Caring about the notifiable data breach: The human impact on victims

by **DARREN HOPKINS** *Advisory Partner, McGrathNicol*, and **DARREN LIM MANAGER** *McGrathNicol*, and **LEAH MOONEY** *Executive Director and Company Secretary, IDCARE*

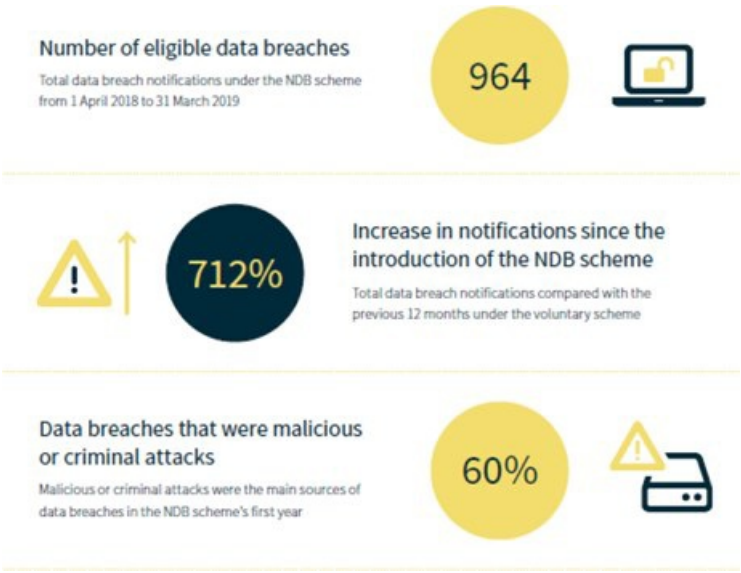
With the Notifiable Data Breach (NDB) scheme under the *Privacy Act 1998* in full force, the threat of financial and reputational impacts to organisations often overshadows the human element of the data breaches; in essence, we tend to forget what it means to be an individual impacted by a data breach. In this article, we seek to examine not only the financial hardships and lost opportunity in terms of time that individuals may suffer, but also the potential psychological impact they may endure from a breach. We also analyse the need for more informed decisions from organisations in notifying an individual impacted by a breach, as sometimes the act of notifying an individual can cause more harm than the breach itself.

Back to basics: Why the Notifiable Data Breach scheme was created

When the Notifiable Data Breach (NDB) scheme was first introduced in February 2018, there was a huge level of anticipation and trepidation for Australian organisations. While not the first of its kind conceptually (with similar data breach regulations in force worldwide), the NDB scheme was definitely a modernised concept and generally welcomed by privacy advocates in Australia. Organisations took action to bolster their own data security and breach response procedures in an effort to comply with the newly introduced NDB scheme.

Under the NDB Scheme, organisations are required to notify only 'eligible data breaches' to the Office of the Australian Information Commissioner (OAIC) and impacted individuals. An eligible data breach is an unauthorised access or disclosure (or loss likely to result in same) that is likely to result in serious harm to the individuals impacted. Part of the reasoning behind notifying only eligible data breaches is so that individuals may take steps to remediate the risk of harm to themselves.

Diagram 1 – the first year of the NDB Scheme



Statistics released by the OAIC one year after the NDB scheme introduced: https://www.oaic.gov.au/resources/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics/ndb-scheme-12%E2%80%91month-insights-report.pdf

Certainly, the potential financial, operational, reputational and regulatory impacts that organisations suffer from a data breach occurrence has been an effective motivator in encouraging compliance. However, what is often forgotten is the human impact. As the OAIC have quoted, the goal of the NDB scheme at the end of the day is to seek outcomes in the public interest. The OAIC also encourages organisations to go beyond doing the minimum compliance steps required from the Scheme by 'taking steps to put the consumer first'; in essence, consider their duty of care for their customer's personal data and appropriately protect it.

