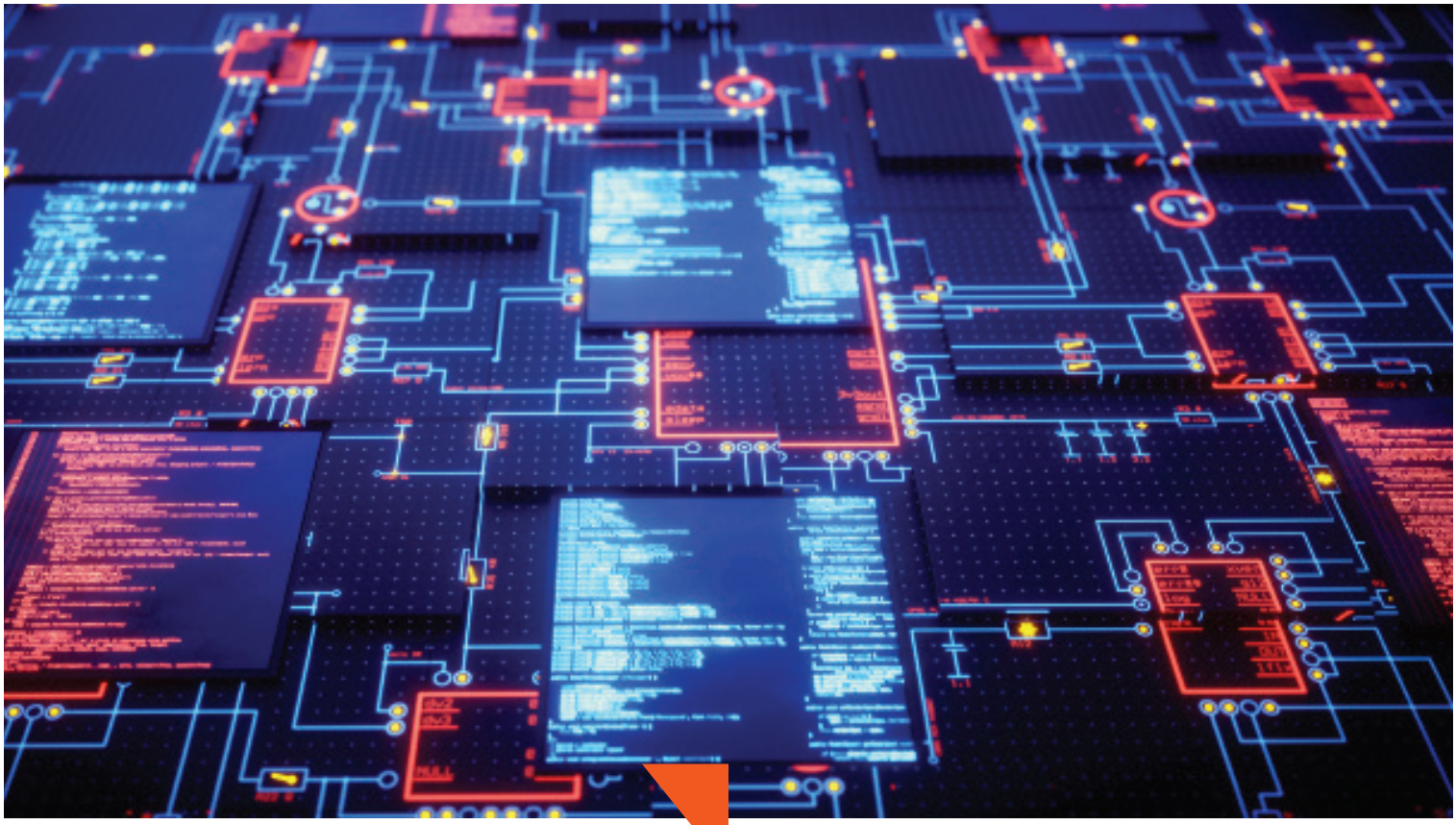


Cybersecurity Survey Report

FY 2017

FASKEN

In June 2017, Fasken conducted a survey concerning the measures implemented by small, medium and large organizations in order to address cybersecurity threats.

Two 2016 regulatory actions regarding well publicized data breaches – namely, (i) the joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner and (ii) the U.S. Federal Trade Commission's investigation into LabMD, Inc. – provided previously lacking guidance on what security requirements constitute "reasonable and appropriate" security. This survey provides insight into whether companies are meeting these new security requirements.

Our survey reveals general trends regarding which cybersecurity measures have been implemented and which have still not caught on with our respondents. This provides a glimpse into what truly is "industry standard" in cybersecurity. Survey results were provided by those who are familiar with information security and cybersecurity measures (i.e. Chief Technology Officers, Chief Information Officers and other C-level executives), as well as informed legal counsel.

