Australian Government

Office of the Australian Information Commissioner

Notifiable Data Breaches Scheme 12-month Insights Report

OAIC

Please attribute the content of this publication as:
Office of the Australian Information Commissioner Notifiable Data Breaches Scheme 12-month Insights Report.

Contact

Mail: Director, Strategic Communications
Office of the Australian Information Commissioner
GPO Box 5218
Sydney NSW 2001

Email: enquiries@oaic.gov.au
Website: www.oaic.gov.au
Twitter: @OAICgov
Phone: 1300 363 992

Non-English speakers

If you speak a language other than English and need help, please call the Translating and Interpreting Service on 131 450 and ask for the Office of the Australian Information Commissioner on 1300 363 992.

Accessible formats

All our publications can be made available in a range of accessible formats. If you would like this report in an accessible format, please contact us.

Contents

Commissioner's foreword

In this report we look back on the last 12 months of the Notifiable Data Breaches scheme (NDB scheme). The NDB scheme introduced new obligations for Australian Government agencies and private sector organisations (entities) that have existing information security obligations under the *Privacy Act 1988* (Cth) (the Privacy Act). For a little over a year, it has been a legal requirement for entities to carry out an assessment whenever they suspect that there may have been loss of, unauthorised access to, or unauthorised disclosure of personal information that they hold. If serious harm is likely to result, they must notify affected individuals so they can take action to address the possible consequences. They must also notify the Office of the Australian Information Commissioner (OAIC).

The requirement to notify individuals of eligible data breaches goes to the core of what should underpin good privacy practice for any entity—transparency and accountability. Being ready to assess and, if appropriate, notify of a data breach provides an opportunity for entities to understand where privacy risks lie within their operations, to address the human and cyber elements that contribute to data breaches and to prevent or minimise harm to individuals and the community. And, of course, prevention is better than cure. The requirements under the NDB scheme incentivise entities to ensure they have reasonable steps in place to secure personal information.

This report examines the trends that have emerged under the NDB scheme in its first full year of operation. The NDB scheme commenced in February 2018, and this report draws on the four complete quarters of data collected since that time, from 1 April 2018 to 31 March 2019. We highlight practices of regulated entities over this period and look to where the opportunities for improvement lie. We intend that this report will assist entities and others to understand the common causes of data breaches and to implement proactive strategies for better prevention into the future.

The report also presents us with an opportunity to reflect on the purposes of the NDB scheme and how these purposes have been served in the first year.

The Explanatory Memorandum supporting the introduction of the NDB scheme states that a key objective of the NDB scheme is consumer protection.[1] Introduction of the NDB scheme followed recommendations of the Australian Law Reform Commission[2] and the Parliamentary Joint Committee on Intelligence and Security.[3] The NDB scheme also intended to incentivise entities to improve security standards relating to personal information.

Specifically, the NDB scheme aims to address any underreporting and delays in reporting under the voluntary scheme preceding it. Delays can reduce the opportunities that a consumer would otherwise have had to take steps to prevent harm resulting from a data breach.

Overall, it was anticipated that the NDB scheme would raise confidence amongst consumers about the entities that they are dealing with, and the increased transparency would provide consumers with more information to make informed choices about whether to transact with particular entities.

Over the past year, my office has directed its efforts to driving awareness of the NDB scheme's requirements, the causes of data breaches and better data breach management practices. We have focused on providing support to regulated entities to assist them to comply with their notification obligations and understand the causes of data breaches to prevent them in the future. This is consistent with our general approach of working with entities to encourage and facilitate voluntary compliance with their obligations.[4] We have also examined security practices and conducted inquiries to ensure containment, rectification and future mitigation of security risks. There have also been times when further regulatory action has been necessary, including issuing a direction to notify under s 26WR of the Privacy Act.

In this period, we have observed efforts by many entities to lift their practices, such as by developing and implementing data breach response plans and improving security and privacy standards, and efforts by some entities in adopting data minimisation policies to reduce overall exposure.

Many entities have taken a proactive approach in engaging with the OAIC, and we have been able to work constructively with those in their response. This includes assisting entities to navigate the reporting threshold. As the year has progressed, some maturation has been evident in entities assessing the likely consequences of a data breach and in their subsequent notification processes.

The OAIC has reported quarterly on the NDB scheme during its first year of operation, supplementing statistical insights with analysis and detailed trend data. We believe that by understanding causes and sectoral trends, entities can drive real improvements to people, process and technology measures which prevent data breaches.

While the NDB scheme does not generally permit the OAIC to publish details about which entities have reported eligible data breaches, there has been a sustained interest from the media in reporting data breaches over the year, which has meant that in many cases, entities that have experienced a data breach have been in the public eye. This has led to growing awareness of privacy rights and issues amongst consumers and the risks inherent in putting information online, as well as proactive measures that every person can take to protect themselves. While there have not been high numbers of consumer complaints to the OAIC following a data breach, those that we receive can result from a perception that the response from the responsible entity is not adequate.

The past year has also led to collaboration across industry and between the OAIC and other organisations charged with supporting the Australian community to deal with data breaches and threats. The first reported multi-party breach, which affected a recruitment and human resources services provider and many of its customers, is an example where the OAIC, IDCARE and the Australian Cyber Security Centre (ACSC) cooperated to support affected individuals and the public with information clarifying the data breach and mitigation steps available.[5] We have continued to collaborate with the ACSC and IDCARE throughout the year and thank them for the support they provide in turn to regulated entities and affected individuals. I also thank the ACSC and IDCARE for sharing insights on the first year of the NDB scheme in this report.

As we move into the second year of operation of the NDB scheme, the OAIC expects entities to understand the causes of data breaches and take proactive steps to prevent them. This means taking reasonable steps to ensure that the necessary people, processes and technology are in place to prevent and respond to breaches.

We also encourage entities to move beyond compliance to effectively support consumers. While the law obliges entities regulated under the Privacy Act to provide transparent and useful information to consumers, it is those entities who focus on the consumer and navigate beyond compliance to support affected individuals to take steps to minimise or prevent harm in a meaningful way who will differentiate themselves and maintain trust over time.

In the coming year, the OAIC will take a proportionate and evidence-based regulatory approach in relation to the NDB scheme, including by exercising our enforcement powers where necessary. Through these actions, we will support the NDB scheme's purpose of protecting consumers by elevating the security posture across the economy and increasing transparent and accountable personal information handling practices.

I encourage entities regulated by the Privacy Act to review the report and use the learnings to enhance their prevention and response strategies for the benefit of all Australians.

Angelene Falk
Australian Information Commissioner
and Privacy Commissioner

Report at a glance

Entities regulated by the Privacy Act should review this report and use the learnings to enhance their prevention and response strategies for the benefit of all Australians. One of the key messages that we take from this inaugural review of the NDB scheme is that entities must put individuals first.

Number of eligible data breaches

Total data breach notifications under the NDB scheme from 1 April 2018 to 31 March 2019

964

712%

Increase in notifications since the introduction of the NDB scheme

Total data breach notifications compared with the previous 12 months under the voluntary scheme

Data breaches that were malicious or criminal attacks

Malicious or criminal attacks were the main sources of data breaches in the NDB scheme's first year

60%

153

Number of breaches attributed to phishing

Phishing and spear phishing continue to be the most common and highly effective methods by which entities are being compromised

Cyber incidents where credentials were obtained by unknown means

The notifying entity wasn't aware of how the credentials were obtained, because they had not detected any phishing-based compromise

28%

< 1000

83%

Data breaches that affected fewer than 1,000 people

The vast majority of data breaches reported in the first year of the NDB scheme each affected fewer than 1,000 people

Data breach notifications attributed to human error

Many data breaches involved human error, such as through unintended disclosure of personal information or the loss of a data storage device

35%

55%

Health sector data breaches due to human error

Human error was the leading cause of data breaches in the health sector, compared with an average of 35% for all sectors

Finance sector data breaches due to human error

In the finance sector, human error accounted for 41% of data breaches, compared with an average of 35% for all sectors

41%

86%

Notifications that involved contact information disclosure

Contact information was the most common form of personal information disclosed through data breaches during the period

The international landscape

The NDB scheme came into effect in the 30th year of operation of the Privacy Act in what would prove to be a landmark year for privacy. Along with the Privacy (Australian Government Agencies—Governance) APP Code 2017 (also introduced in 2018), the NDB scheme was a significant reform, providing greater transparency and accountability for personal information handling in Australia.

