# Global Information Assurance Certification Paper

# Extranets: The Weakest Link
# &
# Security

**Name: Slawomir Marcinkowski**
**Version number: 1.2e**

## Table of Contents



## Figures



## Tables

## 1. Introduction

Web-enabled technology has made possible interorganizational e-business systems (extranets). Extranets are attractive to many organizations for they can significantly reduce the associated transaction and coordination costs between the organization and its vendors and customers (trading partners). Extranets enable organizations to link their value chains with those of their trading partners. Each succeeding stage in the value chain chains (Porter, 1980; Porter & Millar, 1985) needs to be assured that the information coming from the previous stage and upon which it will act is correct and available when needed. Extranets linking trading partners need to be secure (Phaltankar, 2000; Schwartz, 2000), and need the following security services: access controls, integrity, availability, confidentiality, repudiation, and authentication. The following is a list of tools and technologies for the security enabled enterprise: Public Key Infrastructure (PKI), Digital Signature, Authentication, Authoritization, Firewalls, VPN, Anti-Virus Software, Intrusion Detection, Single-Sign On, Smart Cards, Biometric Devices.

When the value chains of two trading partners are joined via an extranet it becomes vital that the data associated with the transaction not be manipulated in any way (data integrity), using a digital signature ensures information integrity. Moreover, the two trading partners need to be confident that they are communicating with each other and not with some imposter (authentication). Authentication technology (e.g., passwords, smart cards, biometric devices) ensure that the individual is who or she claims to be, but says nothing about the individual's access rights. The trading partner only is able to interact with the extranet according to rules that have been set up (authoritization). Authorization is the set of rules that define what resources someone has access to once they are authenticated. In addition, one trading partner cannot deny that they originated or they failed to receive the information on the extranet (non-repudiation).

This paper does not focus on the technologies for a secure extranet, for technology is only one aspect of the security picture. This paper focuses on the management processes needed to secure an extranet. Management processes need to be in place in the respective extranet organizations to secure the extranet from the overly "curious" trading partner, or from a malicious user who has compromised the trading partner's network as a means to get to the extranet connection and make use of this trusted connection to compromise the organization.

The WWW environment provides organizations new opportunities to take advantage of, and also poses new challenges in the form of risk that need to be addressed if e-business is to succeed. Security ought to be considered an enabler of e-commerce (e.g., extranets) (Armstrong, 2000a; Armstrong, 2000b; Armstrong, 2000c). With the proper management security processes, an organization can take full advantage of what Web-based technologies have to offer, for then security is seen as an enabler and not as an inhibitor to e-commerce. Proper security processes along with risk management processes at organizations reduce the uncertainty and security risk associated with using Web-based technology.

## 2. Extranet: The Weakest Link

The saying "the chain is as strong as its weakest link" is very much applicable to security -- security is as strong as the weakest link. To minimize risk to themselves and to increase the probability of success, attackers will attack their target's weak spot. Attackers will look for the weakest security in an organization's information infrastructure. When the weakest point is

found, the attacker will focus its attack resources. Organizations understand this, and attempt to minimize risk by fortifying their information systems from attack.

When an organization (Company A) implements an extranet with its trading partners (Company Z), the extranet may very well be the weakest link (Schwartz, 2000). Unbeknownst to it, Company A without the proper security measures in place on its extranet may be at risk to industrial espionage. The "trusted" trading partner may be overly "curious", and will begin exploring Company A's network and may potentially discover proprietary information that Company A never intended to share with its trading partner (e.g., pricing models, production schedules, customer list, wholesale prices). Furthermore, in many instances companies are partners on one front, and fierce competitors in another market segment. Preventing unauthorized access is a must. Moreover, Company A needs to guard against the malicious worker be it in its own organization or that of its trading partner. Security needs to be layered.

Organizations implementing an extranet need to use the defense in depth concept. Even if the trading partners network is compromised, and the extranet connection is used to attack the network, defenses are still in place to protect the organization's extranet and internal network. At the minimum Company A needs a firewall connecting its extranet to each of its trading partners. Such protection is prudent from two perspectives, 1) protects against an outside attack; 2) protects against an extranet partner and its employees from being overly curious or performing industrial espionage. On one hand, the two companies may be partnering together, and yet in another arena they may be fierce competitors, and could use the extranet connection to gain competitive information.

