THE OFFICE OF THE
Data Protection Authority

Trends and Insights:
two years of personal data breach statistics

May 2018 – May 2020

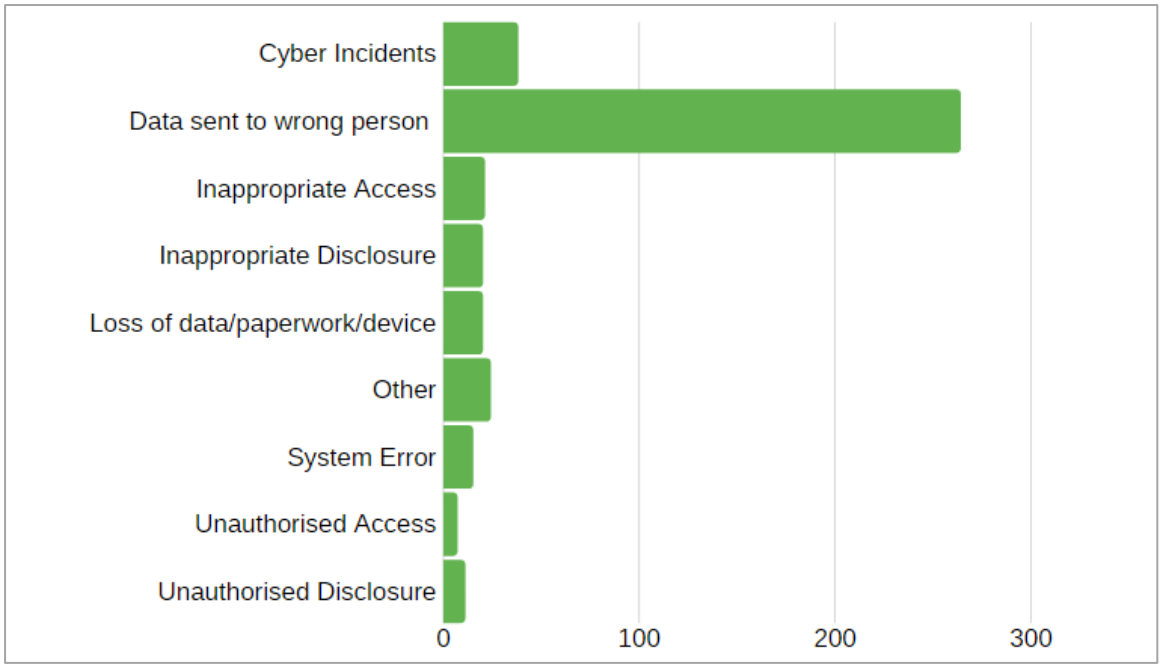
In this document we take you through what can be learned from two years' worth of breaches. There are two key trends to be aware of, and three insights we want to share with you. We end on eight steps you can take to deal with the aftermath of a breach.

We have proactively published regular statistics of the breaches reported to us since 2018 to:

- raise awareness of organisation's **legal requirement** to report breaches
- raise awareness of the **range of breaches** that occur locally
- share **insights** so lessons can be learned
- **prevent** the same mistakes happening repeatedly.

We analysed all personal data breaches reported to us in the period **25 May 2018 - 22 May 2020**.

Here is a breakdown of the number of breaches by category:



BREACH CATEGORY	COUNT	PERCENTAGE OF TOTAL
Cyber incidents	38	9%
Data sent to wrong person (by email, by fax, by post, or in person)	264	63%
Inappropriate Access	21	5%
Inappropriate Disclosure	20	5%
Loss of data/paperwork/device	20	5%
Other	15	4%
System Error	7	2%
Unauthorised Access	11	3%
Unauthorised Disclosure	24	6%
TOTAL *(date range: 25 May 2018 - 22 May 2020)*	**420**	**100%**

Trend #1 wrong person

The clear trend evidenced by the above statistics is that personal data being sent to the wrong person is **by far the most common breach reported to us**. To understand more about this broad breach category, at the beginning of 2020 we started subdividing it into whether the breach occurred by email, fax, or post. But for the purposes of the two year analysis we are just looking at the broader category.

What can we take from this?

There may be 'reporting bias' at play here - it could be that this is the most well-known type of potential data breach, so this may result in a higher incidence of this type of breach being reported to us. Whereas, other less obvious breach categories such as 'loss of data/paperwork/device' and 'inappropriate disclosure' are perhaps not as well recognised as being a potential breach and so many of those incidents may not be reported to us.

But if we assume that this category is indeed the most common breach, it is clear that everyone would benefit from considering this common sense advice:

- take **all reasonable precautions** when handing personal data over to someone else, regardless of whether this is via electronic or physical means
- **avoid complacency** by taking a moment to consider the potential implications of the personal data you are handling falling into the wrong hands

Trend #2: human error vs. system error

The other very clear trend is that human error, as opposed to system error, poses the larger risk to the safety of personal data. So we have a big opportunity to make a real positive impact on it, by focusing on the people handling the data in your organisation's care.

