Law Council OF AUSTRALIA
Legal Practice Section
AUSTRALASIAN Law Management Journal

Edition: November 2019

Email faux pas – how to avoid and respond to message blunders

Most office staff use email every day, but the ubiquitous nature of this important work tool can lead to careless behaviour that threatens a firm and its clients if there are not protocols and procedures in place to minimise risks, writes Merinda Timpany.

You have drafted the email, you've clicked 'send' and … OH NO!

Most people have a story about someone who sent an email by mistake – the wrong recipient, the wrong content, the wrong attachment, or an attachment with unintended metadata. What should you do if that person is you? First, how does this even happen (that is, why you should be sympathetic if your staff member tells you they have done this)? Here are some common reasons.

1. *Email is an informal communication technique*. It is easy, therefore, to be less careful, or more loose, in your approach compared with how you would treat sending a formal letter.
2. *Auto-completion of recipient name.* Most email systems will 'find' similar names when you are typing the intended recipient and it may default to a similar name you have emailed previously.
3. It can be tempting to reply to the top email in a chain and not *review the chain* to consider whether or not all the content is relevant to your recipient.
4. *Reply all*. Used unintentionally, you can easily share inappropriate information. Used intentionally, it can be a great time waster. So, use with caution.
5. Sending the *wrong attachment* or *failing to remove metadata* from the right attachment. This can happen either if you have relied on someone else or are retrieving files from a document-management system. More metadata may be accessible than you realise (for example, all the internal mark-ups and comments may be visible either immediately or when the document is being reviewed by IT).

Law Council OF AUSTRALIA
Legal Practice Section
AUSTRALASIAN Law Management Journal

These scenarios, and others, happen more than we might like to think – but we often only notice them when they cause a problem and confidential information goes where it should not be.

What to do to avoid it happening to you

Nothing beats habitual proof-reading. Check twice. Once for content, a second time for the recipient, email chain, attachment etc. You can also:

- set up habits that slow down your emails – this includes spell checking, automated filing into the document management system, or a delay function (that holds your email in your outbox for a specified period);
- regularly clear auto-completion records in your email; and
- talk to your IT team about setting up prominent warnings (e.g. for emails going outside your organisation, or to check for the removal of metadata on attachments).

More broadly, however, law firms must have a data breach plan. Human error is a key risk factor in a high proportion of data breaches affecting Australian citizen data, according to the most recent Notifiable Data Breach (NDB) Scheme statistics from the Office of the Australian Information Commissioner (OAIC) – this includes clicking on phishing emails, reusing passwords across services or sending email communications in error.

So your organisation also needs to adopt a multi-pronged approach to increase your awareness of human error and related data breach risks and take the necessary precautions. This should include:

- comprehensive staff training on the risks, including security issues and threats and the cyber risk environment in which the organisation operates. This includes training on the importance of checking carefully on email correspondence prior to opening and sending; confirming recipient and/or sender addresses to ensure legitimacy; recognising phishing emails and spear phishing (through the use of social engineering of reliable company information); protecting staff credentials (passwords and log-on details) and adoption of strong password protection strategies (e.g. don't re-use the same passwords across multiple devices or sites or apps);

- preparation, maintenance, implementation and testing of a comprehensive data breach response plan for the organisation to contain, assess and respond to data breaches quickly when they arise, to help mitigate potential harm to affected individuals and to support compliance with the NDB scheme under the Privacy Act. This would include, at a minimum:

    - being clear in the plan as to what constitutes a data breach (and the broad

parameters of this) for your organisation – noting that *any* unauthorised access to or unauthorised disclosure of personal information, or *any* loss of personal information, howsoever arising, must be protected against under the Privacy Act;

- setting out as a framework the roles and responsibilities within the organisation who will be involved in responding, assessing and managing a data-breach incident (always reflecting the capability of such individuals). This will almost always include board representatives, IS/IT, legal and HR at a minimum.

- a clear, effective and immediate strategy for containing, assessing and managing data breaches, including
  - a communications strategy for key stakeholders (internal and external), including any media management;
  - legislative and contractual requirements and impacts;
  - strategy as regards prompt notification of individuals and the OAIC (meeting the requirements under the NDB scheme where an 'eligible data breach' is considered to arise. Being clear in the plan as to what an 'eligible date breach' means practically for your organisation is also key) as well as notification to other affected entities;
  - notification to insurers, where applicable.

- recording and reviewing incidents and post-breach management, as well as the success of your plan to improve data handling and breach management in the future.

- ensuring that all staff are aware of the existence and contents of the data breach response plan, and that regular testing of roles and responsibilities for staff are carried out to ensure effectiveness, sustainability and suitability of the plan to changing environments.

Other actions to take if you make an email error?

Do not:

- rely on the recall function – we can all testify as to how much more compelling an email is when the sender has tried to recall it! Also, the recall may not work; or
- panic and do nothing, or try to fix it without anyone finding out – any mistake is usually made worse if you don't obtain an objective judgment (more for a future column).

Law Council OF AUSTRALIA
Legal Practice Section
AUSTRALASIAN Law Management Journal

Do:

- contact the recipient as soon as possible:
    - contact them by email so that the correction is in their inbox. Do not reply to the message you sent (perpetuating the sharing of incorrect information). If it is not sensitive information, you might use the same subject line, along with something to indicate the error (e.g. SENT IN ERROR – [previous subject]).
    - also contact the recipient by telephone if you have their contact details;
- ask the recipient to delete the original message and any related messages (e.g. if they have replied to you or forwarded it internally). Importantly, also ask the recipient to delete those messages from their deleted items;
- ask the recipient to confirm in writing that they have deleted the messages from all these locations;
- ask the recipient to confirm in writing that that they have not read the contents of the email (or, if that is not possible, to confirm the extent of what they have read);
- review the sensitivity of the information – does it include confidential information, what impact does the sharing of that information have on the course of the matter;
- talk to someone senior as soon as possible. This may be your supervising partner, managing partner, professional indemnity partner, or insurer, or someone in the risk/general counsel team. It should be someone not connected to the matter and the mistake as this brings objectivity that you may not have; and
- consider whether you need to notify anyone else:
    - the person whose confidential information was sent in error. This is generally not mandatory but is highly recommended – it is much better that the person (client or otherwise) hears it from you rather than a third party;
    - your PI insurer, if there is a possible loss/potential claim;
    - a regulator if there is price-sensitive information at stake; and
    - the court, if proceedings are on foot and the disclosure could have an impact
    - the Australian Information Commissioner (or alternative overseas privacy regulator) if the email contains personal information (that is; information relating to individuals).

As with all incidents, prevention is better than cure – so be aware, be prepared, test regularly and ensure that your organisation is well protected against the increasing risks of data breach and cyber-related incidents.

Merinda Timpany is Regional Risk Manager & Senior Legal Counsel, Australia & Middle East, for DLA Piper.

www.dlapiper.com