Organizations using extranets need to defend themselves against the eggshell model of defense, whereby once an intruder gets access to the extranet connection it has free reign over the network. Defense should be in depth. Unfortunately, as evidenced by alerts from the National Infrastructure Protection Center (NIPC) (NIPC, 2000; NIPC, 2001) e-commerce sites are following more the eggshell security model rather than the defense in depth (Arnold, 2001).

Company Z may not have the same security posture as Company A. A survey conducted by Information Systems Audit and Control Foundation (ISACF) has found that few organizations use third parties to verify the security of their trading partners (ISACF, 2000). Company A has no knowledge of how secure their trading partner's networking infrastructure is. An attacker attempting to compromise Company A will no doubt do his or her due diligence and will determine that Company A has a hardened perimeter and that it has an extranet. The attacker through reconnaissance will undoubtedly discover that one (Company Z), if not more, of the companies that are part of Company A's extranet is not secure. The attacker will focus on Company Z's infrastructure as a means of compromising Company A's network security.

## 3. Uncertainty & Risk Management

Use of information technology is one of balancing benefits and risks. On the one hand, information technology enables an organization to gain competitive and strategic advantage. The use of an extranet by an organization is the balance of risk versus benefit. Extranets are attractive to many organizations for they can significantly reduce the associated transaction and coordination costs between themselves and their vendors and customers. However, the same technology that brings benefits can also put an organization at risk if the proper security mechanisms are not in place. After all, it is much easier to download thousands of pages of

proprietary documents than it is to photocopy and physically remove these same files in paper form from the premises.

The uncertainty and the inherent risk stem in part to the ever increasing pace that new applications are developed and employed. The need to be first in a market segment with a new e-commerce application is paramount. Organizations implementing an extranet may not have given much thought to security, and in many instances security is an afterthought (Morgan, 2001). As reported in a survey of executives conducted by ISACF, for the majority of executives, security never really entered into the decision-making process whether to proceed with an e-commerce initiative or not (ISACF, 2000). Of those executives that did consider security in their decision making process, by a majority of 2 to 1 the view was that security was an enabler and not an inhibitor. By incorporating security early on in the process (Lord, 2001), security allows the organization to deploy e-commerce applications that gain them competitive advantage by conducting business in this new and efficient way, and be confident that the confidentiality, integrity and the availability of the link is assured, as well as the non-repudiation of information. The value of incorporating security from the start should not be underestimated, for when a security incident happens it will setback the e-commerce initiative if not kill it entirely within the organization (Armstrong, 2000b).

Even more worrisome is the rush by software organizations to get the latest software out into the market place, and therefore producing software that is written poorly and has inherent vulnerabilities (e.g., buffer overflows) (Securityfocus, 2001; Shmoo, 2001). It is using this software that extranets are deployed. Once again the security in depth concept needs to be adhered to. Even if security is compromised due to a software flaw, there need to be other security precautions to detect and limit the potential damage.

As (Figure 1) illustrates, along with the latest technology come new vulnerabilities that can be exploited. As countermeasures are developed against these vulnerabilities, there always exist the chance and hence the risk that someone will discover a new vulnerability to exploit in order to compromise a network and the information transported or stored on the network. The more valuable the information asset processed or supported by the information system the more incentive there is develop new exploits to take advantage of the inherent vulnerabilities that exist.

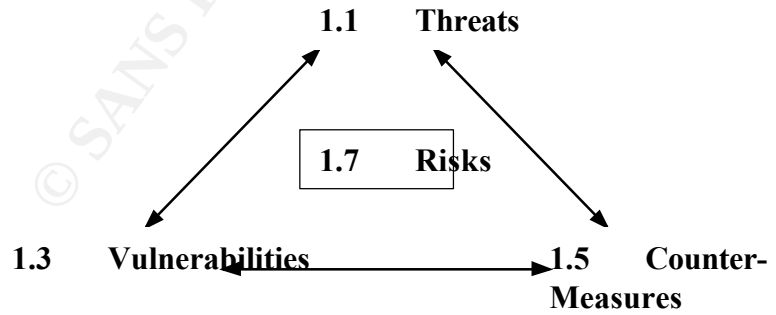


**Figure 1, Risks arise because an attack can exploit a vulnerability. Countermeasures reduce risk by lowering vulnerabilities, but new ones may appear** (Caelli, Longley, & Shain, 1991)

