# Cybersecurity: 2017 Report & 2016 Reflections

## What Businesses and Boards Need to Know

Bennett Jones

Where Clients Matter Most.

# Preface

In 2016, cybersecurity continued to grow as a primary business risk for companies worldwide. Data breaches continued to escalate both in number and magnitude and the landscape of legal and regulatory liability evolved and expanded. In this report, the Bennett Jones Cybersecurity team analyses the key events in 2016 with a view to those issues that should be front and centre for companies and their directors in 2017.

# Table of Contents

What is a Cyber Event or Cyber Breach Event? ..... 1

Cybersecurity Governance: The Board's Role ..... 3

Developing Trends in Cybersecurity Regulation in Canada ..... 4

Cybersecurity in Law Firms and Other Suppliers ..... 5

The Importance of Cyber Insurance Coverage ..... 7

Expanding Scope of Invasion of Privacy Claims ..... 8

National Mandatory Breach Notification Comes to Canada ..... 9

Cybersecurity Class Actions: The Next Big Thing? ..... 10

Lessons from the Ashley Madison Decision in the Context of Cybersecurity ..... 11

International Exposure from Cybersecurity Attacks: Yahoo! Inc.'s Cautionary Tale ..... 12

Ransom Attacks and the Bitcoin World ..... 13

References ..... 14

# What is a Cyber Event or Cyber Breach Event?

In 2016, "cyber" has entered the mind of the general public and the boardroom more than ever before.

Cyber events occur on, or are conducted through, a company's computer network in an attempt to gain unauthorized access to compromise the confidentiality, integrity or availability of the company's information, communication systems, or networks.

For the business community, cybersecurity incidents are intended to damage customer or stakeholder confidence, or financial, reputational, health or safety interests. These cyber incidents can affect an enterprise or group of commercial entities and their stakeholders. Preparing for cyber incidents has become an important risk-management focus for companies and their boards.

Cyber incidents are not restricted to ID theft or privacy breaches, and may also include things like:

- ransomware;
- distributed denial of service (DDoS) or local denial of service (LDoS);
- web defacement;
- physical or infrastructure harm (control devices harmed, *e.g.*, Stuxnet);
- theft of trade secrets, intellectual property, insider information; and
- loss of data integrity.

Cybercrimes are often committed as a means to another end, typically to make money (theft of insider information from Wall Street law firms, in aid of criminal insider trading schemes; identity theft to compromise systems, or to perpetrate further commercial fraud such as bank and credit fraud).

In 2016, we saw non-commercial cyber incidents, such as "doxing", the publication of private information to the Internet (*e.g.*, the Panama Papers information theft and disclosure, the Democratic National Committee email system information theft and disclosure, and cyber warfare attacks by national governments during regional conflicts in Estonia, Crimea, Ukraine, Syria, Egypt and Iraq).

**Lessons Learned**

Cyber breaches of 2016 have broadened our understanding of cybersecurity:

- Cybercrime is becoming multi-pronged and no a longer simple breach or theft events.
- Cybersecurity threat actors are becoming much more sophisticated. No longer are cyberattacks reserved for closet computer enthusiasts or the Anonymous movement. Organized criminal elements have adopted elements of IT network systems and social collaboration and media (*e.g.*, dark-web presence and sophisticated business methods, targeting, tools, and black markets for tools, stolen information).
- Cybercrime is being industrialized and scaled up at the social network scale.
- Targets vary; while credit card information remains attractive, new focuses on healthcare, law firms and governments have emerged, with gambits like ransomware and extortion becoming common.
- Cyber incidents may be the first event in a chain of criminal activities of some sophistication.
- Unsophisticated analytical models are no longer useful in tackling either prevention or response to cyber incidents.
- There is no activity more fruitful in avoiding cybersecurity risk than preparedness.

## Next Steps

To combat cybercrime, you will need to:

- understand what information and systems your organization controls, and whether they are valuable targets;
- understand what can be done to harden your systems to be a less tempting target;
- prepare for a seemingly inevitable cyber incident by understanding what could happen, providing for early detection and response, and planning mitigation steps (such as an incident response plan, insurance coverage, response readiness);
- gain an awareness of local resources (law enforcement, IT response consultants, backup systems, external legal advisors); and
- become thoughtful about your information and your systems.

Training your people about risks and risk avoidance is one of the most important steps. Your people are your best "intelligence agents" to enlist to protect your information and systems.

Bennett Jones has assembled a team with the skills, experience, expertise and connections able to help in cybersecurity preparedness and incident response and mitigation in the event of a cyber event. External legal counsel is an important element of your planning to deal with these types of problems.

# Cybersecurity Governance: The Board's Role

When it comes to protecting your company's data, the most important place to start is the boardroom.

