GPEN Sweep 2019

‘Data Breach Notifications’

December 2019

Office of the Privacy Commissioner, New Zealand
(Te Mana Mātāpono Matatapu)

Background

The 2019 GPEN Sweep considered how organisations in various jurisdictions handle and respond to data breaches. Given the mass of information that is collected and held by organisations, it is inevitable that at certain times personal information will be accessed, disclosed, or otherwise acquired in a way which is not authorised. How an agency responds to a data breach incident (including both notification as a response and steps taken to prevent future breaches) is of key importance to data protection authorities (DPAs) and the individuals whose personal information is affected.

This year 16 DPAs participated in the Sweep out of the 17 who expressed an interest in doing so.

Participating DPAs reached out to organisations with a set of pre-determined questions which focused on their current practices for recording and reporting data breaches. Various methodologies were adopted during this year's Sweep, including, but not limited to:

- Writing to organisations with a list of set questions via email or post;
- Directing organisations to complete online polls;
- Conducting interviews over the telephone.

To narrow the focus of the Sweep, many participating DPAs focused on a sector or sectors which were of particular relevance to them. These included:

- Healthcare;
- Insurance;
- Banks;
- Universities;
- Government Departments;
- Local Councils;
- Telecommunications;
- Retail;
- Professional Associations;
- Internet Hosting Services;
- Manufacturing;
- Legal; and
- Tourism.

Some DPAs looked at more than one sector. Other sectors were considered, but for the purpose of this report, only the most reviewed sectors are listed.

Summary Observations

Of the 1145 organisations contacted as part of this year's Sweep exercise, only 21% provided substantive responses (258). It is important to note that two DPAs reached out to a combined total of 659 organisations, of which only 31 responded, which has impacted the percentage of responses received overall. Across all other DPAs, there was an average response rate of 47%.

The low response rate from organisations asked to participate could indicate concerns from organisations about potential follow up enforcement actions and could indicate that a large number of organisations do not consider themselves compliant with breach reporting obligations in their jurisdictions or are otherwise not keeping adequate records of privacy breaches. The following results need to be read in light of the low overall response rate.

Data breach notification is mandatory in 12 of the 16 jurisdictions who participated in the Sweep. Almost all organisations that responded were aware of the relevant legal framework, including reporting thresholds and timeframes. Only 5 organisations demonstrated poor understanding of the legal framework.

It was positive to note that a large percentage of organisations that responded (84%) across all sectors and jurisdictions reported having appointed a team or group responsible for managing data breaches, to whom breaches should be reported.

The organisations which responded reported having internal guidance in place to assist staff in recognising what a data breach or potential data breach may look like, as well as clear policies about how data breaches should be escalated internally and reported to relevant external parties.

Sixty five percent of organisations rated their own procedures for preventing a recurring data breach as 'very good' or 'good'. However, the rest had either poor procedures in place or failed to specify.

When it comes to monitoring internal performance in relation to data protection standards, organisations were found to fall short in this area, with more than 30% of organisations having no programmes in place to conduct self-assessments and/or internal audits.

Around 45% of the responding organisations indicated that they maintain up to date records of all data breaches or potential breaches.

Tombstone Data

Data Protection Authorities who submitted results: 16 of 17

Organisations contacted: 1145

Responses received from organisations: 258

Methodology Note: Not all DPAs reported on every reporting field. The statistics for this Sweep were developed based on the actual data received for a reporting field as a percentage of those organisations swept by those DPAs that reported on that field.

Note that various methodologies were used when collecting data for the purpose of this Sweep. For instance, some participating DPAs reviewed the responses provided by organisations and gave them a rating based on the information provided, while others required organisations to rate themselves and provide evidence where possible. In the case of the latter methodology, the responses were taken at face value. It is then up to the participating agency to decide whether they want to follow up on these responses with further investigation once the Sweep is complete.

One DPA completed an independent review of data breach reporting in its jurisdiction one year after mandatory breach notification had been introduced. The results of this were translated to the Sweep reporting form.

Awareness of relevant data breach framework (Indicator 1)

Participating DPAs indicated that around 99% of responding organisations were aware of the legal framework in their jurisdiction (including reporting thresholds and timeframes). Ninety-three percent reported that the responding organisations' reporting mechanisms reflected their awareness of the legal framework.

In a few cases while a respondent answered that they were aware of the breach reporting requirement, the answers regarding the reporting mechanisms didn't fully demonstrate knowledge or understanding of the relevant legal requirements. In other cases, the respondent's reporting mechanisms seemed to be merely formal. The impression gathered was that they are not fully embedded in day-by-day activities.

Internal procedures for handling data breaches (Indicator 2)

A high number of reporting organisations (86%) had internal guidance in place to assist staff in recognising a breach or potential breach. A large percentage of reporting organisations (84%) across all sectors and jurisdictions had appointed a team or group responsible for managing data breaches, or to whom breaches should be reported. Ninety one percent had sufficiently clear policies outlining how data breaches should be escalated internally. Some respondents reported that they educate the wider organisation about what to do in the event of a breach, but often policies and procedures are not easily accessible to all staff.