An organization must come to terms on the level of risk it is willing to tolerate. The organization must weigh the cost of economic loss it is willing to bear versus the cost of information security. The more important and critical the asset, the network, or the information is to the organization, the larger the potential economic loss to the organization in the event of a security breach (Figure 2). Examples of economic loss range from the loss of revenue, loss of reputation with customers all the way to lawsuits and/or criminal prosecution stemming from the compromise of information protected by Federal privacy laws.

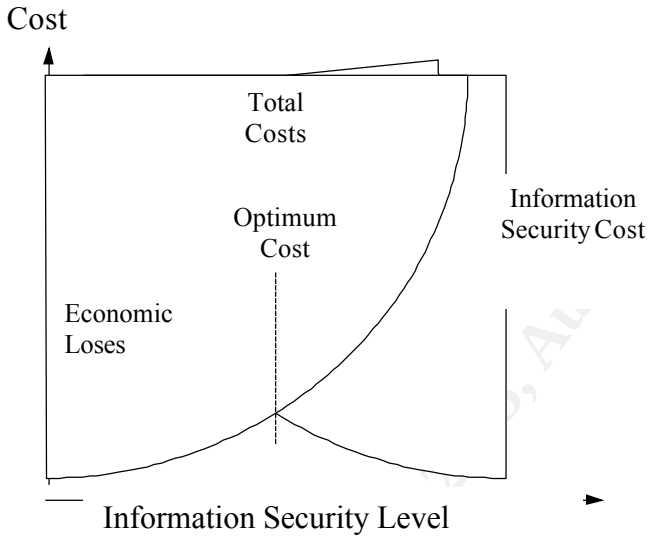


**Figure 2, The level of information security and associated economic costs, and security measure costs**

The level of economic loss decreases as security for the information and the network increase. However, security comes at a cost as illustrated in Figure 2. The higher the security level desired the higher the costs associated with providing that level of security. The level of security needs to be proportional to the information type/value being secured. In other words, the costs associated with providing security should not exceed the economic loss the organization would suffer if security was compromised. In general, any security measure or combination of such measures must cost no more than it would cost to tolerate the problem addressed by the measures (NBS, 1981). This optimum point is illustrated in Figure 2 by the intersection of the Information Security Costs and the Economic Loses lines. Ultimately, the organization must decide what risk it is willing to tolerate. Security is never 100% guaranteed. By going to an extranet, in effect the organization has decided to take on risk. The appropriate cost benefit versus potential economic loss needs to be considered, and thus the appropriate level of security for the type of information to be protected needs to be employed. An organization when deploying an extranet needs to conduct risk management and consider the balance between the cost of security measures and the potential economic loss if the information is not secured .

Because every security control has a cost associated with it, there needs to be a business reason (e.g., protecting proprietary information, safeguarding in formation as required by Federal

Privacy laws) for the control to be in place. The exact optimum point will vary from organization to organization and is dependent on the criticality of the information and the network to the organization's capability to conduct business.

## 4. ISO/IEC 17799 Standard

The ISO/IEC 17799 Standard derives from the British Standard 7799. The ISO Standard is divided into two parts: ISO/IEC 17799:2000 (Part 1) and BS7799-2:1999 (Part 2). ISO/IEC 17799 is a code of practice which list 36 objectives in ten categories (Table 1). There are 127 different controls that can be selected -- each is provided with explanatory information. Using the Standard users can identify the security controls which are appropriate to their business or specific area of responsibility.

