2000

WebTrust program : security principle and criteria, Version 3.0, October 16, 2000; Exposure draft (American Institute of Certified Public Accountants), 2000, October 16

American Institute of Certified Public Accountants (AICPA)

Canadian Institute of Chartered Accountants

The CPA. Never Underestimate The Value.℠

Chartered Accountants of Canada

Comptables agréés du Canada

Exposure Draft

AICPA/CICA

WebTrust SM/TM Program

Security Principle and Criteria

October 16, 2000

Version 3.0

Comments on this exposure draft should be sent to Sheryl Martin, WebTrust Team Leader, Assurance Services, AICPA, 1211 Avenue of the Americas, New York, NY 10036-8775 or Bryan Walker, Canadian Institute of Chartered Accountants, 277 Wellington Street West, Toronto, Canada M5V 3H2 in time to be received by December 15, 2000. Responses also may be sent by electronic mail via the Internet to smartin@aicpa.org or bryan.walker@cica.ca

The Principles and Criteria contained in this program supersede Version 2.0 of the WebTrust Principles and Criteria insofar as they relate to security and are effective for examination periods beginning after February 28, 2001. Earlier adoption is encouraged.

COMMITTEE AND TASK FORCE MEMBERS

AICPA
Assurance Services Executive Committee

Susan C. Rucker, Chair

Gari Fails

Ted Horne

Everett C. Johnson, Jr.

John Lainhart

George Lewis

Edward F. Rockman

J. W. Mike Starr

Wendy E. Visconty

Darwin Voltin

Neal West

Staff Contact:

Alan Anderson,
Senior Vice President, Technical Services

Anthony J. Pugliese,
Director of Assurance Services

AICPA / CICA Electronic Commerce
Assurance Services Task Force

Everett C. Johnson, Jr., Chair

Bruce R. Barrick

Jerry R. DeVault

Joseph G. Griffin

Christopher J. Leach , Vice Chair

Patrick J. Moriarty

William Powers

CICA
Assurance Services Development Board

John W. Beech, Chair

Douglas C. Isaac

Marilyn Kuntz

Doug McPhie

Steven E. Salterio

David W. Stephen

Doug Timmins

Keith S. Vance

Staff Contacts:

Cairine M. Wilson,
Vice President, Innovation

Gregory P. Shields,
Director
Assurance Services Development

Kerry L. Shackelford

Donald E. Sheehy

Christian R. Stormer

Alfred F. Van Ranst

Staff Contacts:

Bryan Walker, CICA
Principal, Assurance Services Development
Sheryl Martin, AICPA
WebTrust Team Leader

CONTENTS

WEBTRUST SECURITY PRINCIPLE AND CRITERIA

Introduction

In the course of communicating and transacting business over the Internet, consumers and business must send and receive information about the other party. In most instances, parties who are interested in engaging in electronic commerce (e-commerce) will be anxious to ensure that the information they provide is only available to those individuals who need access in order to complete the transaction or follow-up on any questions which arise.

Information which is provided to another party is susceptible to unauthorized access during transmission over the Internet and while it is stored on the other party's computer systems. For example, personal information, credit card numbers, etc., may be intercepted by an unauthorized party while it is being transmitted over the Internet. However, if the information is encrypted, it will be very difficult for the unauthorized party to decipher it. Also, if the computer system where the data is stored is not protected by a firewall and a rigorous systems of passwords, the information may be accessed by unauthorized personnel.

The WebTrust Security Principle sets out an overall objective in respect to the security of data transmitted over the Internet and stored on an e-commerce system. In the course of a WebTrust audit, the practitioner will use the WebTrust Criteria as the basis for assessing whether the Principle has been achieved.

The WebTrust Security Principle

> *The entity discloses key security policies, complies with such security policies, and maintains effective controls to provide reasonable assurance that access to the electronic commerce system and data is restricted only to authorized individuals in conformity with its disclosed security policies.*

The WebTrust Criteria[1]

The WebTrust Criteria are organized into four broad areas – disclosures; policies, controls and objectives; procedures and technology tools; and monitoring/performance measures.

