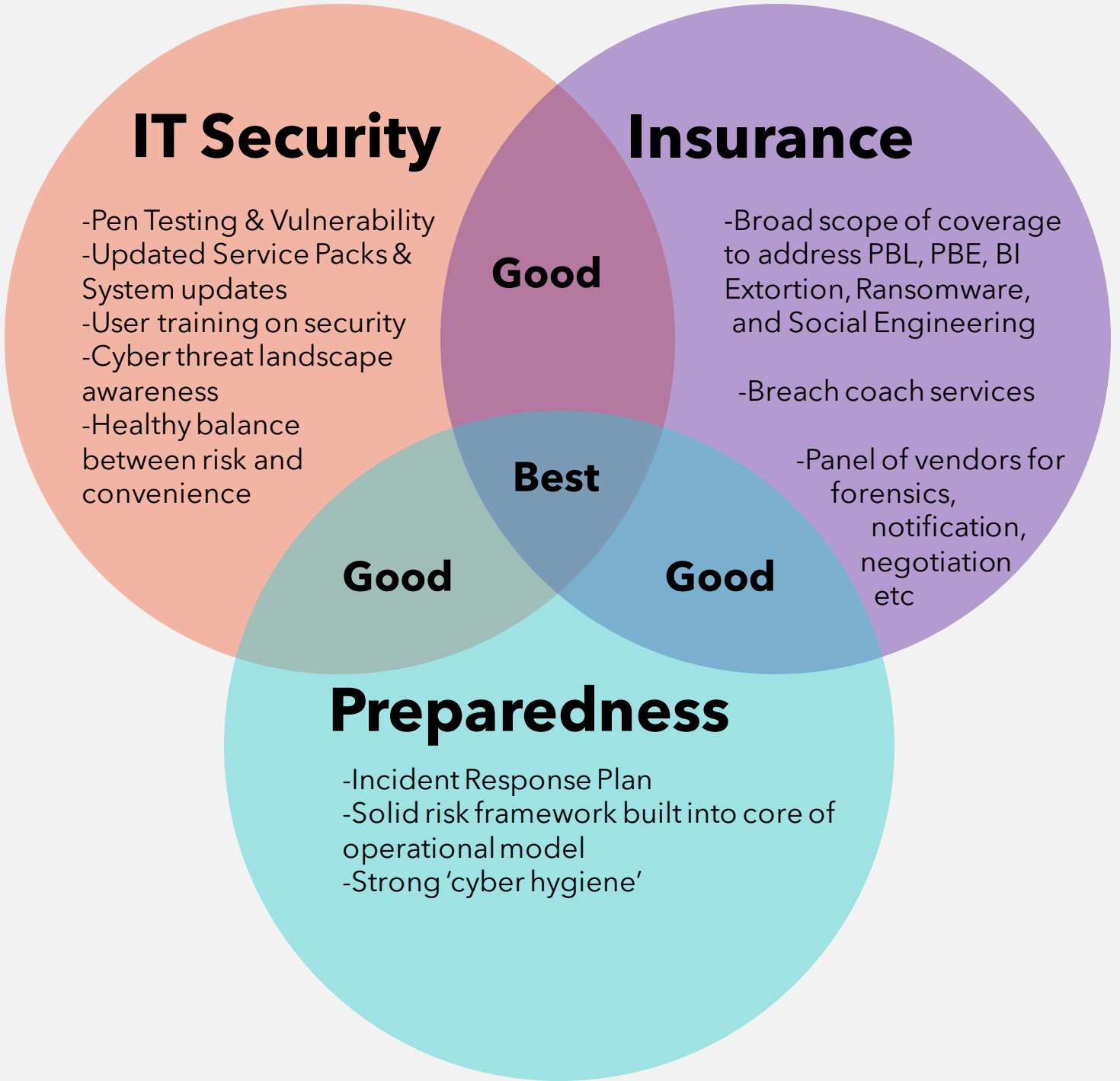
Impact of a breach for small business can be catastrophic and can put them out of business...

Factors that impact the cost of a breach



Ponemon Institute LLC – 2018 2018 Cost of a Data Breach Study – sponsored by IBM

How best to protect ourselves...



