Privacy Breach Response Prevention of Future Breaches

June 19, 2019

Canadian privacy commissioners have emphasized the importance of the final step of a privacy breach response process –prevention and lessons learned. The recent decision by the British Columbia Court of Appeal in *Ari v. Insurance Corporation of British Columbia* confirms that an organization's failure to learn from past privacy breaches and prevent future privacy breaches might justify an award of punitive damages.

Breach Response – a Multi-Step Process

Canadian privacy commissioners have issued guidance for a multi-step process for responding to a privacy breach. The recommended steps are: (1) containment; (2) risk evaluation; (3) notification/reporting; and (4) prevention of future breaches/monitoring. See *Tips for containing and reducing the risks of a privacy breach*,*Privacy Breaches: Tools and Resources*,*Key Steps in Responding to Privacy Breaches*, and *What to do in case of loss or theft of personal information*.

The recommended incident response process generally aligns with cybersecurity best practices and guidance issued by other regulators, including the *Computer Security Incident Handling Guide* issued by the United States National Institute of Standards and Technology (NIST) and the Investment Industry Association of Canada's *Cyber Incident Management Planning Guide*.

With respect to the prevention of future breaches,*Tips for containing and reducing the risks of a privacy breach* explains:

"Once the immediate steps are taken to mitigate the risks associated with the breach, organizations need to take the time to investigate the cause of the breach and consider whether to develop a prevention plan. The level of effort should reflect the significance of the breach and whether it was a systemic breach or an isolated instance. This plan may include … a security audit of both physical and technical security … a review of policies and procedures and any changes to reflect the lessons learned from the investigation and regularly after that … a review of employee training practices … and a review of service delivery partners …".

The Office of the Privacy Commissioner of Canada has *observed* that the final breach response step "may tend to get short-shrift", and incidents that appear to be one-off events might not get sufficient attention to identify underlying systemic problems. Similarly, the NIST*Computer Security Incident Handling Guide* notes: "One of the most important parts of incident response is also the most often omitted: learning and improving".

Punitive Damages Possible for Failure to Prevent Future Privacy Breaches

The British Columbia Court of Appeal decision in*Ari v. Insurance Corporation of British Columbia* involved a proposed class action against the Insurance Corporation of British Columbia (ICBC) for the statutory tort of violation of privacy. An ICBC employee allegedly accessed the information of 78 ICBC customers and provided it to a criminal organization. After the privacy breach was discovered, ICBC cooperated with police and enhanced its security protocols. The chambers judge certified the class proceeding but declined to certify the issue of punitive damages. The chambers judge focused on ICBC's laudable conduct after the breach was discovered and held that there was no basis in fact for any finding that ICBC's conduct justified an award of punitive damages. On appeal by the plaintiff, the Court of Appeal held that the chambers judge had erred by refusing to certify the issue of punitive damages. The Court of Appeal stated:

"Rather than consider the past history of breaches of privacy by ICBC employees – the evidence supported that at least 7 employees have been terminated by ICBC between 2008 and 2011 for privacy breaches – the chambers judge considered the steps taken since the breach in this case was discovered. While laudable on ICBC's part, subsequent conduct is not the sole basis upon which punitive damages are determined. The chambers judge should have accepted as true the allegation that ICBC has a history of employees breaching private information."

The Court of Appeal concluded that the history of privacy breaches by ICBC's employees constituted a sufficient basis in fact for certifying the punitive damages issue as a common issue for the class proceeding.

Comment

The decision in *Ari v. Insurance Corporation of British Columbia* is an important reminder for organizations to ensure that their incident response procedures include a post-incident assessment and implementation of appropriate preventative measures and monitoring. For more information, see BLG bulletins *Data Security Incident* Response Plans – Some Practical Suggestions, and Cyber Incident Response Plans – *Test, Train and Exercise*.

Organizations should also consider implementing a legal privilege strategy to help avoid inadvertent and unnecessary disclosures of privileged legal advice given during a post-incident assessment. For more information, see BLG bulletins *Cyber Risk Management* - Legal Privilege Strategy – Part 1,Cyber Risk Management – Legal Privilege Strategy – *Part 2*,*Legal Privilege for Data Security Incident Investigation Reports*, and *Loss of Legal Privilege over Cyberattack Investigation Report*.

Expertise

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749