A Model and Framework for Online Security Benchmarking

Graeme Pye and Matthew J. Warren
School of Information Systems, Deakin University
Geelong, Victoria, Australia, 3217
E-mail: graeme@deakin.edu.au, mwarren@deakin.edu.au

Keywords: online, security, benchmarking.

Received: March 9, 2007

The variety of threats and vulnerabilities within the online business environment are dynamic and thus constantly changing in how they impinge upon online functionality, compromise organizational or customer information, contravene security implementations and thereby undermine online customer confidence. To nullify such threats, online security management must become proactive, by reviewing and continuously improving online security to strengthen the enterprise's online security measures and policies, as modelled. The benchmarking process utilises a proposed benchmarking framework to guide both the development and application of security benchmarks created in the first instance, from recognized information technology (IT) and information security standards (ISS) and then their application to the online security measures and policies utilized within online business. Furthermore, the benchmarking framework incorporates a continuous improvement review process to address the relevance of benchmark development over time and the changes in threat focus.

Povzetek: Razvito je novo testno okolje za preizkušanje varnosti internetnega poslovanja.

1 Introduction

Online security measures and policies are essential for protecting both the information of any online business and that of its customers. It is also imperative to maintaining an online business's competitive edge, building trust, customer confidence and enhancing the business reputation while maintaining and operating a secure online business environment (Standards Australia 2001). To this end this research paper represents the initial research including the model framework in an online context utilising the online security benchmarking approach and this research contributed to the evolution of the research into a final formalised E-business security benchmarking model and framework (Pye & Warren 2007).

A key finding of the 2004, 2005 and 2006 AusCERT surveys (AusCERT 2004, 2005, 2006) is that organizations are showing a preparedness to protect their IT systems across three areas: the use of information security policies, their practices and procedures; the use of information security standards or guides; and the number of organizations with qualified, experienced and trained personal. This indicates that Australian organizations are placing greater importance on managing the security of their information systems against latent online security threats and vulnerabilities. Similarly, the online components of Australian businesses can seek to deal with such security issues by applying the minimal best practice security recommendations outlined within the current Australian and New Zealand Information Security Management Standard, AS/NZS ISO/IEC 17799:2001 (Standards Australia 2001). Alternatively, they can apply the recommendations of various reports, guidelines, frameworks and security best practice publications that deliver advice on securing an online business implementation (NOIE 2002). Also in 2007, the Australian Federal Government allocated $13.6 million over four years in the national budget to improve e-security at a national level, to raise awareness of e-security issue for home users and small businesses including teaching e-security within schools (Coonan, H, 2007) and this will help to improve e-security awareness and in the long term security management.

Therefore, the authors propose that the development and application of online security benchmarks can provide both guidance and an assessment methodology for online security measures and policies. Furthermore, by incorporating a regime of continuous improvement, any online business can proactively strengthen security measures and policies through periodic revision. This paper establishes a dynamic benchmarking model applicable to the online business environment and proposes a managerial framework for establishing, reviewing and continuously improving online security benchmarks that also takes into consideration the passage of time, while still remaining applicative to Australian online business.

2 Benchmarking and Continuous Improvement

Benchmarking in traditional business models plays a major role in the ongoing assessment of business performance and return on investment. Similarly,

benchmarking is also applicable to an online business or component thereof as a method to gauge performance and promote continuous improvement of online business processes (McGaughey 2002).

2.1 Benchmarking

Traditional business has utilized the systematic evaluation provided by benchmarking as a standard against which to compare and measure performance (Koch & Robertson 2002) and as an analysis tool focused on competitive performance factors such as costs, strategies and products within their competitive business domains. From such analyses an understanding can be gained of how the business compares with its peers and to what extent it deviates from the 'norm' or established benchmarks, over a given number of parameters (Codling 1996).

Therefore, benchmarking enables identification and targeting of business areas that are not meeting the established benchmark measures. Furthermore, by coupling the element of continuous improvement to the benchmarking process, sub-standard business areas become the focus of regular audits, assessment and ongoing monitoring through a periodic review process. Additionally, continuous improvement applied through revision of the benchmark itself incorporates the betterment of the set benchmark standard in an ongoing continuous manner too.

