Advances in Robotics & Automation

Hon Keung, Adv Robot Autom 2013, 2:3
DOI: 10.4172/2168-9695.1000e115

Editorial | Open Access

How to Set Security Policy for Electronic Commerce Services?

YAU Hon Keung*

Department of Systems Engineering and Engineering Management, City University of Hong Kong, Kowloon Tong, Kowloon, Hong Kong

Introduction

Data leakage has been one of the most important concerns for many big companies since this problem could bring enormous loss to the company. In this information technology era, data security has become significantly essential and useful yet difficult task since technology is evolving so fast everyday or even minute. Electronic commerce is popular all over the world, however, people face a lot of security problems when they perform the transaction through the web site. Calder [1] mentioned that the standard (ISO/IEC27001:2005) can enable organizations throughout the world to ensure that they are applying information security best practice in their organizations.

Security Policy for Electronic Commerce Services

This section covers these cure use of electronic commerce services and information available in public accessible systems. The following are included:

1. Electronic Commerce and Web Servers
2. On-line Transactions
3. Publicly Available Information.

Electronic commerce and web servers

Objective: To protect the companies' electronic commerce when using public networks.

Justification: Electronic commerce needs to be protected as it is vulnerable to a number of network threats that could result in fraudulent activity, contract dispute, and dis closureor modification of information.

Guidelines: The following need to be considered

1. The identity of the other party must be authenticated through authentication mechanism like public key, digital signatures, digital certificates or even trusted third parties
2. Only authorized users (members) may place orders, set prices or sign trading contracts
3. Confidentiality, integrity, proof of dispatch, order transactions, payment information, delivery address details, confirmation of receipts and contracts should be determined and maintained
4. Liability associated with any fraudulent transactions must be addressed
5. Use the most appropriate settlement form of payment to guard against fraud
6. Payment information supplied by a customer must be verified
7. Avoid loss or duplication of transaction information
8. Addressed considerations by cryptographic controls, taking into account compliance with legal requirements
9. For electronic commerce arrangements with trading partners, a documented agreement including details of authorization and agreed terms of trading should be made.

On-line transactions

Objective: To protect the companies' information used in on-line transactions.

Justification: To protect company and customers from incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. On-line transactions include contractual and financial amongst others.

Guidelines: The following measures must be considered for on-line transactions. The level of therisk associated should be considered:

1. Use electronic signatures by both parties involved in the transaction.
2. Ensure that user credentials of all parties are valid and verified
3. Ensure that the transaction remains confidential
4. Ensure that privacy associated with all parties involved is retained
5. The communications paths must be encrypted and the protocols used t must be secured so that transaction details must be stored in a non-public accessible environment and not directly accessible via the internet.
6. Where a trusted authority for the purposes of issuing and maintaining digital signatures and/or digital certificates is used, security must be integrated and embedded throughout the entire end-to-end certificate/signature management process.
7. Ensure that transactions comply with laws, rules, and regulations

Publicly available information

Objective: To protect the integrity of information made available on publicly available ystems

Justification: Information on a publicly available system could be subject to unauthorized modification or deletion if not properly protected. This could damage the company's reputation.

***Corresponding author:** YAU Hon Keung, Department of Systems Engineering and Engineering Management, City University of Hong Kong, Kowloon Tong, Kowloon, Hong Kong, Tel: 852-3442-6158, E-mail: honkyau@cityu.edu.hk

Received December 03, 2013; **Accepted** December 05, 2013; **Published** December 07, 2013

Citation: Hon Keung YAU (2013) How to Set Security Policy for Electronic Commerce Services? Adv Robot Autom 2: e115. doi: 10.4172/2168-9695.1000e115

Guidelines:

1. Exploit able vulnerability should be identified and fixed by having penetration test before publishing information
2. Formal approval process must be made before publishing information
3. All data obtained from outside sources should be verified and approved.
4. Feedback and direct information entering systems should be carefully controlled that it complies with the law, rules, and regulations and is accurate in a timely manner
5. Sensitive information will be properly protected a tall stage
6. Only authorized users can have access to the system

Reference

1. Calder A (2005) Nine Steps to Success: AnISO27001 Implementation Overview. London: IT Governance Publishing.