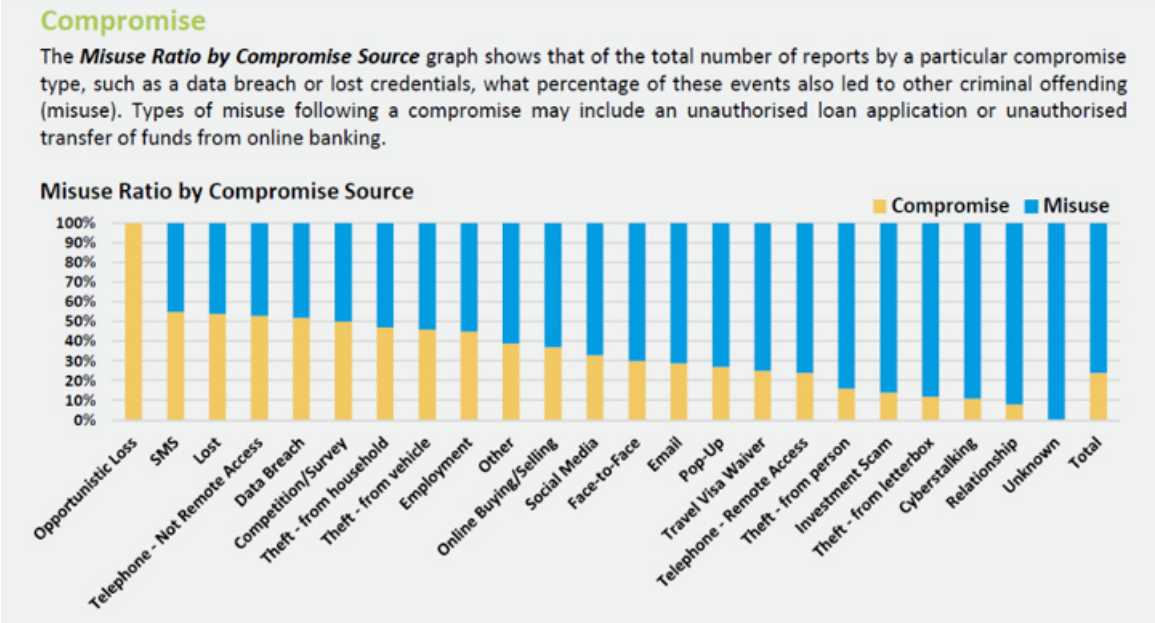
To further reinforce that data breaches really are about the impacted individuals, a hard-hitting example to consider is the Ashley Madison data breach. This breach, involving adult introduction services, caused significant embarrassment and thereto demonstrated the emotional and psychological impact a data breach can have on impacted individuals. Further, through the insights gleaned from his 'haveibeenpwned' tool, security researcher Troy Hunt reported the impacts of the Ashley Madison data breach on the many husbands, wives, families, and friends that had their lives transformed and broken up: 'This incident needs to be approached with the understanding that for many people, this is the worst time of their life and for some, it feels like the end of it.' Tragically, it is believed that one of the individuals impacted did end up taking their life.

What it means to be impacted by a data breach

Data breaches can have varying degrees of impact upon the individuals involved, depending on the context of the breach and the risk attached to the personal information credentials compromised. While exposure of low-risk personal information credentials such as phone numbers and email addresses are common, the exposure of high-risk credentials such as credit card numbers, bank account details, scans of passports and personal health information often results in emotional distress. The individual may be concerned that their credit cards will be maxed out, bank account funds depleted, and passports and personal health information freely sold on the Dark net for malicious purposes. Also worthwhile considering is the importance of context - sometimes low risk credentials such as a name and address in the context of a protected person may lead to a real world attack such as physical assault and stalking.

Further, sometimes the very act of notifying individuals of a data breach may result in a harmful impact.

Being called a victim and being told you were 'breached' does not sit well with impacted individuals. IDCARE reports that, based on the data collected by their National Case Management Centre, a significant proportion of individuals experience emotional harm as a result of a data breach notification. By way of contrast, the reported level of actual misuse was less than 50%. This finding supports the need for reflection for organisations whose strategy is to proceed to notify data breaches under the NDBS before making the effort to properly assess the risk of harm (or attempting to remediate the harm).



IDCARE Diagram: Misuse Ratio by Compromise Source

While it is difficult to measure and quantify the exact amount of emotional harm individuals actually experience as a result of a breach, IDCARE have received many requests for counselling as a result of the anger, distress and other psychological impacts resulting from individuals being notified of a data breach, regardless of whether their data was actually misused. The challenge for organisations is balancing the knowledge that the act of notifying can cause emotional distress and making an informed yet timely judgement call of whether notification is required from a regulatory (and customer-focused) perspective.

Widening the circle: Considering others impacted by breach

There are other individuals impacted by a data breach 'that are not always identified. Consider the image below:

The **primary impacted individual(s)** is as described above: the primary individual impacted by a data breach. They ultimately face the consequences over the loss of their personal data.