Seventy five percent of reporting organisations said that they had procedures in place that covered key steps such as containment, assessment, evaluation of the risk associated with breaches. Eighteen percent of responding organisations rated their own procedures as “poor”, suggesting that there is room for improvement in this area.

Those organisations without internal policies indicated that they relied on the guidance published by the DPA in their jurisdiction, where needed. One respondent described their breach assessment system, and indicated that they had implemented a red, amber, green (RAG) rating system, which took into consideration the number of records affected, the sensitivity of the data, the distress caused, the containment or otherwise of the breach, whether the information has been recovered and whether the data was encrypted..

Responding to data breaches (Indicator 3)

As with indicator 2, a high number of responding organisations (84%) had policies or procedures in place around reporting breaches to relevant external parties (the individual/s affected and or the regulator) on top of their policies and procedures for internal reporting. However, only 74% of responding organisations reported the appropriate level of information to these parties.

Some of the responding organisations indicated that they discuss every breach with the relevant DPA. This indicates that a greater understanding of the relevant legal framework and the establishment of internal policies would enable internal assessment to take place in the first instance.

Management (Indicator 4)

Eighty three percent of responding organisations indicated they keep records on data breaches or potential data breaches. However, when it came to monitoring internal performance in relation to data protection standards, more than 30% of respondents had no programmes in place to conduct self-assessments and/or internal audits. Many noted that they only undertake monitoring in the event of a data breach.

An example of good practice included monthly senior management reporting, quarterly information governance board meetings and periodic audits. Some respondents used external companies to conduct audits. Others included conducting assessments on data protection level to ensure the regulatory standards were met, e.g. the adequacy/frequency of training, number of complaints related to data privacy, the level of security, etc. The policies are reviewed at least every two years

to ensure they are in line with the latest data protection standards.

Preventing future breaches (Indicator 5)

Only 65% of the responding organisations reported that following a data breach they took steps to prevent future breaches.

Organisations who did take these steps noted that these reporting and record keeping activities has enabled them to identify breach trends and consequently, query the root causes of these breaches. This improved understanding of the cause of breaches has then allowed the organisation to act to prevent potential future breaches. For example, certain organisations have potential future breaches by delivering staff training for specific risks such as phishing communications.

Most reporting organisations considered the root cause of an incident in deciding steps to prevent a similar incident from occurring in future. Larger organisations were better equipped to implement necessary changes to prevent future breaches. Smaller organisations noted that any steps taken to prevent future breaches would be dependent on the nature of the specific breach that had occurred.

Other findings

- 1198 data breaches occurred across the 258 organisations in the last 12 months. Thirty-six of these were reported to the regulator, and 157 were reported to the affected individual/s. Not all organisations were asked this question, for example in jurisdictions where breach reporting was not mandatory. It is assumed that not all breaches reached the threshold for reporting, however there may be issues around under-reporting.
- In jurisdictions where data breach reporting is not mandatory, most organisations felt they would be equipped to report breaches, although many noted that they would need to educate the wider organisation about their responsibilities in the event of a breach.
- In jurisdictions where data breach reporting is mandatory, the steps organisations reported having taken to prepare for implementation included:
    - Staff training, implementing proper procedures, and designating someone to be responsible for handling data breaches;
    - Producing guidance and setting up internal awareness training for staff (either via e-learning or outsourced externally).
    - External parties brought in to assist with organisations to prepare for mandatory breach schemes and provide training.
- Ninety two organisations reported that the guidance and resourcing around data breach reporting currently made available by the regulator in their

jurisdiction is useful. Smaller organisations commented that they struggled to understand their legal obligations under the law and struggled to remember the vast amount of guidance. They also noted lack of resources made it difficult for them to develop detailed data breach management policies and procedures; data breach response plans; and to provide awareness training across their organisation. There was a “difference in consciousness of incidents such as data breaches depending on the size of the organisation and the kind of industry.”

Conclusion

The results of the Sweep revealed a low level of engagement from organizations contacted. However, those organizations that responded reported a high level of awareness of managing data breaches. The majority had an appointed individual, team or group responsible for managing data breaches, or to whom breaches should be reported. They also provided evidence of clear policies and guidance about recognising, escalating, and reporting these.

While there were examples of good practice, more than 30% of the organisations that responded did not have programmes in place to conduct self-assessments or internal audits of their practices against data protection standards. Sixty five percent reported that following a data breach they took steps to prevent future breaches. One DPA observed that organisations who undertook these reporting and record keeping activities were able to identify breach trends and consequently, query the root causes of these breaches. This improved understanding of the cause of breaches has then allowed the organisation to act to prevent future breaches. Auditing and self assessment, along with reporting and prevention activities, may decrease the overall occurrence of data breaches.

Most responding organisations reported finding the guidance produced by their DPA to be useful. However, smaller responding organisations have struggled to absorb large amounts of guidance and lack of resourcing has prevented them from developing sophisticated data breach policies and procedures.

Based on the Sweep's findings it appears that most responding organisations have good policies around handling and responding to data breaches. However, provided the low response, it is clear that not all organisation are yet comfortable voluntarily reporting on their breach handling practices. Participants in the Sweep ultimately note that there is scope for DPAs to consider whether they are providing guidance which is appropriate for all the organisations within their jurisdiction.