Part 2 is a standard specification for an Information Security Management Systems (ISMS) process (Figure 3). ISMS is a process by which senior management in an organization can minimize risk. The organization formulates a security policy based on what information is in need of securing and at what level. What exactly is the scope, after all not everything can be secured or needs to be secured. Only what is most important to the organization needs to be secured. An organization first needs to take an inventory of the information that it considers important. The organization undertakes a risk assessment that identifies the threats, vulnerabilities, and potential impacts to the organization. The organization then decides how it will manage the risks, and then selects the means by which the risks will be mitigated. Finally, the organization justifies why it has chosen the particular security controls and why others have been omitted. This is based on a thorough review of the organization's mission, laws and mandates, the information technology used, and the level of information security needed.

The Standard provides organizations with guidance and a Code of Practice enabling the organization to come up with a secure infrastructure. The focus of the standard is not the how of doing security, but the what -- for it provides a general set of guidelines for security management (Johnston, 2000) (Gautier, 2000). Organizations in Europe are undergoing ISO/IEC 17799 accreditation as a means of showing that their organization is following best practices when it comes to security. This accreditation reassures trading partners connected via an extranet, that the partner is taking security seriously. The accreditation shows that companies are following best practices and thus are reducing the risk that their information infrastructure will be compromised.

The Standard recognizes the ever growing importance organizations to connect with trading partners (e.g., via extranets). Both partners need to protect the information traveling over the network. Both parties find value in using the network through lower coordination and transaction costs, however both parties can only continue deriving benefits if all the parties on the extranet manage their business in a secure manner. Any single partner on the extranet who fails to manage its connection in a secure way (meeting acceptable security best practices) puts everyone at risk -- the weakest link concept. Organizations need to have confidence and trust that their partners are secure. As the expression goes "Trust, but verify." is very applicable to security. Being accredited, allows one's trading partner to be more confident that your organization is following best information security management and technical practices.

| |
|---|
| **1. Business Continuity Planning**<br>The objectives of this section are: To counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters. |
| **2. System Access Control**<br>The objectives of this section are: 1) To control access to information 2) To prevent unauthorised access to information systems 3) To ensure the protection of networked services 4) To prevent unauthorized computer access 5) To detect unauthorised activities. 6) To ensure information security when using mobile computing and tele-networking facilities. |
| **3. System Development and Maintenance**<br>The objectives of this section are: 1) To ensure security is built into operational systems; 2) To prevent loss, modification or misuse of user data in application systems; 3) To protect the confidentiality, authenticity and integrity of information; 4) To ensure IT projects and support activities are conducted in a secure manner; 5) To maintain the security of application system software and data. |
| **4. Physical and Environmental Security**<br>The objectives of this section are: To prevent unauthorised access, damage and interference to business premises and information; to prevent loss, damage or compromise of assets and interruption to business activities; to prevent compromise or theft of information and information processing facilities. |
| **5. Compliance**<br>The objectives of this section are: 1) To avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements 2) To ensure compliance of systems with organizational security policies and standards 3) To maximize the effectiveness of and to minimize interference to/from the system audit process. |
| **6. Personnel Security**<br>The objectives of this section are: To reduce risks of human error, theft,<br>fraud or misuse of facilities; to ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work; to minimise the damage from security incidents and malfunctions and learn from such incidents. |
| **7. Security Organisation**<br>The objectives of this section are: 1) To manage information security within the Company; 2) To maintain the security of organizational information processing facilities and information assets accessed by third parties. 3) To maintain the security of information when the responsibility for information processing has been outsourced to another organization. |
| **8. Computer & Network Management**<br>The objectives of this section are: 1) To ensure the correct and secure operation of information processing facilities; 2) To minimise the risk of systems failures; 3) To protect the integrity of software and information; 4) To maintain the integrity and availability of information processing and communication; 5) To ensure the safeguarding of information in networks and the protection of the supporting infrastructure; 6) To prevent damage to assets and interruptions to business activities; 7) To prevent loss, modification or misuse of information exchanged between organizations |
| **9. Asset Classification and Control**<br>The objectives of this section are: To maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection. |
| **10. Security Policy**<br>The objectives of this section are: To provide management direction and support for information security. |

