



 **ERNST & YOUNG**

FROM THOUGHT TO FINISH.™

E-Security and Privacy

The role of web seals on the internet

An expert paper by Ernst & Young's E-Security and Privacy specialists



It is no secret one of the biggest hurdles faced by companies promoting e-commerce is user fears about the privacy and security of personal information disclosed on the Internet. Survey after survey in the US, Europe and Australia indicate that security is a key concern for consumers, businesses and other stakeholders. While these perceptions exist we can expect many users to shy away from e-commerce.

In this paper, Ernst & Young looks at the numerous forces driving companies with e-commerce operations to provide assurance their sites are secure and user privacy is guaranteed. It also examines some of the difficulties faced by companies implementing e-commerce assurance solutions.

The lust for trust

E-commerce is evolving at an incredible speed. Just over five years ago, commentators were still speculating about whether the Internet would transform business. Today, the question is not whether there will be transformation, but what will the change be tomorrow.

There are many stakeholders influencing this rapid development of e-commerce: businesses, consumers, governments, organisations — and cyber criminals. For this reason, trust is fast becoming one of the most valuable currencies on the Internet.

E-businesses acknowledge this barrier for many users. To publicly flag their trustworthiness, and help users overcome their online fear, many businesses are now seeking a seal or certificate of e-commerce assurance for their web site.

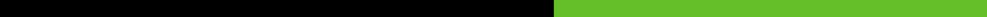
Nowhere is the Internet security dilemma more pronounced than in the burgeoning online shopping industry. It is a fear that we can all relate to - the feeling of trepidation you get after entering your credit card details, with finger poised to click the 'buy' button on a web site.

That fear is not without cause. In the first three months of 2000, the Australian Computer Emergency Response team recorded more than 5,000 attacks on Australian systems¹ — more than were recorded for the whole of 1999. By taking advantage of a simple hidden network problem, a cyber criminal can obtain confidential information such as client credit card numbers, private information, passwords, or possibly wipe out an entire company with the click of a button.

There is a theory that consumer fears about online shopping will gradually dissolve as more and more people are exposed to Internet shopping. Ernst & Young's global online retail research has found that consumer fears in countries that are less engaged with e-commerce are higher than in countries where online shopping has a deeper penetration.

¹ *The Canberra Times*, 'Australia: Belt and braces approach to web security advised', 6/11/00.

expert PAPER



In Australia...credit card security concern is the third biggest factor discouraging online buying,..

In Australia, credit card security concern, although no longer top of mind for consumers, is still the third biggest factor discouraging online buying. Clearly companies must take this issue very seriously. Especially for bricks-and-mortar companies coming online, proactive security practices are vital to protecting brand integrity and ensuring consumer trust that has been established on land.

Although consumer fears have reduced over time Ernst & Young research in the US indicates consumer trust has plateaued. In fact, credit card security concern is the fourth biggest factor discouraging online buying world-wide, and 'guaranteed security' ranks third as the improvement consumers would most like to see on the Internet.²

Also reflecting this distrust is the increase in consumer demand for online control. This is indicated by recently introduced web sites facilitating anonymous purchases anywhere online, such as privatebuy.com.