The cyberattack on Ashley Madison (the dating site for extramarital affairs) highlighted potential exposure for directors, should they fail to take reasonable steps to avoid and respond to an attack. The Joint Report between the Canadian and Australian Privacy Commissioners on the Ashley Madison breach does not expressly identify exposure for the company's directors; however, the report underscores that the standards expected of companies fall within the responsibility of the board.

The board's role in IT infrastructure matters is no different from its role in dealing with other risks in the business. The board's role is one of oversight. The directors do not need to be or become experts in cybersecurity or IT. The board can rely on management to design and implement the IT infrastructure; but the board should ask sufficient questions to be satisfied that the right issues are being considered and addressed. The failure of the board to take appropriate steps in relation to cybersecurity matters can expose the directors to liability.

Accordingly, directors should have a basic understanding of the company's IT infrastructure so that they can identify risks that the company faces and assess whether those risks are being addressed.

"The board's role in IT infrastructure matters is no different from its role in dealing with other risks in the business."

**Assessing the Risks**

The first issue for a director is to consider the nature and extent of the company's reliance on its IT infrastructure. A board should have a reasonable understanding of how the company acquires, uses and depends upon its IT infrastructure in its ordinary course of business. Based on that understanding, the next question is the impact that any degree of failure of the IT infrastructure may have on the company. The three key potential cybersecurity risks to the company may be categorized as follows:

(i) Business operational risk: interruptions in the company's business operations.

(ii) Liability risk: for example, class actions from individuals whose information has been compromised; regulatory non-compliance risk (including Privacy Commissioners and Securities and Financial Institution regulatory regimes, which provide requirements for management and reporting of material security breaches and vulnerabilities).

(iii) Reputational risk: harm to company's reputation.

**Conclusion**

Technology is a fundamental aspect of business value and risk. The issues involved go well beyond technological ones to fundamental questions of governance and risk management.

# Developing Trends in Cybersecurity Regulation in Canada

Navigating the cybersecurity regulation in Canada (and elsewhere) has been a challenge for companies as it is an area of continued growth and change. Staying abreast of regulatory developments is critical for companies in order to understand their growing responsibilities in this domain.

Historically, cybersecurity threats have been addressed by governments in a piecemeal process through the adoption of various laws and regulations requiring the protection of certain categories of data (such as financial, health or personal information), the protection of certain key industries (such as critical infrastructure or banking) and the criminalization of certain activities (such as, *Security of Information Act* (Canada) section 19 (economic espionage) and *Criminal Code* (Canada) sections 342(3) (unauthorized use of credit card data), 342.1 (unauthorized use of a computer), 380 (fraud), and 402.2 (identity theft and identity fraud)).

As a result, a complex, fragmented, patchwork of legislation and industry practices has evolved which has generally focused on particularly sensitive data or 'at risk' assets.

"We have also seen a growing recognition that the existing patchwork of laws and regulations can result in increased costs and complexity, impacting the competitiveness of enterprise."

Addressing the increasingly sophisticated and evolving cyber threats which are becoming more obvious now poses a significant challenge to regulators and organizations alike, and we have recently recognized a number of trends developing in the regulatory approach to cyber threats. In particular, there is an increased focus on: (i) cybersecurity incident disclosure; and (ii) the harmonization of regulation.

To counter-balance reluctance of organizations to disclose cyber incidents to help satisfy a perceived need for timely and relevant information to enable law enforcement to respond to cyber threats, there has been a focus on cyber incident disclosures by victims. For example, the tentative adoption of mandatory breach reporting has sprung up in a number of jurisdictions (such as the recent amendments to the *Personal Information Protection Act* (Alberta)) and the issuance of specific guidance on the disclosure of cybersecurity risks and incidents by publicly traded enterprises (see the *Securities and Exchange Commission* cybersecurity guidance (U.S.) and similar guidance for Financial Institutions).

We have also seen a growing recognition that the existing patchwork of laws and regulations can result in increased costs and complexity, impacting the competitiveness of enterprise. Although the United States has formally withdrawn from the *Trans-Pacific Partnership* (TPP) trade deal, the text of the TPP highlights a growing trend towards a coordinated, international response to the cyber threat.

It is anticipated that there will be continued developments on the regulatory front. In the meantime, these two trends highlight the current state of affairs and provide some guidance to companies regarding expectations that will be imposed on them by regulatory authorities.

# Cybersecurity in Law Firms and Other Suppliers

Cybersecurity is top-of-mind for many businesses, particularly at organizations which deal with valuable or sensitive information such as member or user identities, credit card or account payment processing, industrial trade secrets, and similar obvious targets.

Increasingly, other sensitive information is being targeted as well:

- sensitive pricing or merger and acquisition information, which could affect share prices;
- research and development information and patent-development material, which could give a competitive advantage in a market or process; and
- sensitive information such as email archives, which could be used to embarrass or harass the target or be used to extort other things of value (passwords, access, or other behaviours).

