Katten
Katten Muchin Rosenman LLP

Privacy, Data and Cybersecurity Advisory

September 14, 2016

Keeping Your Cybersecurity Affairs in Order: How to Avoid Becoming the Next Ashley Madison

In late August, the Privacy Commissioner of Canada and the Australian Privacy Commissioner published the results of their joint investigation into the hack of notorious infidelity site, Ashley Madison, and its parent company, Avid Life Media (ALM).

The Privacy Commissioners found that ALM's information safeguards were inadequate at the time hackers exposed information from approximately 36 million user accounts. Among other things, the Privacy Commissioners found that ALM failed to create and implement a documented information security program that adequately protected the sensitive personal information stored on Ashley Madison's servers, and they highlighted misrepresentations that ALM made with regard to its security practices. As a result, the Commissioners put together a list of remedial and proactive measures ALM is required to take in order to comply with Canadian and Australian data privacy laws.

As data protection expectations become more standardized globally, the report from the Privacy Commissioners provides useful lessons on the basic data protection and information security requirements with which companies are expected to comply.

Key Takeaways

- Maintain written information security policies, processes, procedures and systems.
- Assess your security risk profile and implement appropriate corrective actions as part of a comprehensive risk management program. Regularly re-assess risks and update your program accordingly.
- Ensure that your protections are appropriate for the data that you hold.
- Provide appropriate privacy and security training for all personnel.
- Understand and comply with the legal requirements in each jurisdiction in which you operate.
- Make sure that your cybersecurity practices match your marketing promises.

Lesson One: Never Cheat on Your Information Security Program

Unfortunately, the Privacy Commissioners' findings reflect an all-too-common organizational failure: many businesses do not have appropriate information security procedures and programs in place.

In their report, the Privacy Commissioners found that, despite handling deeply sensitive personal information of millions of users, ALM failed to implement some of the most

For more information, please contact any of the following members of Katten's **Privacy, Data and Cybersecurity** practice.

Doron S. Goldstein
+1.212.940.8840
doron.goldstein@kattenlaw.com

Megan Hardiman
+1.312.902.5488
megan.hardiman@kattenlaw.com

Matthew R. Baker
+1.415.293.5816
matthew.baker@kattenlaw.com

Joshua A. Druckerman
+1.212.940.6307
joshua.druckerman@kattenlaw.com

fundamental components of an information security program, such as developing and documenting adequate policies and procedures, conducting appropriate risk assessments and properly training its personnel.

Takeaway: Informal, oral, unwritten or ad hoc information security policies and practices do little to protect sensitive data and are insufficient to mitigate or reduce an organization's exposure from security incidents.[1] Organizations that store critical or personal data electronically should, at a minimum:

- implement detailed written information security policies, processes, procedures and systems;
- regularly assess security risks, and implement appropriate corrective actions (including revision to existing policies/procedures or adoption of new ones) as part of a formal risk management program. This process should be repeated on a periodic basis (i.e., at least annually) and in response to changes in the threat environment or business operations; and
- provide appropriate privacy and security training for all personnel.[2]

Lesson Two: Always Use Appropriate Protection

ALM's poor information security practices and procedures led the Privacy Commissioners to find that ALM provided inadequate protection for the sensitive consumer information stored on its servers.[3] The Privacy Commissioners noted that security measures should be reasonable and adequate in light of the organization's size and capacity, the amount of stored personal information and the potential for harm associated with the disclosure of the stored personal information.[4]

ALM collected and stored users' billing information, email addresses and information about users' sexual fantasies and preferences.[5] Further, Ashley Madison's infidelity-related business model meant that even a passing association with the site could be damaging to the site's users if disclosed. When user information was posted publicly in August 2015, the consequences were severe for those named: reputations and relationships were damaged, and some reportedly even committed suicide.

Notwithstanding ALM's rapid growth immediately preceding the breach, the Privacy Commissioners found that the quantity, nature and sensitivity of the information stored by ALM, combined with the foreseeable harm to individuals that would result from its disclosure, meant that ALM's less-than-comprehensive information security program was simply inadequate to protect its customers.[6]

Takeaway: When developing and implementing a cybersecurity program, an organization should weigh its resources, size and sophistication against the amount and types of personal information stored. The greater the potential harm from loss or disclosure of stored personal information, the greater the obligation to protect that information. Finally, organizations undergoing rapid growth need to take extra care that their security program keeps pace.

