Office of the Victorian Information Commissioner

Case Study: Email errors

Email errors are some of the most common privacy breaches reported to OVIC. They include emails being sent to the wrong person, or incorrect attachments being included in emails. Email errors can severely impact an individuals' privacy rights, the organisation's ability to comply with its information security obligations and its reputation. In some cases, these errors could constitute a serious breach of the *Privacy and Data Protection Act 2014.*

This case study outlines the experience of a large government organisation which set out to reduce email errors, and will highlight key lessons for other public sector organisations experiencing this type of privacy breach.

What happened

The government organisation involved in this case study sends over 1.2 million outgoing emails each year, many of which contain personal or sensitive information of members of the public.

In the 2024–25 financial year, the organisation reported 78 privacy incidents to OVIC. The most common incident type was email errors, including 32 incidences of emails being sent to the wrong email address or recipient, and a further 13 incidences of emails containing the incorrect attachments. Most incidents related to personal information (95.1%), with a small number involving health information.

Types of email errors

The first step for the organisation was to understand the different types of email errors. It found that common causes of email errors included:

- employees having multiple case files open at the same time, resulting in copy and paste errors
- employees using email addresses from their own local address books rather than obtaining the email address from the organisation's main database, which is considered the 'single source of truth' for contact details
- employees using auto-population of email addresses without confirming addresses in the organisation's main database, or checking the address bar before sending the email
- legacy data and inaccurate information contained in the source database, often stemming from employees' failure to update the database when a change of details is provided, or emloyees making transcription errors when entering or changing details in the database.

In terms of incorrect attachments sent with emails, this was attributed to manual workflows, whereby documents are downloaded from one system, saved to an employee's desktop then attached to an email.

Understanding and fixing the problem

To better understand the root causes of the email errors, the organisation categorised them into 6 key themes:

1. Policy or process errors occurred where rules or instructions were missing, confusing or outdated. This meant staff were not always aware of the correct process or required standards.
2. Some staff did not have the training or confidence needed to complete tasks accurately. This led to employees relying on one another rather than from proper training, leading to mistakes.
3. There were some staffing and resourcing gaps, and a lack of clarity around certain roles and responsibilities. This meant that people felt stressed, delays grew, work was being rushed and tasks were sometimes missed.
4. The organisation's systems and processes did not always work well together. This meant that information was entered more than once, documentation was inconsistent, compliance risks increased and employees created manual processes to make things work.
5. The organisation's technology was old, slow and not supported properly. Some employees did not know how to use the technology, leading to reliance on manual processes which increased the risk of security incidents occurring.
6. Leadership did not always give clear direction or help employees to understand roles and responsibilities. This led to some confusion among employees, slow decisions and risks remaining unresolved. It also resulted in employees not feeling safe to speak up, teams working in silos, resistance to change, and the organisation becoming reactive rather than proactive in addressing privacy issues.

Understanding the above themes meant that the organisation was able to identify and implement a range of targeted actions to help reduce the number of email errors.

Based on the agency's self-assessments of the breaches, its communication with OVIC about the breaches, and the remediation actions currently underway, OVIC is not proposing to take further regulatory action at this stage. OVIC will continue to monitor the agency's compliance with its privacy and information security obligations.

Lessons

Privacy is everybody's responsibility

The first major take-away from this case study is that the reduction of privacy incidents is the responsibility of all employees, from the executive and the Board, to the relevant governance committees, through to the frontline employees using the organisation's email system.

Build a strong reporting culture

As there are numerous causes of email errors, organisations need to capture and analyse each incident to ensure accurate reporting and statistical analysis, and to help identify remediation strategies. This requires building a strong culture of self-reporting through induction and training and ongoing awareness raising activities.

Technological processes should also be implemented where possible to assist in the detection of privacy and information security incidents, and to provide another oversight mechanism beyond self-reporting.

There should be a simple and effective process for the immediate and accurate reporting of privacy incidents, including email errors, to the organisation's privacy officer, and incidents should be captured in an incident register.

Monitor and assess incidents

Individuals tasked with privacy oversight should identify and monitor trends in email errors and provide incident statistics for the corporate scorecard and regular reporting to the executive leadership team. The leadership team should disseminate the lessons arising from this reporting to frontline employees. This may be through including metrics in the organisation's strategic plan and annual report, on noticeboards or in internal newsletters.

Privacy incidents, including email errors should also be considered as part of an organisation's cyclical internal audit program.

Implement controls

Once organisations have a sound understanding of root causes and systemic issues, they should develop multiple, targeted system controls, including process and technological controls and staff training and awareness activities.

Organisations should develop business processes and practices that directly address the employee behaviours that lead to email breaches. These processes and practices should be clearly and thoroughly documented and monitored for compliance.

Technological controls should address both the business systems used in the creation, sending and management of emails, as well as the technology that supports timely and accurate privacy incident reporting.

Technological solutions may involve a major platform redesign, or simple automated processes such as the scanning of emails to detect anomalies such as the address of the recipient being different to the person referred to in the body of the email, or the email attachment title not matching the name of the document attached.

Raise awareness and provide support

An organisation should put strong emphasis on raising awareness among employees. This should be through initial induction and mandatory ongoing privacy training, newsletter articles, staff noticeboards, activities linked to Privacy Awareness Week, and direct outreach into frontline teams that influence the email error rate.

Counselling and support should be available to employees who make email errors, having regard to the severity of the incident, number of similar incidents and whether documented work practices were followed.

Notify affected individuals

Finally, organisations must ensure they have well-established policies and processes for notification of incidents to affected individuals so that they can take any necessary steps to protect themselves against any consequences associated with the misuse of their information.