Frank Cowan Company

# Privacy & Personal Information:
# An Emerging Risk for Municipalities

AMO

August 2014

# LAS Partnership

- Why?  Municipalities must be aware of new and emerging risk management issues
- Together we can promote education, knowledge, and best practices, about municipal risk
- Partnership includes presentations at various LAS events and other forums to encourage learning related to organizational risk management

***Through education, there is an opportunity to make a positive difference in every municipality across Ontario.***

# The Legal Framework

- Privacy Legislation
  - Privacy Act, R.S.C., 1985, c. P-21
  - Personal Information Protection and Electronic Documents Act S.C. 2000, c.5 (PIPEDA)
  - Freedom of Information and Protection of Privacy Act R.S.O. 1990, CHAPTER F.31 (FIPPA)
  - Personal Health Information Protection Act S.O. 2004, CHAPTER 3, SCHEDULE A (PHIPA)

- Jones v. Tsige
- New Anti-spam legislation
- Class Actions

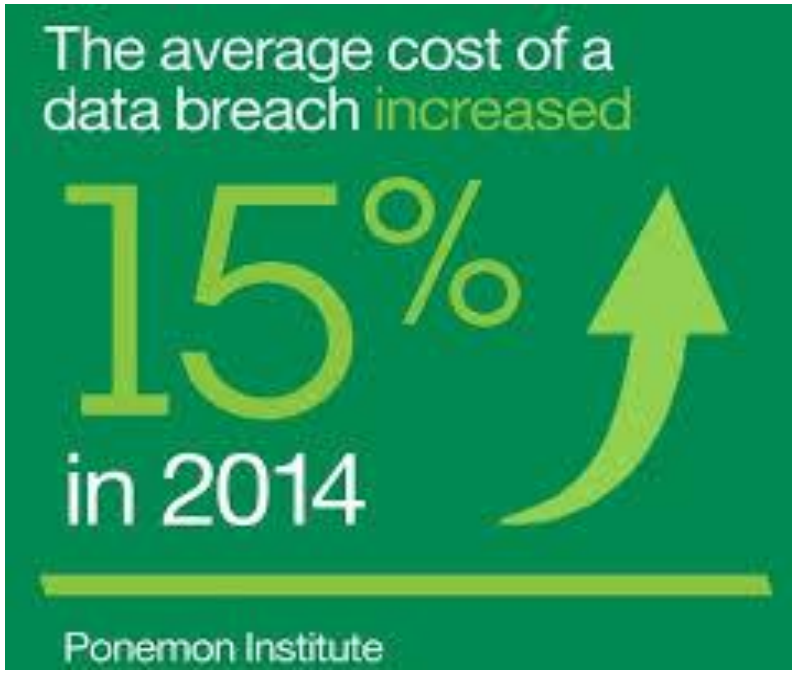
# Privacy Breaches

# What is a ‘Privacy Breach’

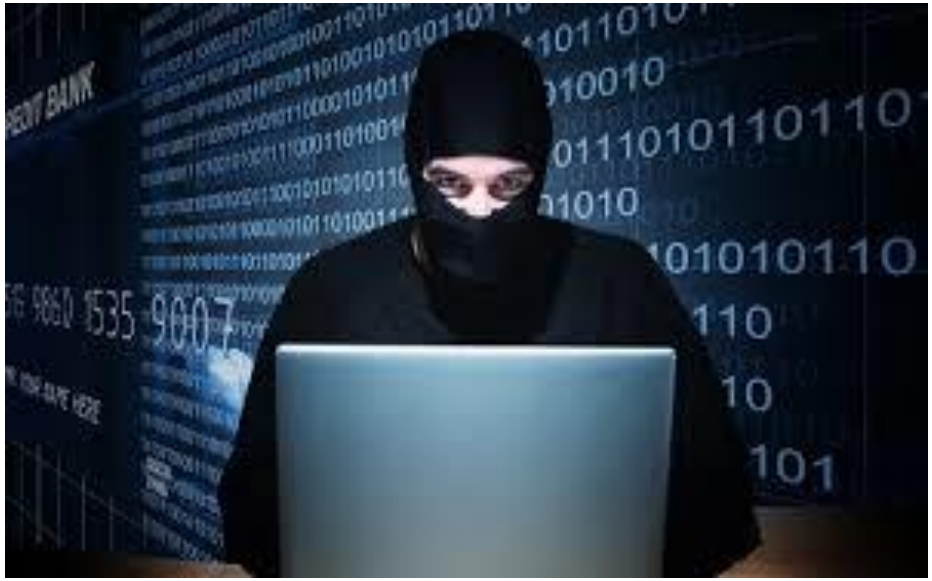
- A privacy breach is the result of an unauthorized access to, or collection, use or disclosure of personal information.