Indeed, information targeted by a cybersecurity breach is often only one step in a larger crime or attack. For instance, several Wall Street firms' email accounts were compromised by criminals who used the stolen insider information for illegal trading gains; the Democratic National Committee email information was published to embarrass the organizers and affect a national presidential election campaign; and a law firm was compromised in the Panama Papers hack to gain access to tax-avoidance plans related to public and political figures over the world to embarrass or negatively affect those persons' careers and reputations.

In addition, analyses of a variety of large scale cybersecurity events reveals that the attack vector, or the "way in" to these systems was via vulnerabilities in vendor or supplier systems or operations. The Target breach is a prime example, where an air-conditioning subcontractor's accounts were breached and then used to infiltrate Target's systems. Bad guys seeking to breach a system will test for and attack the weakest link, which may sometimes be outside of the organization's direct control.

In light of these broadening risks, and the hacking of consultants and suppliers (in some cases law firms, banks and accountants, not just IT or air-conditioning suppliers), part of the focus of any cybersecurity initiative has shifted to the security and preparedness of suppliers–to safeguard the organization's information assets.

### What Can an Organization Do?

1. Understand the nature of the information and systems which are accessible to third-party suppliers, the risks associated with subcontracting or permitting third-party accesses, and the consequences of a cyber event affecting that information or those systems.

2. Review consultant and supplier contract terms to ensure that there is at least a duty or obligation to keep the organization's information and systems secure and confidential.

3. Ensure that the organization will be informed by a supplier whenever a cyber breach is experienced by the supplier organization; consider whether this should apply to all breaches they experience, or just breaches they identify as directly involving the organization's systems or information.

4. Consider the scope and scale of access by the supplier to information and whether access can be restricted or the scope and scale of the information or systems available can be limited, thereby containing the risk.

5. Obtain assurances that the supplier or contractor has adequate and appropriate security systems, people and processes in place to protect the organization's interests; consider auditing those security arrangements periodically and controlling the contractor's right to subcontract.

6. Understand the location and control over sensitive information or systems (the "cloud" problem), and ensure that there is adequate accountability to the organization if these are offshore or under third-party control not subject to privity of contract with the organization.

We mentioned that law firms might be targeted as an 'attack vector'. U.S. law enforcement authorities have been warning the industry for several years that law firms are increasingly targeted in information crimes. Law firms hold very sensitive information and information of great value–they trade on trust and confidence. Until recently, law firms were also the 'soft underbelly' in terms of risk, thought of as being relatively undisciplined and lax in information protection in the IT realm (although acknowledged as being very sensitive and protective in policy, ethics and professional realms).

2016 saw a dramatic increase in the awareness within law firms of these cyber risks, sharing of risk and threat information, hardening of IT systems and processes, and tightening of ethical and professional governance rules. Still, organizations are prudent to discuss concerns about cybersecurity with all suppliers, including their most trusted legal advisors.

At Bennett Jones, we take our duties and obligations to protect our clients' interests and information very seriously. As a part of our prudential and protective approach to information, we have implemented systems, policies and procedures which in 2016 attained certification after third-party audits proved us to be fully compliant with the ISO 27001 standard. By working in this area of law, including work on compliance and policy involved in the ISO Certification process, we have unique insights and expertise which we make available to our clients.

# The Importance of Cyber Insurance Coverage

In the world of inevitable cybersecurity breaches, companies have increasingly set their sights on insurance policies that purport to protect against the risks of an attack. However, experience teaches that some policies do not protect against the full scope of risks.

A 2016 United States decision highlights the importance of involving legal counsel to help protect against liability arising from a cyberattack.

In *P.F. Chang's v Federal Insurance Co*,[1] hackers obtained and posted on the internet 60,000 credit card numbers belonging to P.F. Chang's customers. This resulted in an assessment by the credit card companies against P.F. Chang's servicer, Bank of America. In turn, Bank of America pursued indemnification under its service contract with P.F. Chang's. A federal district court held that P.F. Chang's insurance policy did not provide coverage for this claim because the policy required that the claimant suffer a personal injury. In this case, Bank of America was the claimant and Bank of America did not suffer a personal injury, as the stolen records belonged to the customers. The court came to its conclusion even though the insurance company marketed the policy as "a flexible insurance solution designed by cybersecurity risk experts to address the full breadth of risks associated with doing business in today's technology-dependent world."[2] The court also noted that the parties were sophisticated and that the policy did not apply in the circumstances even though a "[c]ourt is expected to broadly interpret coverage clauses so as to provide maximum coverage for an insured."[3]

> "Given the novelty of cybersecurity breaches and the continuing development of Canadian jurisprudence and legislation, companies are advised to retain legal counsel to assist with identifying the scope of insurance coverage required."

This case highlights the importance of ensuring that the insurance policy covers for all possible contingencies arising from a cyberattack. Given the novelty of cybersecurity breaches and the continuing development of Canadian jurisprudence and legislation, companies are advised to retain legal counsel to assist with identifying the scope of insurance coverage required.

