Edith Cowan University

Research Online

Research outputs pre 2011

2005

# Benchmarking e-business security: A model and framework

Graeme Pye

Matthew J. Warren

Follow this and additional works at: https://ro.ecu.edu.au/ecuworks

 Part of the Information Security Commons

Pye, G., & Warren, M. J. (2005). Benchmarking e-business security: A model and framework. In *Proceedings of 3rd Australian Information Security Management Conference* (pp. 80-87). Edith Cowan University. Available here.
This Conference Proceeding is posted at Research Online.
https://ro.ecu.edu.au/ecuworks/7315

# Benchmarking E-business Security: A Model and Framework

Graeme Pye and Matthew J. Warren
School of Information Systems,
Faculty of Business and Law,
Deakin University,
Geelong, Victoria, Australia, 3217.
graeme@deakin.edu.au; mwarren@deakin.edu.au

## Abstract

*The dynamic nature of threats and vulnerabilities within the E-business environment can impede online functionality, compromise organisational or customer information, contravene security implementations and thereby undermine online customer confidence. To negate these problems, E-business security has to become proactive, by reviewing and continuously improving security to strengthen E-business security measures and policies. This can be achieved through benchmarking the security measures and policies utilised within the E-business, against recognised information technology (IT) and information security (IS) security standards.*

**Keywords**

E-business, IT security standards, information security, E-business security measures and policies, benchmarking, continuous improvement.

## INTRODUCTION

Security measures and policies are essential for protecting both the information of an E-business and that of its customers. It is also imperative to maintaining an E-business's competitive edge, building trust, customer confidence and enhancing the business reputation of the E-business (Standards Australia 2001).

A key finding of both the 2004 and 2005 AusCERT surveys is that organisations 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 organisations with qualified, experienced and trained personal. This indicates that Australian organisations are placing greater importance on managing the security of their information systems against latent security threats and vulnerabilities.

Similarly, Australian E-business 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 E-business (NOIE 2002).

The authors propose that the development and application of E-business security benchmarks can provide both guidance and an assessment methodology for E-business security measures and policies. Furthermore, by incorporating a regime of continuous improvement, an E-business can proactively strengthen security measures and policies through periodic revision. This paper seeks to establish a general benchmarking model applicable to E-business and provide a framework for establishing, reviewing and continuously improving benchmarks that are applicative to an Australian E-business.

## 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 can be applied to an E-business as a methodology to gauge performance and promote continuous improvement of E-business processes (McGaughey 2002).

### Benchmarking

Traditional business has utilised the systematic evaluation provided by benchmarking as a standard against which to compare and measure performance (Kock & 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 analysis's an understanding can be gained of how the business compares with its peers and to what extent it deviates from the "norm" *(sic)* or established benchmarks, over a given number of parameters (Codling 1996).

Therefore, benchmarking enables us to identify and target areas of the business that are not meeting the established benchmark measures. Furthermore, by coupling the element of continuous improvement to the benchmarking process, sub-standard business areas are not only improved upon, but can be monitored by periodic review. Additionally continuous improvement through revision of the benchmark itself incorporates the betterment of the benchmark standard in an ongoing manner.

**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 set higher benchmark goals with every iteration and appraisal 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 can then be applied to the dynamic environment of E-business security, through the application of continuous improvement benchmarks for E-business security measures and policies.

## A BENCHMARKING AND E-BUSINESS SECURITY MODEL

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

This reactive perception can be addressed through the utilisation of continuous improvement benchmarking techniques that proactively assess security measures and policies in an ongoing manner. Figure 1 depicts the authors' perception of the traditional reactive E-business security model and illustrates how the application of a proactive benchmarking model can be applied to enhance E-business security.

