

## Providing Online Assurance About Security

a report by

**Chris Potter**

*Certified Information Systems Auditor (CISA) and UK Partner, Global Risk Management Solutions Practice, PricewaterhouseCoopers*

Research has shown that, on average, new sites installed on the Web are accessed within 28 seconds and attacked within five hours. It has been shown that 65% to 75% of worldwide organisations surveyed recently have suffered significant security breaches in the last year, ranging from financial fraud to theft of proprietary information to laptop computer theft.

Businesses are incorporating new information management and communication technologies and introducing new ways of conducting business as part of daily operations. New security technologies are critical enablers to these. Without effective security, the risks associated with e-business become unacceptable, both to management and, because e-security is a double-edged sword, to potential business partners. Recent surveys have highlighted concerns about security and trust as the biggest obstacles to the uptake of both business-to-consumer (B2C) and business-to-business (B2B) e-business.

The challenge that businesses face is how to inspire confidence in their e-security. Customers want security where there is risk, simplicity where there is complexity and clarity where there is uncertainty. Increasingly, businesses are realising that they can obtain a marketing advantage from being perceived as having the best online security and that, if they do not, others will set the standard for their customers' expectations.

This article will explain some of the e-assurance techniques that online businesses are using to inspire confidence and trust in their customers.

### Spoiled for Choice

As businesses investigate their options in building a trusted brand online, there are a growing number of e-assurance standards available. Businesses need to consider carefully the associated costs and benefits that are involved with obtaining accreditation against one or more of these standards.

All e-assurance standards seek to achieve broadly the same objective, namely, to provide the audience with assurance about the business's online security.

However, the form of e-assurance varies based on the audience and what the audience expects to see. There are two distinct audiences for assurance about e-security: consumers and businesses.

### Web Seals

There are many different Web seals available. Each provides a graphic logo or kitemark that can be displayed on the website to provide consumers with assurance about the website's security and operations.

Some Web seals are relatively easy to obtain since they involve only self-certification, i.e. they represent a statement by management that the business operates in a particular way with little or no independent audit of that statement. Web seals that fall into this category include, for example, seals indicating:

- the use of trustworthy technology on the website;
- merchant processing ability;
- compliance with consumer protection standards; and
- compliance with disclosure standards.

While these Web seals do not involve any independent audit, they do provide the audience with some assurance that, at the very least, management has considered the issues and is making a statement about their security and business practices. For some of these seals, the process for gaining the seal involves some form of gap analysis, i.e. a management check that they comply with all aspects of the relevant standard and make any necessary improvements to their business processes before adding the Web seal to their site.

From a marketing perspective, the suitability of a particular seal depends critically on the extent to which the target audience has heard of and trusts the Web seal or the organisation that promotes the Web seal. Consumers tend to trust consumer protection agencies more than technology companies, so their Web seals provide more assurance to consumers within their jurisdiction. However, consumer protection agencies suffer from being territory-specific, posing issues for global websites. A company of e-business advisors can advise on the advantages



Chris Potter is a UK partner in PricewaterhouseCoopers' (PwC's) Global Risk Management Solutions Practice, specialising in e-business security. He has worked in the UK financial services sector for the last 15 years and has broad experience in business advice, internal control and systems development. He is a qualified chartered accountant and a certified information systems auditor. Since 1998, he has run PwC's UK Information Security Practice and has led many information security assignments, for example, to develop security policies, facilitate BS7799 adoption, implement public key infrastructure (PKI) technologies, establish firewalls and secure e-mail infrastructures, investigate cybercrime incidents, carry out penetration testing and benchmark security against good practice and that found in other similar organisations. He also played a leading role in the development of PwC's good practice standards for e-business, based on worldwide experience of clients operating in this area, and has led many assignments to develop e-business risk management frameworks for clients, or carry out health check reviews of significant e-business projects. Before joining PwC, Mr Potter gained a Masters degree in Theoretical Physics at Trinity College, Cambridge.

and disadvantages of the available options and help to obtain the suitable Web seals for particular websites.

As online consumers become more sophisticated, they appreciate the limitations of self-certification Web seals. In the absence of an independent audit, it is important to determine how much assurance the consumer can derive from a Web seal. To address this assurance gap, leading websites are commissioning independent opinions on their e-business, resulting in Web seals such as WebTrust<sup>SM</sup> appearing on their sites.

### WebTrust<sup>SM</sup>

WebTrust<sup>SM</sup> was developed by the American Institute of Certified Public Accountants (AICPA) and is supported internationally. A WebTrust<sup>SM</sup> seal of assurance, with its underlying attestation report located on a website, demonstrates visually to other companies, customers or business partners that a business has maintained a high level of control over critical aspects of e-business. The WebTrust<sup>SM</sup> seal of assurance requires a business to meet high standards for:

- business and information privacy practices;
- transaction integrity; and
- information protection and availability regarding e-commerce conducted on the certified site.