Lesson Three: Keep Your Word

ALM marketed discretion and security to its users as a central part of its services, but failed to implement fundamental information security practices. As a result, the Privacy Commissioners found that ALM deceived and materially misled its users about its security policies and practices.[7]

---

1 OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, PIPEDA REPORT OF FINDINGS #2016-005: JOINT INVESTIGATION OF ASHLEY MADISON BY THE PRIVACY COMMISSIONER OF CANADA AND THE AUSTRALIAN PRIVACY COMMISSIONER/ACTING AUSTRALIAN INFORMATION COMMISSIONER ¶ 10 (August 22, 2016), *available here*. [hereinafter *Report*].

2 Report, ¶ 9.

3 Report, ¶ 80.

4 Report, ¶¶ 54–55.

5 The types of information collected by Ashley Madison would be considered "sensitive" under the privacy and data protection laws of many jurisdictions. For example, the EU considers information "specifying the sex life of the individual" to be a category of "sensitive information" subject to heightened protections. Australia similarly defines "sensitive information" to include information about an individual's "sexual preferences or practices."

6 Report, ¶¶ 54–55.

7 Report, ¶¶ 50, 194.

Users who visited the home page of the Ashley Madison webpage viewed a number of "trust mark" icons that suggested a high level of security and discretion. These included an award-style icon labeled "Trusted Security Award," a lock icon next to "SSL Secure Site," and a statement in which Ashley Madison promised that it provided a "100% discreet service" for its users. Even the image on its home page was that of a woman holding a finger to her lips in the universal gesture for secrecy.[8]

The Privacy Commissioners, however, determined ALM's inadequate information security program failed to fulfill these representations. In addition to lacking a documented, comprehensive information security program, ALM employees stored passwords in online Google drives and in plaintext emails and text files on their systems.[9] Access to servers containing sensitive data only required single-factor authentication and one server had an unprotected SSH key, which would allow a hacker to access other servers through it without providing a password.[10]

Takeaway: Organizations must ensure that any representations made about privacy and information security practices, including those described in any privacy policies and terms of use, are accurate and reflect actual practices. Further, organizations should be particularly wary of making difficult-to-verify representations such as "exceeds industry standards" as those statements are difficult to defend in the event of a false advertising or unfair or deceptive practices claim.

Lesson Four: Privacy and Cybersecurity is an International Affair

ALM marketed Ashley Madison worldwide and collected information and money from individuals in many jurisdictions. This enabled Ashley Madison to reach a much wider audience and generate correspondingly greater profits. These multinational benefits, however, subjected ALM to a range of privacy and data security notification obligations around the world.

As a result of this international exposure, ALM faces global liability arising from the breach. Class action lawsuits have been filed in multiple jurisdictions. Privacy authorities in Canada and Australia investigated ALM and obtained a compliance agreement and enforceable undertaking, respectively.[11] The US Federal Trade Commission has also begun an investigation.

Takeaway: Organizations that operate in multiple countries have to consider the privacy and cybersecurity laws of those jurisdictions and comply with applicable laws. In addition to legal and regulatory compliance, it is critical for organizations to have incident/breach response plans and crisis communications plans that help them respond quickly and effectively in all relevant jurisdictions.

Conclusion

While it is impossible to prevent every security incident or data breach, there are still steps that organizations can and should take to limit the risks presented by such incidents. These basic measures highlighted by the Privacy Commissioners can help reduce both the likelihood of an incident and the potential for harm in the event of a breach, allowing organizations to better protect their customers and themselves.

---

[8] Ashley Madison's Terms of Service contained a disclaimer warning customers that the security and privacy of information could not be guaranteed and they accessed or transmitted content through Ashley Madison websites at their own risk. The Privacy Commissioners found that this disclaimer was not enough to absolve ALM of its obligations under applicable privacy laws. Report, ¶ 52.

[9] Report, ¶ 75.

[10] Report, ¶¶ 72, 75.

[11] Report, ¶ 12.

Attorney advertising. Published as a source of information only. The material contained herein is not to be construed as legal advice or opinion.

©2016 Katten Muchin Rosenman LLP. All rights reserved.

Katten refers to Katten Muchin Rosenman LLP and the affiliated partnership as explained at kattenlaw.com/disclaimer.