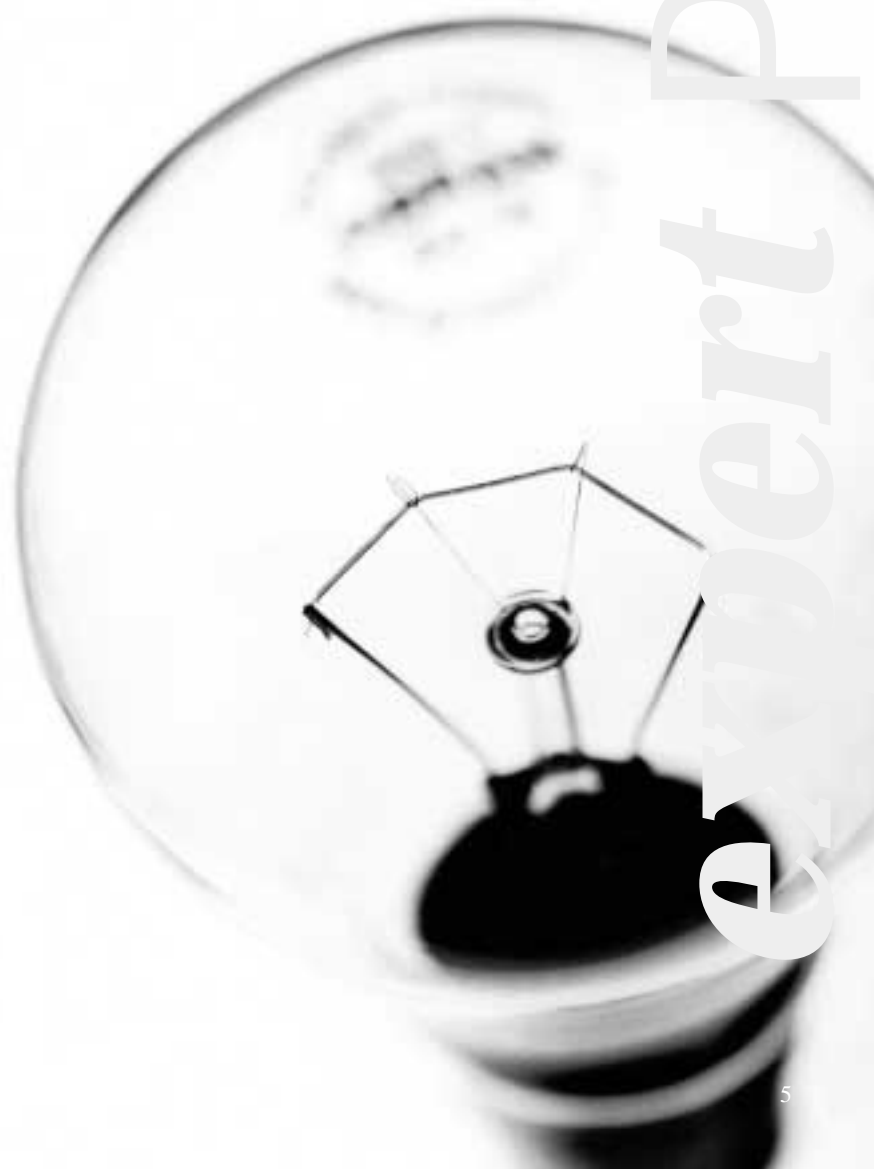
Clearly companies must take consumer security and privacy concerns seriously and resolve this issue. With concern levels so high, any e-business that can demonstrate security and privacy for customers immediately gains a significant competitive advantage.

² From *Global Online Retailing: An Ernst & Young special report*, January 2001

What's at stake

E-businesses will earn trust by delivering their customers' expectations: good product, clear and competitive pricing, easy site navigation, consumer support, independent product review, privacy statements, sound systems and reliable delivery. E-businesses can independently and publicly verify their delivery of many of these issues with a web seal.

It seems the public will respond to these seals. Ernst & Young's Online Retailing Report found 80 per cent of consumer respondents are at least somewhat more willing to use a web site with encryption capability or if it offers digital certificates. However, while 41 per cent of Australian online retailers believed having a seal of approval on their site would make consumers much more likely to use it, only 15 per cent of those surveyed in 2000 actually had a seal.



The value of a web seal

As in the offline world, seals of approval online are designed to foster user confidence by ensuring a business has agreed to follow a set of rules or guidelines. While seals of approval are designed to help Internet users identify reputable businesses, they are not ultimately a guarantee of good business practice.

Most seal-bestowing organisations have no binding enforcement mechanisms to deal with offenders who break the rules, no jurisdictional rights and the protection they offer users is limited. Users may also become skeptical as they realise that the number of seals is growing.

