Cybersecurity Survey Report No.2 (2021)

John Beardwood
Partner, Fasken, Toronto

IFLCA (Barcelona)
October 1, 2021

FASKEN

Agenda

1. About the Survey
2. Findings and Trend Analysis (from 2017 to 2021)
3. Takeaway
4. Q&A

1. The Cybersecurity Survey

Purpose of the survey

- To assist organizations to understand
  - (a) current information security compliance legal obligations, and
  - (b) the degree to which those organizations are complying with those obligations.

Recap of the first survey (2017)

- Four elements of the necessary base framework for cybersecurity*:
  - 1. Data Assessment: Understand your data and its sensitivity
  - 2. Risk Assessment: Assess the security risks relating to each dataset
  - 3. Adopt Safeguards: Assess the security safeguards which need to be adopted to address those specific risks
  - 4. Adopt Ongoing Policies/Procedures: Adopt clear, appropriate policies and processes regarding the foregoing on an ongoing basis

- Summary of the findings:
  - Almost all respondent organizations are taking some steps to protect against cybersecurity threats.
  - However, most of these organizations were only "partially compliant" and fell below the "reasonable and appropriate" cybersecurity security compliance level.

*(*As outlined in the Report published by the Office of the Privacy Commissioner of Canada and the Australian Privacy Commissioner on their joint investigation of Ashley Madison, which is operated by AvidLife Media Inc.)*

- Example: Ashley Madison breach.
  - Owner Avid had long list of security measures
  - Nevertheless, according to the Report, the Avid security framework failed to meet the standard of an "adequate and coherent" framework, as it lacked:

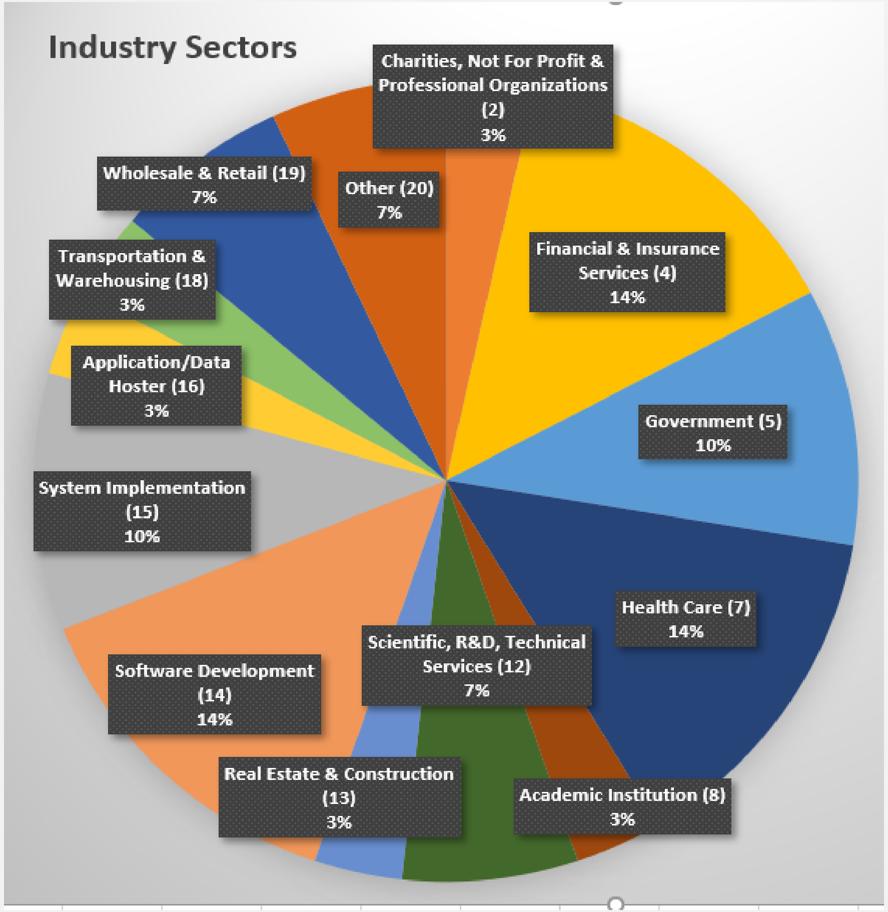
1. documented information security policies/practices
2. an explicit risk management process; &
3. adequate training to ensure all staff properly

The Surveys
(From 2017 to 2021)

Respondents

Respondents represented a broad range of industries.