**Table 1, The ISO/IEC 17799 Standard (Source: http://www.securityauditor.net/iso17799/what.htm)**

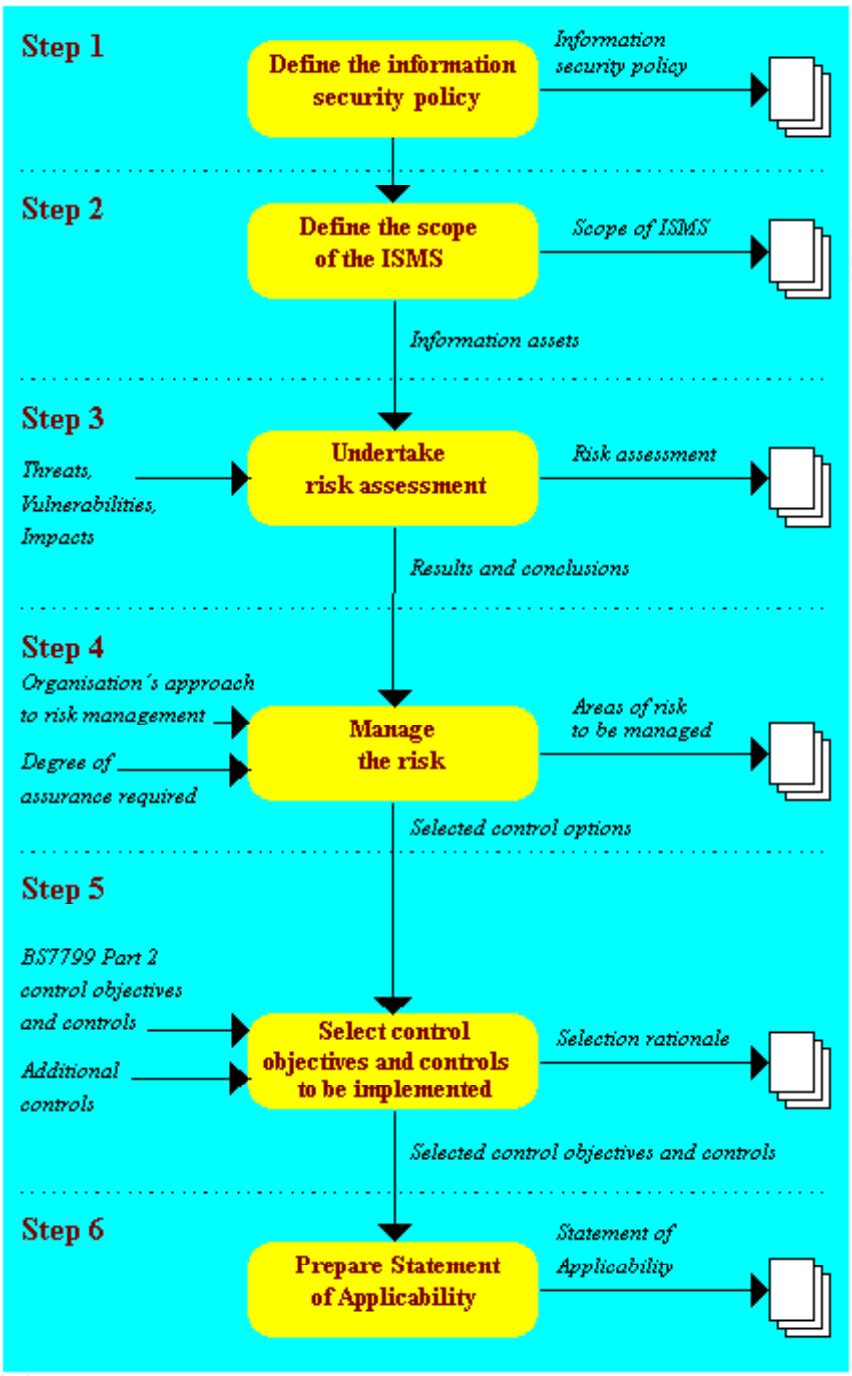


**Figure 3, ISO/IEC 17799 Information Security Management Systems Process (Source: http://www.gammassl.co.uk/bs7799/works.html**

## 5. Security Policy

The success of the information security function is dependent in part on how successful it is in controlling who has access to what information, and who can install what hardware and software on the network. For example, in many computer break-in instances, organizations have

failed to secure their information systems and networks from known vulnerabilities and exploits. Computers have been connected to networks straight out of the box without being configured properly. Proper configuration entails installing software patches for known software or operating system vulnerabilities, and turning off services and ports that are on by default. Such basic steps can go a long way in protecting an organization's information assets, only if they are applied consistently across the organization. Unfortunately, even these basic security steps are not followed as evidenced by break-ins into electronic commerce Web sites. The lack of even basic configuration management exposes the organization to virus attacks and attacks using tools and exploits available on many hacker and underground Web sites.