2.2 Continuous Improvement

Continuous improvement is the process of revising and improving upon previous assessment criteria to raise the level of functionality, improve efficiency and strengthen the assessment criteria with each application of the continuous improvement process (McGaughey 2002). Ideally, the continuous improvement process itself is an endless circular process that aims to establish higher goals with every iteration and reappraisal of the assessment criteria (Zajacek 2002). Benchmarking with continuous improvement will establish benchmarks that are continually reviewed, improved upon and strengthened in an ongoing manner. This proactive concept begins to address the dynamic environment of online business security, through the application of continuous improvement benchmarks for online security measures and policies.

3 A Benchmarking and Online Business Security Model

The concept of proactive online security benchmarking utilizes the continuous improvement principles of Total Quality Management alluded to by Saylor (1996). However, management of online security measures and policies has tended to be reactive and addressed only the perceived threats and vulnerabilities to the online business at the point in time of their implementation. Hence, online security generally remains static and is not reviewed, assessed or upgraded until after a detected security incident has run its course (Kolokotronis et al. 2002).

One way to address this reactive perception of security is through the utilization of continuous improvement benchmarking techniques that proactively assess security measures and policies in an ongoing manner. This ensures that both the business online security measures and policies and the security benchmarks are continually improved, strengthened and remain up-to-date as time passes. By applying benchmarking that incorporates a systematic self-assessment regime, but vigilance is still required so that the application of 'best practice' online security does not lapse and become static once again and therefore incapable of addressing and meeting the changing nature of online threats and vulnerabilities.

Figure 1 depicts the authors' perception of a traditional reactive online business security model and conceptually illustrates how the application of a proactive benchmarking model would exist and function to enhance online business security measures and policies.

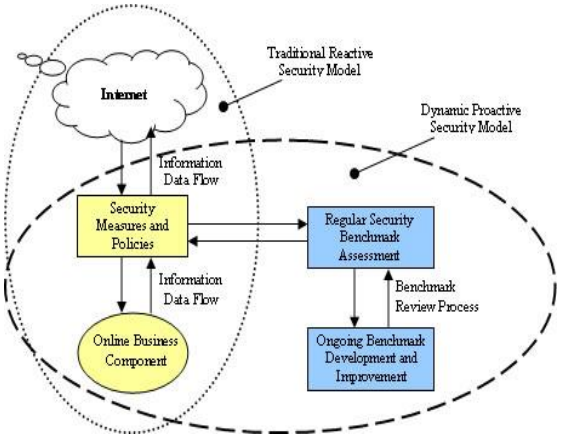

Figure 1: Online Security Benchmarking Model.

The essence of this proactive benchmarking process is the continual security benchmark review and improvement leading to the strengthening of online security measures and policies. Therefore, the results of this process will better reflect the business and customer security expectations for secure operation and continue to meet the economic expectations of the online business enterprise (McGaughey 2002). While this model (Figure 1) illustrates in general terms where online security benchmarking would be applied within the online business environment, there are a number of differing areas within an online business environment that need further consideration in terms of vulnerability types and the likely security criterion that should be benchmarked within these areas.

4 Online Business Security Criteria for Benchmarking

In general, online threats and vulnerabilities can fall within five broadly applicable criteria to online business security, namely Organizational Security, Infrastructure

Security, Application Security, Network/System Security and User Management Security. Each of these security criteria addresses a specific area of online business security and incorporates security standards' based recommendations that relate to the establishment and development of security benchmarks applicable to online business security (Pye & Warren 2003).

4.1 Organizational Security

The diffusion and complexity of technology within the online business environment demands that a reasonable level of security be implemented and maintained. This requires online organizations to develop and establish considered plans that organize and efficiently implement online security measures and policies via a functional and systematic security management plan (BSI 2003) and some of the key areas that should be benchmarked are identified as follows (Standards Australia 2001).

Organizational Security Management Policy Benchmarks ensure that an unambiguous security management policy is applied and readily available across the organization that clearly states the direction and goals for security management by outlining the organization's approach to online security.

Information Security Management Benchmarks relate to the management practices within an online business and ensures that a consistent organizational wide approach to secure management and storage of information within the possession of the business applies consistently at all levels of personnel.

Personnel Security Management Benchmarks ensure that adequate background checks are in place prior to the employment of new staff to address and minimize the risks of human error, theft, fraud and misuse of the organization's assets.

