THE COSTS OF LOSING CUSTOMER DATA

The 2017 data breach of US credit reporting agency Equifax exposed the personal information, including names, birthdays and social security numbers, of nearly 150 million Americans. The information obtained could be used to steal an identity, having a lasting impact on the lives of those affected. The breach has been reported to have cost Equifax between US$400m and US$600m, with the cost potentially increasing as ongoing disputes are resolved.

In 2018, Marriott discovered that, when they acquired Starwood, they also acquired an advanced persistent threat actor that reportedly stole data from 500 million customers over a four-year period, including names, contact information, passport numbers and other personal information.

Here in Australia, there have been numerous events too, including the 2017 breach of nearly 50,000 Australians' information from a private contractor that worked with federal government departments and several ASX-listed corporations.

Incidents like the above can have significant impacts on a business' reputation and financial performance, however, the extent that Australian entities will be fiscally penalised in the event of a breach is not yet known. In February 2018, the Notifiable Data Breaches Scheme (the Scheme) was enacted in Australia, which puts in place an expectation that organisations are responsible for how they handle our data, and creates a system of trust and transparency that should something go wrong, we have a way of knowing about it and the potential harm that may be caused.

Failure to comply with the Scheme can result in penalties of up to $1.8 million for organisations, and $360,000 for individuals.

As these penalties show, this is an issue that senior executives and risk committees must take seriously. However, it can be difficult to know where to start. Understanding the issue in more detail can be helpful in putting things into perspective.

The data explosion

As businesses move into the information age, the quantity and types of data they are collecting have grown. The opportunities this data and the overlying analytics provide are myriad, and the benefits can be seen in everything from better recommendations on Netflix, to more personalised offers from our favourite stores. It allows businesses to make more informed decisions and offer improvements to their products and services. With the increase in size and spread of our data comes increased risk that a breach could occur. This extends far beyond a straightforward customer contact database or the payment records that typically come to mind when we think about customer data. Consider the following examples:

- your workplace uses an external facing email address to communicate with customers;
- you have digital product development teams using services like Amazon Web Services (AWS) to develop a new customer product or marketing tool; or
- your customers fill out application forms which are stored electronically on your servers.

In each of the above scenarios, the risk of a data breach involving customer information is high. For example:

- Customer facing email accounts are often used to send identification and other supporting documents such as for the 100-point checks, and information in these accounts is very rarely deleted due to the use of cloud email environments like O365 and the removal of the requirement to purge data to fit within mailbox size limits.
- Product development teams could be using customer data to build new marketing tools leveraging powerful cloud-based servers. Failure to properly secure your cloud services or de-identify your customer data can lead to unauthorised access and theft.
- Application forms are highly likely to contain personal information and, since they are usually handwritten forms that have been scanned in, they pose unique challenges when it comes to identifying and quantifying the information they contain.

With more data, and data-sprawl, comes increased risk to your organisation and an increased chance that a data breach may occur.

What exactly is a data breach?

Simply put, a data breach occurs when personal information that an entity holds is subject to unauthorised access or disclosure, or it is lost. You do not need to be the victim of a sophisticated hack that results in a loss of data; you could simply have an employee send an email to the wrong address, or lose an unencrypted USB device with sensitive personal information on it.

TIP 1: DEVELOP A DATA BREACH RESPONSE PLAN BEFORE YOU NEED ONE

Each entity must develop their own procedures for assessing any suspected data breach, so the Office of the Australian Information Commissioner (OAIC) and impacted individuals can be notified. The purpose of a data breach plan is to outline your strategy for containing, assessing and managing the incident from start to finish. Your plan should set out roles and responsibilities for managing a data breach and also describe the steps your organisation will take should a data breach occur.

The OAIC website (https://www.oaic.gov.au) has useful guidance on developing a plan.

What to do if you have a breach

In the event of a data breach, it is important that in-house and external counsel are notified as part of the response plan. It is easy for the technical experts to be solely focussed on containing a breach that they may lose sight of the obligations entities have under the Scheme. This is where it is important that counsel maintains oversight of the process that assesses the data breached and importantly determines if a data breach is a notifiable event.

Per the OAIC, your assessment of a data breach should consider:

- if there has there been any Personally Identifiable Information (PII) involved in the breach;
- the circumstances of the breach, including causes and the extent. These factors will help you understand the potential impact; and
- the nature of the harm to affected individuals and if remedial action can reduce this harm.