However, the toll on **primary responsible persons** is often overlooked in a data breach scenario. The investigation often focuses on the responsible people for the breach. Experts within the industry are often quick to judge, stating that the responsible individuals should have known better. Unfortunately, cybersecurity evolves at such a rapid pace that commonly accepted practices are suddenly a security risk. The impact may be wide ranging and emotional for the responsible persons (and families by extension), sometimes resulting in humiliation and loss of reputation, loss of bonuses or job. Organisations should therefore treat the Primary Responsible Person with empathy, and offer training and other support to uplift their cyber security knowledge. It is also important to create a culture whereby staff feel comfortable reporting incidents that may lead to breaches.

The **primary responsible organisation** is also impacted in a data breach scenario. While breaches may occur due to a lack of awareness or other human error, sometimes there is a technical cause (such as a scenario where a misconfigured security control which was overlooked during a project go-live led to a large database leak). For larger organisations, sometimes the consequences of the breach is easily absorbed. But for medium and smaller organisations, an incident could have devastating impacts which potentially lead to the organisation becoming defunct. This may results in a loss of jobs, which impacts the employees and their families.

The **remediation parties** are the people and teams within the Primary Responsible Organisation tasked with remedying the breach caused at the primary organisation. The remediation parties face the weight of responsibility of attempting to detect, analyse, respond and contain the breach before further damage is caused to the impacted individuals. This often requires lengthened working hours for the teams and the additional stress knowing that each hour counted. Feelings of helplessness and resentment are common amongst these teams who would be working against very tight deadlines in these situations.

Third parties are also impacted in different ways by data breaches. While not directly responsible for the breach, security experts argue that it is an organisation's responsibility (particularly larger organisations) to perform ongoing due diligence measures to uncover instances of these third party security risks. Data breaches may result in loss of business by existing or potential customers, increased overhead dedicated to call centres addressing breach concerns and additional remediation efforts to

bolster their cybersecurity posture. Teams within the impacted Third Parties may face similar stress and elevated workloads to the Remediation Parties alongside feelings of resentment towards the organisations primarily responsible for the breach.

Getting the right equilibrium in the response

In event of a data breach, it is important to make a timely decision. Every minute that passes in a data breach increases the likelihood of personal data being misused by threat actors. With the introduction of the New Payments Platform in Australia, everyday payments occurring at a rapid and real-time pace now means only a matter of minutes is the difference between a bank account being depleted or a bank account's details being changed to prevent unauthorised access and transfer.

At the same time, organisations must adequately analyse the data breach to have a clear picture on the extent of the breach and the severity of the perceived harm. They are required to determine whether actual serious 'harm' has occurred (or is likely), otherwise the notification of breach may result in a more adverse impact to data breach impacted.

Takeaways for organisations

- **Be prepared for a data breach**. This includes developing a breach response plan, establishing roles and responsibilities for a breach scenario and formalising the process for evaluating whether serious 'harm' has occurred. In addition, have a communication plan prepared. Be prepared to make a statement to regulatory authorities as well as affected customers in event of a breach.
- **Be transparent about the data breach**. Give visibility and answers to customers. There is no point of making them paranoid if no real tangible harm had occurred. Clearly articulate the categories of personal information used in the breach.
- **Invest in your staff's Cyber Awareness.** The most effective and bang-for-your-buck strategy is to take the time to train your people and raise awareness about different ways your organisation may be breached. It is also important to build a culture which encourages reporting and escalation.
- **Collect and use only what you need.** Less personal information means less exposure in a data breach. Reduce the records of personal data you hold and adopt anonymisation when data usage is required. Protect yourself by reducing your threat surface.
- **Offer clear advice to breach impacted individuals on how to get help**. Where possible, offer identity protection services and counselling to the impacted individuals. If in doubt, IDCARE's identity and cyber support services are available to organisations, with fees charged on a cost-recovery basis. By engaging IDCARE, organisations can obtain a unique referral code to refer individuals to IDCARE directly. This ensures impacted individuals get the right advice from the outset and helps to boost the impacted persons' confidence and satisfaction in the support you provide them after the breach.

When it comes data breaches and the NDB scheme, it is important for organisations to broaden their view past their own organisation risk and recognise the real human impact of a data breach.

Empathising with the impacted individuals of a breach and recognising the need for mature breach practices will help us all protect what is truly important at the end of the day.

McGrathNicol

Darren Hopkins can be contacted on +61 7 3333 9870 or by email at dhopkins@mcgrathnicol.com. Darren Lim can be contacted on +61 2 9248 9927 or by email at dlim@mcgrathnicol.com and you can reach Leah Mooney via her LinkedIn.