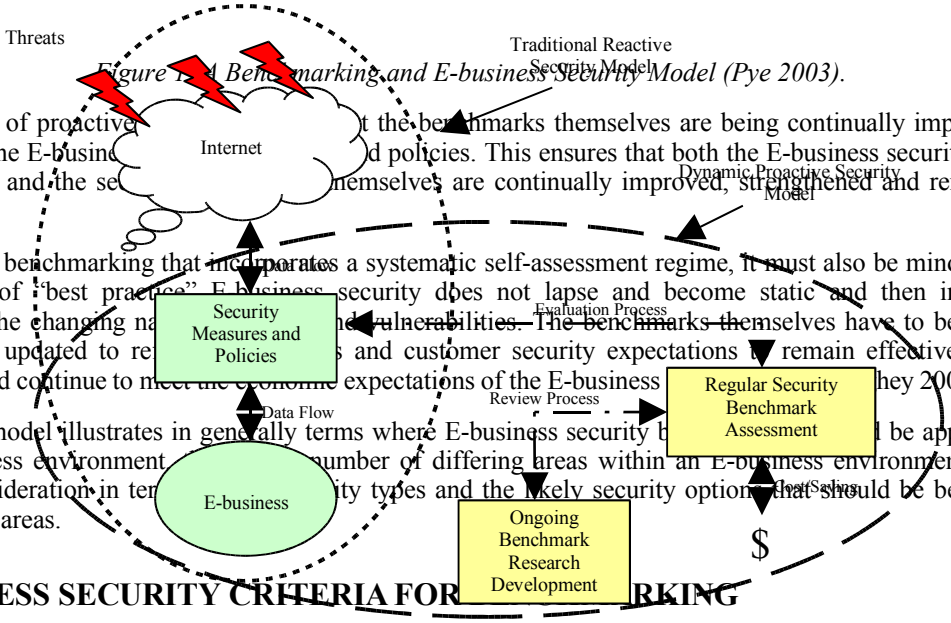


*Figure 1. A Benchmarking and E-business Security Model (Pye 2003).*

The essence of proactive [illegible] the benchmarks themselves are being continually improved upon along with the E-busine[illegible]d policies. This ensures that both the E-business security measures and policies and the se[illegible]hemselves are continually improved, strengthened and remain up-to-date.

By applying benchmarking that incorporates a systematic self-assessment regime, it must also be mindful that the application of "best practice" E-business security does not lapse and become static and then incapable of addressing the changing na[illegible]d vulnerabilities. The benchmarks themselves have to be constantly revised and updated to re[illegible]s and customer security expectations to remain effective, secure in operation and continue to meet the economic expectations of the E-business [illegible]hey 2002).

While this model illustrates in generally terms where E-business security b[illegible]d be applied within the E-business environment[illegible]number of differing areas within an E-business environment that need further consideration in ter[illegible]ity types and the likely security options that should be benchmarked within these areas.

## E-BUSINESS SECURITY CRITERIA FOR [illegible]RKING

In general, threats and vulnerabilities to E-business fall within five broadly applicable criteria to E-business security, namely Organisational Security, Infrastructure Security, Application Security, Network/System Security and User Management Security. Each of the following security criteria addresses a specific area of E-business security and incorporates security standard based recommendations that relate to the establishment and development of security benchmarks applicable to E-business security (Pye & Warren 2003).

**Organisational Security**

The diffusion and complexity of technology within the E-business environment demands a reasonable level of security be implemented and maintained. This requires that E-business organisations develop and establish a well

thought out plan that organises and efficiently implements E-business security measures and policies via a functional and systematic security management plan (BSI 2003).

Some of the key areas that should be benchmarked are as follows (Standards Australia 2001):

- Organisational Security Management Policy Benchmarks;

An E-business should establish an unambiguous security management policy across the organisation that clearly states the direction and goals for security and the management thereof. Such policy documents should clearly outline the organisation's approach to E-business security, as approved by management and be readily available to all staff.

- Information Security Management Benchmarks;

Management practices within an E-business are critical to developing a consistent organisational wide approach to secure the management of information within the possession of the E-business. Such information management is the shared responsibility of all associated personnel, has clear direction, managerial support and resources to promote information security within the E-business organisation.