In the past year, the cyber insurance marketplace has matured dramatically, with new cyber insurance products which are meant to mitigate risks not handled by other business coverage. Premiums and costs, however, seem to be volatile, as insurers gain more loss experience and are able to refine their underwritings. Enterprises seeking cyber insurance are well-advised to be particular in choosing coverage and integrating insurance policies to mitigate cyber risk.

# Expanding Scope of Invasion of Privacy Claims

A 2016 Ontario decision may signal increasing exposure for companies which are subject to a cyberattack under an "invasion of privacy" claim.

**Background**

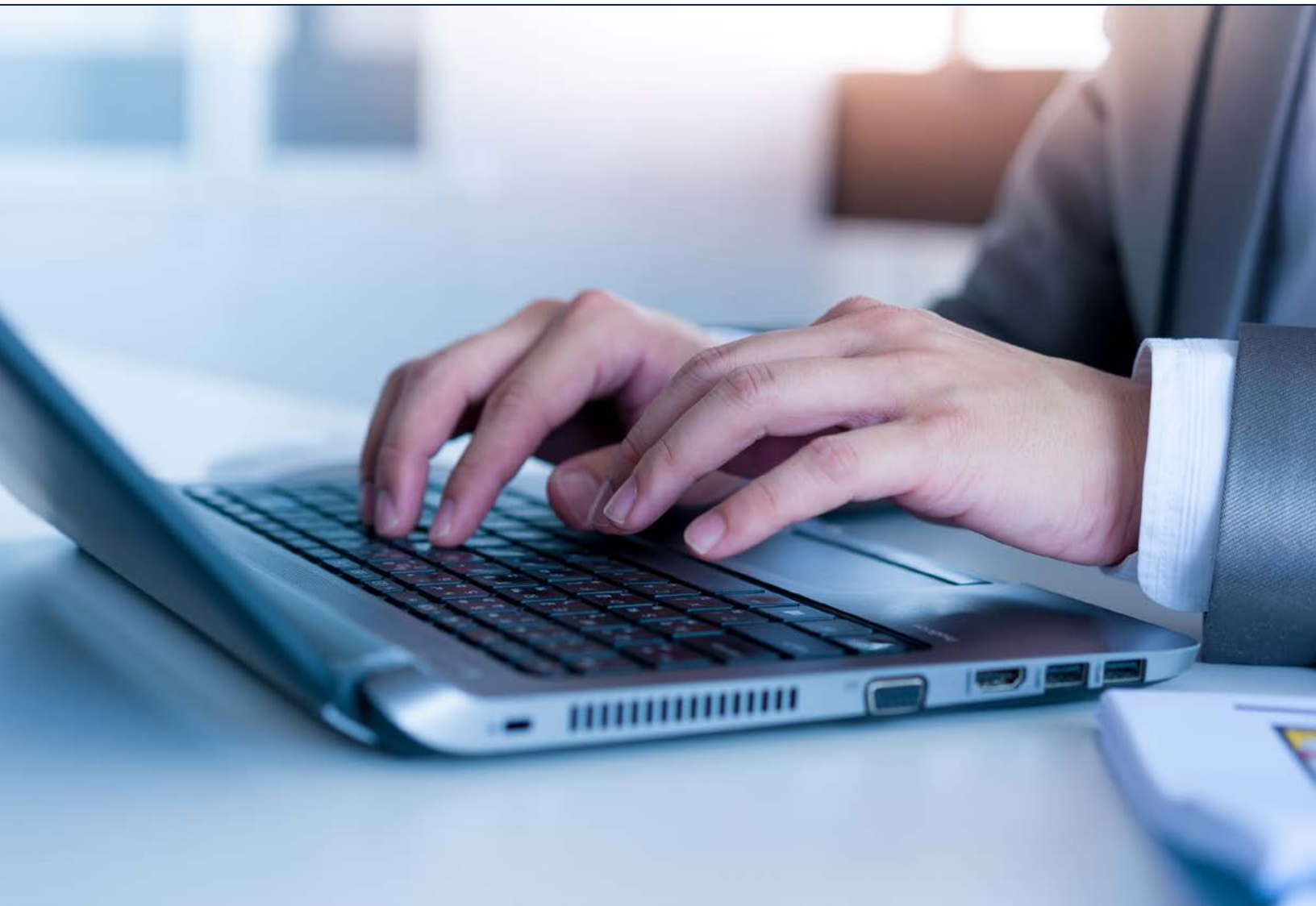
In its 2012 decision *Jones v Tsige*, 2012 ONCA 32, the Ontario Court of Appeal recognized a right of action for invasion of privacy. In short, this means that a person may be liable to another if they intentionally (or recklessly) intrude upon the other's private affairs. Proof of harm to an economic interest is not required.

