Cyber Risk Summit

Cyber Risk Legal Update

NetDiligence®

Panelists

- **Alex Cameron**, Partner and Leader, Privacy & Cybersecurity Group, Fasken (Moderator)
- **Brian Beamish**, Information and Privacy Commissioner of Ontario
- **Abubakar Khan**, Director, Toronto Regional Operations, at the Office of the Privacy Commissioner of Canada
- **Ian Birdsey**, Partner, Pinsent Masons LLP

Presentation Overview

- Breach litigation and class action update and impacts
- Privacy Commissioner requirements and expectations
- Legislative changes regarding breach notification
- Legal risk management, settlements and defences

Cyber Risk Summit

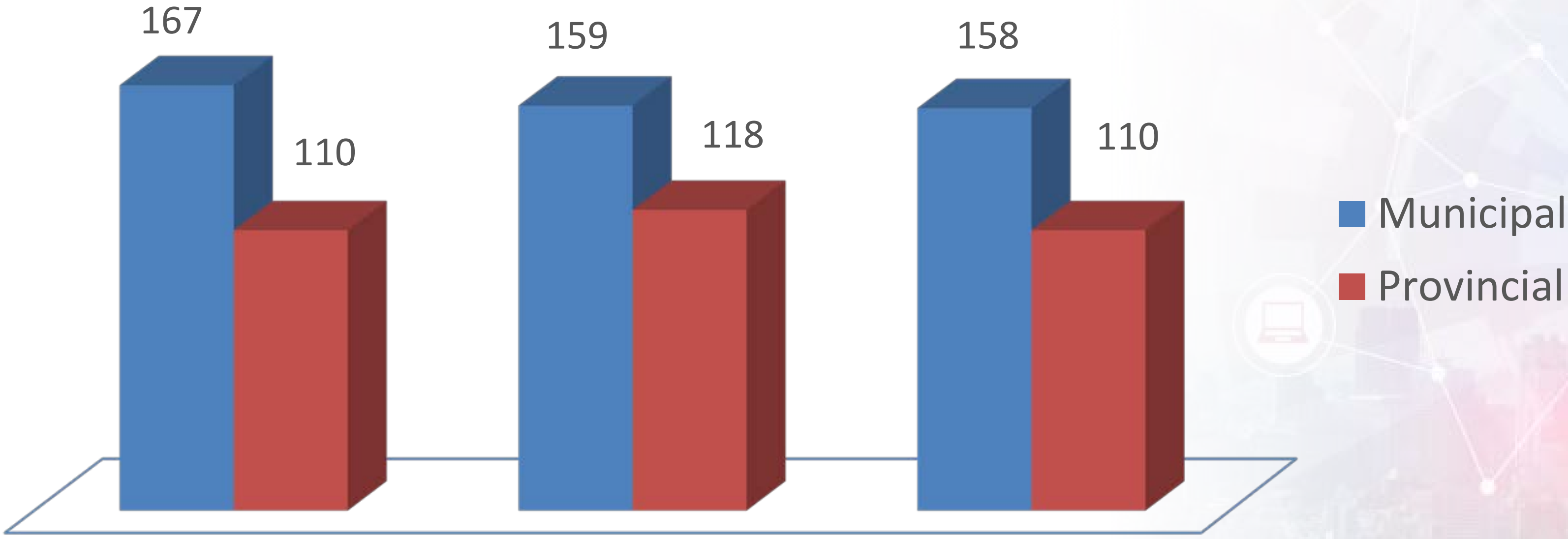
Ontario Update

Brian Beamish

Information and Privacy Commissioner of Ontario

NetDiligence®

Public Sector Privacy Complaints 2015 - 2017



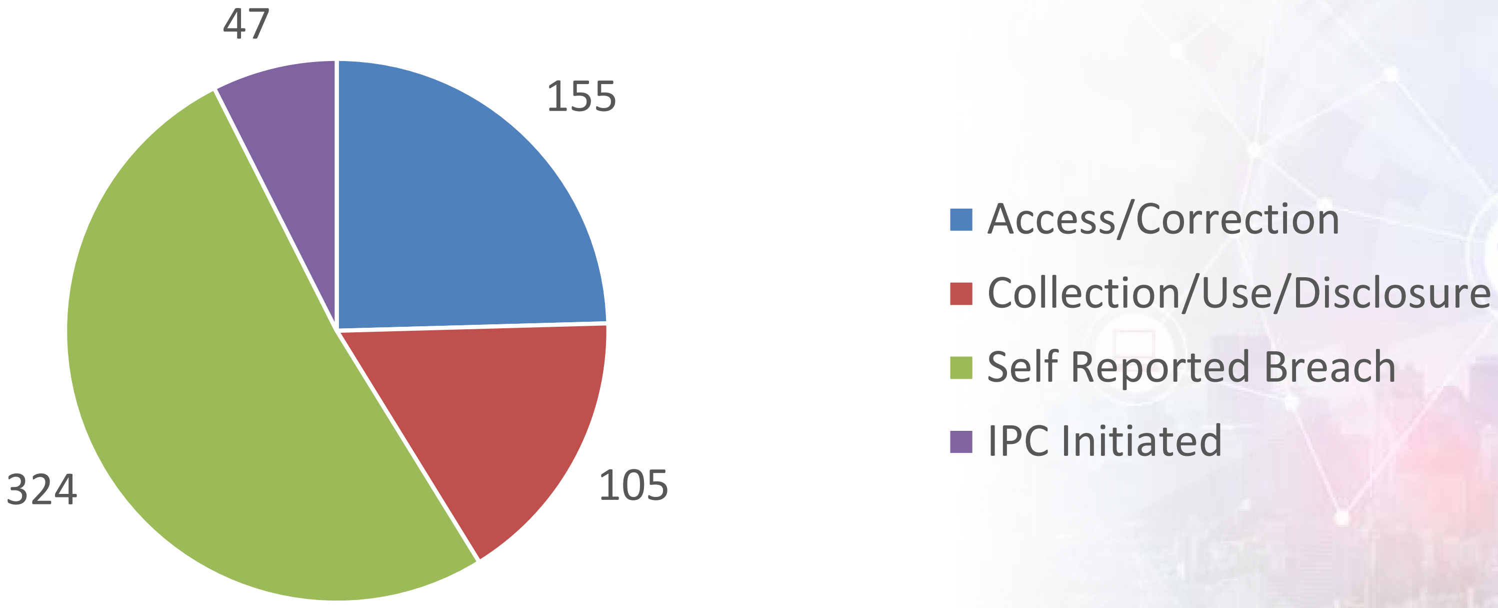
2015 (Total: 277)

2016 (Total: 277)

2017 (Total: 268)