In a data-driven economy, it is clear that commercial and other uses of data enable innovation and provide opportunities for economic growth and social benefit. As the use of data has increased, there has been a shift in the public conversation about data use, and an international focus on the responsible and ethical use of data. In order to build community trust in a data-driven economy, all entities must treat personal information holdings with the highest levels of care and protect their customers, members and others from harm, including rectifying the negative impacts of breaches when they occur.

Over the last 12 months we witnessed major reforms to privacy laws internationally and some of the world's leading brands face scrutiny over their privacy policies and practices alongside a number of highly publicised international cyber security incidents. Allegations that Facebook profile information was collected and used by a political consultancy, Cambridge Analytica, prompted investigations in Australia and overseas, with parliamentary and congressional interest in the United Kingdom, Canada and the United States. Similarly, decisions by regulators in the European Union about Google's privacy policies and collection practices have concentrated attention on how entities obtain an individual's consent to the collection of their personal information.

The last 12 months have also seen an increase in public reporting on major cyber security incidents, which has focused attention on mandatory data breach reporting schemes internationally. These have included data breaches involving: the hotel chain Marriot International,[6] property valuer LandMark White,[7] and the airlines British Airways[8] and Cathay Pacific.

The European Union's General Data Protection Regulation (GDPR) commenced in May 2018, following a two-year transition period, bringing with it stronger data subject rights, new governance and accountability requirements and a strict 72-hour mandatory data breach notification reporting regime.

In recent years, additional privacy protections have arisen in other parts of the globe. In the Asia Pacific, new data protection regulations took effect in China, Singapore, the Philippines and Japan between 2016–18. Latin American countries such as Brazil have taken a lead from the GDPR, drafting comprehensive data protection regulations for the first time. In North America, Canada's new data breach notification laws came into effect in late 2018, while California's new data protection legislation (set to commence in 2020) features enhanced consent and breach reporting requirements. These developments come alongside a continued national conversation in the United States about possible federal privacy law.

The OAIC has engaged with international counterparts over the past year, including sharing lessons from the first year's operation of the NDB scheme as other jurisdictions considered or looked to implemented similar schemes (see Figure 1).

July 2003

California, United States

Businesses and state agencies must notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorised person. The data breach must affect more than 500 California residents.

January 2016

Netherlands

Autoriteit Persoonsgegevens must be notified of a data breach where there is a considerable likelihood of the data breach having serious adverse effects on the privacy of the affected individuals.

February 2018

Australia

The Office of the Australian Information Commissioner and affected individuals must be notified of a data breach that is likely to result in serious harm to any affected individual.

May 2018

European Union

EU data protection authorities must be notified of a data breach that is likely to result in a risk to the rights and freedoms of natural persons. Affected individuals must also be notified if the risk is high.

November 2018

Canada

The Privacy Commissioner of Canada, and affected individuals, must be notified of a breach of security safeguards involving personal information that pose a real risk of significant harm to individuals.

Proposed

New Zealand

The Office of the Privacy Commissioner NZ and affected individuals must be notified of any data breach that has caused, or is at risk of causing, harm.

Figure 1 — Selected data breach notification laws around the world

Insights from the NDB scheme in its first year of operation

The first year of the NDB scheme provided unprecedented visibility into how Australian entities are meeting the challenges associated with protecting personal information. Each quarter, the OAIC published detailed statistical reports summarising notifications made under the NDB scheme. The aggregated insights contained in each report allowed other entities and the broader public to learn from the experiences of notifying entities. The following section provides an overview of key insights from the NDB scheme for the period April 2018 to March 2019.

The introduction of the NDB scheme in February 2018 was widely expected to herald an increase in notifications from entities, in line with the community's expectations for greater accountability and transparency. This proved to be the case, with a 712 per cent increase in total data breach notifications compared with the previous 12 months under the voluntary scheme.

The growing number of data breaches notified to the OAIC is consistent with trends experienced by its counterparts overseas and indicates many entities are complying with their notification obligations.

Figure 2 — Data breaches notified under the NDB scheme, from 1 April 2018 to 31 March 2019

The NDB scheme has also shed light on the causes of data breaches, allowing entities to better understand how they might be avoided and implement prevention strategies. Malicious or criminal attacks were the main sources of data breaches in the NDB scheme's first year, reflecting the continued challenge organisations and governments face in mitigating risks from cyber security threats.

Still, most data breaches—including those resulting from a cyber incident—involved a human element, such as an employee sending information to the wrong person or clicking on a link that resulted in the compromise of user credentials.

Finance and health were the top industry sectors to report data breaches. This is likely a reflection of the high-volume data holdings in these industries and may also indicate comparatively mature processes for identifying and reporting data breaches. Both sectors face strong regulatory scrutiny around data protection, and the costs associated with data breaches may also be higher.[9]

Most data breaches reported in the first year of the NDB scheme each affected fewer than 1,000 people, with contact information the most common form of personal information lost.

In the past year, there were also 11 multi-party notification events, varying between two and 60 notifications per incident.

These themes are explored in more detail below.

Notification volumes

The OAIC received a total of 1,132 notifications (under the NDB scheme and on a voluntary basis) between 1 April 2018 and 31 March 2019. This comprised 964 eligible data breaches (see Figure 2) under the NDB scheme and 168 voluntary notifications (that is, notifications for breaches not deemed 'eligible data breaches' under the NDB scheme, usually because the threshold has not been reached or the reporting entity is not bound by the Privacy Act). There were 159 voluntary notifications in the year prior (1 April 2017 to 31 March 2018), meaning the 1,132 figure represents an increase of 712 per cent in data breach reporting over 12 months.

Prior to the NDB scheme, there were 114 voluntary notifications in the 2016–17 financial year and 107 voluntary notifications in the 2015–16 financial year. A key difference between voluntary notifications and the NDB scheme is that there was no obligation to inform affected individuals under the voluntary scheme.

Figure 3 illustrates the increase in data breach reporting to the OAIC (and affected individuals) following commencement of the NDB scheme. At the time of publication, the final column only includes data breaches notified in the first three quarters of the current financial year, and would likely reflect a higher figure at the end of the full financial year.

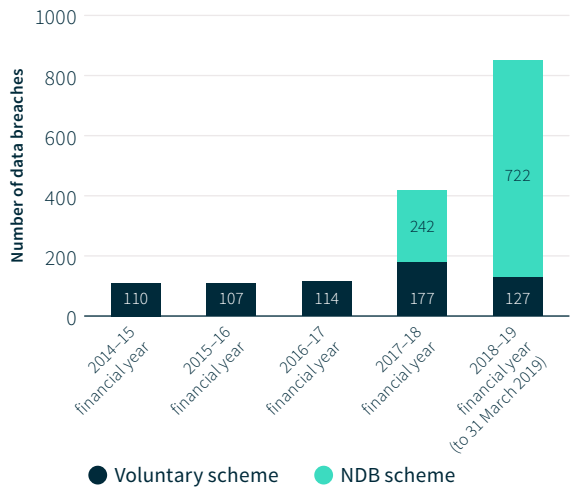

Figure 3 — Number of data breaches notified to the OAIC from 2014 to 2019

The increase in notifications reflects a significant increase in entities' awareness of and compliance with their obligations to notify the OAIC and affected individuals where a breach of personal information is likely to result in serious harm. This increased awareness is at least partially attributed to awareness and outreach activities by the OAIC and ongoing media coverage about the NDB scheme throughout the year. For example, 'data breaches' was the leading topic associated with the OAIC in national and major metro publications in 2018, according to analyses of online media mentions.

Table 1 sets out reporting volumes by quarter since the NDB scheme commenced.