- Such activity is “unauthorized” if it occurs in contravention of applicable privacy legislation.

# Cost of Privacy Breach



# Risk Exposures



# What are the Key Risk Areas or "Threat Environments"?

- Social Media/ networking
- Internal
  - Rogue Employees/ disgruntled employees
  - Careless Staff
  - Human error
  - Lost, stolen or discarded devices
  - Mobile devices – prone to loss and theft; also, they are always on, so more vulnerable to network attacks

- External
  - Organized Crime (foreign & domestic)
  - Hackers

- Technology
  - Viruses
  - Structural vulnerability & Systems error
  - New technology risks
    - Cloud computing - shared public infrastructure, limited control of services/ data flow
    - BYOD – use of personal devices on organizations network
    - Working from home - what sort of security/ management is in place

- Old School
  - Laptop theft
  - Dumpster Diving
  - Phishing

- “…while security products and technology could have mitigated many of these unfortunate events, we are seeing more than ever how systems interconnectedness, poor policy enforcement, and human error, if far more influential than any single security vulnerability…”

  - IBM on the several high profile businesses that have had to deal with the fallout of leaked passwords and other personal date in 2012

# Mitigating the Risk

# Mitigating the Risk

- Risk management is the responsibly of the entire organization.

- As new technologies and social media become increasingly predominant, each employee must be accountable for protecting the information, reputation, and security of the organization.

# Mitigating the Risk

- Examine internal practices
- Change passcodes when someone leaves, change admin passcode when IT staff leave
- Screen potential employees, have strong non-disclosure clauses in your employment agreements
- PCI – security standards counsel, look to for anytime you are accepting a credit card payment
- Have policies and procedures in place that deal with privacy, cyber risks and what to do when a breach occurs

# Creating a Privacy Policy

1. Appoint a chief privacy officer.
2. Ensure that the collection of information is appropriate.
3. Periodically do risk assessments and introduce rules and controls for privacy risk management.
4. Create introductory and refresher privacy training and ensure that any new staff, volunteer or contractor receives the training.

5. Periodically audit the enforcement and use of the privacy policy by staff members.
6. Continually train, refresh and remind staff as to the importance of privacy threats.
7. Keep your policy up to date with any new legislation or new privacy threats.
8. Create a ‘clear screen’ policy for computers left on.

9. Create a ‘clear desk’ policy.
10. Create a ‘document destruction’ policy for the destruction of paper materials.
11. Create a ‘data destruction’ policy for the removal of information off of old computers and other information storage devices.

# Mitigating Cybercrime Exposure

- Install & maintain anti-virus software, firewalls
- Analyze business operations to identify areas vulnerable to IT risks
- Practice regular diagnostic testing and monitoring
- Remove unused software
- Access reputable outside help or technical expertise when required

- Disable access to network as soon as possible after termination
- Limit or restrict use of wireless hot spots as well as chat rooms, blogs and instant messaging
- Do not allow downloads including music, movies and software

# The Risk Management Centre of Excellence

- Who
  - Municipalities, medical care providers, service organizations, schools
- How
  - http://excellence.frankcowan.com
  - Anywhere 24/7, 365 days a year
- What
  - Risk management info on current topics and emerging trends
  - content provided by risk management, legal and claims professionals
- Why
  - One stop
  - Easy to use
  - interactive

# Cyber Insurance

# Cyber Insurance

- Zurich Insurance study
  - Only 19% of organizations have purchased insurance specifically designed to cover cyber risk

- Harvard Business Review Analytic Services
  - Surveyed 152 private sector and public sector organizations
  - 76% expressed concern about information security and privacy
  - Only 16% have a designated chief information security officer

- An interesting finding is the important role cyber insurance can play in not only managing the risk of a data breach but in improving the security posture of the company. While it has been suggested that having insurance encourages companies to slack off on security, our research suggests the opposite.

  - Ponemon Institute, May 2014

# Remember…

Don’t just test your systems,
test your people.

**Jessica Jaremchuk  BA, LL.B**
Manager, Risk Management Consulting Services
jessica.jaremchuk@frankcowan.com
excellence.frankcowan.com
frankcowan.com