Cyber Risk Summit

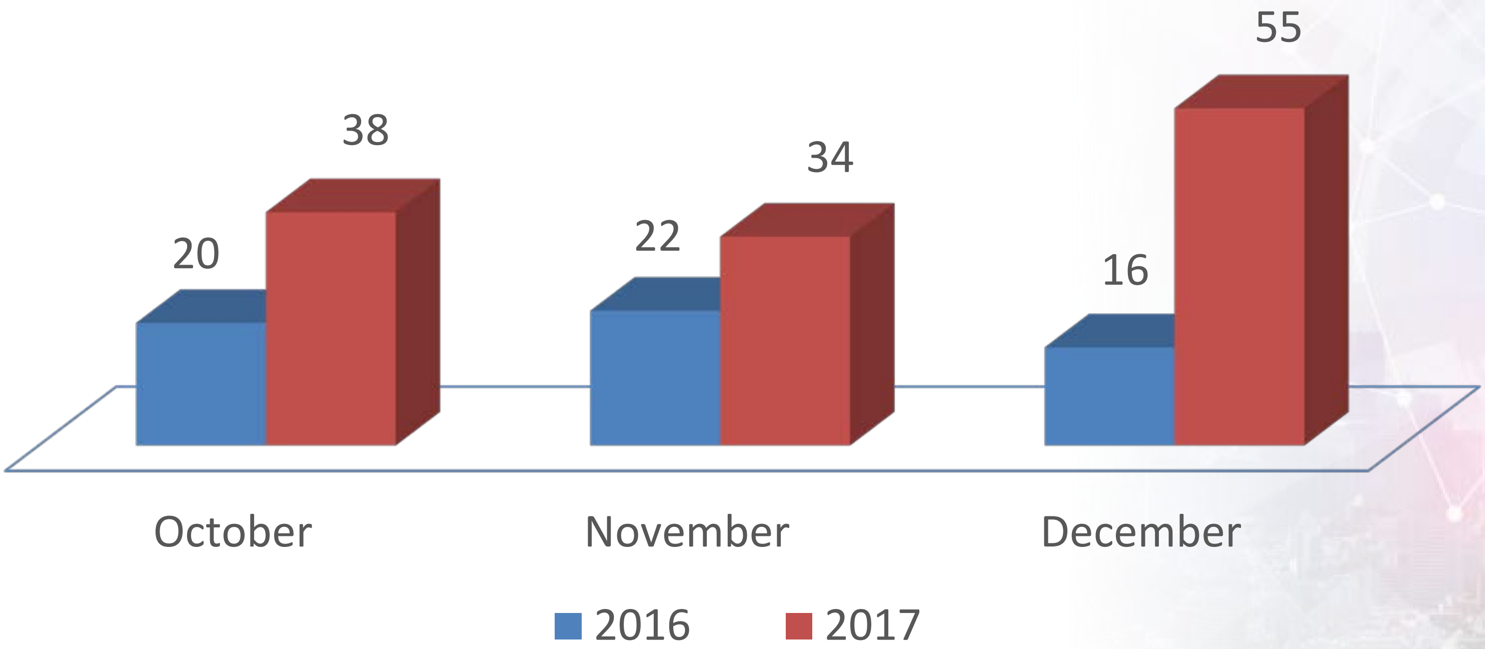
Health Sector Privacy Complaints 2017



Total: 631

Cyber Risk Summit

Health Privacy Breach Reports



(Total: 58) (Total: 127)

Cyber Risk Summit

GDPR: breach response and Canadian organisations

- Agenda:
  - What is the GDPR?
  - Application to Canadian organisations
  - Mandatory breach reporting
  - Significant financial penalties
  - Liability and claims environment

What is the GDPR?

- New General Data Protection Regulation (GDPR) will take effect in all 28 EU Member States from 25 May 2018
- Major changes from Data Protection Directive (95/46/EC)
- Network and Information Security (NIS) Directive must be implemented by 9 May 2018
- Brexit

Application to Canadian organisations

GDPR will apply to Canadian organisations with operations established:

- **Outside** the EU which process personal data:
  - in order to offer goods or services to data subjects within the EU; or
  - in order to monitor the behaviour of data subjects within the EU
- **Inside** the EU which process personal data (whether relating to EU data subjects or otherwise)

Mandatory breach reporting

- Mandatory notification of personal data breaches:
  - Data controller to notify the supervisory authority, without undue delay and, where feasible, within 72 hours of becoming aware of it unless it is unlikely to result in a risk to the rights and freedoms of natural persons
  - Data processor to notify data controller without undue delay after becoming aware of personal data breach
  - Data controllers to notify affected data subjects without undue delay where personal data breach likely to result in a high risk to the rights and freedoms of natural persons

Significant financial penalties

- Article 83 introduces a two tier system of fines, depending on circumstances and which provisions of the GDPR are breached
  - The maximum amount of fine in the higher tier is €20,000,000 or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher
  - The maximum amount of fine in the lower tier is €10,000,000 or up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher
- Both controllers and processors may be subject to these fines

Liability and claims

- Processor liability including fines (up to 2% or €10 million)
- Data subject claims: data subject can pursue either controller or processor
- Data protection claims on the rise
- Distress only damages
- Group litigation and representative actions on the rise
- Vicarious liability
- Opt out class actions on the horizon?
- New rights and mechanisms:
  - Article 80 GDPR introduces a new mechanism which entitles representative bodies such as a not-for-profit body, organisation or association, acting on behalf of data subjects, to lodge complaints with supervisory authorities, seek judicial remedies against a decision of a supervisory authority and seek judicial remedies against controllers or processors
  - Representative bodies may have the right, independently of a data subject's mandate, to exercise the above rights (Articles 77 to 79), if it considers that the data subject’s rights have been infringed as a result of the processing

Questions