Table 1 — Reporting volumes by quarter since the NDB scheme commenced

Period	Total number of notifications
January to March 2018[10] (NDB scheme commenced on 22 February 2018)	63
April to June 2018	242
July to September 2018	245
October to December 2018	262
January to March 2019	215

Heightened awareness of and compliance with the NDB scheme's obligations by entities was immediate and consistent throughout the year, with 242 notifications from April to June 2018, 245 notifications from July to September 2018, 262 notifications from October to December 2018 and 215 notifications from January to March 2019.

On occasion, the OAIC also received multiple notifications relating to the same data breach, where that data breach affected more than one entity (referred to as 'multi-party breaches' in this report). These notifications are counted as a single notification under the NDB scheme. Multi-party notifications are discussed in more detail later in this report.

Growth in the number of data breaches after the introduction of mandatory reporting is consistent with trends overseas. In the Netherlands, Germany and United Kingdom, approximately 15,400, 12,600 and 10,600 breaches were notified to supervisory authorities respectively in the first eight months after the GDPR took effect.[11] (Note: notification thresholds under each country's respective schemes and population sizes differ substantially compared with Australia.)

Sources of data breaches—overall

Figure 4 shows the breakdown of data breaches by source over the period 1 April 2018 to 31 March 2019.

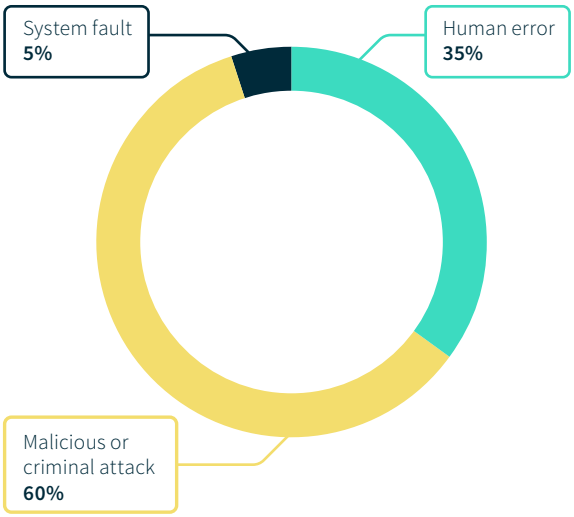

Figure 4 — Sources of data breaches by percentage—all sectors, from 1 April 2018 to 31 March 2019

Whether through direct human errors, such as sending personal information to an unauthorised recipient, or where cyber breaches were traced back to a human compromise, employees were centrally involved in most of the data breaches reported to the OAIC in the period.

Nevertheless, malicious intent was the primary motivation behind most data breaches. This trend is reflected in malicious or criminal attacks accounting for 60 per cent of data breaches, or 580 notifications reported to the OAIC in the period. Of these, 394 data breaches (68 per cent) are attributed to incidents resulting from common cyber threats such as phishing, malware, ransomware, brute-force attacks, compromised or stolen credentials and other forms of hacking. The remaining 186 data breaches (32 per cent) attributed to a malicious or criminal attack were the result of theft of paperwork or a data storage device, social engineering or impersonation, or an act of a rogue employee or insider threat. Further breakdowns of the causes of data breaches can be found in our detailed reports for each quarter (see **www.oaic.gov.au**).

Cyber incident breaches

Figure 5 shows the breakdown of cyber incident data breaches by source over the period 1 April 2018 to 31 March 2019. See the Glossary for a description of each breach category.

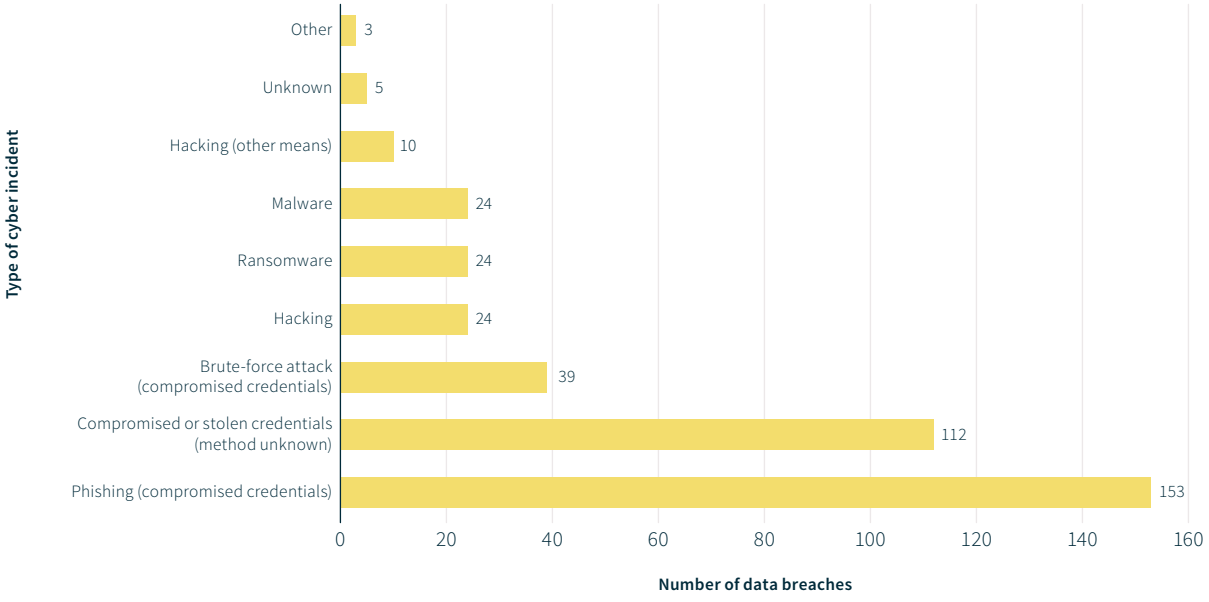

Figure 5 — Cyber incident breaches—all sectors, from 1 April 2018 to 31 March 2019

Notably, phishing and spear phishing continue to be the most common and highly effective methods by which entities are being compromised—whether large or small—in Australia or internationally.[12] Within the period, a total of 153 data breaches were attributed to this method.

Attackers typically use phishing to elicit credentials—usually a username and password—from a user to gain access to systems. Attacker techniques continue to evolve in this area, making phishing emails increasingly difficult to detect without sustained and focused user education.

After phishing, the second most prevalent cyber incident data breach involved compromised or stolen credentials where the method of compromise was not known by entities reporting to the OAIC. An explanation may be the growing prevalence of 'credential stuffing' attacks using breached user credentials that have been leaked or posted online.

Excluding cyber breaches, social engineering or impersonation and actions taken by a rogue employee or an insider threat were also significant contributors to data breaches, as was theft of paperwork or data storage devices.

Credential compromise

Compromised or stolen credentials underpinned most cyber incidents that led to data breaches in the first year of the NDB scheme.

Phishing provides one explanation for how cyber attackers gain access to credentials. So-called 'credential phishing' typically involves attackers tricking a user into giving up their login details by emailing them a link to a realistic looking login page for a service they trust. Common examples include password reset requests that purport to be from legitimate web-based email providers such as Gmail or Office 365. When the user enters their login details into the fraudulent site, they are handing over their credentials to cyber attackers.

Credentials obtained this way account for 39 per cent of cyber incidents.

However, in 28 per cent of cyber incidents, the notifying entity was not aware of how the credentials were obtained, most likely because they had not detected any phishing-based compromise.

The trend of 'credential stuffing' offers a likely explanation. This involves attackers trying out usernames and passwords obtained from other data breaches on an entity's digital services. In recent years, large troves of credentials have repeatedly been posted online by hackers. These troves typically aggregate credentials from previous data breaches. A recent dump of credentials, dubbed Collection 1-5, totals 100 billion records.[26]

The primary reason credential stuffing works is that many users re-use usernames and passwords across multiple accounts and services. Typically, attackers automate much of the work involved in this technique.

How entities can reduce the risk of credential compromise

- Educating users on how to detect phishing emails.
- Implementing multi-factor authentication.
- Implementing anti-spoofing controls (such as DMARC or SPF).[27]
- Educating users about password re-use and security measures (for example, password managers and services such as 'Have I Been Pwned'[28] to detect compromised accounts).

