How does Information Security Impact You?

Trusted Impact Pty Ltd, Level 9, 22 Albert Road, South Melbourne 3205
secure@trustedimpact.com, (03) 8623-2890

Are executives & directors breaching their obligations?

Safeguarding sensitive information is not just a specialised technology issue residing somewhere deep in an IT department. It has become a much broader, pervasive issue whereby **now Executives and Boards can be held personally liable for breaches of sensitive customer data.**

"Identity Theft" is now considered the crime of the 21st century. And recent, high-profile breaches of sensitive customer data have exposed systemic problems in the way enterprises manage sensitive data across the entire business. These breaches have drawn critical scrutiny from customers, shareholders, and lawmakers.

In response, **legislation continues to be developed which requires formal early notification of breaches, and imposes liability at the Board level under a range of civil, ASIC, and criminal proceedings** in situations where a prudent duty of care has not been exercised.

The Issue

Many Australian enterprises have improved service levels, reduced costs and increased productivity by using information technology to instantly provide information to their customers, suppliers and the communities they serve. In fact, access to reliable and accurate information has become an indispensable element of successful organisations, and indeed, in many enterprises today, information "is" the business.

As technology has been leveraged for the enterprise, for a long time the issue of "IT security" was considered to be a specialised technology discipline, residing deep within an IT department to protect networked computers from external intrusion.

But the environment has changed and the issue of securing sensitive customer information has become a much broader, pervasive issue. This is because a number of high profile breaches of sensitive customer data in other countries have exposed systemic problems in the way enterprises manage this data, and these breaches have drawn critical scrutiny from the public, shareholders and lawmakers.

Pervasive "Identify Theft" has thrust liability for protecting sensitive data out of the IT department and into the Boardroom

In some cases, this scrutiny has taken the form of specific legislation requiring enterprises to formally register losses of sensitive customer data, and to implement comprehensive programmes to inform customers of these breaches so they can protect against personal "Identity Theft" [1], now regarded by many experts as the "crime of the 21st Century" because of its low risks and high rewards.

[1] Identity theft is a term first appearing in literature in the 1990s. According to the non-profit Identity Theft Resource Center (http://www.idtheftcenter.org/cresources.shtml), identity theft is sub-divided into four categories: Financial Identity Theft (using another's name and unique identifying number(s) to obtain goods and services), Criminal Identity Theft (posing as another when apprehended for a crime), Identity Cloning (using another's information to assume his or her identity in daily

Whilst Australia has yet to experience a high profile incident, it is only a matter of time. The foundation for significant risk has now been laid whereby Australian executives and boards can be held personally liable for civil, ASIC and criminal proceedings if they do not exercise their duty of care to protect this sensitive customer data.

As illustrated in the following table, the obligations to protect customer data are now quite clear.

The Privacy Act: Your business is required to protect the personal information it holds from misuse and loss, unauthorised access, modification or disclosure. Serious fines apply for non-compliance or a careless attitude.

Corporations Act: Under the Corporations Act 2001, you must have 'adequate protection' over information at your disposal. Also, the Corporations Act imposes obligations to keep copies of business records for a number of years.

Trade Practices Act: Another party may sue the business operator if they incur loss or damage through a security breach at your business.

Directors' Liability: A director is obliged to protect the corporate assets at their disposal, otherwise civil, Australian Securities and Investments Commission (ASIC) and criminal proceedings may result. As most small businesses now have some form of corporate entity structure or protection, this is even more relevant than ever.

Criminal Liability: If delegated employees act in a criminal manner, the business operator may be held responsible for their activities.

Card Schemes: Under card schemes such as MasterCard and Visa, merchants are responsible for keeping all customer information safe and secure. If a merchant site is identified as a point of compromise this may result in heavy penalties and/or termination of merchant facilities.

(source: http://www.protectfinancialid.org.au/Protecting-your-customers/default.aspx)

Whilst there is a wave of additional legislation gaining momentum on a global scale, it is imminent in Australia as well. For example, in mid-March, "… in a move that demonstrated the Australian government's stern sentiments on the issue, Privacy commissioner Karen Curtis proposed that all Australian data breach incidents need to be disclosed in a recommendation to the Australian Law Reform Commission (ALRC)" [2]. This was reinforced in September when the Australian Law Reform Commission (ALRC) gave "the thumbs up to the introduction of data breach disclosure laws in Australia, which would put it in line with current US and European legislation."[3]

The legal foundation has been laid to make executives and boards directly liable to protect its customers from identity theft. It is only a matter of time before these regulations are more aggressively enforced and formal notification is required.

