Journal of International Information Management

Volume 12 | Issue 2

Article 9

2003

All Integrated Model for Improving Security Management in the E-Commerce Environment

Hossein Bidgoli

California State University, Bakersfield

An Integrated Model for Improving Security Management in the E-Commerce Environment

Hossein Bidgoli
California State University, Bakersfield

ABSTRACT

Security issues and threats in the e-commerce environment are varied and can be caused intentionally and unintentionally by insiders and outsiders. Many experts believe that insiders create the majority of the security threats and issues. Security issues and threats related to e-commerce environment can be categorized as controllable, partially controllable and uncontrollable. This article presents an integrated model that identifies various security issues and threats in the e-commerce environment and then offers a comprehensive e-commerce security plan. The integrated model includes six steps: identification of basic e-commerce security safeguards, identification of e-commerce general security threats, identification of intentional e-commerce threats, identification of e-commerce security measures and enforcements, identification of computer emergency response team services and formation of a comprehensive e-commerce security plan. The integrated model, if carefully followed, should significantly improve the chances of success in keeping the e-commerce hackers and crackers at bay (Bidgoli, 2002).

INTRODUCTION

Security issues and threats in the e-commerce environment are varied and can be caused intentionally and unintentionally by insiders and outsiders. Security issues and threats related to e-commerce environment can be categorized as controllable, partially controllable and uncontrollable. This article presents an integrated model that identifies various security issues and threats in the e-commerce environment and then offers a comprehensive e-commerce security plan.

STEP 1: IDENTIFICATION OF BASIC E-COMMERCE SECURITY SAFEGUARDS

Computer hackers and criminals are making national and international news. It's no wonder that executives in private and public organizations are taking computer and e-commerce security very seriously. A comprehensive e-commerce security system protects customers, buildings, terminals, printers, CPUs, cables, and other hardware and software in an organization. Moreover, an e-commerce security plan protects data resources, the second most important resource (after human resources) in an organization. The data resources can be an e-mail message from a division supervisor to the CEO, an invoice being transferred using EDI, the blueprint for a new product design, the outline of a new advertising strategy, the credit card number of a customer or financial statements. Security threats exceed merely stealing data; they include everything from sharing passwords with a co-worker, leaving the system unattended while logged onto the network, to spilling coffee on a keyboard. A comprehensive e-commerce security system includes hardware, software, procedures, customers, and personnel that collectively protect the e-commerce resources and keep intruders and hackers at bay. E-commerce security is broken down into three important aspects: secrecy, accuracy, and availability (Sanders, 1996). Let's briefly explain each aspect.

A secret system must not allow information to be disclosed to anyone who is not authorized to access it. In highly secure government agencies (Department of Defense, the CIA, and the IRS) secrecy ensures that only the users who are supposed to have access are granted that access. In business organizations, confidentiality ensures the protection of private information (payroll, personnel, and corporate data). In the e-commerce world, confidentiality ensures that customers' data is protected and will be used only for the intended purpose.

Accuracy ensures the integrity of data resources within the organization. This means that the security system must not allow the data to be corrupted or allow any unauthorized changes to the corporate database. Database administrators and webmasters must establish comprehensive security systems for corporate databases. Authorized users must be identified and they must be given proper access privileges. Just imagine that the addition or elimination of a zero would be the difference between $100,000 and $10,000. In e-commerce transactions accuracy and secrecy are important aspects of a security system and they are the prerequisite for any data quality implementation throughout the system.

Availability ensures the efficient and effective operation of an e-commerce site and a computer system. In the e-commerce environment availability ensures that the virtual storefront is always available and accessible. A secure e-commerce system must make information available to authorized users. It should also ensure quick recovery of the system to its normal operation in case of a disaster. In many cases, availability is the baseline security need for all authorized users. If the system is not accessible to its authorized users, the secrecy and accuracy objectives of the system cannot be properly assessed.