Larger percentage of respondents are from Software Industries (14%), Financial and Insurance Services (14%), Health Care (14%) and System Implementation (10%).



Respondents

- Company size:
  - We received respondents from organizations of all sizes. Small cap companies (50%) and start ups (43%) represented the largest portion.
- Jurisdiction:
  - Most respondents represented companies within Canada (83.5%). We also have international respondents from US (8%) and Europe (4.5%).

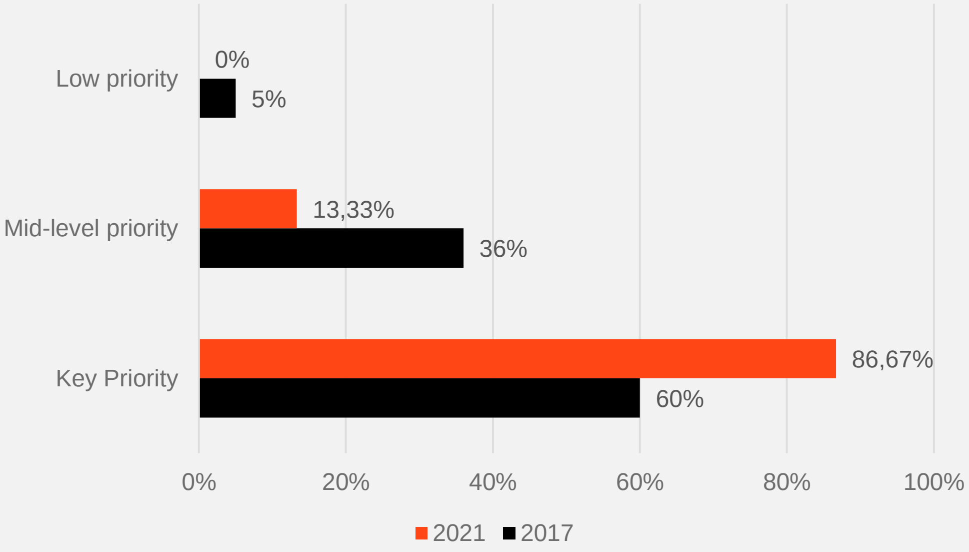
Findings and Trend Analysis

(From 2017 to 2021)

1. Information Security is a Key Priority

- 87% of the respondents identify that information security is a **key priority** for their organization.

Priority level of information security



2. The Four Steps

- More conformance with the four security steps

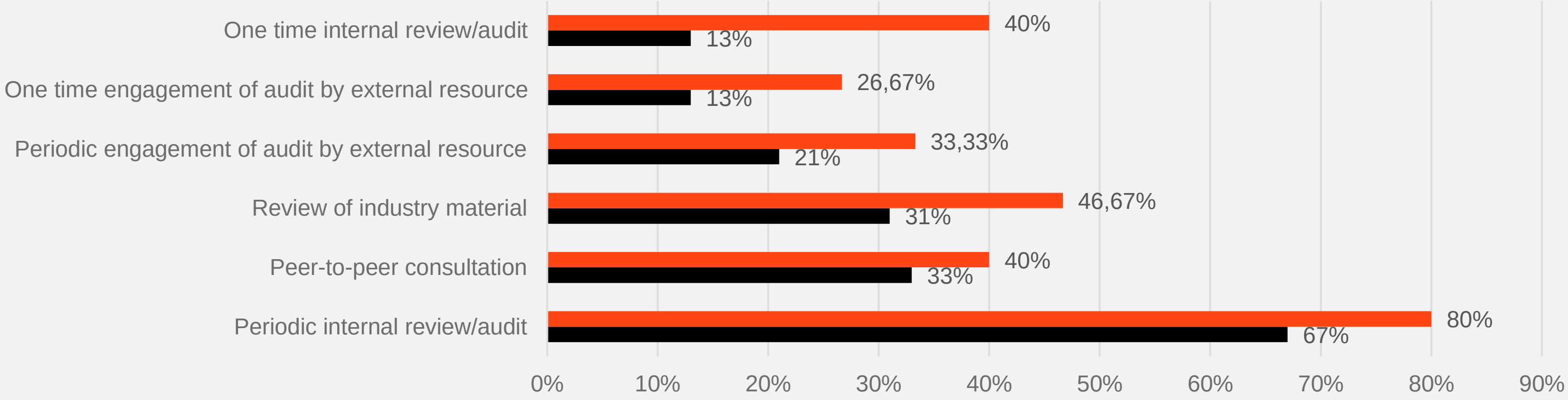
1. **Data Assessment**
   - 87% of the respondents' organizations reviewed the nature, volume, location and importance of their information assets.
   - Over 90% of the organization surveyed reviewed the sensitivity of the information that it collects, uses and discloses.
2. **Risk Assessment**
   - 75% surveyed conducted regular and documented risk assessments of its systems and information, <u>increased from only 42% in 2017</u>.