Security Incident Reporting Benchmarks measure the management and prompt activation of contingency plans that are paramount to minimizing damage from security incidents and malfunctions. It is imperative to report all security incidents as soon as practicable to the designated point of managerial contact irrespective of its magnitude to evoke a response action and ongoing incident monitoring for further subsequent analysis.

All staff and external contractors must be aware of the reporting procedures for incidents to minimize the potential impact on organizational assets of security breaches, threats, weaknesses or malfunctions.

4.2 Infrastructure Security

Infrastructure security is a vital consideration to the overall security of buildings, offices and the equipment within the physical boundaries of the online business. Physical security controls should utilize physical barriers to protect assets from unauthorized access, damage, interference, and removal (Australian Standards 2001) and benchmarked as follows.

Physical Security Management Benchmarks ensure measures are in place to prevent unauthorized access, damage and interference to the premises by physically protecting critical equipment and sensitive business information within the building. Therefore, the emplacement of the online business processing hardware should be within a clearly defined secure area behind appropriate barriers and entry controls.

Equipment Security Management Benchmarks appraise equipment asset security to prevent loss, theft and damage and guard against the compromise of sensitive information and the protection of such equipment from physical threats and potential environmental hazards.

General and Media Management Benchmarks evaluates security controls to protect against disclosure, modification and theft by unauthorized persons by ensuring the controlled handling of computer media and its disposal is physically protected with procedures to protect documentation, computer storage media, data and system documentation from damage, theft and unauthorized access.

4.3 Application Security Benchmarks

Software applications are integral to a functional online business and protective policies and measures should be in place to combat malicious software and establish appropriate electronic communications standard using encryption techniques to protect data in storage or during transmission across insecure public networks, benchmarks can address the following aspects (Standards Australian 2001).

Malicious Software Security Management Benchmarks measure the safeguards against the introduction of malicious software into the system, user education, security controls, and policies used to protect business information assets.

Electronic Mail Security Management Benchmarks ensure that the controls in place protect against loss, modification or misuse of information exchanged, email access should be controlled, monitored and compliant with the relevant legislation and user behaviour education should be adopted to reduce risk.

Encryption Management Benchmarks ensure that the cryptographic controls adopted to safeguard confidentiality, integrity or authenticity of information transmitted across public networks.

4.4 Network/System Security

Computer networks and systems convey the communication and exchange of data for online business and it is imperative that security controls and policies are in place to regulate how such systems are utilized and accessed. These safeguards protect the information within internal and public networks as well as supporting the protection of the network infrastructure and suggested benchmarks are as follows (Standards Australia 2001).

Network/System Communication Control Benchmarks relating to the control of internal and external network communication and network services is necessary to ensure users who have access do not compromise the security measures and policies in place

(Australian Standards 2001). Firewalls define the online boundary by providing communication control between internal networks and the publicly accessible external networks (BSI 2003).

System Security Management Benchmarks ensure planning is in place to minimize the risk of system failures to ensure system availability, adequate capacity, and enough resources exist for future expansion and growth of the online business (Standards Australia 2001).

Network/System Security Management Benchmarks focus on protecting the information and supporting infrastructure of the local network within the physical boundaries of the online business and includes all the activities and controls for securing the network (Standards Australia 2001).

System Use Monitoring Benchmarks measure the effectiveness of system monitoring in detecting unauthorized activities and records deviations from access control policy by logging system events to provide an audit trail and evidence in the event of security breaches or incidents caused by internal or external users (Standards Australia 2001)

4.5 User Management Security

Validation and authentication of internal business staff and online customers can deliver a protective barrier to unauthorized access and this should cover the entire life-cycle of the user's access to services from new registrations to final deregistration by benchmarking the following aspects (Standards Australia 2001).

Password Management Benchmarks measure the strength and enforces regular changing of passwords for validating the identity of the user prior to the granting of access to a particular online service or system (Standards Australia 2001).

Authentication Management Benchmarks ensures that authentication mechanisms for online business systems and applications identify the users uniquely and authenticate prior to permitting further interaction between the online business system and the user.

The pursuit of business activities and transactions across public networks involving the exchange of sensitive data exposes the online business to potentially damaging threats and vulnerabilities that may result in fraudulent activity, contract disputes and the disclosure or modification of sensitive information.