A comprehensive security system in the e-commerce environment must provide three levels of security:

- Front-end servers must be protected against unauthorized access. (Level 1)
- Back-end systems must be protected to ensure privacy, confidentiality, accuracy and integrity of data. (Level 2)
- The corporate network must be protected against intrusion and unauthorized accesses. (Level 3)

The goal in designing a comprehensive e-commerce security system is first to design a fault tolerance system and then take all the possible measures for protecting the e-commerce data resources (Garfield, 1997). A fault tolerance system is a combination of hardware and software techniques that improves the reliability of an e-commerce site. There are several techniques and tools that can improve the fault tolerance of an e-commerce site. The following are among the popular techniques:

- Uninterruptible power supply (UPS)
- Redundant arrays of independent disks (RAID)
- Mirror disks

STEP 2: IDENTIFICATION OF E-COMMERCE GENERAL SECURITY THREATS

E-commerce security is concerned with the unauthorized access to important data resources. Some e-commerce threats are controllable, some are partially controllable, and some are completely uncontrollable. Some are intentional while others are made unintentionally (Bidgoli, 2002 and Marion, 1995). Table 1 summarizes several potential e-commerce disasters.

Natural Disasters	Other Disasters
Cold weather	Blackouts
Earthquakes	Fires
Floods	Gas leaks
Hot weather	Neighborhood hazards
Hurricanes	Nuclear attacks
Ice storms	Oil leaks
Ocean waves	Power failure
Severe dust	Power fluctuations
Snow	Radioactive fallout
Tornadoes	Structural failure

Table 1: Potential E-commerce Disasters

Insiders or outsiders intentionally create certain security threats such as the spreading of a computer virus by a hacker or a disgruntled Webmaster. Certain security threats are unintentional, such as, the eraser of a computer file or formatting a data disk unintentionally by an employee. Some security threats such as earthquakes are natural and are not controllable (or are partially controllable). A comprehensive e-commerce security system should allow only authorized employees to have access to e-commerce facilities. Table 2 summarizes the threats posed by insiders and outsiders.

	Sources of Threats					
Type of Threat	I/O Operator	Supervisor	Programmer/ Webmaster	Systems Engineer/ Technician	User	Competitor
Changing codes	x		x			
Copying files	x		x			
Destroying files	x	x	x		x	x
Embezzlement			x	x		x
Espionage	x	x	x			x
Installing bugs			x	x		x
Sabotage	x		x	x		x
Selling data	x	x	x		x	
Theft		x	x		x	x
Overwhelming the e-commerce site					x	x

Table 2: Internal and External E-commerce Threats and Vulnerability

The damage from natural disasters is somewhat controllable. Buildings with special designs for earthquake protection are now available, and flood damage usually can be controlled. Frequently, computer rooms are designed separately from the rest of a structure to minimize potential hazards. Wiring, air conditioning, and fire protection should be of special concern. Locks and physical deterrents should prevent most computer thefts.

STEP 3: IDENTIFICATION OF INTENTIONAL E-COMMERCE THREATS

Intentional computer and e-commerce threats usually fall into one of the following categories:

- Computer viruses
- Computer worms
- Trojan horse programs
- Logic bombs
- Trap doors
- Denial of access attacks

The most highly publicized computer and e-commerce threat is the computer virus. A computer virus is a program or a series of self-propagating program codes triggered by a specified time or event within the computer system. When the program or the operating system containing the virus is used again, the virus attaches itself to other files and the cycle continues. The seriousness of computer viruses varies, ranging from springing a joke on a user to completely erasing or corrupting computer programs and data (Miastkowski, 1998).