The larger the organization, the more difficult it is to control behavior. Organizations introduce controls to reduce the behavior variability with the ultimate aim to control the behavior. Behavior can be formalized through policy defining appropriate behavior. The existence, implementation, and enforcement of an information security policy and procedures play a critical role in mitigating security risks associated with information. Information security policies "typically include general statements of goals, objectives, beliefs, ethics, controls, and worker responsibilities" (Wood, 1997, p.3). Policy defines the roles and responsibilities of employees making them accountable for their actions. Security policy also defines what needs to be protected and at what level. Only with policy in place can an organization say that its information infrastructure is secure. Because, only then does the organization have a security baseline. This is based on a thorough review of the organization's mission, laws and mandates, the information technology used and the level of information security needed (Figure 4).

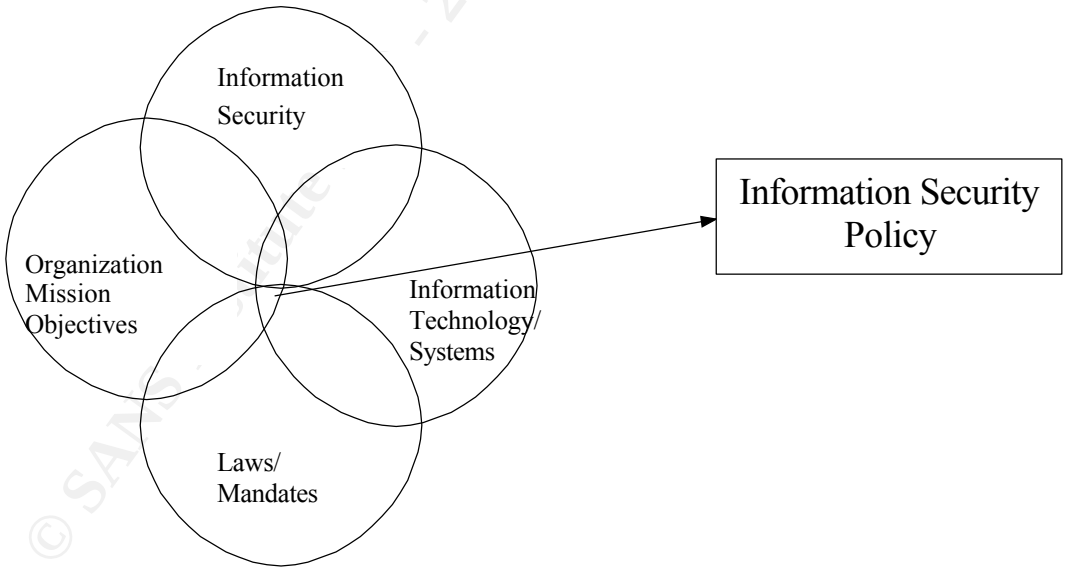


**Figure 4, Security Posture Reflective of Organizational Objectives, Business Processes, Information Technology, and Laws and Mandates Governing the Information**

## 2. Conclusion

When an organization has an Internet connection, the organization exposes itself to all who are connected to the Internet. Metaphorically speaking, an organization having an

Internet/WWW connection on any of its networks has placed a "door" on that network through which anyone in the world having an Internet connection and the know-how can enter. The tools of the trade to break into networks are available on the many hacker and underground sites on the WWW. These software tools enable the user to scan a network, identify known weaknesses, and then apply known methods to exploit known vulnerabilities. Many of these tools have a graphic user interface (GUI) along with instruction manuals, making these tools easy to use by anyone. The increased attempts in break-ins and actually break-ins is a function of the availability of easy-to-use hacking tools on the Internet (PricewaterhouseCoopers, 2001); an organization may be targeted based on its vulnerabilities discovered through the use of a network scanning tool (e.g., Nessus) and the availability of an exploit on the Intenet that can take advantage of the vulnerability(s). Organizations with extranets need to be extra careful. The security posture of its trading partner may be the organizations weakest link.

