Level 8, 66 King Street
Sydney NSW 2000 Australia
Telephone +61 2 9290 4444
or 1300 922 923

An article on

Data Security for the Not-For-Profit Sector

Organisations invest a lot of time, money and effort in collecting, storing and mining data to derive positive outcomes for their business or operation. Not for Profit (NFP) organisations have valuable data relating to donors and their business operations; and service providers to the NFP industry produce and collect data for the purposes of marketing and deriving income through various channels.
Information may be collected in various formats (paper; online; telephone) and may be converted to other formats (scanned documents; spread sheets; entered into databases) along the lifecycle that the data takes. It is possible that the data may exist in many, or all, of these formats particularly if the original is not deleted or destroyed.

At the end of the day data was collected for a reason and therefore the data has an intrinsic value. Organisations needs to determine if appropriate measures are in place to protect their investment in the data. In order to protect the data the following parameters will need to be identified:

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 NFP's are likely collecting sensitive data relating to their donors, sponsors and information regulated by standards (e.g. credit card data which is regulated by the Payment Card Industry Data Security Standard - PCI DSS).

Where is the data?

Identifying where the data resides is a pre-requisite to determining how it can be protected. As mentioned previously, data can exist in various formats throughout its lifecycle. Before the data is converted from one format to another it should be determined if 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 on-site, 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. The security of the data may also be affected. For example, some countries, such as the USA, may have laws that compel service providers to disclose or make available data to authorities.

"44% of all breaches involve a malicious or criminal act that results in the loss or theft of personal information"

"The average organisational cost of a data breach is $1.97 million"

(2009 Annual Ponemon Study on Australian Cost of a Data Breach)

With some cloud service providers, the data may actually be across numerous international jurisdictions where inter connected data centres are located across the globe. This may further complicate compliance reporting and forensic investigations in the event they are required.

Broadly, electronic data may be assigned to two classes: structured 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 the 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, datacentres) 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?

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 the data, appropriate measures are required to securely delete (destroy) data.

Archiving and purging strategies should be defined and the method will need to be commensurate with the value or sensitivity of the data e.g. secure shredding or document destruction vs unsecured bins; physical destruction of hard drives vs selling or disposing old computers; external secure archiving facilities vs internal cupboards; unencrypted traditional tape/online backups vs encrypted backups.

"Australian organisations experience very costly data breaches, which include activities intended to prevent a loss of customer or customer trust".

"44% of participating companies engage an outside consultant to assist them over the course of a data breach incident"

(2009 Annual Ponemon Study on Australian Cost of a Data Breach)

Implications if compromised

Particularly for organisations operating in regulated industries, which include NFP organisations, 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; possibly not being able to process credit cards if facility is terminated due to breach.

It is also important to note 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 who's 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!

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 recent access to the records and determine which subset was breached should a breach occur.

About Sense of Security

Sense of Security is a leading independent provider of information security and risk management services to the NFP sector and their service providers in Australia. Our broad spectrum of services includes security governance, risk, compliance, application and network assurance, mobility, virtualisation and audit. We have also developed information security documentation suites specifically adapted to the NFP sector, enabling organisations to readily adopt industry proven frameworks to align with regulatory requirements. Our consultants are information security experts with a thorough knowledge and understanding of the technical, commercial, and regulatory aspects of information and communications technology (ICT) security.

Sense of Security is accredited as a Qualified Security Assessor (QSA) company by the PCI Security Standards Council and employs QSA's who are authorised and trained to provide these services to assess compliance in line with the Payment Card Industry Data Security Standard (PCI DSS).

Web: http://www.senseofsecurity.com.au
Email: info@senseofsecurity.com.au
Tel: 1300 922 923

"96% of breaches are avoidable through simple or intermediate controls"

"143 million records compromised in 2009"
(2010 Data Breach Investigation Report by Verizon Risk Team)

"Sense of Security is a leading provider of information security and risk management services to the NFP sector and their service providers"