2. The Four Steps

3. **Safeguard Adoption**
    - 80% surveyed conducted meaningful assessment of the level of safeguards required in order to ensure the ongoing confidentiality, integrity and availability of its information.
4. **Policies/Procedures Adoption**
    - 80% surveyed indicated that their organizations adopted clear and appropriate policies, processes, procedures and systems to implement and support the information security safeguards.

3. Ongoing Risk Mgmt Process

How does your organization continue to ensure the adequacy of your information security safeguards?



	Periodic internal review/audit	Peer-to-peer consultation	Review of industry material	Periodic engagement of audit by external resource	One time engagement of audit by external resource	One time internal review/audit
🟥 2021	80%	40%	46,67%	33,33%	26,67%	40%
■ 2017	67%	33%	31%	21%	13%	13%

🟥 2021 ■ 2017

4. Safeguards – Physical

- Regarding physical safeguards
  - Top three options are 1) asset and inventory tracking (90%); 2) on-site security (73%); and 3) asset surveillance (64%).
  - Increased adoption of “clear desk policy” (55%) compare to 2017 (15%).

5. Safeguards – Technological

- Regarding technological safeguards
  - In the 2017 survey and reports, we highlighted two areas of concerns – more than 1/3 of the organizations surveyed did not use anti-virus or malware software, and did not authorize remote access only on a per user basis.
  - In 2021, we saw an increased adoption of anti-virus and anti-malware software (82% in 2021 vs 67% in 2017)
  - However, there are still 1/3 of organizations surveyed in 2021 that do not authorize remote access only on a per user basis.