- Personnel Security Management Benchmarks;

An E-business has to ensure that adequate checks are in place prior to the employment of new staff to address and minimise the risks of human error, theft, fraud and misuse of the organisation's assets.

- Security Incident Reporting Benchmarks;

Security incidents management and the prompt activation of the contingency plans are paramount to minimising damage from security incidents and malfunctions. Such incidents should be reported as soon as practicable to the designated point of managerial contact and monitored to learn from these incidental experiences and it is imperative that all security incidents, regardless of magnitude, be reported. All staff and external contractors need to be aware of the reporting procedures for incidents such as, security breaches, threats, weaknesses or malfunctions, to minimise the potential impact on organisational assets.

**Infrastructure Security**

The security of infrastructure is an important consideration to the overall security of buildings, offices and the equipment within the physical boundaries of the E-business. Physical security controls should utilise physical barriers to protect assets from unauthorised access, damage, interference and removal; this should also address the management of portable data devices and their secure disposal (Australian Standards 2001).

Infrastructure security should benchmark the following physical aspects (Standards Australia 2001):

- Physical Security Management Benchmarks

Physical security is required to prevent unauthorised access, damage and interference to the premises by the physical protection of critical and sensitive business information and the equipment within the building. E-business processing computer hardware should be housed in a clearly defined secure area that is contained by appropriate barriers and entry controls.

- Equipment Security Management Benchmarks

Security of equipment assets is required to prevent loss, theft and damage and to guard against the potential compromise of information regarding E-business activities. The protection of such equipment from physical security threats and potential environmental hazards should also be considered.

- General and Media Management Benchmarks

Security controls should be in place to negate any compromise of sensitive information and to protect against disclosure, modification and theft by unauthorised persons; these controls should also minimise loss and damage. Furthermore, the handling of computer media should be controlled and physically protected with procedures established for protecting documentation, computer storage media, data and system documentation from damage, theft and unauthorised access.

**Application Security Benchmarks**

Software applications are an integral part of a functional E-business and protective policies and measures need to combat malicious software. Additionally, security policies and measures are required for electronic communication

together with the application of encryption techniques to protect data in storage or during transmission across insecure public networks (Standards Australian 2001).

Benchmarks that can be applied to the following Application security aspects are (Standards Australia 2001):

- Malicious Software Security Management Benchmarks

Precautions and safeguards can prevent and detect against the introduction of malicious software into the system, users should be informed of the integrity consequences of utilising unauthorised or malicious software, security controls, and policies should be implemented to protect E-business information assets.

- Electronic Mail Security Management Benchmarks

Loss, modification or misuse of information exchanged between parties should be controlled and compliant with the relevant legislation, in particular for electronic mail (E-mail) communications. E-mail differs from traditional communication methods due to its delivery speed, message structure, informality and vulnerability to unauthorised actions and therefore consideration needs to be given to controls that will reduce security risks.

- Encryption Management Benchmarks

Cryptographic controls should be adopted to safeguard confidentiality, integrity or authenticity of information regarded to be at risk for which other security measures fail to provide adequate protection.

**Network/System Security**

Computer networks and systems form the backbone of the communication and exchange of data for E-business and it is imperative that security controls and policies are in place to regulate how such systems are utilised and protected. These safeguards protect the information within internal and public networks as well as supporting the protection of the network infrastructure (Standards Australia 2001).

Network and system security can have benchmarking applied in the following areas:

- Network/System Communication Control Benchmarks

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). A Firewall acts as the single junction point between two separate networks. Firewalls define the boundary of E-business security and control by providing communication control between internal networks and the publicly accessible external networks (BSI 2003).

- System Security Management Benchmarks

To minimise the risk of system failures, planning and preparation needs ensure system availability, adequate capacity and that resources are allocated for future expansion to minimise the risk of system overload (Standards Australia 2001).

- Network/System Security Management Benchmarks

Network security management is focused on protecting the information and the supporting infrastructure of the local network within the boundaries of the E-business and includes all the activities, controls and safety measures for effectively securing the use of the network (Standards Australia 2001).