The OAIC and the ACSC have also developed tips to assist entities to prevent and mitigate data breaches, including how to prevent credential compromise.[13]

Human error breaches and system faults

After malicious or criminal attacks, human error accounted for 35 per cent of data breaches over the period 1 April 2018 to 31 March 2019 (see Figure 6 and the Glossary for a description of each breach category).

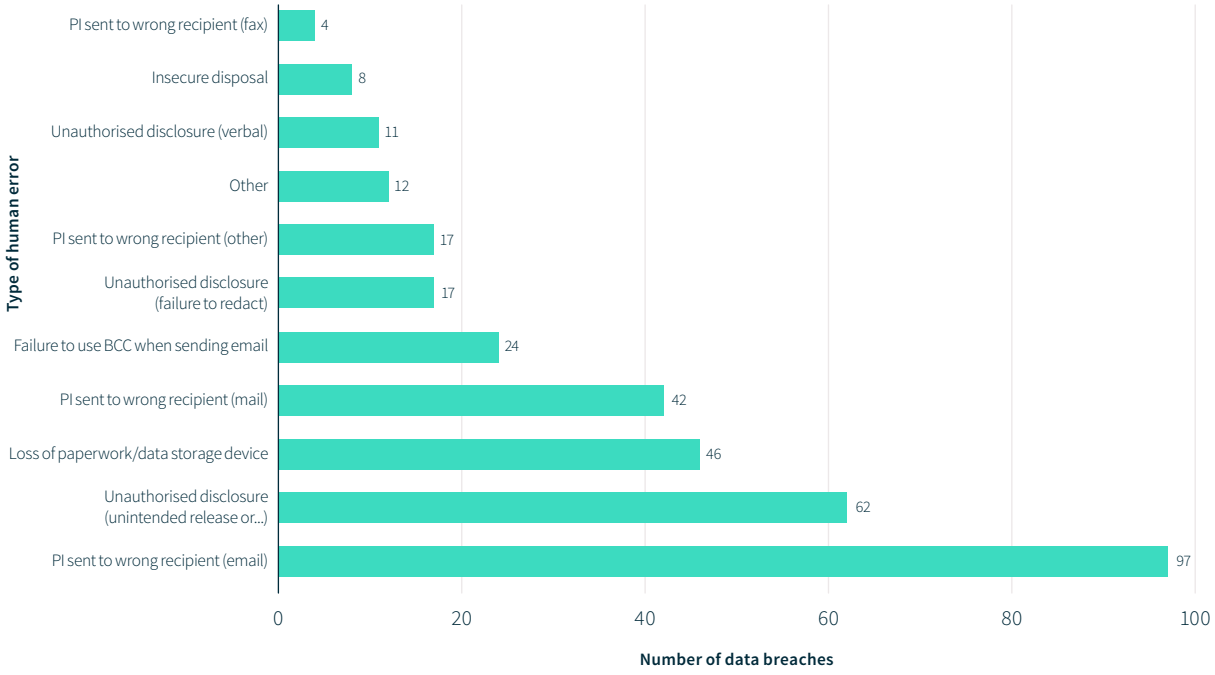

Figure 6 — Human error breaches—all sectors, from 1 April 2018 to 31 March 2019

Many data breaches involved human factors, whether through error or through malicious attack. The prominence of human factors pre-dates the NDB scheme. In the 2016–17 financial year, 46 per cent of voluntary data breach notifications received by the OAIC were attributed to human error.

This trend is evident in international jurisdictions as well. In the United Kingdom, most data breaches were the result of cyber incidents in which people were tricked into handing over credentials. In the Netherlands, the most common cause of data breaches was accidentally sending personal information to the wrong recipient.

The predominance of human factors in data breaches emphasises the importance of education and training for all employees who handle personal information. Implementing technological solutions, such as multi-factor authentication or system requirements that force users to choose a strong password and change it regularly, are also valuable.

Finally, system faults (for example, a bug in the web code or a fault that results in a document being sent to the wrong person) accounted for 5 per cent of data breaches between 1 April 2018 and 31 March 2019. Typically, a system fault resulted in the unintended release or publication of personal information.

Top reporting sectors

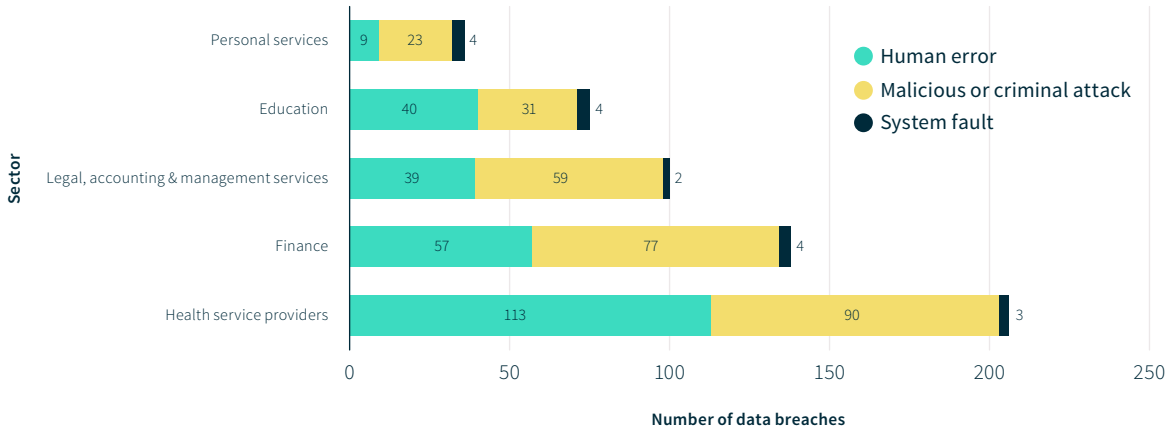

Figure 7 — Sources of breaches—top five sectors, from 1 April 2018 to 31 March 2019

Figure 7 shows that in the period of reporting (1 April 2018 to 31 March 2019), health service providers and finance were the sectors that made highest number of data breach notifications under the NDB scheme.

The consistent presence of the health and finance sectors at the top of the rankings throughout the year likely reflects the scale of data holdings, volume of processing activities and/or sensitivity of the personal information held by those sectors, as well as those sectors' higher preparedness to report data breaches. Both industries have also been subject to long-standing information protection obligations (including duties of confidentiality and strict regulatory frameworks) which have likely contributed to their relative maturity and preparedness to meet obligations under the NDB scheme.

The health sector's position as a leading reporter of data breaches is also consistent with international trends. Jurisdictions with mandatory data breach reporting for the health sector have also seen a high level of notifications, most notably the United Kingdom and the Netherlands.[14,15]

Human error was the leading cause of data breaches in the health sector—accounting for 55 per cent of data breaches, compared with an average of 35 per cent for all other industries. This underscores the need for strong privacy governance in the health sector that includes robust and regular employee training and technological solutions to assist employees. Personal information sent to the wrong recipient was the most common human error breach in the health sector, whether by email, mail or other forms of communication. Throughout the year, the OAIC has worked with health sector stakeholders to provide advice and guidance on data breach prevention strategies.

In the finance sector, human error accounted for 41 per cent of data breaches (higher than the cross-sectoral average of 35 per cent). Like the health sector, a number of these data breaches were the result of personal information sent to the wrong recipient. Finance has also long been a target of cybercriminals given the financial rewards possible, and attacks on the industry have been observed to have risen in recent years.[16,17] Accordingly, a high proportion of finance sector breaches—56 per cent—were attributed to malicious or criminal attacks.

Regulators such as the Australian Prudential Regulation Authority (APRA) are introducing new standards, such as Prudential Standard CPS 234 Information Security, to help ensure regulated entities in the finance sector are resilient to information security incidents, and promptly notify APRA of material information security incidents.

Size of breaches

Figure 8 shows the breakdown of data breaches by the number of affected individuals during the period 1 April 2018 to 31 March 2019.