Therefore, the application of regular benchmarking of online business security measures and policies will provide the online business with the ability to review their security status and continue to strengthen and update online security measures and policies. Pursuant to this view however is the need for a framework in which to develop these security benchmarks.

5 Online Security Benchmark Framework

Before developing meaningful online security benchmarks, it is necessary to ascertain a starting point to devise the essential benchmarking elements necessary to assess online business security. An internationally recognized published standard is an obvious starting point for developing online security benchmarks, such as the Australian and New Zealand Standard AS/NZS ISO/IEC 17799:2001 (2001). In utilizing the Australian and New Zealand Standard (2001) as the minimal benchmarks for online security, it is also important to have benchmarks that indicate improved online security goals. One such security standard that sets a higher security baseline than the Australian and New Zealand Standard is the German IT Baseline Manual (BSI 2003).

The premise for the German IT Baseline Manual (BSI 2003) being at a higher baseline standard than the Australian and New Zealand Standard is supported by a comparative evaluation of information security, baseline standards undertaken by Brooks and Warren (2001). This research concluded that the information within the Australian and New Zealand Standard (2001) focuses on enhancing information security awareness and authorization security at the minimal 'best practice' level. While the German IT Baseline Protection Manual (BSI 2003), documented baseline security features that were of a higher minimal standard, although its focus is technically orientated towards the implementation of security controls needed to secure IT systems. Through applying the Australian and New Zealand Standard (2001) as the minimum benchmark threshold and the German IT Baseline Protection Manual (BSI 2003) as a reasonable benchmark to aim for, this premise can then be applied to benchmarking online security to measure the current status of an online business's security criteria. Furthermore, a framework can standardize benchmark development and deliver consistent and methodical application of such security benchmarks.

5.1 The Online Security Benchmark Framework

Table 1 illustrates the online security benchmark framework that incorporates the Australian and New Zealand Standard (2001) information as the initial minimal security requirement benchmark and similarly applies the recommended German IT Baseline Protection Manual (BSI 2003) information as an improved security benchmark that an online business should endeavor to achieve.

1	Initial Security Benchmark	Minimum Benchmark: Australian and New Zealand Standard (2001). Maximum Benchmark: German IT Baseline Protection Manual (2003).
2	Online Security Assessment	Online Security Assessment Against Applicable Benchmark: Pass/Fail.
3	Current Benchmark Analysis	Analysis of Current Online Security Benchmark: Pass/Fail
4	Continuous Improvement Analysis	Future Security Benchmark Development and Implementation.

Table 1: Online Security Benchmark Framework.

The framework shown in Table 1, consists of a four stage process that can be applied as a circular development process to initially create a security benchmark and then continue to improve upon such benchmarks developed, this with the following assessment methodology can then be applied to benchmark or determine the security status of online business policies and measures, while further guiding the proactive development and implementation of continuously improved benchmarks for online security.

5.2 Methodology for Applying the Security Benchmark Framework

The methodical application of the online security benchmark framework within an online business is essential to correctly apply the benchmarking concept to online security policies and measures. The following outlines the methodology to apply when benchmarking online business security.

Initially, it should be determined within the security criteria of the online business, which security measure or policy is applicable to which particular benchmark, this ensures consistency of assessment and sets a minimum and maximum security benchmark.

Next, an assessment of the particular online business security measure or policy in comparison to the minimum security benchmark listed determines if it meets the minimum benchmark standard.

Then an assessment analysis on the current benchmark establishes its effectiveness and assists the development of an improved security benchmark as the new minimum benchmark thus strengthening the security benchmarking criteria with a higher-level benchmark.

The final step in the methodology promotes proactive benchmark development and ongoing continuous improvement research. This is to determine new and improved security benchmarks that exceed the current minimum security benchmark and to potentially define a new maximum benchmark as recorded in the framework, with the intention of becoming the future minimum benchmark.

However, there is a need to be mindful of the initial level of security advice provided by the relevant information security standard, as this is the underpinning foundation of the security benchmarking process and the initial security benchmark development starting point, irrespective of the current online security environment.