As our commissioner, Emma Martins, commented in September 2019:

> '*We must all recognise that it is people's awareness, attitudes, behaviour and choices that often pose the biggest risk to the protection of personal data, rather than our IT systems. Because of this, my office is laser-focused on raising everyone's appreciation and awareness of data protection, in the hope that we can create positive cultural change around how people think, and feel, about taking care of personal data.*'

What can we take from this?

Here are six common sense steps you could consider to reduce human error in your workplace:

1. Be aware of human error, and know that **no-one is immune** from it. We've all done it, and we'll all do it again. You will never eradicate it entirely, but you can reduce it.
2. **Pause when the stakes are high**, focus on what the impact could be on the person whose data you are handling. Ask for help.
3. Train, support, and **look after your staff**, especially in times of stress when they are more likely to default to habitual responses that may lead to errors, rather than considered reasoning.
4. **Prime your work environment** with reminders for staff to be vigilant.

5. Maintain a workplace culture that allows for **supportive development and learning** when things go wrong. Have each other's backs, rather than pointing the finger of blame at an individual that has made an honest mistake.

6. Encourage a work environment that allows staff sufficient **time and space** to work in a considered, calm, unhurried fashion (especially when performing high-risk activities).

Insight #1: breach reporting threshold

A personal data breach is defined in section 111(1) of the Law as any incident that meets the following criteria:

- 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'

There will likely be a breach whenever any personal data is accidentally lost, corrupted or disclosed, or if someone accesses it or passes it on without proper authorisation to do so.

But you are **not legally obliged** to report any incidents that meet the definition above if the incident is 'unlikely' to result in a risk to the 'significant interests' of any person whose data has been affected by the incident. Whilst you are not legally obliged to report the breach to the ODPA, you are encouraged to do so because it can be difficult, and sometimes inappropriate, for organisations themselves to judge whether there is a risk to a person's significant interests.

A person's 'significant interests' are defined in the local Law as any aspect of their life that could be put at risk due to their personal data being breached. This could include their physical safety, their reputation, and could extend to placing them at risk of identity theft, fraud, financial loss, psychological distress or humiliation.

Insight #2: beware the secondary breach

If you experience a breach and report it to the ODPA, take care not to commit a secondary breach in the process. For instance, as part of an initial self-reported breach you don't need to send ODPA the **specific evidence** of the breach, you just need to disclose **how** it happened, **what** personal data has been put at risk, **how many** people's data are affected, **the category** of person affected (i.e. staff members, customers, suppliers), and the **category** of personal information affected.

For example:
If you sent a breach report similar to the below, it would constitute a secondary breach, as it **exposes** the data and individuals concerned:

✗ *"I've sent details related to Mrs A. Bloggs positive pregnancy test results to Mrs C. Bloggs."*

Instead, you should submit a breach report in the below format, which **protects** the data and identities concerned:

✓ *"At 13:10 on 19 October 2018, I sent special category medical data related to a patient's pregnancy to an individual with a similar name."*

Insight #3: the human stories behind the statistics

It is all too easy to focus energy and attention on compliance programmes, cyber security, privacy policies etc and lose sight of what all the effort is for. The aim of data protection legislation is to avoid people being harmed. We must always come back to focus on that aim.

Each of the 420 breaches listed above may have caused irreparable harm to someone:

- loss of crucial medical records;
- inaccurate descriptions of events leading to someone losing their job;
- disclosing someone's sensitive information to their colleagues.

Avoiding these very real, and often life-changing, harms is not a waste of anyone's time. Harms due to data misuse or loss often cannot be undone, so we must all do everything we can to predict where our risks are and prevent breaches from happening.

Data protection = People protection.

Keep calm and carry on:

8 steps to help you deal with a data breach:

1. Make sure your organisation has a **defined breach response plan**: **test** it regularly, make sure all relevant people (internal and external to your organisation) have an **up-to-date hard copy** of it stored safely.

2. Once you become aware a data breach has occurred: don't panic, **establish the facts** before you do anything else, and make sure all relevant staff members are made aware.

3. Assemble your **response team** and allow the rest of your organisation to carry on with business as usual. Make sure all staff are given regular updates on the situation especially if it's a serious breach as they may be approached by media.

4. Once you've established the facts of the breach: do your best to **contain it**, **minimise the harm** that could be caused to the people whose information has been breached, and take all reasonable steps to **preserve evidence** for any potential forensic investigations that may become necessary.

5. You have a **statutory duty to report the breach** to The Data Protection Authority within 72 hours of you becoming aware of it. You only need to report breaches that meet certain criteria.

6. Think about the people whose data has been breached: **be decent** – consider contacting them to let them know and to say sorry. And keep in mind that they may tell the media.

7. Your response plan should include your **communications plan**: your approach will be dictated by the exact circumstances of your breach, but you are advised to – **tell the truth, tell it fast, and tell it repeatedly**.

8. Finally, make sure you **learn** from the experience: as far as possible, close down the risk that led to the breach so that it doesn't happen again, this will help you start to **re-build trust** between your organisation and the people whose data you look after. **Update** your response plan with what you learned.

Excellence Through Ethics.

+44 (0) 1481 742074 | enquiries@odpa.gg | odpa.gg