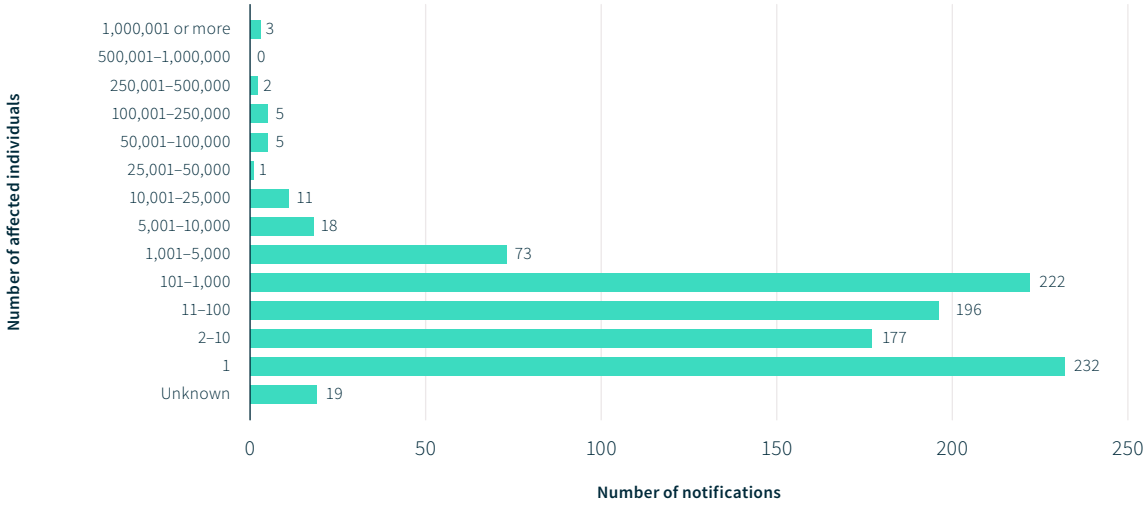

Figure 8 — Number of individuals affected by breaches—all sectors, from 1 April 2018 to 31 March 2019

Most breaches notified during the period impacted a small number of individuals—83 per cent affected fewer than 1,000 people. The large numbers of smaller scale breaches may reflect the prevalence of poor workplace practices by one employee, resulting in scenarios where dozens of records are breached, rather than high-volume data loss incidents from single system compromise. This points to the need for improved data handling practices at operational levels within entities.

Data breaches affecting larger numbers of individuals include a number of multi-party breaches, which involve the compromise of a supplier to a number of entities. The scale of these data breaches reflects the interconnectedness of the digital ecosystem, and the multiplying impact a supply chain breach can have through that ecosystem. There are key lessons to be learned in managing notification obligations and minimising the risks of individual harm in relation to multi-party breaches.

Types of information

Figure 9 shows the breakdown of data breaches by the types of personal information involved, during the period 1 April 2018 to 31 March 2019.

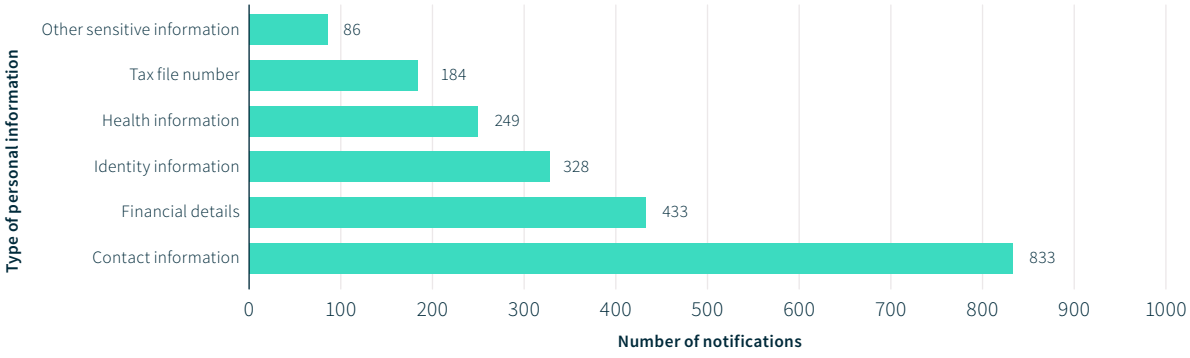

Figure 9 — Kinds of personal information involved in breaches—all sectors, from 1 April 2018 to 31 March 2019

Contact information was the most common form of personal information disclosed through data breaches during the period—it was involved in 86 per cent of notifications.

Assessing the seriousness of harm in relation to the type of personal information involved in a data breach is recognised as a challenge for entities and an area where maturity must continue to develop. Loss of contact information may not result in immediate or financial harm in the same way as losing credit card information. However, in assessing incidents involving contact information as eligible data breaches under the NDB scheme, many entities recognise the risk of further harm that can arise from activities such as phishing and social engineering, tactics that are aided by the use of contact information compromised in a data breach.

The prospect of serious financial harm resulting from breached financial information (such as credit card numbers) and identity information (such as passport numbers) appears to be well understood and regularly triggers reporting under the NDB scheme. This generally reflects the kinds of harm that can result when this information is obtained by cybercriminals, with financial information and identity information among the most valuable information traded on the dark web.[18]

Breached entities may find it more difficult to quantify the nature of the harm that can arise from a data breach involving other kinds of information, such as health information. In these instances, the likelihood and nature of the harm to affected individuals may be less immediate, but nonetheless serious in nature. The OAIC's guidance identifies examples of kinds of serious harm that entities may need to consider in their assessment of a data breach, such as the likelihood that a data breach will result in threats to an individual's physical safety, humiliation or damage to reputation or relationships, or workplace or social bullying or marginalisation.[19] Entities may need to take a longer term approach to monitoring and responding to the risk of harm to affected individuals in such circumstances.

IDCARE insights

IDCARE is a not-for-profit charity providing support to individuals in Australia and New Zealand with identity and cyber security concerns. Over the period of this report (1 April 2018 to 31 March 2019), a total of 213 breach events were reported to IDCARE by organisations or impacted individuals. Most entities that report to IDCARE are regulated by the NDB scheme, but not all.

IDCARE reports that, on average:

- of those contacting IDCARE for assistance, 9 per cent did so because they were notified of a data breach
- 11 per cent of impacted individuals who reported to IDCARE had experienced the misuse of their breached information (such as fraudulent credit card applications)
- the average time between a data breach and misuse of credentials is 9.55 days which means that time is often of the essence in notifying individuals to act to minimise the impacts of a data breach
- however, on average, it takes 90 days for a breached organisation to detect the initial data breach event and 28.25 days more to notify individuals of the data breach.

This last statistic is broadly consistent with the OAIC's experience of the time taken to notify, as Figure 10 shows. (Entities subject to the NDB scheme are required to conduct an assessment of suspected eligible data breaches and take reasonable steps to complete this assessment within 30 days.)

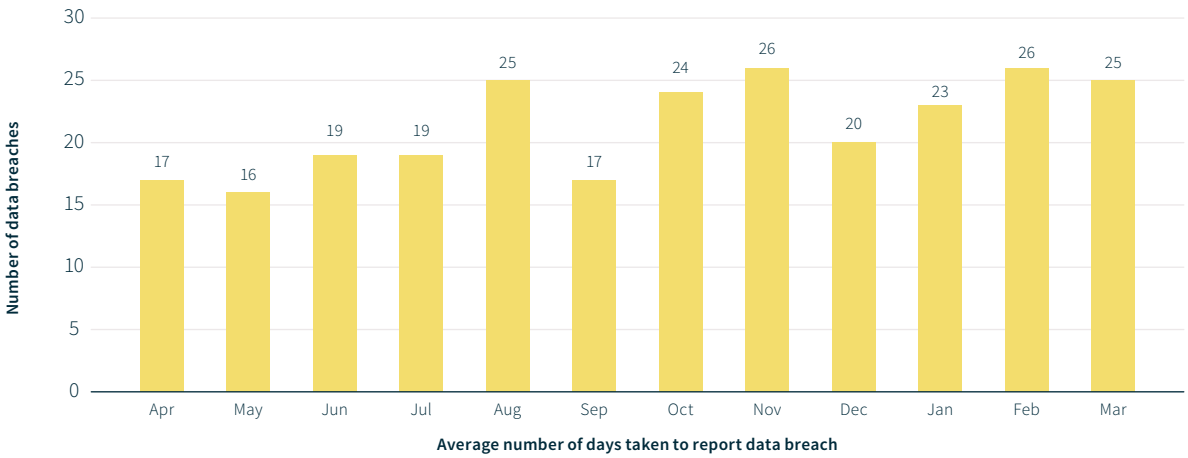

Figure 10 — Average time to notify OAIC after becoming aware of breach (in days), from 1 April 2018 to 31 March 2019

Multi-party breaches

In the past year, there have been 11 multi-party notification events with between two and 60 notifications per incident. The NDB scheme recognises that entities often hold personal information jointly. For example, one entity may have physical possession of the information, while another has legal control or ownership.