6 Information Security Standards (ISS)

Therefore, as the initial online security benchmarks are set, based on the relative Australian Standard New Zealand Standard (2001) and German IT Baseline Protection Manual (2003), there remains the point that the intention of such technology ISS is what do they actually deliver. The intention of the ISS is to deliver comprehensible and precise meanings to describe various technological actions as is related to IT security in a consistent, unambiguous and comprehensive manner. The Standard itself has to be flexible enough to allow for innovation and reconcile user issues while still delivering guidance for resolving both technical and political problems. Therefore, Standards are particularly useful as a starting point for solving particular issues and are very appropriate where many systems function in a similar manner. However, while Standards remain regarded as technical document devices for the achievement of specific ends and essential to progress, they can also be a hindrance to innovative creativity and can encourage mediocrity due to their very convenience as a required minimum measurement (Libicki, 1995).

Therefore, it is with this in mind that the authors have developed the Online Security Benchmark Framework as a means to initially create a specific online security benchmark and to encourage continuous improvement by employing a circular process whereby the security benchmark is continually improved. Continuous improvement is imperative to proactive security benchmarking development to avoid, falling into the trap of mediocrity whereby the security benchmark is set once using the relevant security Standard and never improved upon or reassessed until necessary.

Furthermore, the aim of the authors is to encourage continuous improvement as a means of negating the passage of time and ensuring that the security benchmarks established by an organization will continue to measure the effectiveness and strengthen security measures and policies applicable to protecting the online security of an organization.

7 The ISS Verses Security Benchmarking Over Time

An often ill-considered aspect of developing and implementing online security measures and organizational security policies is the consequence of time. When considering that every person, society and environment occupies a point in time that is dynamically changing as time passes, all too often security measures and policies are created and implemented initially but thereafter remain unchanged as time passes. The authors submit that a lack of appreciation of the perception of time passing is a security weakness, but not from the perspective of security where a ‘set and forget’ static approach is generally applied.

From a philosophical aspect the ‘perception of time’ expression exists as one of three states: past, present and future and these states are perceived by changes or events in time and what is perceived as the present and what is going on right now. Furthermore, perceptions of past, present and future are important for social enquiry and action as they draw on past events that influence the present, but may not determine the future specifically although may enable a perceived range of likely futures (Le Poidevin 2004). Therefore, by incorporating an appreciation of the perception of time in the benchmark development process, the authors consider that online security can indeed utilize past and present perceptions of time related to the changes in the online security

environment to promote continuous improvement. Thus as applied in the online security benchmarking framework (see Table 1), the application of a continuous improvement process can deliver continually improved upon online security benchmarks into the future.

The advantage of adopting a continuous improvement benchmarking process is that over time the security benchmarks will be strengthened through regular review and updating. Whereas the ISSs' only deliver a static security reference that is applicable at a specific historical point in time, which is valuable in providing a starting point for the establishment of the initial online security benchmark. However, over time the ISS only represents a historical reflection of security and is very slow to update in comparison to the proposed benchmarking framework for online security. Therefore, the online security benchmarking framework offers an improved method of proactive online security maintenance of polices and measures that continues to take into consideration, not only the historical security aspect, but also adopt changes relevant to the present situation that can or may be incorporated and applied in the future. By utilizing the perception of time in the security benchmarking development process, this is addressing the dynamic nature of the online environment and potentially insulates the online components and protects the information of the organization in a way that is proactive to the online environment and continues to strengthen security measures and policies.

8 Conclusion

The benchmarking model and framework illustrated here for online security measures and policies, is designed to deliver guidance, manageability and consistency to the development, ongoing protection and improvement to the security features of an online business. Thus enabling a business to develop applicable security benchmarks, determine their current online security status and implement a continuous improvement plan to improve and strengthen their online security measures and policies. The technology ISS offers a starting point for development of online security benchmarks only and fails to address the ongoing changes and developments that occur in the online environment that can adversely impinge upon the secure function of an organization's online business component.

The practical application of this research would be beneficial to raising the awareness of security issues and policies within an online business and would perhaps encourage a culture of security awareness within any organization. This may be a consequence of the benchmarking regime as it lends itself to the management, monitoring and continuous improvement of online security measures and policies protecting the information within a business's possession, but this remains speculative. An indicative example of an application of the benchmarking methodology would be the benchmarking the security of an electronic supply chain, where a number of individual co-operating supply chain members would be able to apply the online security benchmarking framework and methodology proposed here, to ensure that all members of the electronic supply chain meet and continue to improve their security status, as proposed by Pye et al (2005).