A company that is subject to a cyber breach, could be liable if the company's employee is responsible for the breach[4] or if the company failed to maintain an adequate system to safeguard personal information in its possession.

**2016 Decision**

In *Jane Doe 464533 v ND*, 2016 ONSC 54, the Ontario Superior Court expanded the scope of claims that could be advanced under "invasion of privacy". In this case, the court recognized a right of action for invasion of privacy in the context of public disclosure of embarrassing facts.

This decision signals the expansion of claims that may be advanced based upon theories of invasion of privacy. For companies hit with a cyber breach, this decision may open them to claims by those individuals whose personal information has been disclosed by a cyber breach.



# National Mandatory Breach Notification Comes to Canada

A key factor in mitigation of risk in instances of a cybersecurity breach is notification of the affected individuals. Most U.S. states have mandatory breach notification requirements.

The Canadian scene is changing. While Alberta has had mandatory breach notification since 2010, in 2015 the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA), will bring mandatory breach notification to all entities subject to its jurisdiction.

The national mandatory breach notification rules are broadly modelled on the earlier Alberta rules. PIPEDA includes a mandatory requirement for organizations to give notice to affected individuals and to the office of the federal Privacy Commissioner about data breaches, where it is reasonable to believe that the breach creates a "real risk of significant harm to the individual." This test is similar to the test under Alberta's law. Under PIPEDA, "significant harm" includes, humiliation, damage to reputation or relationships, and identity theft. A "real risk" requires consideration of the sensitivity of the information, the probability of misuse, and other factors that may be set out in regulations.

The notification under PIPEDA is to be given "as soon as possible" after the breach has occurred. A form of notification may be set out in regulations.

Unlike the Alberta law, PIPEDA also requires an organization to notify other organizations and the government where such notifications may reduce risks or mitigate harm. PIPEDA will require organizations to keep and maintain records of every breach of safeguards involving personal information under their control. Where required those records may be provided to the federal Commissioner.

Additional nuances for these new rules, which have yet to come into force, are to be developed by regulation. The government has sought input on various issues to be addressed by the new regulations but has not yet issued draft regulations.

Organizations preparing for cyber breaches should contemplate that breach notification can be risk-mitigating and will soon be mandatory for more organizations in Canada. Notification responsibilities will arise under law and under many relationships such as, insurance contracts and financing covenants. Evidence from cyber breaches shows that time and money can be saved if an organization has assessed its notification responsibilities before an incident has occurred.

# Cybersecurity Class Actions: The Next Big Thing?

Are cybersecurity cases the next big thing in Canadian class actions? Several well-known data breach cases have received significant media exposure, including those involving Ashley Madison and Yahoo! Inc. These cases involve novel areas of law, including the the liability of a company for its employee's breach of customer privacy. Last year saw representative plaintiffs file a number of cases with similar allegations.

Several data breach cases are awaiting certification. One class action seeks $50 million in damages from Casino Rama on behalf of employees, customers and vendors whose confidential information was stolen in a cyberattack on the casino.[5] Another seeks $75 million in damages from the Family and Children's Services of Lanark, Leeds and Grenville, which provided affected individuals with child and family welfare services.[6] In addition to alleging negligence, breach of fiduciary duty, breach of confidence, negligent misrepresentation and invasion of privacy, this case argues a breach of the Canadian *Charter of Rights and Freedoms* because the defendant operated under the Ministry of Children and Youth Services.

> "These cases involve novel areas of law, including the the liability of a company for its employee's breach of customer privacy."

At the same time, 2016 saw courts certify and approve settlements for a number of cybersecurity class actions. Though *R v John Doe*[7] did not deal strictly with a cyber breach, the plaintiffs made claims under the same causes of action after Health Canada sent class members large envelopes labelled "Marijuana Medical Access Program". The Federal Court of Appeal certified the class action in negligence and breach of confidence.

Courts also approved settlements in *Drew v Walmart Canada Inc.*[8] and *Lazanski v The Home Depot, Inc.*,[9] based on allegations of data breaches compromising customers' private information. Those cases settled for up to $750,000 and $520,000 respectively–which are small settlements as class actions go.

Cybersecurity class actions will only be the next big thing when they command significant damages awards. One thing is for certain: you do not want your company name to become synonymous with data breach liability if and when they do.

# Lessons from the Ashley Madison Decision in the Context of Cybersecurity

On August 22, 2016, the Office of the Privacy Commissioner of Canada (OPC) issued a joint decision with the Australian Privacy Commissioner/Acting Australian Information Commissioner regarding the highly publicized data breach that Avid Life Media . (ALM) experienced in 2015. This decision articulates key considerations for companies that collect, use or disclose personal information.

**The Facts**

By way of background, ALM, since renamed Ruby Corp., operates a number of adult dating websites, including Ashley Madison, which targets individuals seeking to have discreet extramarital affairs. ALM is headquartered in Toronto, Canada, but its websites can be accessed globally, with users in over 50 countries. In July 2015, hackers stole data from ALM and published a large number of files online, including profile, account and billing information from approximately 36 million Ashley Madison user accounts.