Yet, according to a recent Federal Privacy Commissioner's report³, 'seals could come into their own as a powerful facilitator of globalisation of consumer transactions if indeed they are able to provide acceptable and enforceable privacy protection across jurisdictions.'

While there may be some enforcement, jurisdictional and perception hurdles to overcome, with full e-commerce assurance from independent, reputable organisations, web seals can ensure security and privacy policies are followed, aid market differentiation, build and support brand strength, support dispute resolution and offer indemnification and regulatory compliance.



³*Web Seals: A Review of Online Privacy Programs*, A joint project of The Office of the Information and Privacy Commissioner/Ontario and The Office of the Federal Privacy Commissioner of Australia, Venice, September 2000.

An independent seal of approval

The accounting industry globally advocates a process of independent verification such as WebTrust, which has been developed by the American Institute of Certified Practicing Accountants and the Canadian Institute of Chartered Accountants. In Australia WebTrust is offered by the Institute of Chartered Accountants Australia. WebTrust certification is awarded only if a company passes an independent examination of its site and of all its business practices and procedures.

The historical model supporting the need for independent verification, or auditing, can essentially be found last century. It was only after the 1929 stock market crash that the US Securities and Exchange Commission required publicly traded companies to submit to independent audits. This step was key to bringing trust back into financial markets.

When an independent party audits a company, you have reasonable assurance that the financial statements are free from misstatement. It is this 'reasonable assurance' that is missing from the online world. Web sites are not required to independently assure the privacy of personal information or the security and reliability of the technology they use. As a result today's consumers - like stockholders in the 1920s, do not know whether a company is backing up its words with deeds.

PAPER
expert



Strategic risk

the shareholder view

The shift of funds into new economy stocks means that professional investors are scrutinising listed companies' e-commerce strategies much more closely. As has been the case for a significant period with the non-online economy, the value of independent assurance is acknowledged as being critical by investors as it provides comfort that the fundamentals of good business are being executed.

Those companies that don't measure up against these criteria are seeing their share prices discounted in the market, or worse, they are being shut down. This is further reflected in the increasing dominance of traditional businesses in the online market place following the technology market correction in April 2000.

Building brand strength

Consumers need to trust a brand in order to buy from its web site. After all, how can they be sure the web site is run by a real company, how do they know whether their request for no marketing information will be respected, how do they know whether their personal information will be kept private, whether the company has the systems to order, deliver and bill on the sale as expected or that their credit card information is secure?

The rampant activities of hackers and the use of unrequested cookies and web bugs —which collect click-stream data to support high-pressure selling — on many sites make it hard for online consumers to trust the Internet as a medium. An independent web seal lets consumers know that they can trust a site. In turn, this can significantly build brand strength and provide a key market differentiator.

For some e-commerce businesses, security and privacy can be instrumental to the success of that business. A good example is business-to-business (B2B) exchange company PaperExchange.com. This company has captured a space in the highly competitive US B2B market place and sets a high security standard having developed innovative tools to safeguard the confidentiality of its members.



Regulators waiting in the wings

Despite the competitive pressures that exist in e-commerce, user concerns and the rapid growth of this industry, means that government interest in its development is also growing. If the industry fails to quickly develop a robust system of self-regulation then it is quite possible that more governments will begin legislating to implement their own controls.

Governments have already legislated to deal with privacy issues. On 1 January this year, Canada enacted the Personal Information Protection and Electronic Documents Act, offering its citizens sweeping protections.

In Australia, from 22 December this year, organisations will need to comply with the National Privacy Principles embodied within the 1998 Federal Privacy Act or have an approved privacy 'Code of Practice'.

..there is an increasing demand for effective information security management and ways of protecting critical IT assets,..