Additionally, further research is still required to assess the effectiveness, value and cost that the application of the security benchmarking techniques alluded to in this paper would impose on the business itself and whether these benchmarking techniques deliver practical assessments of the online security status of any business. Additionally, further research is required to determine if the continuous benchmarking techniques, as outlined in the framework (see Table 1) would prove to be advantageous to the assessment, application and monitoring of IT governance requirements of any business that utilizes information systems as an underpinning support to their online business, business processes and ambitions.

9 References

[1] AusCERT (2004) Australian Computer Crime and Security Survey, AusCERT. URL: <http://www.auscert.org.au/render.html?it=2001> Accessed: May 2004.

[2] AusCERT (2005) Australian Computer Crime and Security Survey, AusCERT. URL: <http://www.auscert.org.au/images/ACCSS2005.pdf> Accessed: May 2005.

[3] AusCERT (2006) Australian Computer Crime and Security Survey, AusCERT. URL: <http://www.auscert.org.au/images/ACCSS2006.pdf> Accessed: May 2006.

[4] Brooks W., Warren M.J. (2001) A Security Evaluation Criteria for Baseline Security Standards. Technical Report TR C 01/18, Deakin University, Geelong.

[5] BSI (2003) IT Baseline Protection Manual. Federal Agency for Security in Information Technology. Bundesamt für Sicherheit in der Informationstechnik (Multimedia CD-ROM).

[6] Codling S. (1996) *Best Practice Benchmarking.* Gulf Publishing Company, Houston, Texas.

[7] Coonan H. (2007) Improving e-security for home users and small business – Media Release, May, 2007, Accessed 11th May 2007, URL: http://www.minister.dcita.gov.au/media/media_releases/improving_e-security_for_home_users_and_small_business.

[8] Koch H., Robinson P.E. (2002) Evaluating Electronic Commerce Initiatives with Benchmarks: Insights from Three Case Studies, *Eighth Americas Conference on Information Systems.* pp.1251-1258.

[9] Kolokotronis N., Margaritis C., Papadopoulou P., (2001) An integrated approach for securing electronic transactions over the web, *Benchmarking: An International Journal* Vol: **9** (2): pp.166–181.

[10] Le Poidevin R. (2004) The Experience and Perception of Time. The Stanford Encyclopedia of Philosophy, URL:

<http://www.plato.stanford.edu/archives/win2004/entries/time-experience> Accessed: May 2006.

[11] Libicki M.C. (1995) *Information Technology Standards. The Quest for the Common Byte*, Digital Press, Newtown, MA.

[12] McGaughey R.E., (2002) Benchmarking business-to-business electronic commerce, *Benchmarking: An International Journal* **Vol. 9** (5): pp.471-484.

[13] NOIE (2002) trusting the internet. small business guide to e-security, NOIE, URL: <http://www.noie.gov.au/publications/NOIE/trust/trusting_the_internet.pdf> Accessed: December 2002.

[14] Pye G., Pierce J.D., Warren M.J., Mackay D.R. (2005) Supply Chain Security: The Need for Continuous Assessment, *Supply Chain Practice* **Vol. 7** (1): pp.4–16.

[15] Pye G., Warren M.J. (2003) Development of I.T. Evaluation Criteria for Common E-business Security Issues. Technical Report TR C 03/12, Deakin University, Geelong.

[16] Pye G., Warren M.J. (2007) E-business security benchmarking: a model and framework, International Journal of Information and Computer Security, Inderscience Publishers (Vol. 1, No. 4, pp. 378-390).

[17] Saylor J.H. (1996) *TQM Simplified. A Practical Guide*, 2nd Ed. McGraw-Hill New York.

[18] Schneider G.P., Perry J.T. (2001) *Electronic Commerce*, 2nd Ed., Course Technology.

[19] Standards Australia (2001) *Information Technology - Code of practice for information security management. AS/NZS ISO/IEC 17799:2001*, Standards Australia, Barton.

[20] Zajacek M. (2002) Continuous Development Process. URL: <http://www.unimelb.edu.au/develpoment/wag/index.html> Accessed: July 2003.