Still Phishing: The Notifiable Data Breaches Scheme One Year On

Rebecca Lindhout, Special Counsel, and **Andrew Miers**, Partner, HWL Ebsworth Lawyers,
reflect on the OAIC's Notifiable Data Breaches Scheme 12-Month Insights Report.

Key Points

- The Notifiable Data Breaches Scheme 12-month Insights Report issued by the Office of the Australian Information Commissioner (**OAIC**) on 13 May 2019 (**Annual Report**) revealed that malicious or criminal attacks which exploit vulnerabilities involving a human factor continue to be the main reasons for notifications under the Notifiable Data Breaches Scheme (**NDB Scheme**).
- According to the Annual Report, phishing and spear phishing are the most common and highly effective methods by which entities are being compromised - whether the entity is large or small, and within Australia and internationally.
- The OAIC's findings are broadly consistent with our experiences in handling data breaches during the first 12 months of the NDB Scheme. In particular, the impact of phishing emails, often resulting in business email compromises, dominate the cyber incident landscape.
- While entities generally appear to be taking steps to comply with their obligations under the NDB Scheme, the OAIC notes that there is still an opportunity to be more proactive in approaching privacy and data security compliance and to build further trust with individuals, particularly in relation to harm minimisation and prevention of further data breaches.
- As a result, we recommend clients take this opportunity to review and update their approach to data security and handling data breaches including prevention, harm minimisation and their notification procedures, particularly based on the observations and recommendations of the OAIC.
- We also recommend clients seek expert advice in dealing with data and cyber breaches and, if they have a cyber insurance policy, engage with their insurer in responding to any breach, including any breach response solution the insurer may offer.

Continued on page 8 >

Snapshot of the statistics

Volume of notifications	As expected, the introduction of the NDB Scheme resulted in an increase in notifications of data breaches. • The OAIC received 1,132 notifications in total, of which 964 were eligible data breaches (for which notification was mandatory) and 168 were voluntary (either because they were not 'eligible data breaches' under the NDB Scheme or because the reporting entity is not bound by the Privacy Act). • This was a 712% increase in data breach reporting compared with the previous 12 months under the voluntary scheme that existed prior to the NDB Scheme. Reporting was fairly consistent during the year with 242 notifications during April - June 2018, 245 notifications from July - September 2018, 262 notifications from October - December 2018 and 215 notifications from January - March 2019.
Cause of data breaches	Of the reported data breaches: • 60% were caused by malicious or criminal attacks; • 35% were caused by human error such as incorrectly addressed emails and lost data storage devices; and • 5% were caused by system faults such as a bug in the web code. Malicious intent was the primary motivation behind most data breaches, with: • 68% attributable to common cyber threats such as phishing, malware, ransomware, brute force attacks and other forms of hacking; and • 32% attributable to theft of paperwork or data storage devices, social engineering or impersonation. While the report distinguishes between data breaches caused by 'malicious or criminal attacks' and those caused by 'human error', it is worth noting that human error still plays a significant role in most malicious or criminal attacks as well. For example, while phishing incidents are initiated by a malicious actor, they only succeed when an employee falls for the trick and clicks on the offending link or enters their credentials. Our experience of handling data breaches suggests that phishing emails, often leading to business email compromises, are rife in Australia. The Australian Cyber Security Centre has described business email compromise as the 'major current cybercrime threat to business'. Apart from the potential for unauthorised access to personal information, business email compromise also often results in other significant business risks such as the sending of fraudulent payment requests.
Affected data	The most commonly compromised data is contact information, being 86% of personal information affected by data breaches. Often this will be in combination with other forms of data and it is that combination that can lead to the potency of the potential harm.

Key learnings

Reducing the risk of credential compromise

Credential compromise includes phishing attacks which accounted for 39% of cyber incidents during the first year of the NDB Scheme. Phishing is where confidential information is stolen by sending fraudulent emails to victims. This becomes 'spear phishing' (i.e. more targeted phishing) when individuals or companies are specifically targeted based on company information sourced from publicly available sources such as annual reports and media releases.

To reduce the risk of credential compromise, the OAIC recommends that entities:

- educate users on how to detect phishing emails and about password re-use and security measures;
- implement multi-factor authentication and anti-spoofing controls such as DMARC or SPF; and
- refer to their further guidance about preventing credential compromise.

We also recommend that entities:

- rethink how they effectively secure the types of personal information they hold, including by implementing the Australian Cyber Security Centre's "Essential Eight" Strategies to Mitigate Cyber Security Incidents;
- develop a cyber security policy (and then regularly review and update it);
- prepare a cyber incident response plan (including incorporating a data breach response plan); and
- consider cyber security insurance to offset the cost of responding to cyber incidents and data breaches and potential losses that may arise. An entity's cyber insurance policy will also often provide a breach response solution to assist in responding to an incident.

Managing Data Breaches

Putting individuals first

According to the Annual Report, one of the key areas where there is room for improvement is in putting individuals first.