Organizations electronically connected with trading partners, need reassurance that their extranet connection to their trading partner will not compromise their security. The development of a standard such as ISO/IEC 17799 is one step in helping organizations come to terms with security management processes. Security needs to be viewed as an enabler and not an inhibitor to business-to-business (B2B) e-commerce. Trading partners need to feel confident that the others' security meets a certain standard -- the extranet is secure.

## 3. References


Armstrong, I. (2000a). Flimsy Security Betrays B2B Upsurge. *SC Magazine, 11*(10), 36-40.

Armstrong, I. (2000b). Security Fights for Internet Foothold. *SC Magazine, 11*(10), 23-30.

Armstrong, I. (2000c). Web Commerce Trading Securely. *SC Magazine, 11*(10), 32-34.

Arnold, T. (2001). *A Method for Securing Credit Card and Private Consumer Data in E-Business Sites* : CyberSource Corporation.
URL: http://www.siia.net/sharedcontent/divisions/ebus/citadel.pdf

Caelli, W., Longley, D., & Shain, M. (1991). *Information Security Handbook*. New York, New York: Stockton Press.

Gautier, R. A. (2000, July). Big Bucks for BS 7799. *Information Security*.
URL: http://www.infosecuritymag.com/articles/july00/departments2_viewpoint.shtml

ISACF. (2000). *e-Commerce Security Status Report* . Rolling Meadows, IL: Information Systems Audit and Control Foundation.
URL: http://www.isaca.org/ecomm.htm

Johnston, R. E. (2000, June). 86ING BS 7799. *Information Security*.
URL: http://www.infosecuritymag.com/articles/june00/columns4_logoff.shtml

Lord, G. (2001, July). Managing the Full Portfolio of Risks is Key to E-Business Success. *SC Security Magazine*.
URL: http://www.scmagazine.com/scmagazine/sc-online/2001/article/025/article.html

Morgan, L. (2001, April 9). Security Haste Makes Waste. *InternetWeek*.
URL: http://www.internetweek.com/indepth01/indepth040901.htm

NBS. (1981). *Guidelines for ADP Risk Analysis* (FIPS Publication 87). Washington, D.C.: National Bureau of Standards U.S. Department of Commerce.

NIPC. (2000). *E-Commerce Vulnerabilities* . Washington DC: National Infrastructure Protection Center.
URL: http://www.nipc.gov/warnings/advisories/2000/00-060.htm

NIPC. (2001). *Advisory 01-003 Update to NIPC Advisory 00-060 "E-Commerce Vulnerabilities"* (Advisory 01-003). Washington DC: National Infrastructure Protection Center.
URL: http://www.nipc.gov/warnings/advisories/2001/01-003.htm

Phaltankar, K. M. (2000). *Practical Guide for Implementing Secure Intranets and Extranets*. Norwood, MA: Artech House Inc.

Porter, M. E. (1980). *Competitive Strategy*. New York: The Free Press.

Porter, M. E., & Millar, V. E. (1985). How Information Gives You Competitive Advantage. *Harvard Business Review*(July-August), 149-160.

PricewaterhouseCoopers. (2001). *European Economic Crime Survey 2001* : PricewaterhouseCoopers.
URL:
http://www.pwcglobal.com/Extweb/service.nsf/docid/3BF554C29B80063D80256A72005ACB9F

Schwartz, M. (2000, October 2). Good Fences, Good Neighbors. *Computerworld*.
URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO51553,00.html

Securityfocus. (2001). Secure Programming.
URL: http://www.securityfocus.com/frames/?content=/forums/secprog/secure-programming.html

Shmoo. (2001). How to Write Secure Code.
URL: http://www.shmoo.com/securecode/

Wood, C. C. (1997). *Information Security Policies Made Easy*. Sausalito, CA: Baseline Software

Inc.