In addition, the business has to disclose its practices and prove compliance to the WebTrust<sup>SM</sup> principles governing confidentiality, non-repudiation and customised disclosures. WebTrust<sup>SM</sup> provides visible, independent assurance over e-business applications. Only accounting and auditing companies can issue a WebTrust<sup>SM</sup> seal. It is revalidated every 90 to 180 days to ensure that the company is adhering to WebTrust<sup>SM</sup> requirements.

### Focusing on Information Security – ISO 17799 Accreditation

Some websites have focused on security as a key issue for online consumers. To establish their security credentials, they have obtained accreditation against the industry best practice standard for information security – International Organization for Standardization (ISO) 17799. ISO 17799 originated in the UK as British Standard (BS) 7799 in the early 1990s and has been adopted progressively by other countries worldwide before becoming ISO 17799. The 10 modules of the ISO 17799 standard cover all aspects of information security within an organisation.

A business can choose to adopt ISO 17799 over its entire business operations or over a specific business process, for example, its e-business activity. In adopting ISO 17799, a business identifies the security

controls it has implemented to achieve compliance with the control objectives in the standard. Not all control objectives will always apply, so part of the adoption process is to identify which areas of ISO 17799 apply based on the scope.

Once a business has adopted ISO 17799, it must obtain independent accreditation. Auditors or security consultants will carry out the independent accreditation, which involves an independent review of the steps that management has taken to adopt ISO 17799. Typically, the reviewer checks that:

- management has justification for any control objectives not adopted;
- adequate controls have been implemented to achieve compliance with each control objective adopted, i.e. gap analysis;
- the controls selected are commensurate with the risks identified, in particular, that appropriate controls are in place over high-risk areas; and
- controls that have been selected by management are actually in place, i.e. through testing.

Once the review has been completed satisfactorily, the independent reviewer allows the business to affix a Web seal or equivalent statement to its website, indicating ISO 17799 accreditation.

### Online Reports for Business Partners

ISO 17799 accreditation can also be applied to B2B applications, providing business partners with assurance in the form of an online report. Other options that businesses should consider for B2B e-assurance include:

- SysTrust<sup>TM</sup> attestation, aimed at business partners; and
- SAS 70 reports, aimed at the auditors of business partners.

### SysTrust<sup>TM</sup>

The AICPA SysTrust<sup>TM</sup> attestation service was developed to create trust between business parties performing e-commerce and focuses on systems' reliability. It reports on the availability, security, integrity and maintainability of an organisation's system. A SysTrust<sup>TM</sup> report attests to any or all of the following principles of a system: availability, security, integrity and maintainability.

All of the SysTrust<sup>TM</sup> criteria for all four principles must be satisfied for a system to be deemed reliable.

For engagements that do not address all of the four principles, all of the criteria related to the principle(s) under examination must be satisfied. In addition, the report must indicate which principles were not examined in the engagement.

### SAS 70

SAS 70 is a US auditing standard that provides a framework under which a service organisation, for example, an application service provider (ASP) or outsource provider, can provide assurance about its controls to the auditors of its users. To achieve this, the service organisation commissions an independent auditor to review the service organisation's controls and issue an independent report in respect of them.

An SAS 70 audit report is intended for user auditors and provides information about the service organisation's controls. It is designed to meet specified control objectives, whether the controls as designed are in operation and, in some cases, whether the controls are operating effectively to achieve the objectives. An SAS 70 report covers the design, implementation and effectiveness of controls at the service organisation. The report is used explicitly to support the financial audit process of organisations that use the service organisation. Typically, an SAS 70 report contains large

amounts of detail on the description of the control environment, the control objectives and the controls that are in place to meet those control objectives. It may also cover whether the controls are operating effectively to achieve the objectives.

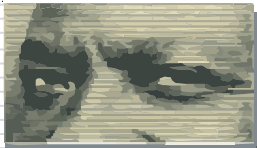
SAS 70 reports are restricted to the service organisation, its customers and the independent auditors of its customers and, therefore, would not normally be posted online without security restrictions on those who can access the online report.

### Conclusion

Trust is essential in conducting e-business with customers and business partners. It is essential that organisations are able to identify and manage e-business risks to leverage fully the opportunities that are found in a connected economy. e-Assurance can assist an organisation to achieve the security, reliability, effectiveness and assurance that is necessary to build trust in the e-business world. ■

### Additional Information

*The complete version of this article may be found in the Reference Library on the CD-ROM accompanying this business briefing.*



## Safeguard your Network before Hackers Exploit It!

QualysGuard can help you:

- See your network's vulnerabilities in a new way, from a hacker's "inside-out" perspective
- Obtain expert recommendation to secure your mission critical systems
- Deploy the latest online security solutions
- Analyze and assess the relative risk of each vulnerability

ACT NOW for a **FREE Scan!**  
[http://www.qualys.com/form\\_trial2.html](http://www.qualys.com/form_trial2.html)

Automate Your Internet Security