Our special thanks to all those who participated. Their contributions were invaluable and are particularly appreciated in an environment where organizations are often reticent to go into detail as to which security measures they have adopted.

Executive Summary

Privacy legislation in Canada, the U.S. and elsewhere, while setting out detailed frameworks regarding issues like privacy consent and consent exemptions, almost universally reverts to high level principles when it comes to outlining privacy "safeguards" or security obligations. One concern of the legislators has been that by providing more detail, the laws could make the mistake of making a "technology pick," which, given the pace of evolving technology, could very well be out of date in a few years. Another concern is that what constitutes appropriate security measures can very contextual. Nevertheless, however well-founded those concerns, the result is that organizations seeking direction from the law as to how these safeguard requirements translate into actual security measures, are left with little to no clear guidance on the issue.

On August 22, 2016, the Office of the Privacy Commissioner of Canada and the Australian Privacy Commissioner provided detailed guidance on cybersecurity requirements in their published report (the "**Report**") on their joint investigation of Ashley Madison, which is operated by Avid Life Media Inc. ("**Avid**").

Contemporaneously with the Report, in the U.S. Federal Trade Commission's (the "**FTC**") opinion *In the Matter of LabMD, Inc.* published on July 29, 2016,[1] (the "**Opinion**"), the FTC provided its guidance on what constitutes "reasonable and appropriate" data security practices, in a manner that not only supported, but supplemented, the key safeguard requirements highlighted by the Report.

Between the Report and the Opinion, organizations have finally been provided with reasonably detailed guidance as to what the expected cybersecurity standards are under the law: that is, what measures are expected to be implemented by an organization in order to substantiate that the organization has implemented an appropriate and reasonable security standard to protect personal information. The question then is (a) whether organizations are aware of these requirements, and (b) whether they are complying with these requirements.

Our survey findings support the argument that almost all respondent organizations are taking some step to protect against cybersecurity threats. However, these same survey findings show that most of these organizations fall below the compliance level set out by the Report and the Opinion.

[1] While the Opinion was vacated on appeal on June 6, 2018, it still provides valuable insight as to the expectations of the FTC regarding appropriate data security measures.

This is concerning in light of recent substantial data breaches, such as Ticketmaster's breach of payment data of up to 5% of its customer base. Technical details of the Ticketmaster breach have not been publicized. However, we speculate that compliance with the cybersecurity standards set out in the Report and the Opinion might have mitigated the scale of this data breach and the damage incurred. More importantly, perhaps, compliance with these new cybersecurity standards might have reduced the risk of legal liability. Our goal for our survey and this report is to provide organizations with information concerning industry cybersecurity requirements and compliance so that these organizations can meet such requirements.

Respondents

Respondents represented a broad range of industries, including energy and utilities, financial and insurance services, health care services, life sciences and biotechnology, manufacturing, mining, software, and telecommunications, as well as academic institutions, charities and non-profits, and government. The industry group with the largest percentage of respondents was the software industry (25% of respondents).

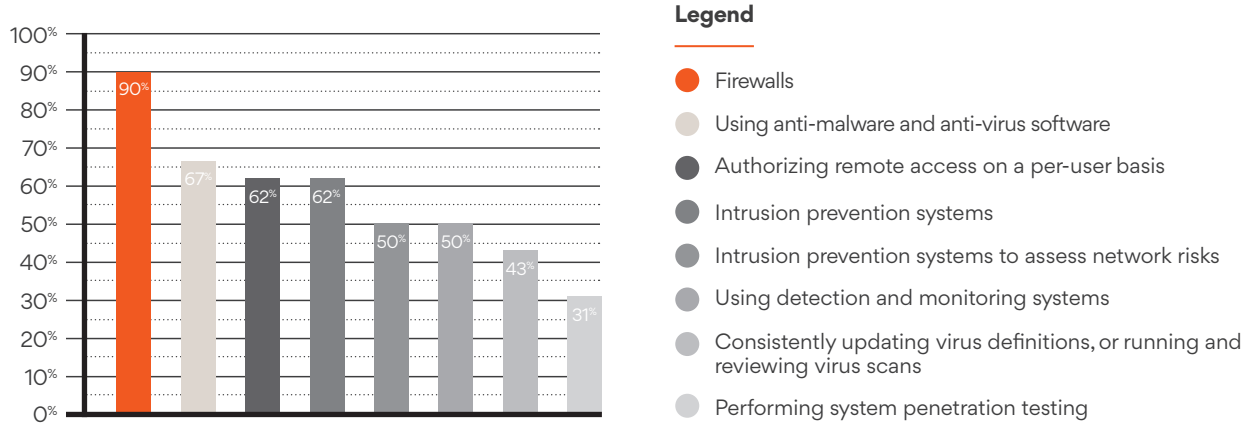
Organizations of all sizes (start-up, small cap, large cap (private) and large cap (public)) were well represented, with small cap companies representing the largest portion of respondents (38%).