Importantly, you must take all reasonable steps to complete the assessment within 30 calendar days after your organisation becomes aware of the grounds (or information) that caused it to suspect an eligible data breach.

What is PII?

Personally Identifiable Information, known as PII, is a broad term for any details that can be used to distinguish or trace an individual's identity. Names, birthdays, addresses, biometrics such as fingerprints, and driver's licences are all prime examples of PII. As noted above, much of this information is valuable to businesses – both for the business itself and its customers. Many organisations, such as banks and AUSTRAC reporting entities, are even required to collect and store this kind of data to prevent potential money laundering.

If your business deals with individuals, then you are probably holding some form of PII.

TIP 2: KNOW YOUR RISK – IDENTIFY AND CLASSIFY YOUR DATA

Undertaking a project to identify and classify the data your organisation holds is a significant first step in understanding the risk. Work through each of your key business processes to identify the points where data is collected, stored or transferred between systems. Review these data points and determine if they contain PII or not, and create a register with classifications as to the type of PII. These registers are useful for assessing risks and building controls, and are a useful tool for assessing a data breach at the time of an event.

The complexities of a notifiable event

On face value, it may seem reasonably straightforward to inform customers should a notifiable breach occur, and, in some circumstances, it is. Consider the scenario where an Excel file containing customer contact details is sent to the wrong person. In this situation, the following is true:

- you know exactly what data was subject to the breach;
- the data is structured in a table, making the assessment straightforward; and
- knowing the individuals impacted allows you to easily look up their contact details for the purpose of notifying them.

Executing your response plan in the above situation would be reasonably straightforward, and completing the assessment within 30 calendar days is quite feasible.

However, most situations are not this straightforward, and identifying the people potentially impacted and notifying them has unique challenges. Now, consider the following, more complicated scenario:

- your IT experts identified that someone has accessed a corporate email account and likely downloaded the entire mailbox;
- the email was used by customers to send in scanned copies of identification and other 100-point-check documents that contain a large amount of personal information; and
- there are thousands of emails and attachments to review for PII.

In this scenario, you still have 30 days to complete your assessment, however, now the process of identifying and assessing the data breach has become a lot more complex. How will you analyse the thousands of emails and create a detailed list of potentially impacted individuals? In these complex situations, you require the assistance of Cyber Information Risk and Analytics specialists to manage the response and analyse the data.

- Cyber Information Risk specialists are able to capture forensic copies of data and event logs in a forensically sound manner to preserve the integrity of the information. They are experienced in managing the end-to-end process of responding to a data breach and can perform a post-incident review with your team to make sure the organisation is able to learn from the incident and adjust accordingly.

- Data Analytics specialists can use analytical techniques to help identify the different types of PII and link them to individuals using text analytics and pattern matching. Identifying the individuals in unstructured data such as emails is a complex task. By using Named Entity Recognition and similar entity extraction processes, they are able to automatically scan through vast amounts of unstructured data and identify the names of the individuals potentially impacted.

TIP 3: TEST YOUR PLAN WITH A DESKTOP EXERCISE

If you have developed a plan, outlined the roles and responsibilities and created a data register, then why not test it? Enacting a desktop exercise with the relevant people where a data breach is staged and the plan is worked through is a useful way for your people to become familiar with the process and creates a safe environment in which to do so.

It is impossible to say that a data breach can be completely avoided. However, ensuring you are proactive in identifying and classifying the data your business needs to hold and developing a detailed response plan is the next best thing. In the event you do have a data breach, you will be prepared, know which actions to take and will have met your obligations. By demonstrating that your organisation is compliant with the Scheme and takes data privacy seriously, you will be able to maintain the trust of the Commissioner and public in your organisation.

Shane Bell

A Partner at McGrathNicol Advisory, Shane has more than 18 years' experience managing technology and information risk in business, with a particular focus on cybersecurity, digital forensics, data and information governance, eDiscovery and technology-led investigations. With a background in active military service, Shane is highly trained in management and leadership in stressful situations.

Robin Tarr

A specialist in forensic and regulatory investigations, anti-bribery and fraud risk management advisory, as a Partner at McGrathNicol Advisory, Robin has more than 20 years of investigative and consulting experience, several of which were spent with a 'Big 4' firm where Robin was the National Head of Forensic Investigation Services for Australia.