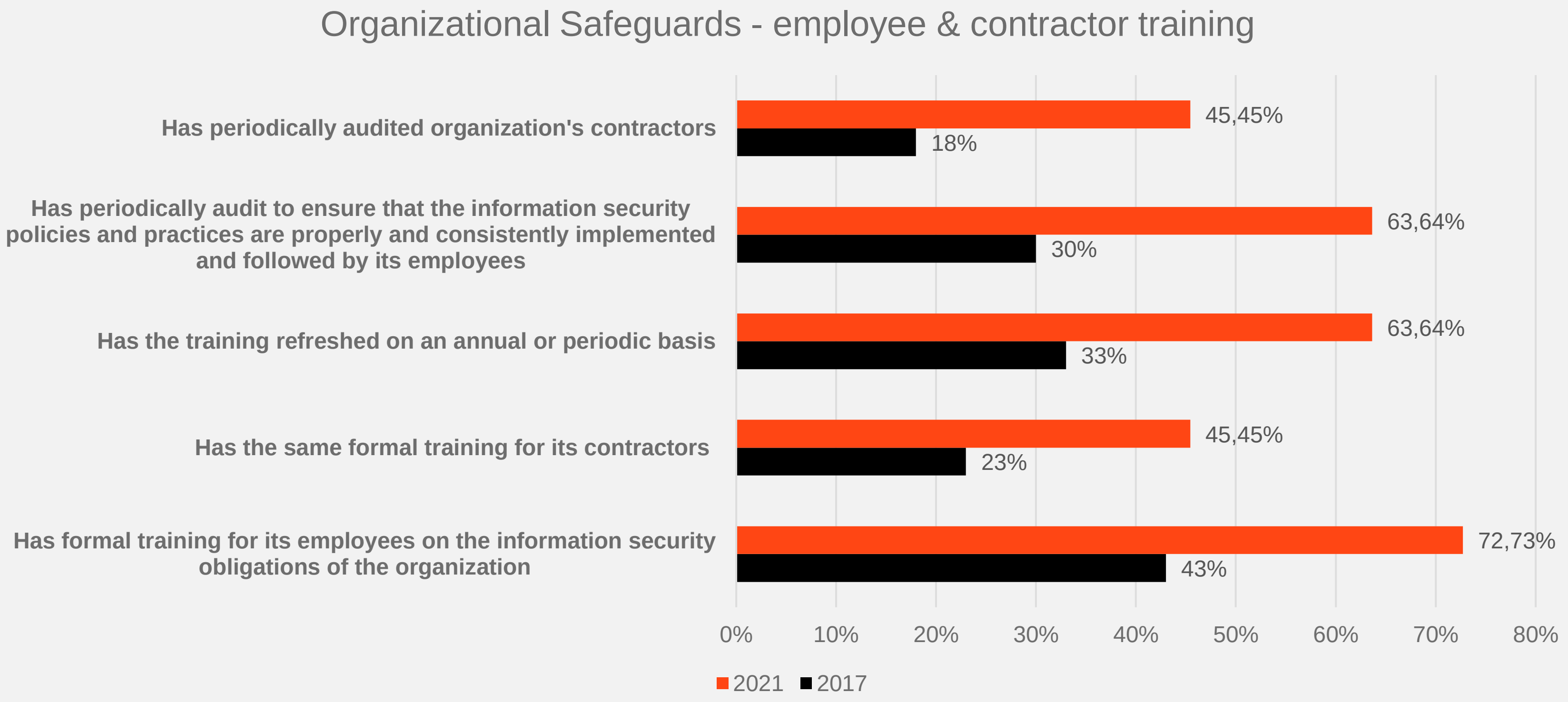
5. Safeguards - Technological

- While firewalls were the most commonly used technological safeguard in 2017 (90%), this year’s survey revealed a diverse selection of choices:
    - Using 2-factor authentication for controlling remote access to its networks and systems - 90.91% (e.g. Avid)
    - Network segmentation - 81.82% (e.g. Avid)
    - Having all systems/server's password protected- 81.82%
    - Consistently updating virus definitions, or running and reviewing virus scans- 81.82%

6. Safeguards – Organizational

- One of the biggest concerns from the 2017 survey was the lack of organisational safeguards. In this year's responses we noticed dramatic improvements:
  - Over 90% organizations now have written information security policies, practices and standards that are available to its employees (versus only 56% in 2017)
  - Over 80% of the organizations:
    - Having an adequate and coherent governance framework
    - Having a data deletion policy
    - Implementing a security information and event management system