In response to e-security threats, there is an increasing demand for effective information security management and ways of protecting critical IT assets as highlighted by the recent launch of the AS/NZS Standard 4444. The standard delivers known levels of security, is a safe method of information transfer, allows for comparability as well as international mutual recognition and flexibility, enabling adoption in a range of industries.

By embracing a comprehensive self-regulation model, businesses complement existing government legislation, minimising the threat of over-regulation that may result in impractical and burdensome requirements.

The Australian Office of the Privacy Commission has started assessing seals against the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. It feels, 'objective assessment of the extent to which seals provide acceptable and enforceable privacy protection may be a crucial factor in determining the degree and speed with which they become more accepted by consumers. Such assessment could help consumers' differentiation between seals that offer effective privacy protection and those that offer only a compromise.'⁴

The commission's report also states 'the profile and potential importance of web seals has been further heightened by the recently announced Safe Harbour Agreement reached between the European Union and the United States. The agreement identifies privacy self-regulatory organisations (such as web seals) as acceptable mechanisms for determining compliance with its privacy principles.'

The accreditation issue has for some time also concerned the National Electronic Authentication Council (NEAC) in Australia. To address the issue it is planning to create a national assurance framework for electronic authentication of products and services. This framework is planned to contain the costs of accreditation, exploit existing knowledge and experience, ensure technology neutrality and meet the real needs of e-business.

⁴From Web Seals: *A Review of Online Privacy Programs*, A joint project of The Office of the Information and Privacy Commissioner/Ontario and The Office of the Federal Privacy Commissioner of Australia, Venice, September 2000.

Finding the right track towards trust

There is no simple template to follow to build trust on the Internet. However, for many e-businesses, providing users with an independent assessment of online assurance is a valuable start.

Just as a company's financial statements need to be independently audited on a regular basis, so do its measures to protect information security and privacy given that a company's systems are constantly changing and so too is the Internet landscape.

A seal of assurance may prove to be an effective tool in building trust with web site users. By embracing a comprehensive self-regulation model, businesses complement existing government legislation, minimising the threat of over-regulation.

To maximise the investment in a web seal, companies need to understand what each seal offers and to choose a reputable independent third party to carry out the audit.

To get the full benefit of online assurance, a company needs to communicate its investment in assurance as effectively as possible, providing a point of difference from competitors and ensuring users are fully aware of the benefit of using their e-commerce services. A small number of online businesses' have made this commitment; others will surely follow either by force or through need.



Adelaide

Roger Milton

(08) 8233 7032

roger.milton@ernstyoung.com.au

Brisbane

Mark Hayward

(07) 3011 3385

mark.hayward@ernstyoung.com.au

Francois Van Der Wait

(07) 3011 3378

francois.van.der.wait@ernstyoung.com.au

Melbourne

Stephen Woolley

(03) 9288 8854

stephen.woolley@ernstyoung.com.au

Andrew Pearce

(03) 9288 8573

andrew.pearce@ernstyoung.com.au

Kenneth Michael

(03) 9288 8351

kenneth.michael@ernstyoung.com.au

Jodie Stow

(03) 9288 8717

jodie.stow@ernstyoung.com.au

Jennifer Berensen

(03) 9288 8998

jennifer.berensen@ernstyoung.com.au

Perth

Iain Burnet

(08) 9429 2486

iain.burnet@ernstyoung.com.au

Sydney

Bruce Young

(02) 9248 4520

bruce.young@ernstyoung.com.au

Fu-Kiang Lee

(02) 9248 4601

fu-kiang.lee@ernstyoung.com.au

ERNST & YOUNG

www.ey.com/au/ecEnablement

© 2001 Ernst & Young. All Rights Reserved. Ernst & Young is a registered trademark.

This communication provides general information current as at the time of production. It is not intended that the information provide advice and should not be relied on as such. Professional advice should be sought prior to actions on any of the information contained herein.

Liability limited by the Accountants Scheme, approved under the Professional Standards Act 1994 (NSW).

Business Development EYA (MEL015595)