**Key Takeaways from Decision**

1. Personal information under the custody or control of an organization must be protected by safeguards appropriate to the sensitivity of the information. The determination of the necessary safeguards must be: (i) context-based; (ii) proportionate to the sensitivity of the personal information; and (iii) guided by the potential risk of harm to individuals arising from a data breach. In making this determination, an organization should not focus exclusively on financial harm, (*e.g.,* fraud or identity theft); the impact of an individual's "physical and social well-being", including "potential impacts on relationships and reputational risks, embarrassment or humiliation" should be considered too.

2. Safeguards adopted by an organization should be based on an "adequate and coherent" information security governance and risk management framework that is appropriate to the sensitivity and amount of personal information collected.

3. Organizations should document their security policies and procedures regarding measures to prevent cyberattacks and measures to detect intrusions.

4. Organizations must monitor indications of intrusion or other unauthorized activity on a regular basis and document their risk assessments.

5. Organizations should rely upon multi-factor authentication for controlling remote administrative access by authorized users.

**Conclusion**

This decision sets some key parameters for organizations trying to understand obligations when it comes to protecting data. However, there is no clear road map on how to implement these principles for any given organization. Businesses are advised to seek legal counsel on how best to meet the known standards for preventing and responding to cyberattacks.

# International Exposure from Cybersecurity Attacks: Yahoo! Inc.'s Cautionary Tale

The fallout from the multiple data breaches suffered by Yahoo! Inc. (Yahoo), which were reported in late 2016, highlights the cross-border ramifications for a company hit with a cyberattack.

**Yahoo Cyberattacks**

In September 2016, Yahoo announced hackers stole account information–including names, emails, addresses, birth dates, and encrypted passwords–of at least 500 million users in 2014 (2014 breach).[10] At the time, the 2014 breach was the largest in history into a company's computer network, but it was only the beginning of Yahoo's data breach troubles.[11]

In mid-December 2016, Yahoo announced that it discovered a separate cyberattack that occurred on its network in 2013, which compromised more than 1 billion user accounts. Similar to the 2014 breach, the 2013 breach resulted in stolen information, including names, emails, addresses, birth dates, and encrypted passwords.[12]

These breaches are thought to comprise the largest technical breach to date. In addition to obtaining personal account information of its customers and users, hackers accessed Yahoo's cookie creation software and users' security questions and answers, enabling further hacks.

**Litigation and Regulatory Proceedings**

As a result of Yahoo's data breaches, the company is currently facing significant litigation and regulatory exposure, spanning a number of jurisdictions across the globe.

In relation to the 2014 breach alone, Yahoo reported that it was subject to 23 consumer class action lawsuits in the United States and other jurisdictions.[13] While the report does not specify, the number of lawsuits likely includes one of the two class actions commenced against Yahoo in Canada.

In December 2016, the Securities and Exchange Commission opened an investigation of Yahoo and issued requests for documents relating to the data breaches. The Commission's investigation is in its early stages but is focused on whether Yahoo's disclosures about the data breaches complied with reporting requirements and securities laws.[14] It remains to be seen whether the Commission will bring an enforcement action against Yahoo as a result of the data breaches. Whatever the result, the Commission's investigation will likely set a precedent for a company's disclosure requirements in the wake of a data breach.

The European Union's Data Protection Supervisor outlined serious concerns it had about Yahoo's data breaches, and is currently seeking more information regarding the nature and content of the stolen data, the consequences of the breach, and the numbers of people affected in the European Union.[15]

Yahoo is also being "urgently examined" by the Irish Data Protection Commissioner in connection with the data breaches to determine whether any formal investigation will be launched for breaching European data protection laws.[16]

**Cautionary Tale**

The Yahoo breaches highlight the exposure to international claims and regulatory proceedings for a company that is subject to a cybersecurity breach. Heading into 2017, companies must factor in this international risk when assessing the potential exposure from an attack.

As a footnote, a bid by Verizon to purchase Yahoo made prior to these announcements appears to have stumbled, and the breaches may have affected pricing or other terms. Yahoo has announced that its CEO will resign from the company's board after the planned merger.

# Ransom Attacks and the Bitcoin World

In 2016, ransom attacks were on the rise. A data ransom attack is one where the attacker infiltrates an IT system or database, and either locks it up while creating a "key" to unlock the system, or threatens to publicly disclose private information unless a ransom is paid. Victims of ransomware attacks in 2016 included dating sites, retail stores, hospitals, universities, government agencies, financial institutions, casinos and law firms.