6. Safeguards – Organizational – More Training

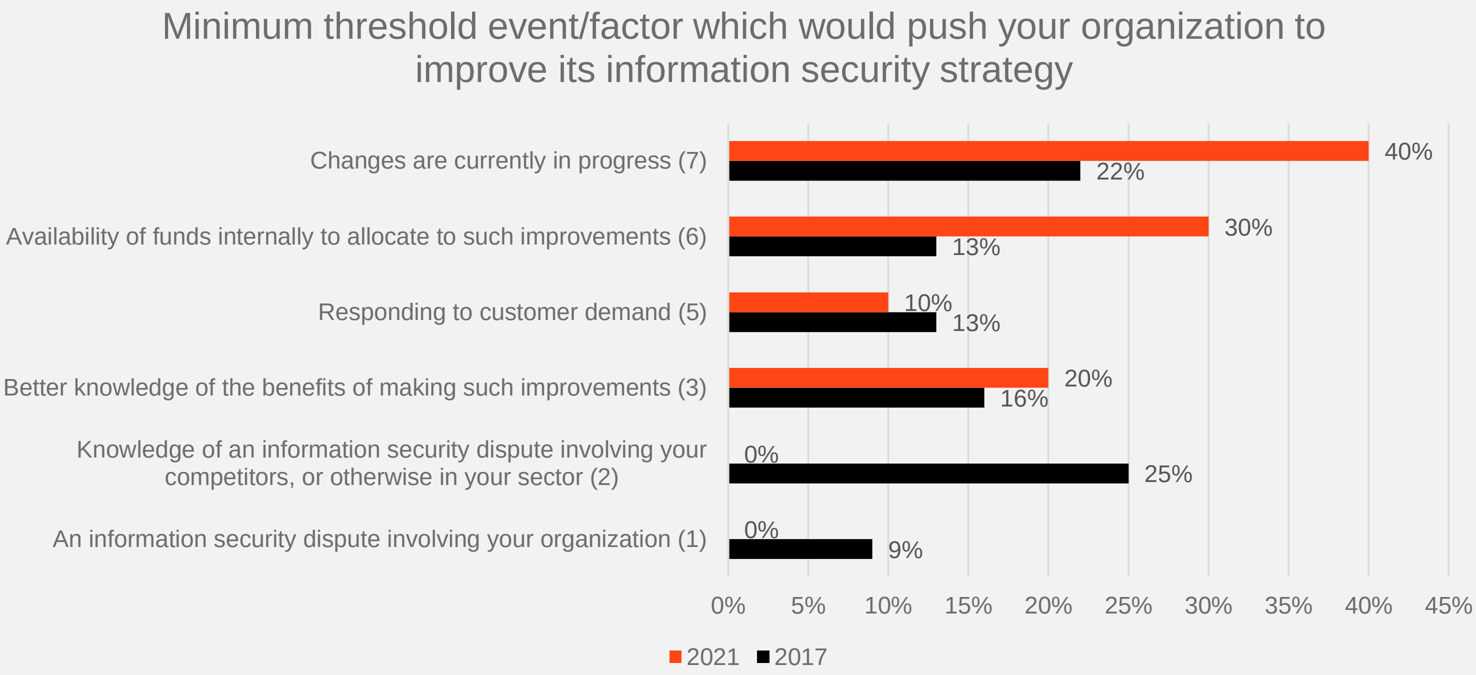


FASKEN

7. Data breach prevention

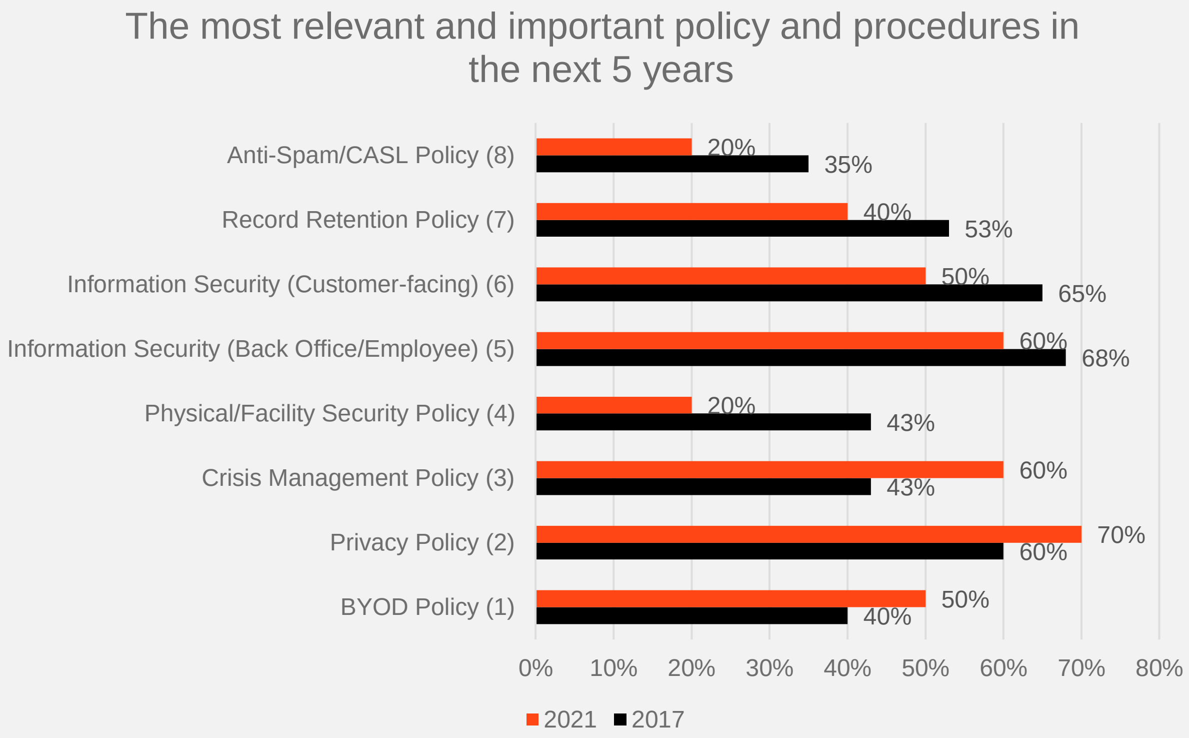
- Less than 1/3 of the respondents this year reported that they have been involved in a data breach or information security event.
  - In 2017, 33% reported they were involved in a data breach while only 27.27% reported such instance this year.
- Compared to the 2017 results, more organizations acknowledged the importance of:
  - having a designated security officer (33% vs 23%), and
  - engaging external information security consultants (33% vs 8%), in preventing the breach and reducing the impact of such breach. (e.g. Avid)