IDCARE (a not-for-profit charity supporting individuals in Australia and New Zealand with identity and cyber security concerns) contributed to the Annual Report and noted a disparity between:

- the time taken between a data breach and misuse of those credentials (9.55 days);
- the average time taken for a breach to be detected (90 days); and
- the time then taken for individuals to be notified (a further 28.25 days).

IDCARE also notes a customer experience score of only 4.1 out of 10 for those affected by data breaches.

In light of the IDCARE insights into how quickly credentials are misused, time is clearly of the essence in both detecting breaches and notifying individuals so they can take preventative action to protect themselves. It is also key to notify individuals in plain English to minimise confusion and enhance trust as much as possible. The OAIC has included additional guidance on how to notify individuals and what to include in notifications in its guide to managing data breaches.

In our experience in dealing with data breaches, this also needs to be balanced against the desirability of not causing undue panic, the guiding principle perhaps being described as 'be alert but not alarmed'.

Assessing the seriousness of harm in relation to a data breach

The OAIC noted that determining whether a data breach is an 'eligible data breach', particularly the likelihood of serious harm, is still a challenge for entities, particularly where the nature of the harm is less immediate but may still be serious. For example:

- breaches involving contact information may result in that information being used in a phishing attempt which seems more real and so is more successful;
- breaches involving contact information may result in threats to an individual's safety (such as where a person who is the subject of domestic violence has their new address mistakenly disclosed to their attacker); and
- breaches of personal information such as health information may result in damage to reputation or relationships or in workplace or social bullying.

Accordingly, the OAIC recommends taking a longer term approach to monitoring and responding to the risk of harm to affected individuals in the case of data breaches.

In our experience, the possibility of contact information being used in phishing attempts is one of the more common forms of potential harm to arise. However, a breach of contact information is also one of the more nebulous breaches to pin down in assessing the risk of harm since the potential impact is far more indirect and requires other intervening steps first to occur before any actual harm materialises.

Managing multi-party breaches

Eleven multi-party breaches were reported to the OAIC during the 12 months. A multi-party breach occurs where one or more entities hold personal information jointly - such as where it is owned by one entity and used by others. In these circumstances, each of the affected entities has obligations under the NDB Scheme but compliance by one entity will generally be taken as compliance by each of the entities who hold the information.

The OAIC suggests that the entity with the most direct relationship with the individuals affected by the data breach should make the notification. We think this stands to reason because, regardless of which third party might be responsible for the breach occurring, ultimately it is the reputation of the entity in direct relationship with the individuals whose reputation is on the line. That entity is going to want to have some control over the messaging.

Accordingly, the OAIC recommends that:

- entities should ensure their contracts with suppliers (and other third parties) who have access to and use of their information address arrangements in the event of a data breach. This includes responsibility for gathering the relevant information, allowing access to premises and systems, responsibility for assessing the data breach, taking steps necessary to minimise the harm and prevent it recurring, and also responsibility for making any necessary notifications; and
- entities' data breach response plans should be consistent with the approach they agree in their third party contracts. Data breach response plans should also consider any international notifications which may also be required (eg under the GDPR).

Taking these steps will help:

- minimise the likelihood of multiple notifications being made to the OAIC and to affected persons, which is likely to result in unnecessary confusion; and
- allow entities and their suppliers (or other affected entities) to work in a collaborative manner which gives comfort about transparency and is also more likely to result in harm reduction.

Harm reduction and preventative measures

The Annual Report contains practical examples of actual breaches and drawn out suggestions from those breaches around harm reduction and preventative measures which can be implemented in the case of a data breach. These include:

- where an employee's email account was compromised:
  - engaging an external firm to notify affected individuals, including advice to delete the phishing email, change their passwords and monitor their bank accounts; and
  - implementing multi-factor authentication, a secure customer relationship management system for document transfer and additional staff training around spotting spoofed emails as preventative measures; and
- where an entity became aware that an unknown third party had gained unauthorised access to some member accounts in its online portal:
  - immediately notifying the individuals and deactivating the affected accounts;
  - only reinstating the affected accounts with additional security measures such as CAPTCHA (i.e. "completely automated public Turing test to tell computers and humans apart") and identity verification checks to prevent future unauthorised access; and
  - where a data breach affected a vulnerable segment of the community, the affected entity used social workers to notify and provide support to affected individuals via phone.

Conclusion

The OAIC concluded that *'the first year of the NDB Scheme has resulted in welcome improvements in transparency and accountability for the protection of personal information'*. With plenty of lessons and recommendations coming out of the first year of the NDB Scheme, including those set out above, entities who focus on achieving an environment where privacy and security are core focuses rather than just a 'compliance issue' have the opportunity to enhance trust with their consumers and end-users, and differentiate themselves.

Contributions & Comments

Contibutions and Comments are sought from the members and non-members of CAMLA, including features, articles, and case notes. Suggestions and comments on the content and format of the Communications Law Bulletin are also welcomed.

Contributions in electronic format and comments should be forwarded to the editors of the Communications Law Bulletin at:

clbeditors@gmail.com