Respondents represented companies operating in Canada, the US and the UK (95%, 35% and 25%, respectively). A large portion of our Canadian respondents operate nationally (28%).

Findings

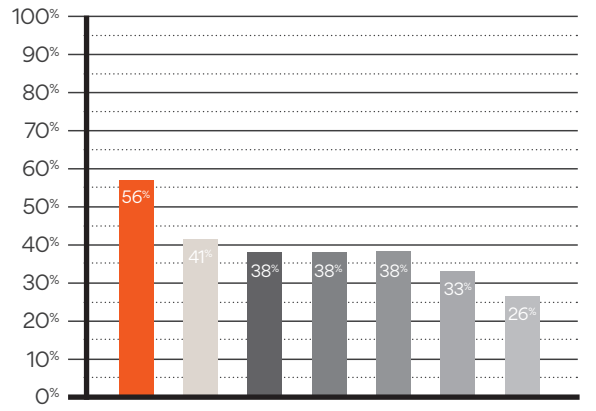
The survey findings – which are also available in a more detailed version of this report (available on request to the authors) – are comprehensive, but a number of them are particularly notable. For example, more than a third of respondents do not use anti-virus or malware software, and fewer still actively update such software to respond to new threats. A third of our respondents also do not authorize remote access only on a per user basis, a safeguard of notable importance which was cited in the Report.

Common technological information security safeguards adopted by responding organizations.



Also, while organizational safeguards can be the most important aspects of a complete cybersecurity program, compliance in this area was lacking. As an example, our survey found that organizations generally fail to regularly update their risk assessments; only 56% of respondents indicated that they had written information security policies in place; and more than half of the respondents neither conduct formal training for their employees, nor audit their employees for cybersecurity compliance.

Common organizational information security safeguards adopted by responding organizations.



Legend

- Having written information security policies, practices and standards that are available to its employees
- Ensuring that information security policies and standards cover both preventive and detective measures, including commonly used detective countermeasures that could facilitate detection of attacks or identify anomalies indicative of information security
- Employing or retaining a high level resource specifically responsible for information security.
- Prohibiting users from having administrative rights over their computers
- Restructuring what information and software employees download onto their work computers
- Understanding the applicable information security compliance obligations placed on it by sources such as PIPEDA, OSFI, CSA, PCI-DSS scans
- Having a documented information security risk management framework

These findings are concerning, as they indicate that the average respondent organization is only partially compliant. Partial compliance is not sufficient: notwithstanding perhaps the general impression left by the media, Avid had implemented a general security framework to protect the Ashley Madison user information, including certain physical, technological and organizational safeguards. However, this was not enough. Avid's security framework failed to meet the standard of an "adequate and coherent" framework.

In light of these survey findings, organizations should take this opportunity to review their cybersecurity measures and ensure that they meet these new legal standards.

Cybersecurity Compliance

As noted above, the survey findings indicate that there is still a notable gap in compliance with the required cybersecurity standards.

While both the Report and Opinion outlined in detail what security measures Avid and LabMD had and had not adopted, thematically the four elements of the necessary base framework for cybersecurity – for any organization, regardless of size - are clear:

1. Understand your data and its sensitivity
2. Assess the security risks relating to each dataset
3. Assess the security safeguards which need to be adopted to address those specific risks
4. Adopt clear and appropriate policies and processes regarding the foregoing

Note that the knowledge and deliverables resulting from implementing the above four steps are susceptible to becoming stale. An organization should periodically re-perform these steps, to ensure that new datasets, and their sensitivity and risks, are understood; that the existing safeguards continue to be appropriate vis-à-vis those risks; and that the organization's policies are updated to reflect the same. Given that these standards are emerging from regulator reports and initiatives (rather than privacy statutes), seeking help from experts, such as our team at Fasken, is highly recommended to help understand how the standard of "reasonable and appropriate" is evolving over time.

Conclusion

Almost all respondent organizations are taking some steps to protect against cybersecurity threats. However, our survey shows that most of these organizations fall below the "reasonable and appropriate" cybersecurity security compliance level set out by the Report and the Opinion. This lack of compliance is a concern. Meeting these cybersecurity requirements can limit an organization's legal liability in the event of a data breach, and may also mitigate the scale of such a data breach and any damage incurred. In short, organizations still have more work to do to comply with cybersecurity requirements.

If you are interested in receiving a more detailed version of this report, please contact John P. Beardwood or Mark Bowman.