Canada's Privacy Law

- **The Privacy Act**
  - Governs and Protects the Federal Government and how they collect and use your information.
- **Freedom of Information and Protection of Privacy Act** (FIPPA)
- **Personal Information Protection and Electronic Documents Act** (PIPEDA)
  - Governs how the private sector collects, uses or discloses personal information.
  - Digital Privacy Act (Bill S-4) – Effective June 2015
    - Amendment to PIPEDA regarding mandatory notification, breach record keeping and Privacy Commissioner powers.
    - As of November 1, 2018, organizations subject to The Personal Information Protection and Electronic Documents Act are required to report to the Privacy Commissioner of Canada breaches of security safeguards involving personal information that pose a real risk of significant harm to individuals.
- **Provincial Privacy Acts**
  - AB, BC, QC have provincial equivalents
- **Provincial Health Privacy Acts**
  - ON, NB, NFLD have mandatory reporting requirements

Mandatory Notice Requirements

When do you have to notify?

- If a “real risk of significant harm” has been found
- Malicious attacks increase this factor vs employee error situations

To whom?

- Privacy Commissioner or other regulatory bodies as required.
- Individuals

How can notification take place?

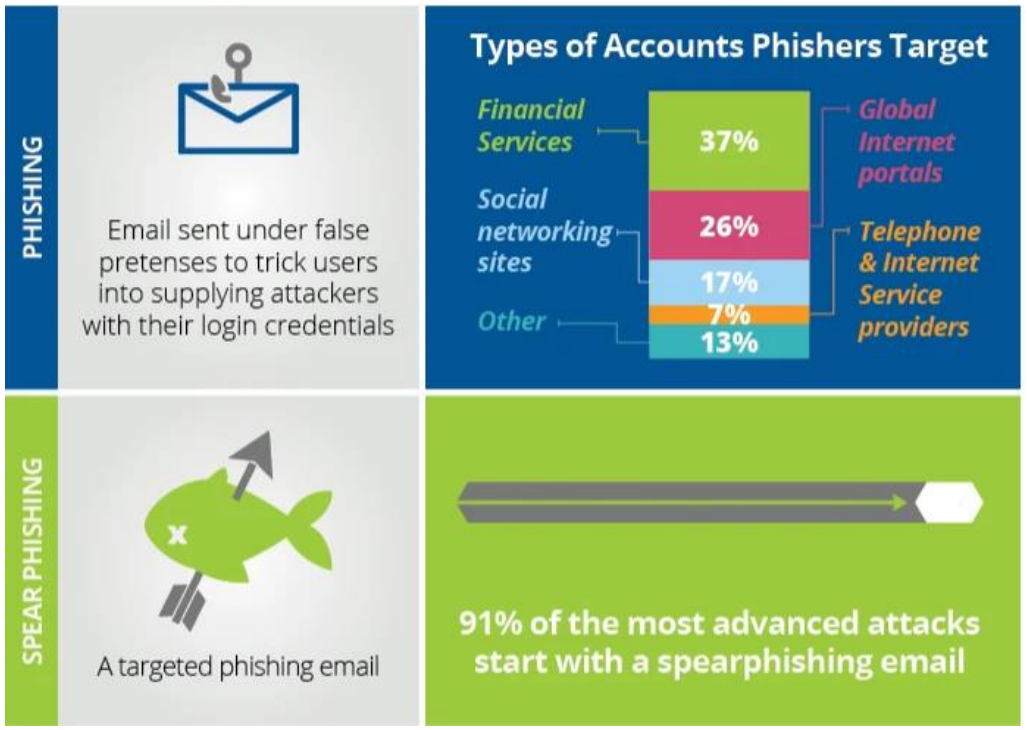
- Internally, by email, phone, letter
- With a third-party mailing or call centres, or
- Broad media reach as notification - website, newspaper

How quickly does notification have to occur?

- As soon as feasible, don’t wait for the Privacy Commissioner!

Top Trending Threats / Exposures

Social Engineering: While many hacking methods are technical in nature, social engineering exploits a human vulnerability. In a social engineering attack people are tricked into revealing sensitive information, opening malicious files, or transferring funds to a perpetrator who might be posing as a supplier, the company's CEO, or someone from the IT team, for example.



Top Trending Threats / Exposures

Social Engineering (continued):

What can we do to help ourselves?

- ✓ Delete any request for personal information or passwords
- ✓ Reject unsolicited offers to help
- ✓ Set your spam filters to high
- ✓ Secure your devices
- ✓ Always be mindful of risks & educate, educate, educate!

Top Mitigation Techniques

(applicable to all threats)

Architecture	**Intrusion Detection/Intrusion Prevention**	**Multi-factor authentication**	**Network Segmentation**	**Sophisticated backups**
Policy / Governance	**Prompt system updates & patching cadence**	**Least-privilege security principles**	**Incident Response Plan**	**Regular Testing & Validation**

Questions

co-operators®