In these circumstances, an eligible data breach of one entity is also considered an eligible data breach of other entities that hold the affected information. All have obligations under the NDB scheme.

In general, compliance with the NDB scheme by one entity will also be taken as compliance by each of the entities that hold the information. This means only one entity needs to take the steps required by the NDB scheme. The NDB scheme leaves it to the entities to decide which of them should do so. If no entity complies with the requirements of the NDB scheme, each entity will be taken to have breached the NDB scheme.

The OAIC suggests that, in general, the entity with the most direct relationship with the individuals affected by the data breach should notify them of the data breach.

Multi-party breaches point to the need for contracts and data breach response plans to address all arrangements necessary in the event of a data breach, including accountabilities for: assessing harm and notification, providing access to premises and information, and other matters relevant to investigating data breaches.

Case studies

Multi-party breach: PageUp

A data breach involving an online recruitment organisation, PageUp People Ltd (PageUp), is an example of a data breach in the public domain that involved personal information held by multiple entities.

On 1 June 2018, PageUp notified its corporate clients about a data incident in which an unauthorised individual gained access to its systems. PageUp also notified the OAIC of the incident, in line with its obligations under the NDB scheme. It also informed the ACSC and other international data protection authorities of the data breach. The PageUp incident generated widespread media coverage. This was likely due to the high-profile nature of its clients, many of whom also issued their own notifications about the data breach.

Several lessons about the operation of the NDB scheme emerge from this data breach:

1 Transparency, harm reduction and collaboration

The PageUp data breach demonstrates the potential of notification to drive transparency and accountability. For example, PageUp:

- notified the OAIC and Australian clients (many of whom were regulated entities) shortly after discovering unauthorised access to data
- issued daily updates to notified clients over subsequent days and held an information event with the Joint Cyber Security Centre
- posted regular and detailed updates to its website; these included FAQs on how the data breach had occurred and advice for consumers on recommended security practices.

The OAIC, the ACSC and IDCARE also provided advice for individuals via a joint statement, underscoring collaborative efforts in the interests of consumers between entities, government agencies and support services, which is also an intended outcome of the NDB scheme.[20]

2 The emergence of multi-party breaches

This incident highlighted the challenges involved in multi-party breaches, in which there is a breach of data held by multiple entities, as is often the case in supplier arrangements. The incidence of multi-party breaches is expected to increase in the coming years, given continued trends towards outsourcing and use of cloud service providers.

Under the NDB scheme, only one entity is required to carry out notification in such a scenario. However, as an example, between April to June 2018 the OAIC received more than 50 notifications from the entity and its clients in relation to this incident.[21] It was reported that individual consumers also received multiple notifications relating to the data breach, creating the potential for confusion.

The OAIC recommends that entities with the most direct relationship with individuals affected by a data breach carry out notification. Confusion and duplication can also be pre-empted by addressing accountabilities for notification and harm assessment in data breach response plans and supplier contracts. Notifications can also make clear to individuals why the notification is being received and how it relates to the overall data breach.

3 International notifications

Managing disclosure across multiple international data breach reporting regimes will likely be a continuing area of maturity for entities. Due to its international presence, PageUp notified its clients in the United Kingdom and the United Kingdom's Information Commissioner's Office of the data breach, as well as its Australian clients.

The OAIC continues to encourage entities to be proactive about reporting. However, where a data breach has been reported under international regimes and it is not yet clear whether an eligible data breach has occurred under the Privacy Act, the OAIC advises that entities can engage the OAIC on the basis that investigations are still underway to determine whether the data breach is notifiable in Australia.

What can we learn from others?

The following case examples are taken from eligible data breaches reported to the OAIC over the past year.

Assessment

This example illustrates the steps an organisation took to assess whether a data breach is likely to result in serious harm.

Using a brute-force attack, an attacker gained access to a shared email account used by the entity. The account contained emails containing personal information such as driver licence numbers, health information and financial information.

In assessing the incident, the entity reviewed audit logs, searched the dark web and criminal sites to determine if any personal information had been exfiltrated, and engaged an IT services company to improve its security practices and processes. On this basis, it concluded no evidence was found that the personal information from the breached inbox had been disclosed further.

The entity's assessment also concluded that while the inbox contained personal information of over 50,000 individuals, only a smaller subset was at risk of serious harm based on the information being held.

The entity subsequently notified the OAIC and those individuals of the data breach, providing advice on steps they could take to mitigate the risk they faced as a result of the data breach.

Harm reduction

Under the NDB scheme, entities have an obligation not only to report eligible data breaches to the OAIC and affected individuals, but also to assist individuals by providing recommendations on what steps they can take to reduce harm they may experience as a result of the data breach.

The first year of the NDB scheme in operation provided numerous examples of organisations taking immediate steps to reduce further harm to affected individuals.

In one example, reported in late 2018, an insurer identified that an unknown third party had gained unauthorised access to several member accounts in its online customer portal. A range of personal information had been accessed, including name, date of birth, address and phone numbers.

Following verbal and email notification to affected individuals, the insurer immediately deactivated relevant online services accounts. When reinstating accounts, this organisation also did so only after implementing enhanced security measures such as CAPTCHA and identity verification checks. Immediately disabling affected accounts to limit further harm was a common action taken by entities that reported data breaches.

In a case affecting another entity, an employee's email account was compromised and used to send phishing emails. The entity engaged an external firm to notify affected individuals, which included advice to delete the phishing email, change passwords, and monitor their bank accounts.

The entity also engaged IDCARE to provide additional support and provided affected individuals with access to a premium identity and credit protection service.

A third case provides an example of best practice support in the context of a data breach impacting a vulnerable segment of the community. The reporting entity used social workers to notify affected individuals by phone. In addition to providing information about the data breach and recommended steps to reduce harm, the social workers also asked questions to identify any individuals at higher risk of harm and accordingly made appropriate referrals for further support.

Preventative measures

The NDB scheme aims to drive continued improvement in the security posture of entities and the overall economy through the implementation of preventative measures.

When notifying the OAIC of an eligible data breach, entities are asked to detail steps being taken to prevent recurrence.

In the following example, an entity experienced a data breach following unauthorised access to the email accounts of an employee. Phishing emails were sent from this account to all its contacts.

To prevent recurrence, the organisation implemented multi-factor authentication and a secure customer relationship management system for document transfer. This reduced the risk inherent in sending sensitive information by email.

In another example involving a data breach originating in an email compromise, the entity introduced enhanced password security requirements in addition to multi-factor authentication. Another organisation that experienced a phishing attack implemented a new security training program for employees and a new policy framework with a set of controls designed to detect and block spoofed emails.[22]

Learnings

Challenges and opportunities for improvement

In its first year of operation, greater transparency and accountability arising from the NDB scheme has been evident. The OAIC has observed entities activating data breach response plans to investigate, assess and notify, to minimise immediate harms and prevent future breaches. Awareness of the NDB scheme appears to be high, aided by international developments and media attention, which have bolstered consultation and engagement efforts by the OAIC and others.

Head of the ACSC, Alastair MacGibbon, provides insight into the work done by the ACSC with entities to address cyber security risks and respond to data breaches.