Just the Tip of the Iceberg

Previously, enterprises were not legally required to register incidents and notify customers if sensitive data had been lost.

Now the magnitude of the problem is being uncovered as enterprises must legally register these breaches. In those select jurisdictions that now require notification, there have been over 500 "registered" incidents in the last 18 months alone – or 1.5 losses per day. Clearly this is only the tip of the iceberg, as it only highlights those incidents which are reported because of legislation.

The empirical evidence indicates that merely one third of the losses relate to technology attacks. For example, the largest category along was comes from lost or stolen laptops (23%). However, the frightening statistic is that whilst this caregory was the largest single source of lost sensitive information, only 6% were password-protected or encrypted. This highlights a lack of understanding, inappropriate controls, and an imprudent duty of care.

In Australia, a 2003 report estimated identity theft is costing it billions of dollars a year[4]. Whilst a more recent August 2007 article found that 87% of Australians were concered about identify theft[5] and almost 2 million had been victims[6].

The issue is real and pervasive – has your company has ever lost customer sensitive information? Has it thought about how it would respond if it led to your customers' identity theft?

life) and Business/Commercial Identity Theft (using another's business name to obtain credit).

[2] "Big brother won't protect data" 15 March, 2007 Negar Salek, itnews.com.au, www.itnewscom.au/print.aspx?CIID=75649&SIID=35

[3] Australia 'must overhaul data disclosure mess', Reported by: Liam Tung, ZDNet Australia, 12 September 2007

[4]] Identity Fraud in Australia, a 2003 report by the Securities Industry Research Centre of Asia-Pacific (SIRCA) for financial intelligence agency AUSTRAC

[5] 29 August 2007, The Australian http://www.australianit.news.com.au/story/0,24897,22327654-15306,00.html

[6] 28 August 2007, National survey commissioned by the Office of the Australian Privacy Commissioner

The Implications Are Significant

The implications and 'cost' of compromised data come from a range of sources including;

Personal Liability: From an enterprise's perspective, direct liability for its executives and directors provides a meaningful incentive to ensure that programs are in place to protect its customer data. But it is not evident how many executives or directors in Australia are aware of their personal liability, nor for that matter, how many actually 'want to recognise' their liability with the hope that a breach will not happen. In this case, "not asking the question, because you may not want to know the answer" does not protect one from their explicit duty of care.

Fines and monitoring cost: Examples from other incidents highlight a range of significant costs; including the imposition of fines, and costs to inform and monitor the customer notification process. One example happened in 2005 when a provider of personal financial records (ChoicePoint) inappropriately compromised over 163,000 personal financial records of end consumers. As a result, nearly $18 million in fines were imposed on the company. It was also required to implement costly new procedures to ensure that it provided consumer reports only to legitimate businesses, to establish and maintain a comprehensive security program, and to obtain independent audits every other year for 20 years.

Reputational Risk and Share Value: Whilst it is often difficult to directly correlate compromises of data with share value performance, one detailed analysis found that in the previous ChoicePoint example, the company saw nearly $1 billion wiped from their share registry over a one month period (21% drop in share price).

The fines were only the tip of the iceberg – the company saw **almost $1 billion wiped from their share registry**

Consumer Defection: The time and effort for individual customers to recover from identity theft can be significant. Identity theft "victims spent on average 175 hours over 14 to 16 months and incur an average of $1,300 to clear their names."[7] For companies that compete for the trust and ongoing business of customers, the impact of negative "word of mouth marketing" can add up. For example, "of those shoppers who experienced problems with a retailer… 31% went on to tell friends and family. Of those, 8% told one person, 8% told two people, and 6% told six or more people".[8] We suspect this number would be much greater in the situation where a company has exposed its customers to identity theft.

Whilst personal liability for executives and directors may be a potent incentive for motivating enterprises to proactively protect sensitive data, the "reactive" costs can be dramatically more significant. A small investment to understand the potential scale of an issue can pay solid dividends over time.

A Stitch in Time Saves Nine

Australian enterprises can realise significant benefits by proactively meeting their legal obligations before they become an issue.