John P. Beardwood
Partner
+1 416 868 3490
jbeardwood@fasken.com

Mark Bowman
Counsel
+1 416 865 4447
mbowman@fasken.com

John P. Beardwood

PARTNER

Toronto

+1 416 868 3490

jbeardwood@fasken.com

https://www.fasken.com/John-Beardwood

Areas of Practice

Corporate/Commercial | Privacy and Cybersecurity | Procurement

Industries

Health | Technology, Media and Telecommunications | Information Technology | Startup and Emerging Company Services

Education

1996, LLB, University of Toronto
1993, MA, McMaster University
1992, BA (Hons), McMaster University

Year of Call/Admission

Ontario, 1998

Languages

English

John is a senior partner who Chairs the firm's Technology practice group, and was Co-Founder of the Outsourcing practice group. His practice is focused on technology, outsourcing and procurement and privacy law matters.

John works closely with clients in advising on and negotiating various technology-related transactions, including outsourcing/procurement, licensing, implementation, distribution, technology transfer, strategic alliance and e-commerce related transactions, including in the health care, financial/insurance institution and public sector contexts. John often advises clients on privacy law and access to information matters, and has been developing and implementing privacy compliance programs for more than twenty years.

John is regularly listed in Who's Who Legal- The International Who's Who of Business Lawyers as one of the ten "most highly regarded individuals" globally; and is also listed as one of only five "Thought Leaders" in TMT- North America. He is listed in Chambers Global - The World's Leading Lawyers for Business, for Information Technology, as " very effective, efficient and remarkably accessible" and "a great lawyer", and in Chambers (Canada) as "very polished and has tremendous amount of experience." John receives rave reviews as 'a go-to expert in Canada for privacy and IT law' from The Legal 500.

Co-editor and contributing author of Outsourcing Transactions: A Practical Guide [Rel.11], John has been interviewed regularly by leading business-media outlets including The Globe and Mail, CBC Marketplace and Canadian Business Magazine. John is recognized nationally and internationally for his technology and outsourcing expertise by Chambers Canada, Chambers Global, The Legal 500 Canada, Who's Who Legal Canada and Best Lawyers in Canada and is highly recommended as an outsourcing practitioner in the PLC Which Lawyer? Yearbook and in the PLC Outsourcing Handbook.

Mark Bowman

COUNSEL

Toronto

+1 416 865 4447

mbowman@fasken.com

https://www.fasken.com/Mark-Bowman

Areas of Practice

Corporate/Commercial | Privacy and Cybersecurity | Procurement |

Industries

Technology, Media and Telecommunications | Information Technology | Startup and Emerging Company Services

Education

2014, JD, Osgoode Hall Law School at York University

2005, BSc, University of Ottawa

Year of Call/Admission

Ontario, 2015

Languages

English

Mark Bowman's broad corporate/commercial practice is focused in technology. An experienced Software Engineer, Mark also holds the Project Management Professional (PMP) and Ontario's Professional Engineer (P.Eng.) designations.

Mark frequently assists clients with information technology, consumer protection, privacy, and intellectual property-related legal matters. Assisting clients with outsourcing, procurement, licensing, privacy and e-commerce transactions, Mark also has experience drafting a variety of agreements, including procurement documents, purchasing terms and conditions, software agreements, software source code licenses, e-commerce and website terms and conditions, and privacy agreements. He is also experienced in filing and responding to freedom of information requests.

Beyond his technology practice, Mark has also been involved in transactions including mergers and acquisitions, going-public transactions, and financings.

An entrepreneur and avid coder, Mark remains an active and supportive member of Toronto's start-up community. He is involved in the firm's Start-Up Entrepreneurial Services initiative, supporting start-ups, early stage companies, and entrepreneurs, and the firm's blockchain, cryptocurrency and smart contract working group.

Ten offices
Four continents
One Fasken

› fasken.com

Canada

Vancouver, BC
550 Burrard Street, Suite 2900
T +1 604 631 3131
vancouver@fasken.com

Calgary, AB
350 7th Avenue SW, Suite 3400
T +1 403 261 5350
calgary@fasken.com

Ottawa, ON
55 Metcalfe Street, Suite 1300
T +1 613 236 3882
ottawa@fasken.com

Québec, QC
140 Grande Allée E., Suite 800
T +1 418 640 2000
quebec@fasken.com

Surrey, BC
13401 - 108th Avenue, Suite 1800
T +1 604 631 3131
surrey@fasken.com

Toronto, ON
333 Bay Street, Suite 2400
T +1 416 366 8381
toronto@fasken.com

Montréal, QC
800 Victoria Square, Suite 3700
T +1 514 397 7400
montreal@fasken.com

Global

London, United Kingdom
15th Floor, 125 Old Broad Street
T +44 20 7917 8500
london@fasken.com

Johannesburg, South Africa
Inanda Greens, Building 2
54 Wierda Road, West
T +27 11 586 6000
johannesburg@fasken.com

Beijing, China
Level 24, China World Office 2
No. 1 Jianguomenwai Avenue
T +8610 5929 7620
beijing@fasken.com

FASKEN