8. Improvement in progress



9. Most important policies

- Increased awareness in Privacy Policy and Crisis Management Policy



9. List of most commonly adopted information security measures

Technical information security measures	2017	2021
Patch applications (2)	67.57%	90.91%
Automated dynamic analysis of email and web content (6)	N/A	**81.82%**
Network segmentation and segregation (10)	N/A	**90.91%**
Multi-factor authentication (11)	40.54%	81.82%
Email content filtering (16)	N/A	**81.82%**
Antivirus software using heuristics and automated Internet-based reputation ratings (19)	40.54%	90.91%
User education & training (25)	51.35%	72.73%
Antivirus software with up-to-date signatures (26)	N/A	**81.82%**
Network-based Intrusion Detection/Prevention System (28)	37.84%	54.55%
Daily backups (33)	N/A	**81.82%**
Disable local administrator accounts (9)	35.14%	45.45%

Key Takeaways

Importance of the Four Steps

Continue to advocate for four step security methodology approach:

1. Data Assessment: Understand your data and its sensitivity
2. Risk Assessment: Assess security risks re each dataset
3. Safeguard Assessment/Adoption: Assess the security safeguards to be adopted to address those specific risks
4. Policies/Procedures Adoption: Adopt clear, appropriate and ongoing policies and processes regarding the foregoing

= document, document, document

Q&A

John Beardwood
Partner
416.868.3490
jbeardwood@fasken.com

John is a senior partner at Fasken LLP, Past-Chair of the firm’s Technology practice group, and Co-Founder of both the Privacy and Information, and Outsourcing practice groups. His practice is focused on technology, outsourcing and procurement, and privacy law matters. John is Past President of ITechLaw; is ranked by *Who’s Who Legal -Information Technology 2021* as one of only four “**Global Elite Thought Leaders**” in North America, and as “**leading our North American research** as a result of his **outstanding practice** handling outsourcing, tech transactions and major procurement proceedings”; by *Who’s Who Legal – Privacy & Protection 2020* as one of only four “**Global Elite Thought Leaders**” in North America, being “endorsed for his **first rate practice**, which encompasses access to information, privacy law and implementation of compliance programs”; and by W*ho’s Who Legal Canada 2020 – Data* as a “**National Leader**”, and one of the **Top Six “Most Highly Regarded”** leading figures in Canada for his work in assisting clients in complex data protection, privacy, cybersecurity and IT matters, noting that “John Beardwood is celebrated for his **20-plus years of experience providing top-notch private compliance advice** to a broad range of clients.”

FASKEN