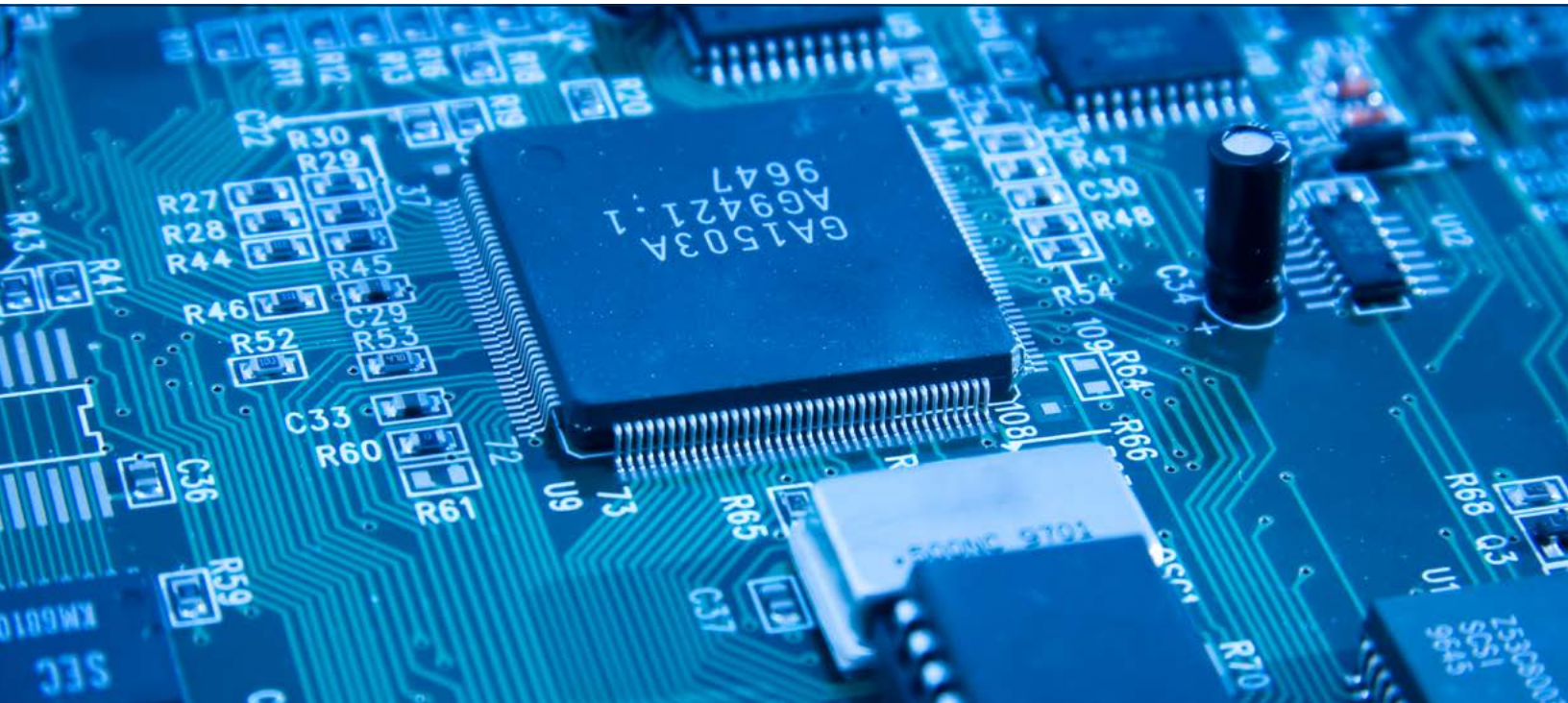
Typically, a data ransom attack mimics a traditional kidnapping in several ways:

1. The demand (usually received by email rather than a disguised phone call) is non-negotiable with a tight 24–48 hour deadline to respond.
2. A sample of the sensitive data that has been compromised is provided at a link to show that the threat is serious and real (just like a photograph of the distressed hostage holding the current newspaper).
3. The victim is cautioned to avoid involving the authorities (which may not assist in any event).
4. The attacker warns of the consequences associated with having to disclose the privacy breach if the ransom is not paid exactly as instructed.

Instead of asking for a suitcase of money to be dropped off at a dark location, today's data kidnappers want payment in bitcoin–the electronic currency which is said to be untraceable.

> "Victims of ransomware attacks in 2016 included dating sites, retail stores, hospitals, universities, government agencies, financial institutions, casinos and law firms."

In the face of a ransomware attack, companies need specialized and experienced advice, an immediate threat assessment, containment on a need-to-know basis, and a communications and mitigation plan. In order to contain the potential damages from the attack, companies are advised to seek legal counsel immediately upon learning of the attack.