No company will ever be able to guarantee that sensitive data will never be compromised. But recognition of the issue is the first step, evaluating the size, scale and scope of a potential issue is the second, and third is putting into place a prudent program of risk mitigation to demonstrate that the Board and its executives have exercised a reasonable duty of care to manage sensitive customer data.

Anticipate the problem, lessen the impact

Reacting after a breach results in a typical 'open wallet, carte blanche, spin control' exercise requiring legal, audit, communications, and public relations professionals charging premium rates whilst operating in 'crisis mode'.

Therefore, asking straightforward questions such as; **WHAT** customer sensitive data exists (electronic and paper), **WHERE** does it reside in within the organisation, **WHO** has access to this data, **HOW** is access and distribution managed or controlled – can provide the basis of understanding the magnitude of an issue before one arises.

A fundamental principle of information and data security is that enterprises collecting or managing sensitive customer data should use reasonable security safeguards to protect that information against unauthorised access, use, disclosure, modifications or destruction. Therefore protection requires more than just a strong physical

[7] "Cost of Identity Theft", Marc Samson, CEO Intelligent Switched Systems, February 7, 2004

[8] "Beware of Dissatisfied Consumers: They like to Blab" Wharton School of the University of Pennsylvania (http://knowledge.wharton.upenn.edu/) March 08, 2006

structure or technology to house this data, but involves an evaluation across a range of categories including;

Acquisition – Understanding if the information is required, and whether the information is gathered in a safe manner. Many fraudulent, internal compromises happen at the point of information acquisition. Are there appropriate checks and balances in place to minimise this risk?

Definition – "Not all data is equal". Has the enterprise segmented its data into different categories so that sensitive information can be separated and controlled more effectively? A segmented approach will minimise cost and enable the enterprise to focus effort in the important areas rather than across the entire enterprise.

Not all data is equal – classifying data enables an enterprise to focus

Access – Is access to sensitive data monitored? In particular, are there suitable approaches in place to ensure usernames and passwords are protected and updated? Are physical, paper records managed appropriately, or does the same sensitive data reside in unlocked file cabinets?

Disposal – How is information disposed? Are electronic or paper documents and databases containing sensitive data rendered unreadable prior to disposal?

Distribution – Are employees trained in the proper procedures of disclosure and are there defined rules about who can or cannot receive sensitive data?

Usage – Are there defined rules, policies or procedures to help employees understand how to gather and secure sensitive data? Are there rules about how information can be distributed via fax, email or over the telephone?

Physical Access – A well-recognised military concept is called "defense in depth", or providing a secure environment at different levels or complexity according to the importance of the asset that is being protected. Has the company considered this approach to protect its employee and customer data?

Policy – Do the policies of the organisation support compliance to secure practices? For example, in the event a procedure is intentionally disregarded, do the Human Resources policies reinforce an appropriate response?

A successful programme means finding the right balance between maximising the free flow of information, whilst protecting the integrity, privacy and availability of the data and systems the organisation relies on.

Therefore, it is also important to understand the interrelated technology, people, and process trade-offs required to find a unique balance that reflects an enterprises' strategy, industry, operations, customers, suppliers and partners.

Effective mitigation of liability is not just about technology, but a **balanced approach** across people, processes and assets, including information

Whilst a comprehensive program may cover a range of issues, it is important to recognise that by applying an experienced "20/80" rule, effective risk mitigation does not have to be costly, time consuming, nor interrupt the normal operations of an enterprise.

The small investment made to understand the potential size or scope of an issue and to manage this risk, is well worth the reactionary cost of an imminent breach of sensitive data.

A Final Thought

Most Board members and senior executives lack a detailed understanding of technology, no less complex security controls. They often ask the IT Manager "are we covered here"? The IT Managers, with many diverse challenges to manage, think they have firewalls in place, so at the risk of not looking bad, the typical response is 'we've got it covered'. The Board, now confident they have asked the question have relied upon their senior leaders to perform their jobs effectively. Everyone is happy – right?

Just remember the IT manager often does not hold personal direct liability to protect sensitive data. Also recall that the empirical evidence indicates over one loss every day with only 1/3 of those losses relating to technology attacks.

Are you really confident that you have exercised your duty of care just by asking a simple question, or is it worth a broader assessment?

You don't know what you don't know...

The Author and Trusted Impact

Tom Crampton is the Managing Director of Trusted Impact Pty. Ltd. He has over 20 years of Australian and international expertise helping clients improve their businesses. For further information, he can be reached on (03) 8623-2890.