Is your data safe and sound?

Murray Goldschmidt outlines methods you can use to better protect one of your organisation's most valuable assets.

Nonprofit organisations and service providers to the nonprofit industry invest a lot of time, money and effort in collecting, storing and mining data relating to donors.

Throughout its lifecycle, data may be collected in various formats (paper/online/telephone) and converted to other formats (scanned documents/spread sheets/entered into databases). It is possible that the data may exist in many, or all, of these formats - particularly if the original is not deleted or destroyed.

Data is collected for a reason and it therefore has an intrinsic value. Organisations need to determine whether appropriate measures are in place to protect their investment in data. In order to protect data, organisations need to consider the following.

What type of data is it?

Determining what type of data you have is the first step to defining the appropriate controls to secure it. For example, charities and service providers to nonprofits are likely collecting sensitive data relating to their donors, sponsors and information regulated by standards, such as credit card data which is regulated by the Payment Card Industry Data Security Standard (PCI DSS).

Where is the data?

As mentioned, data can exist in various formats throughout its lifecycle. Before converting data from one format to another, determine whether the original format is still required. If it is, it should be securely archived. If not, it should be securely purged.

Data could reside in computers and servers onsite, or off-site at a datacentre. Frequently, outsourced service providers are used and data may be stored on shared (multi-tenanted) infrastructure, particularly where cloud based and virtualised services are used. Data can also be on personal devices such as laptops, mobile phones, smart phones and removable storage such as USB keys.

Where data is stored in cloud services, the actual locality of the data may also impact an organisation, as legal requirements may be imposed by the country where the data is stored. For example, some countries, such as the USA, may have laws that compel service providers to disclose or make available data to authorities.

How and where is it stored?

Broadly, electronic data may be assigned to two classes: structure and unstructured data. Structured data is stored in databases; unstructured data is stored in multitudes of other locations such as file servers, emails and applications and may be in a variety of document and image formats.

Whatever class and format the data is in, technology solutions are now available that enable organisations to control access to the data and also audit or report on the use of data. This is of particular importance where regulations demand strict controls for data, such as PCI DSS in relation to accessing credit card information.

Protective controls

Do you know who has access to your data? In general, access should be granted on a business need to know. This is a requirement when dealing with sensitive data, such as credit card data.

Do you have methods in place to restrict access? This could be done by physical measures (locks/doors/data centres) and by logical measures (accounts/passwords/applications).

Has the data been protected in the system that is storing it? For example if credit card information is stored it must either be encrypted or truncated. Have you taken reasonable measures to protect other information such as date of birth, residential address and any financial related data? Is all access to data logged? Is it auditable?

How long can you retain data?

The period that data can be stored will depend on the type of data collected. Data retention may also be regulated by industry or state and federal laws. For example the PCI DSS requires audit trail history (of the access to credit card data) be retained for at least one year, with a minimum of three months immediately available for analysis.

Data destruction

Once you no longer need data, appropriate measures are required to securely delete it. The archiving and purging methods you use will need to be commensurate with the value or sensitivity of the data.

Implications if compromised

The implications for a data breach can be very serious. This could include: financial losses, reputation and brand damage, increased regulatory/audit overhead, exposure to legal risks resulting from violating privacy, loss of business opportunities as a result of lack of trust, impact of downtime resulting from attacks, potential penalties, and possibly not being able to process credit cards if facility is terminated due to breach.

It's worth noting that the Australian government is considering revisions to the Privacy Act to include provisions for mandatory disclosure in the event of a data breach. This would be accompanied by significant expense relating disclosing to parties whose data was lost and also the trailing costs of reputation and brand damage. Consider the costs of being required to notify all record holders on your databases if there had been only a partial breach, but you didn't know which records were lost!

"Data is collected for a reason and it therefore has an intrinsic value. Organisations need to determine whether appropriate measures are in place to protect their investment in data."

Having adequate and practical controls in place is certainly achievable and important. Your investment in data should include clear strategies to minimise the potential for data breach, and be able to promptly report on all access to records. F&P

Murray Goldschmidt

Murray Goldschmidt is co-founder and chief operating officer at Sense of Security, an independent provider of information security and risk management solutions.