# References


1. No CV-15-01322-PHX-SMM (D. Ariz 2016).
2. Yahoo, *An Important Message About Yahoo User Security*, September 22, 2016.
3. *Ibid* at 1.
4. In the class action proceeding against Bank of Nova Scotia, 2014 ONSC 7249, the court permitted a claim against the bank to proceed based on vicarious liability for intrusion upon seclusion by the bank's employee.
5. *Harman v Casino Rama Inc.*, 97892/16.
6. *M.M. v Family and Children's Services of Lanark, Leeds and Grenville*, CV-16-551363-00CP.
7. 2016 FCA 191.
8. 2016 ONSC 8067.
9. 2016 ONSC 5447.
10. *Ibid* at 2.
11. New York Times, *Yahoo Says Hackers Stole Data on 500 Million Users in 2014*, September 22, 2016.
12. Yahoo, *Important Security Information for Yahoo Users*, December 14, 2016.
13. Yahoo, *Form 10-Q Quarterly Report*, November 9, 2016.
14. The Wall Street Journal, *Yahoo Faces SEC Probe Over Data Breaches*, January 24, 2017.
15. Article 29 Working Party, Article 29 Data Protection Working Party letter, October 28, 2016.
16. Data Protection Commissioner, *DPC statement on Yahoo data breach*, December 15, 2016.

# Key Contacts

**Ruth E. Promislow**
Partner, Commercial Litigation, Fraud and Professional Negligence
T: 416.777.4688
E: promislowr@bennettjones.com

**Michael R. Whitt Q.C.**
Partner, Patent Agent, Trademark Agent, Head of Information Technology
T: 403.298.4448
E: whittm@bennettjones.com

# Your Cybersecurity Team

**Stephen D. Burns**
Partner, Trademark Agent, Outsourcing, IT Procurement, IP, Information and Privacy

**Michael A. Eizenga**
Partner, Head of Class Actions

**Martin P.J. Kratz, Q.C., FCIPS**
Partner, Trademark Agent, Head of Intellectual Property

**Steven L. Major**
Partner, Commercial Dispute, Construction, Fraud, Police and Personal Injury

**Barry J. Reiter**
Partner, Head of Technology, Media and Entertainment

**Gary S. A. Solway**
Partner, Technology, Media and Entertainment, Corporate Commercial and Governance

**David A. Cassin**
Associate, Commercial Litigation

**J. Sébastien A. Gittens**
Associate and Trademark Agent, Intellectual Property and Technology Commercialization

**Ethan Z. Schiff**
Associate, Commercial Litigation

Cybersecurity attacks have become an inevitable business risk for companies, large and small. Companies must now develop, and continually update, plans to protect personal data, design an incident response plan should it be attacked, and address the scope of litigation risks and regulatory obligations upon an incident.

As part of our ongoing cybersecurity efforts to ensure safe and reliable service to our clients, we recently became ISO 27001 certified. The work undertaken to achieve and retain this certification gives us unique insight into clients' challenges in minimizing exposure and maintaining compliance in this increasingly complex and threatening area.

# Canadian Offices of Bennett Jones LLP

**Calgary**

4500 Bankers Hall East
855 2nd Street SW
Calgary, Alberta
T2P 4K7 Canada
Tel 403.298.3100

**Edmonton**

3200 TELUS House
South Tower
10020 - 100th Street
Edmonton, Alberta
T5J 0N3 Canada
Tel 780.421.8133

**Toronto**

3400 One First Canadian Place
P.O. Box 130
Toronto, Ontario
M5X 1A4 Canada
Tel 416.863.1200

**Vancouver**

1055 West Hastings Street, Suite 2200
Vancouver, British Columbia
V6E 2E9 Canada
Tel 604.891.7500

**Ottawa**

Suite 1900 World Exchange Plaza
45 O'Connor Street
Ottawa, Ontario
K1P 1A4 Canada
Tel 613.683.2300

# International Offices

**Washington, DC**

1730 Pennsylvania Avenue NW
Suite 875
Washington, DC
20006
United States
Tel 202 207 1049
Fax 202 204 0498

**Bermuda**

Bennett Jones (Bermuda) Ltd.
Hamilton House
10 Queen Street
P.O. Box HM 1154
Hamilton HM EX
Bermuda
Tel 441 292 4229
Fax 441 292 6140

**Doha**

Qatar Financial Centre Branch
37th Floor, Tornado Tower
Al Funduq Street, West Bay
PO Box 11972
Doha
Qatar
Tel +974 4 020 4777
Fax +974 4 020 4799

**Beijing Representative Office**

Bennett Jones Commercial Consulting Inc.
Room 09, Level 14
China World Office Tower 1
1 Jianguomenwai Avenue
Chaoyang District, Beijing 100004, China
Tel +86 10 6535 0123
Fax +86 10 6535 0122

For more information about the firm, please visit us online at www.bennettjones.com

**Bennett Jones LLP** is an internationally recognized Canadian law firm founded and focused on principles of professional excellence, integrity, respect and independent thought. Our firm's leadership position is reflected in the law we practise, the groundbreaking work we do, the client relationships we have, and the quality of our people.

www.bennettjones.com/cybersecurity