- System Use Monitoring Benchmarks

The objective of system monitoring is to detect unauthorised activities and record deviations from access control policy by logging system events to provide an audit trail and evidence in the event of security breaches or incidents (Standards Australia 2001).

**User Management Security**

Validation and authentication of internal E-business staff and customers can deliver a protective barrier to unauthorised access and this should cover the entire life-cycle of the user from new registrations to final deregistration or users who have no further need for access to the system or services (Standards Australia 2001).

The management of user security can be handled by benchmarking the following aspects:

- Password Management Benchmarks

The utilisation of passwords is commonly employed for validating the identity of the user prior to being granted access to a particular computer service or system (Standards Australia 2001).

- Authentication Management Benchmarks

Authentication mechanisms for E-business systems and applications should be designed so that users can be uniquely identified and authenticated prior to further interaction between the E-business system and the user.

The pursuit of E-business activities and transactions across public networks involving the exchange of data exposes the E-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 security measures and development of security policies should be considered in an effort to protect E-business activities and information of the E-business and its customers (Standards Australia, 2001)

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

## E-BUSINESS SECURITY BENCHMARK FRAMEWORK

Before developing meaningful benchmarks that incorporate continuous improvement for E-business security, it is necessary to ascertain a starting point to devise the essential benchmarking elements necessary to assess E-business security. An internationally recognised published standard is an obvious starting point for developing E-business security benchmarks, such as the Australian and New Zealand Standard AS/NZS ISO/IEC 17799:2001 (2001).

In utilising the Australian and New Zealand Standard (2001) as the minimal benchmarks for E-business security, it is also important to have benchmarks that indicate improved security goals for E-business. One such security standard that sets a higher security baseline than the Australian and New Zealand Standard is the German IT Baseline Manual (2003).

The premise of the German IT Baseline Manual (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 (2001). This research concluded that the information within the Australian and New Zealand Standard (2001) is focused on enhancing IT security awareness and authorisation security at the minimal best practice level. While the German IT Baseline Protection Manual (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 (2003) as a reasonable benchmark to aim for, this premise can then be applied to benchmarking E-business security to measure the current status of an E-business's security criteria. However, a framework can standardise benchmark development and deliver consistent and methodical application of such security benchmarks.

### The E-business Security Benchmark Framework

Table 1 illustrates the E-business security benchmark framework that incorporates the Australian and New Zealand Standard (2001) information as the minimal security requirement benchmark for E-business security and similarly applies the recommended German IT Baseline Protection Manual (2003) information as an improved security benchmark that E-business should endeavour to achieve. This framework also delivers guidance to improve progressively the benchmarks set, through the application and management of a continuous improvement aspect applied to the particular benchmark.

*Table1 Continuous Improvement Benchmark Framework (Pye, 2003).*

| | | |
|---|---|---|
| | **Benchmark Name** | |
| | **Security Criteria** | |
| **1** | **Benchmark Definition** | Minimum Benchmark:<br>Maximum Benchmark:<br>Documented security benchmarks set for assessment. |

| | | |
|---|---|---|
| **2** | **Benchmark Reference** | Benchmark Citation:<br>The formal documentation reference citing from where the benchmarks set were sourced. |
| **3** | **Security Benchmark Assessment** | Current Security Assessment Status:<br>Documentation of the actual benchmarking assessment against the particular E-business security measure or policy. Pass/Fail etc. |
| **4** | **Benchmark Assessment Analysis.** | Next Security Assessment Benchmark:<br>Documentation of new security goals in relation to the Security Benchmark Assessment result. Incorporating an analysis of what security improvements can be identified and made to the current security status to promote continuous improvement. |
| **5** | **Continuous Improvement Analysis** | Future Security Benchmark Development:<br>Identification of ongoing research areas to determine improved benchmark development and analysis of the benchmarking assessment procedure for future application. |

The framework, shown in Table 1, consists of an identifying Name for the particular security benchmark and the Security Criteria it addresses and the following:

- Section 1 defines the minimum security benchmark level as defined in the context of the Australian and New Zealand Standard Part One (2001) and a maximum benchmark level as applied in the context of the German IT Baseline Protection Manual (2003).
- Section 2 provides denotative information citing where the particular security benchmark is sourced.
- Section 3 is the documentation of the benchmark assessment criteria and determination is made as to whether the particular E-business security measure or policy meets the established security benchmark.
- Section 4 is where depending on the result of Section 3 that an analysis is made to determine what improvements need to be actioned and put in place prior to the next benchmarking assessment.
- Section 5 is that area of the framework to document and identify areas of ongoing research devoted to the continuous improvement of the security benchmarking criteria.

Both the aforementioned framework and the following assessment methodology can be applied to determine the security status of E-business policies and measures, while assisting in guiding the establishment of continuous improvement benchmarking for E-business security.

**Methodology for Applying the Security Benchmark Framework**

The methodical application of the E-business security benchmark framework within an E-business is essential to correctly applying the benchmarking concept to E-business security policies and measures. The following four steps outline the methodology to follow when benchmarking security against current E-business security policies and measures:

1. Initially, it should be determined within the security criteria of the E-business, which security measure or policy is applicable to which particular benchmark that is appropriate for assessment.
2. An assessment of the particular E-business security measure or policy in comparison to the minimum-security benchmark listed is undertaken to determine if it meets the minimum benchmark required.
3. After assessment, an analysis is undertaken to establish an improved security benchmark that can be implemented into the security benchmarking assessment (Section 3) that strengthens the security benchmark criteria with a higher-level benchmark.
4. The final step in the methodology is dedicated to ongoing continuous improvement research to determine new and improved security benchmarks that exceed the current security benchmark. This is recorded as a future benchmark goal in Section 5 of the framework and will become the minimum benchmark reflected in Section 1 in due time.

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 security benchmarking framework proposed here, to ensure that all members of the electronic supply chain meet and continue to improve their security status as a chain is only as strong as its weakest link as proposed by Pye et al (2005).

The essence of the benchmarking methodology is to establish a minimal level of security in comparison to the Australian and New Zealand Standards (2001) and then establish a regime of regular assessment of the security measures and policies of an E-business organisation against incrementally improved E-business security benchmarks. Through incorporating the development of new security benchmarks for the next assessment, this delivers continuous improvement and thereby strengthens the E-business security in an ongoing manner.

## CONCLUSION

The benchmarking model and framework developed here for E-business 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 E-business. Thus enabling an E-business to develop applicable security benchmarks, determine their current E-business security status and implement a continuous improvement plan to improve and strengthen their E-business security measures and policies.

The practical application of this research would be beneficial to raising the awareness of security issues and policies within an E-business and perhaps would be more likely to encourage a culture of security awareness within any organisation, which applied this regime to the management, monitoring and continuous improvement to security measures and policies protecting the information within a business's possession.

Furthermore, 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 could be applied to practical assessments of the IT security status of any business. Additionally, research is needed to determine if the continuous benchmarking techniques, as outlined in the model (see Table 1) would prove to be advantageous to the assessment, application and monitoring of IT governance requirements of any business that utilises information systems as an underpinning support to their business processes and ambitions.

## REFERENCES:


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

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

Brooks, W., (2001). Developing an Information Security Evaluation Criteria. Honours Thesis, School of I.T., Deakin University.

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

Codling, S., (1996). Best Practice Benchmarking. Houston, Texas, Gulf Publishing Company.

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.

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.

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

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

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.

Pye, G., (2003). Benchmarks for E-business Security. Unpublished Honours Thesis, School of Information Technology, Geelong, Deakin University 2003.

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

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

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

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

Zajacek, M., (2002). Continuous Development Process. (Internet). Available from: http://www.unimelb.edu.au/develpoment/wag/indexhtml (Accessed: July 2003).

## COPYRIGHT

Pye & Warren ©2005. The author/s assign the School of Computer and Information Science (SCIS) & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SCIS & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.