In the last 12 months, the Australian Cyber Security Centre has worked very closely with a number of organisations affected by notifiable data breaches, when cyber security risks have unfortunately been realised. Some organisations have engaged with us in a really collegiate way to secure their systems, to reduce the likelihood of incidents reoccurring. These are organisations that have demonstrated a commendable level of transparency in how they've communicated about and responded to incidents. They came forward quickly, and have engaged openly with their stakeholders, including their customers. They have committed to advising their customers when they have been affected and informing them of the findings of their investigations into incidents.

— Alastair MacGibbon, Head of the ACSC

The OAIC recognises the work being done by entities to comply with the NDB scheme, and to improve their practices to minimise the likelihood of a data breach.

However, areas for improvement and maturation include harm minimisation, navigating multi-party breaches and managing multi-jurisdictional breaches. Over the coming year, entities should seek to understand their data holdings and proactively contemplate the mitigation steps which would genuinely protect consumers from further harm in the event of a data breach.

Entities should also test whether their data breach response plans and contracts adequately address all arrangements necessary in the event of a data breach, including accountabilities for assessing harm and notification and providing access to premises and information and other matters relevant to investigating data breaches.

They should seek to identify how a multi-jurisdictional breach would be best managed to protect consumers, noting the different global notification thresholds which apply.

All entities should also rethink how to effectively secure their personal information holdings taking account of the known causes of data breaches. Best practice entities will also take responsibility for the costs and impacts of rectifying the harmful impacts of data breaches when they occur, and supporting individuals to mitigate the impact of a data breach.

Putting individuals first

One of the key messages that we take from this insights report into the NDB scheme is that entities must put individuals first. Yet, IDCARE reports that over the past year, the average client experience score that an affected individual attributed to the organisation that informed them of the data breach was only 4.1 out of 10.

IDCARE CEO, Professor David Lacey shared the following observations of those entities that emerged in a comparatively positive light, following a data breach.

Over the past year, those breached entities that started with an assumption that affected individuals could be harmed and directed their responses towards individuals' interests rather than minimum compliance obligations generally came out on top—as reflected in media coverage and corresponding complaints and inquiries to IDCARE.

Entities that carefully considered how the wording and timing of a notification could impact (or even harm) individuals did better than those that did not. For instance, if a notification was issued on a Friday, requiring actions which could not be taken over the weekend (for example, actions dependent on agencies or service organisations which were closed over a weekend), it could lead to heightened anxiety and feelings of helplessness amongst impacted individuals.

Similarly, entities that focused on clear and unequivocal statements were of greater help to individuals than those that gave mixed messages. For example, a notification that states that the risk of harm is low while at the same time giving a long list of recommended response actions sends an unclear message to individuals who will usually interpret the risk of harm as being greater.

Where breaches led to consumer complaints and inquiries to IDCARE, a paucity of information or unhelpful advice was usually highlighted. The more effective notifications explained risks in plain English and gave affected individuals a clear understanding of the actions required of them, including the duration for which such action might be necessary.

To assist entities, the OAIC has provided guidance on how and what to include in notification to individuals.[23] The OAIC's website also provides useful information for individuals about how to understand and respond to a data breach notification.[24]

The coming year

The NDB scheme provides valuable insights into the reasons data breaches have occurred, and how organisations can improve their security posture and processes to minimise the risks of a data breach.

In relation to statistical reports issued over the course of the last year, the OAIC has previously stated:

"We expect organisations and agencies to act on the risks highlighted by these reports — whether or not they were directly affected — and take steps to prevent a similar breach of Australians' personal data."[25]

There is also an expectation that entities will employ the following best practice tips in preventing and managing all data breaches.

Five best practice notifiable data breach tips for entities

1 Your people and the role of training

- All employees should be trained on how to detect and report email-based threats (such as phishing), understand basic account security (such as secure passwords) and how to protect their devices. Education should also focus on data handling practices and how to report suspected privacy breaches.
- Typically, best practice approaches in mature organisations involve a dedicated training program comprising face-to-face training and e-learning, supported by tools and ongoing communication on how employees can stay safe from evolving threats.
- Entities should consider their broader workforce (including contractors) when setting awareness strategies.

2 Preventative technologies and processes

- All entities should prioritise investments in improving their overall security posture in line with known security risks. Where necessary, they should engage expert security advice.
- At a user level, technologies such as multi-factor authentication complement user education in mitigating against the risk of compromised credentials. Encryption and secure data transfer technologies also minimise the risk of data loss in everyday communications. Proactive monitoring of systems should be undertaken so that entities can detect and respond to breaches in a timely manner.
- Uplifting these strategies provides a prime opportunity to review data holdings and minimise unnecessary holdings.

3 Preparation

- Entities that have prepared for data breach incidents prove to be best placed to identify and manage data breaches.
- A data breach response plan provides practical guidance on how to reduce the impact of a data breach, meet obligations under the NDB scheme and support individuals to reduce harm. Over the coming year, entities should seek to address multi-party and supplier breaches in data breach response plans and contracts.
- Regular exercises or data breach simulations are also a critical way that organisations can ensure preparedness as they often highlight deficiencies and risky dependencies.

4 Assessment of harm

- Entities that deeply understand their data holdings and how data breaches could impact their customers (and other individuals with whom they deal) will be best placed to assess whether a data breach is notifiable or not following an incident.
- The test for assessing whether an incident is notifiable under the NDB scheme is whether it is likely to result in serious harm for affected individuals. The threshold is designed to be flexible, as each entity is best placed to understand the individuals with whom they engage. There is an opportunity for industry groups to share knowledge to drive strategies which will better support consumers.
- The risk of reporting when the threshold is not reached is that of notification fatigue and resulting inertia when it really matters. These factors point to the need for a thoughtful assessment process which has regard to the particulars of the incident.

5 Post-breach communication

- Transparency and simplicity are key guiding principles in the wake of a data breach.
- Consumers have responded most favourably to those organisations that communicated in plain English about what had occurred and the steps they needed to take to protect themselves. Organisations should also be mindful of the impacts of mixed messages and poor timing, for example, issuing the notification before a weekend or public holiday, when response actions cannot be taken.
- Emerging best practice by entities in the past year have included establishing and maintaining microsites and setting up support lines to provide customers centralised channels to ask questions and find out what they can do to reduce harm. This is increasingly considered best practice.

Conclusion: Further strengthening Australia's protection of personal information

The first year of the NDB scheme has resulted in welcome improvements in transparency and accountability for the protection of personal information. An increase in the volume of data breach notifications by entities is a clear sign of their awareness of, and compliance with, the NDB scheme. It also reflects the implementation of strategies and processes to identify and report data breaches where individuals are likely to face serious harm.

While the apparent increase in entities' intent to notify is welcome, improving efforts to minimise harm to affected individuals must be a continued area of focus. Consumers benefit most from timely notifications in plain English that explain key risks and how they can mitigate them. Improved coordination in the event of multi-party breaches is also an area for improvement.

Preventing data breaches, while challenging in the context of fast-evolving cyber threats, must remain a key goal for all organisations. The NDB scheme's first year has provided valuable insights into the factors that contribute to data breaches.

In particular, entities should reflect on the finding that most data breaches involve human factors. Improving employee knowledge and implementing processes and technologies to support data protection are evidently critical measures. The goal is to foster workplace cultures where privacy and security are organisational priorities and a continuous focus for all employees.

After a full year of operation of the NDB scheme, entities should now be fully aware of their obligations and have in place processes to notify and minimise harm to individuals. The OAIC will consider regulatory action for organisations that fail to respond appropriately, including issuing a direction to notify under s 26WR of the Privacy Act to entities who improperly delay or fail to notify eligible data breaches. The OAIC can also conduct an investigation where there are serious concerns about an entity's compliance more generally with the Australian Privacy Principles. Entities that operate in a global context should also be mindful of obligations internationally as global privacy regimes continue to take shape.

However, organisations must ultimately move beyond a purely compliance mindset. Data breaches can affect any organisation, as is evident in the increasing data breach notification volumes in jurisdictions internationally.

In this context, a proactive approach to protecting personal information represents an opportunity for differentiation and a means to enhance trust.

