OPC releases report card on mandatory privacy breach notification

DECEMBER 2021

AT A GLANCE

- The Office of the Privacy Commissioner (OPC) has released its report on the first year of mandatory privacy breach notification under the Privacy Act 2020. [1]
- The report identifies a number of interesting trends, particularly regarding the prominent causes of privacy breaches notified to the OPC and the nature of the resulting harms.
- The report provides helpful insight for insureds and insurers alike in terms of strengthening and emerging threats and likely claim areas across privacy and cyber.

THE NEW REGIME UNDER THE PRIVACY ACT 2020

The Privacy Act 2020 came into force on 1 December 2020 (see our earlier article). The Act implemented a range of new requirements, including mandatory privacy breach notification obligations. The notification regime requires organisations to notify the Office of the Privacy Commissioner (OPC) and affected individuals of all privacy breaches that pose a risk of serious harm. The assessment of what constitutes serious harm requires consideration of the factors set out under s. 113 of the Act.

As with any new regulatory regime, the Privacy Act 2020 involved a period of adjustment for both the organisations it applies to and the regulator.

In July 2021, the OPC provided updated guidance indicating that it was taking a more robust approach to mandatory breach notification. As we summarised at the time, the OPC expects to be informed of notifiable privacy breaches within 72 hours of breaches being detected. It also expects organisations to notify instances concerning loss or restriction of access (such as ransomware) and indicated its intention to act against organisations where there had been repeated breaches.

THE OPC'S REPORT – MANDATORY PRIVACY BREACH REPORT ONE YEAR ON

The OPC's latest report (which draws on figures from 1 December 2020 to 31 October 2021) paints a vivid picture of the first year of mandatory privacy breach reporting.

Key takeaways include:

- Between 1 December 2020 and 31 October 2021 the OPC received 697 privacy breach notifications, approximately four times as many as were received in the same period the year before.
- Of those notifications, 67% reached the serious harm threshold, while 33% did not. While the number of "not serious" breaches was relatively high, the OPC encouraged organisations to err on the side of caution and report breaches if they thought they could be serious.
- Human error accounted for 62% of notified breaches. Malicious attacks accounted for a further 25%. Theft accounted for 6%. Human errors included accidental disclosure of sensitive personal information, data entry errors, confidentiality breaches, redaction errors, and postal and courier errors. The OPC's solution to these errors is to have robust systems and processes in place.
- The most common harm identified was emotional harm, which occurred in 35% of notified breaches. This was followed by reputational harm (14%) and identity theft (13%). Emotional harm could result from a privacy breach where there was a risk of significant humiliation, significant loss of dignity or significant injury to an individual's feelings.

[1] https://www.privacy.org.nz/publications/insights-reports/december-2021-insights-report-privacy-breach-reporting/

- Privacy breaches were reported across a range of industries, although the healthcare and social assistance (79), public administration (51) and education (24) were the most common. Finance (including insurance) was the fifth most common sector, accounting for 14 of the notified breaches. The public sector accounts for 54% of all reported breaches, with the private sector accounting for 35% and non-profits 11%. The OPC was somewhat circumspect on the implication of these statistics. It noted that the increased representation of some sectors may simply reflect heightened awareness of obligations to report privacy breaches.
- The OPC again emphasised the expectation that notifiable breaches will be notified to the OPC within 72 hours. Only 44% of serious breach notifications were made within this timeframe, while 25% were made within 10 days.

LESSONS LEARNED FOR INSURERS AND INSUREDS

The quadrupling of breach notifications matches the increase observed in other jurisdictions that implemented similar mandatory breach notification frameworks. Research conducted by our Legalign Global partner, DAC Beachcroft in the UK, identified a similar trend when mandatory breach notification requirements were implemented in 2018.

That human error remains the leading cause of privacy incidents should serve as a timely reminder to insurers. While headlines are generally dedicated to malicious attacks, accidental disclosures remain incredibly common, and are regularly the cause of third-party claims. Good information governance is not just a matter of technical information and cyber security. It also involves organisations addressing the human element of privacy and data protection through training, awareness and robust response procedures and policies.

Similarly, an organisation's focus cannot be on pecuniary loss alone. Potential emotional harm was widely reported among breach notifications. When responding to an incident, it remains critical that organisations consider the incident from the perspective of the victim and take a holistic view of potential harms.

Finally, the OPC's requirement to notify breaches within 72 hours continues to be a major focus for the regulator and should reinforce the need to involve breach council as early as possible in an incident. Leaving legal and privacy issues until after systems are restored may leave organisations exposed to increased regulatory scrutiny, particularly if the incident has implicated potentially sensitive information.

wotton kearney

Need to know more?

If you'd like to know more about your obligations under the Privacy Act 2020 or what these latest statistics may mean for your business, or you'd like to review a previous incident or prepare an incident response plan, please get in touch with a member of our Cyber and Data Risk team.

Mark Anderson
Partner (Auckland)
T: +64 9 280 0524
E: mark.anderson@wottonkearney.com

Joseph Fitzgerald
Special Counsel (Wellington)
T: +64 4 260 4796
E: joseph.fitzgerald@wottonkearney.com

© Wotton + Kearney 2021

This publication is intended to provide commentary and general information. It should not be relied upon as legal advice. Formal legal advice should be sought in particular transactions or on matters of interest arising from this publication. Company no 3179310. Regulated by the New Zealand Law Society.