In February 2000, computer hackers temporarily shut down several well-known sites, such as Yahoo!, ZD.net, and Ameritrade by being bombarded with bogus traffic. Later the same year the "I Love You" virus infected millions of e-mail users throughout the world. Viruses have brought to the forefront the necessity of protecting computers from hackers, crackers, extremists, and computer criminals. Billions of dollars are stolen every year by computer criminals. Many organizations are reluctant to report their losses because they do not want to be recognized as vulnerable. With the popularity of e-commerce, this problem will only become worse. Table 3 lists some indications that a computer may have been infected by a computer virus.

Certain programs are bigger than normal
Data disintegrates
Data or programs are damaged
Hard disk space diminishes significantly
Keyboard locks
Memory becomes constrained
Screen freezes (no cursor movement)
Sluggish disk access
Unexpected disk activity
Unusual messages appear on the screen
The computer takes too much time to boot

Table 3: Some Indications that a Computer may have been Infected by a Computer Virus

A computer <u>worm</u> is similar to a computer virus. It is called a worm because it travels similar to a worm from one computer in a network to another computer or site. A worm usually does not erase the data. It either corrupts the data or it copies itself to a full-blown version that eats up computing resources. A worm is distinguished from a virus by copying itself without being attached to a program file, or which spreads over computer networks, particularly via email (Slade, 2004). An example of a computer worm is the one that was unleashed by Robert Morris in November 2,1988, bringing more than 6,000 computers to a halt.

A <u>Trojan horse</u> program contains codes intended to disrupt a computer system and/or an e-commerce site. Trojan horse programs are usually hidden inside a popular useful program. A Trojan horse sometimes pretends to do one thing while performing another, unwanted action (Slade, 2004). Historically, disgruntled programmers who are trying to get even with an organization have created Trojan horse programs. These programs may erase accounting, personnel, and financial data. Unlike computer viruses and worms, a Trojan horse program does not replicate itself. Although a Trojan horse program functions differently than viruses and worms, the end results are basically the same, damage and interruption of the computer and/or network system.

A logic bomb is a type of Trojan horse that is used to release a virus, a worm, or some other destructive codes. Logic bombs are triggered at a certain point in time or by an event or an action performed by a user. An action can be pressing certain keystrokes or running a specific program. An event may be loading a backup tape or the birthday of a famous person.

A trap door, (also called a back door), is a routine that is built into a system by its designer or programmer. This routine allows the designer or the programmer to sneak back into the system to access software or specific programs. A trap door is usually activated by the individual (or his/her agent) who designed the system. Usually the user is not aware of the problem; a keystroke combination or a specific login may set it off.

A denial of service attack is a method hackers and crackers use to prevent or deny legitimate user's access to a computer or Web server. These computer criminals use tools that send many requests to a targeted Internet server (usually Web, FTP or Mail server), which floods the server's resources, making the system inoperable. Any system connected to the Internet running TCP services are subject to attack (Schultz, 2004).

In February 2000, hackers launched denial-of-service attacks against a number of Internet sites, including eBay, Yahoo!, Amazon.com, CNN.com, and E-Trade. Other sites affected included technology news site ZDNet, and Buy.com. According to The Yankee Group the sites experienced slowdowns in service that ranged from two hours and 45 minutes to five hours. The assaults are all of a type known as "distributed denial of service" attacks, in which a web site is bombarded with thousands of requests for information in a very short period of time, causing it to grind to a halt. The attacks usually come from several computers on the Web and this makes it very difficult to trace the attacks. A hacker secretly plants denial of attack tools on several computers on the Web. These computers can be centrally controlled. The methods of how and what resources are flooded differ based on the tools used by the hackers. It is nearly impossible to trace the attack particularly if the attacks come from several sites. Computers that unknowingly have denial of service attack tools installed are called Zombie agents or Drones. Several companies including Symantec offer tools that can reduce the risk of being attacked.

The Yankee Group estimated that these attacks cost the industry approximately $1.2 billion (in 2000) by estimating revenue losses at the affected web sites, losses in market capitalization, and the amount that will be spent upgrading security infrastructures as a result of the attacks, according to the research firm (Niccolai, 2000).