Glossary

Breach categories

Term	Definition
CAPTCHA	Stands for 'completely automated public Turing test to tell computers and humans apart'. Usually implemented as a visual, audio-visual or written test during the user verification process.
Multi-factor authentication	A method of authentication that uses two or more authentication factors to verify a user, generally categorised as something the user knows (such as a password), something the user has (such as a physical token) and something the user is (such as a fingerprint scan).
Spoofing	Where parts of an email, such as a sender's email address and other parts of the email header, are altered to appear as though the email originated from a trusted source.
User credentials	Details used to verify a user's access to a network, system or website—generally a username and password.
Human error	An unintended action by an individual directly resulting in a data breach, for example, inadvertent disclosure caused by sending a document containing personal information to the incorrect recipient.
Failure to use BCC when sending email	Sending an email to a group by including all recipient email addresses in the 'To' or 'CC' field, thereby disclosing them to all recipients.
Insecure disposal	Disposing of personal information in a manner that could lead to its unauthorised disclosure, for example, using a public rubbish bin to dispose of customer records instead of a secure document disposal bin.
Loss of paperwork/data storage device	Loss of a physical asset containing personal information, for example, leaving a folder or a laptop on a bus.
PI sent to wrong recipient (email)	Personal information sent to the wrong recipient via email, for example, as a result of misaddressed email or incorrect address on file.
PI sent to wrong recipient (fax)	Personal information sent to the wrong recipient via facsimile machine, for example, as a result of fax number incorrectly entered or wrong fax number on file.
PI sent to wrong recipient (mail)	Personal information sent to the wrong recipient via postal mail, for example, as a result of transcribing error or a wrong address on a file.
PI sent to wrong recipient (other)	Personal information sent to the wrong recipient via channels other than email, fax or mail, for example, delivery by hand or uploading to web portal.
Unauthorised disclosure (failure to redact)	Failure to effectively remove or de-identify personal information from a record before disclosing it.

Term	Definition
Unauthorised disclosure (unintended release or publication)	Unauthorised disclosure of personal information in a written format, including paper documents or online.
Unauthorised disclosure (verbal)	Disclosing personal information without authorisation, verbally, for example, calling it out in a waiting room.
Malicious or criminal attack	A malicious or criminal attack deliberately crafted to exploit known vulnerabilities for financial or other gain.
Brute-force attack (compromised credentials)	Automated software is used to generate a large number of consecutive guesses as to the value of the desired data, for example, passwords.
Compromised or stolen credentials (method unknown)	Credentials are compromised or stolen by methods unknown.
Cyber incident	A cyber incident that targets computer information systems, infrastructures, computer networks or personal computer devices.
Hacking (other means)	Exploiting a software or security weakness to gain access to a system or network, other than by way of phishing, brute-force attack or malware.
Malware	Software which is specifically designed to disrupt, damage or gain unauthorised access to a computer system.
Phishing (compromised credentials)	An attack in which the target is contacted by email or text message by someone posing as a legitimate institution to lure individuals into providing personal information, sensitive information or passwords.
Ransomware	A type of malicious software designed to block access to data or a computer system until a sum of money is paid or other conditions are met.
Rogue employee/insider threat	An attack by an employee or insider acting against the interests of their employer or other entity.
Social engineering/impersonation	An attack that relies heavily on human interaction to manipulate individuals into breaking normal security procedures and best practices to gain access to systems, networks or physical locations.
Spear phishing	Spear phishing is a particular class of phishing, where a threat actor uses social engineering to impersonate a trusted contact, and sends a very realistic message, to engage with a specific company or individuals.
Theft of paperwork or data storage device	Theft of paperwork or data storage device.
System fault	A business or technology process error not caused by direct human error.

Endnotes

1 Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth) 100 [182].

2 Australian Law Reform Commission, For Your Information: Australian Privacy Law and Practice, Report No. 108 (2008).

3 Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill (2014).

4 Office of the Australian Information Commissioner, Guide to Privacy Regulatory Action, viewed 14 April 2019, Office of the Australian Information Commissioner website <www.oaic.gov.au>.

5 Office of the Australian Information Commissioner, Australian Cyber Security Centre and IDCARE, 'Joint statement on the PageUp Limited data incident' (media release, 18 June 2018).

6 Taylor Telford and Craig Timberg, 'Marriott discloses massive data breach affecting up to 500 million guests', The Washington Post, 30 November 2018.

7 LandMark White, Data Disclosure Incident, viewed 14 April 2019, LandMark White website <www.lmw.com.au>.

8 British Airways, Customer Data Theft, viewed 14 April 2019, British Airways website <www.britishairways.com>.

9 IBM, Cost of a Data Breach Study 2018, viewed 14 April 2019, IBM website <www.ibm.com>.

10 As the NDB scheme commenced on 22 February 2018, data is only available for part of the quarter.

11 DLA Piper, DLA Piper GDPR Data Breach Survey: February 2019, viewed 14 April 2019, DLA Piper website <www.dlapiper.com>.

12 Verizon, Verizon 2018 Data Breach Investigations Report, viewed 14 April 2019, Verizon website <www.enterprise.verizon.com>.

13 Office of the Australian Information Commissioner and the Australian Cyber Security Centre, Information from the Australian Cyber Security Centre about Preventing and Mitigating Data Breaches, viewed 17 April 2019, Office of the Australian Information Commissioner website <www.oaic.gov.au>.

14 Information Commissioner's Office United Kingdom (UK), Data Security Incident Trends, viewed 14 April 2019, Information Commissioner's Office UK website <www.ico.org.uk>.

15 Autoriteit Persoonsgegevens (Dutch Data Protection Authority), Data Breach Notification Facts & Figures, viewed 14 April 2019, Hunton Privacy Blog website <www.huntonprivacyblog.com>.

16 Nick Ismail, 'Cyber crime and the banking sector: top threats and secure banking of the future', Information Age, 27 February 2017.

17 Reserve Bank of Australia, Financial Stability Review, viewed 14 April 2019, Reserve Bank of Australia website <www.rba.gov.au>.

18 Brian Stack, 'Here's how much your personal information is selling for on the dark web' on Experian's Cybersecurity blog (11 March 2019) < https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>.

19 Office of the Australian Information Commissioner, Data Breach Preparation and Response—A Guide to Managing Data Breaches in Accordance with the *Privacy Act 1988* (Cth),p. 37. Office of the Australian Information Commissioner website <www.oaic.gov.au>.

20 Office of the Australian Information Commissioner, Australian Cyber Security Centre and IDCARE, 'Joint statement on the PageUp Limited data incident' (media release, 18 June 2018).

21 Multi-party breaches are captured as one (1) breach in quarterly and annual statistics reports.

22 Australian Signals Directorate and Australian Cyber Security Centre, Mitigating Spoofed Emails Using Sender Policy Framework, viewed 14 April 2019, Australian Signals Directorate and Australian Cyber Security Centre website <www.cyber.gov.au>.

23 Office of the Australian Information Commissioner, Data Breach Preparation and Response—A Guide to Managing Data Breaches in Accordance with the *Privacy Act 1988* (Cth), p. 54, Office of the Australian Information Commissioner website <www.oaic.gov.au>.

24 Office of the Australian Information Commissioner, Data Breach Guidance (e.g. Personal Information Lost, Hacked, Stolen), viewed 17 April 2019, Office of the Australian Information Commissioner website <www.oaic.gov.au>.

25 Office of the Australian Information Commissioner, 'Anniversary of Notifiable Data Breaches scheme' (media release, 22 February 2019).

26 Australian Signals Directorate and Australian Cyber Security Centre, Get Smarter With Passwords, viewed 14 April 2019, Australian Signals Directorate and Australian Cyber Security Centre website <www.cyber.gov.au>.

27 Australian Signals Directorate and Australian Cyber Security Centre, Malicious Email Mitigation Strategies, viewed 14 April 2019, Australian Signals Directorate and Australian Cyber Security Centre website <www.cyber.gov.au>

28 Have I Been Pwned, viewed 14 April 2019, <https://haveibeenpwned.com/>.

OAIC

oaic.gov.au

Office of the Australian Information Commissioner

1300 363 992
enquiries@oaic.gov.au
@OAICgov