A four-column presentation has been used to present and discuss the criteria. The first column presents the criteria—the attributes that the entity must meet to be able to demonstrate that they have achieved the principle. The second, third and fourth columns provide illustrative disclosures and controls for business to consumer transactions, business to business transactions, and for transactions applicable to service providers. These are examples of disclosures the entity might make and controls that the entity might have in place to conform to the criteria. Alternative and additional disclosures and controls also can be used.

[1] These criteria meet the definition of "criteria established by a recognized body" described in the third General Standard for attestation engagements in the United States (AICPA, *Professional Standards,* vol. 1, AT sec. 100.14) and in the standards for assurance engagements in Canada (CICA *Handbook,* paragraph 5025.41).

WebTrust Principle and Criteria
Security

Principle

The entity discloses key security policies, complies with such security policies, and maintains effective controls to provide reasonable assurance that access to the electronic commerce system and data is restricted only to authorized individuals in conformity with its disclosed security policies.

Criteria	Illustrative Disclosures for Business to Consumer E-commerce	Illustrative Disclosures for Business to Business E-commerce	Illustrative Disclosures for Service Providers
A Disclosures			
A.1 The entity discloses its security practices for providing access to its e-commerce system and data. Such disclosures should include practices for: • Registration and authorization of new users • Identification and authentication of authorized users • Maintaining and terminating authorized user access.	You can register on line clicking on "Open a new account" and by providing your name, mailing address, telephone number and e-mail address. This information is encrypted utilizing SSL before being transmitted to us. We will e-mail you a user identification (ID) and password within twenty-four hours, which you can use to log in. You will be asked to change your password the first time you log in and every three months thereafter. You should choose a strong password that is difficult for others to guess and keep your password confidential. Your user ID and password will be deactivated if it is not used for six months.	This site requires the use of a digital certificate from the user to provide authentication, identification and encryption. Your digital certificate can be obtained from management by applying at www.mycertificate.com/ or you may email us at info@mycertificate.com. Your digital certificate will be valid for one year unless revoked sooner. We also require cookies to be set at the site to ease the use of this site and customize the Internet session. We place the following information in the cookie: identification number, product line and date. For more information go to www.mycertificate.com/cookie.html.	To obtain access to this system, a customer needs to complete an application and mail, e-mail or fax it to us. Upon approval of your credit, you will be provided with a user-ID and a Secure ID Token to allow access to the system. You can update the information on your application at any time, either by mail or on-line For additional information contact us at info@mysite.com.
A.2 The entity discloses its procedure for individuals, companies or other entities to inform the entity about breaches or possible breaches to the entity's security of its e-commerce system(s).	Should you feel that there has been a breach to the security of this site please contact us IMMEDIATELY at 1-800-123-1234.		

Criteria	Illustrative Disclosures for Business to Consumer E-commerce	Illustrative Disclosures for Business to Business E-commerce	Illustrative Disclosures for Service Providers
A.3 The entity discloses its procedures for consumer recourse for issues regarding security. This resolution process should have the following attributes: • Management's commitment to use a specified third party dispute resolution service or other process mandated by regulatory bodies, in the event the customer is not satisfied with the entity's proposed resolution of such a complaint together with a commitment from such third party to handle such unresolved complaints. • Procedures to be followed in resolving such complaints, first with the entity and, if necessary, with the designated third party.	Transactions at this site are covered by arbitration and arbitrated by the National Arbitration Forum. They can be reached at www.arb-forum.org or by calling toll free 800-474-2371. For the details of the terms and conditions of arbitration, "click here".	Transactions at this site are covered by arbitration conducted through our designated arbitrator (name of arbitrator). They can be reached at www.name.org or by calling toll free 800-111-2222. For the details of the terms and conditions of arbitration, "click here". Transactions at this site are covered by the Banking (Canadian Banking) Industry Ombudsman of the Bankers Association who can be reached at www.bankom.org.xy or by calling toll free 800-xxx-xxx.	Transactions at this site are covered by arbitration and arbitrated by the National Arbitration Forum. They can be reached at www.arb-forum.org or by calling toll free 800-474-2371. For the details of the terms and conditions of arbitration, "click here".
A.4 The entity discloses the extent to which its security disclosures and controls apply to common application services provided to business customers (for example, application service providers (ASPs)).	N/A	We provide on our Web site facilities for web hosting and the use, by business customers, of the XYZ ERP software. The ERP software has a common configuration for application functionality and customized security configurations to meet the needs of each business customer. Our disclosures on this Web site and the related security controls include the common application functionality of the XYZ ERP software, but exclude the security features and controls that are customized for each business customer.	

Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Business to Business E-commerce	Illustrative Controls for Service Providers
B Policies, Goals, and Objectives			
B.1 The entity's security policy covers the e-commerce	The Computer Security Policy (CSP) is	Our company's defined security policy	The company's security policy details access

Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Business to Business E-commerce	Illustrative Controls for Service Providers
system and data address but are not limited to the following items: • Who is allowed access, what is the nature of that access and who authorizes such access? • What is the procedure to add new users, modify the access levels of existing users and remove users who no longer need access? • Who is accountable for security, system upgrades, backups, and maintenance? • What type of scripts or programming is permitted on served pages? • What testing and evaluation must be performed on software, pages and scripts before they are installed? • How physical access to the system(s) is controlled. • How are complaints and requests about server and page content to be addressed? • What is the procedure to handle security incidents?	fundamental to the existence and integrity of computer security of any organization. This document encompasses all aspects of Security including such areas as: • Identifying threats and assets • Acceptable usage guidelines for users • Risk analysis • Identifying of authority figures • Procedures for day-to-day and other incidental security operations. Qualified users can obtain the complete document for review.	details access privileges, information collection needs, accountability, and other such matters. It is reviewed and/or updated at quarterly management meetings and under goes an intense review on an annual basis by the Information Technology (IT) department. Documented system security objectives, policies, and standards are consistent with system security requirements defined in contractual, legal, and other service level agreements. For example, current policy prohibits shared IDs; each support person has his or her own unique ID to log on and maintain network equipment. A complete policy with details regarding access, scripting, updates, and remote access are available for review by qualified personnel. This document will not be released to the general public for study.	privileges, hardware and software modification procedures (including updates), web access and web posting. In addition, strict procedures are in place to control logical as well as physical access to the system. Documented system security objectives, policies, and standards are consistent with system security requirements defined in contractual, legal, and other service level agreements. Current policies prohibit shared IDs. Each support person has his or her own unique ID to log on and maintain network equipment. A complete policy with details regarding access, scripting, updates, and remote access are available for review by qualified personnel. This document will not be released to the general public for study.
B.2 The employees are aware of and follow the entity's published security policy.	As part of their orientation, the security policy is reviewed with new employees and the key elements of the policy and its impact on the employee are discussed. The employee must then sign a statement signifying that they have read, understand and will follow the policy. Each year, as part of their performance review, employees must reconfirm their understanding of and compliance with the policy.		

	Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Business to Business E-commerce	Illustrative Controls for Service Providers
B.3	Accountability for the security policy has been assigned.	Management has assigned responsibilities for the enforcement of the company security policy to the Chief Information Officer (CIO). Others on the executive committee assist in the review and update of the policy as outlined in the executive committee handbook.		
B.4	The entity has allocated training and other resources to support the security policy.	The company has budgeted for security training for the IT department. This amount is reviewed quarterly to ascertain whether additional training is needed based on employee feed back as well as changes in security.	The company has a quarterly scheduled training for all key information technology employees. The IT department is also charged with holding quarterly security updates for all company employees as it relates to the employee's job function. The CIO oversees this responsibility and reports back to the executive committee on a regular basis.	Management has an on-going security-training program for all employees. IT staff is required to submit an annual training request based on job description. All employees are given periodic security training courses put on by the IT Department. The CIO evaluates these programs and makes a quarterly report to the executive committee.
B.5	The entity secures its programs and data during the backup, off-site storage, and restoration processes.	During the daily backup routine, the data is secured from both physical and logical access by unauthorized personnel. During any restoration process, no access is allowed by unauthorized personnel.		
B.6	Documented security objectives and policies are consistent with disclosed security requirements and applicable laws and regulations.	Management reviews it's disclosed security policies maintained at the Web site on a quarterly basis and evaluates its compliance to these policies. The executive committee makes any changes or needed modifications to the policy or disclosure within five business days.	Management reviews it's disclosed security policies maintained at the Web site on a quarterly basis and evaluates its compliance to these policies. The executive committee makes any changes or needed modifications to the policy or disclosure within five business days. Laws and regulations that affect the disclosed site security policy are evaluated and reported on by the corporate attorney at least annually or when new regulations require an update.	

C Procedures and Technology Tools

C.1 Systems Access

	Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Business to Business E-commerce	Illustrative Controls for Service Providers
C1.1	The entity has appropriate security procedures to establish new users.	New users are given a secure session in which to provide new user information and select an appropriate user ID and password.	New users are given a secure session in which to provide new user information and select an appropriate user ID and password. Passwords must contain at least six characters, one of which is non-alphanumeric.	New users provide information in a secure (SSL) session. User IDs and passwords are provided to the user and contain non-alphanumeric characters.
C.1.2	The entity has procedures to identify and authenticate authorized users.	All users are required to provide a unique user ID and password to place an order or access their specific customer information.	To enter the site all customers are required to provide a unique user ID and password. These passwords are case sensitive and need to be updated every 90 days. Users are required to use the digital ID provided by the company to access, place or update orders. File and directory level user and group permissions are used to further restrict access based on information contained within the digital certificate.	System level access to all production systems (UNIX and Windows NT) is provided via a strong identification and authentication mechanism (digital ID, one-time password, SecureID or other system). Strong, static passwords are used for systems that do not require a strong identification and authentication mechanism. Controlled access by a software authentication product with a strong identification and authentication mechanism is required for access to any routers.
C.1.3	The entity has procedures to allow users to change, update or delete their own user profile.	In order to update, change or delete user information, the user's current ID and password are required. After providing this information in a secure session, the user can proceed to the user profile section for any changes.	The user can only process changes to a user profile after a processing code is obtained from the entity. This code is obtained after verification with the user's company as to the need for the update or change.	All changes to user profiles are done after providing user ID and password. The only changes allowed are updates to the user ID and password. Changes to personal information or deletions must be processed in writing.

	Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Business to Business E-commerce	Illustrative Controls for Service Providers
C.1.4	The entity has procedures to safeguard master or "super user" passwords and limit access to such passwords to an appropriate number of authorized personnel.	Master or super user passwords are known by the members of the Information Security group. For emergency situations, these and other key passwords are written down, placed in a marked envelope and stored in the company safe that is accessible only by the Chief Information Officer (CIO), Chief Financial Officer (CFO), and Chief Executive Officer (CEO).	System passwords and other key passwords are encrypted and stored in the company safe under dual control. Strict policy requires that these passwords can only be accessible by the by at least two of the following: CIO, CFO and CEO.	
C.1.5	The entity has procedures to minimize access to idle workstations by unauthorized personnel.	Customers visiting the site will be automatically redirected to unsecured (non-SSL) pages after a specified period of inactivity. A logout utility runs continuously on the system. It scans the network for idle workstations and logs them off after 10 minutes of inactivity. Company employee workstations will automatically log off the network after a specified period of inactivity.		
C.1.6	The entity has procedures to limit remote access to the internal network to only authorized personnel.	Remote access is provided to key employees - the system accepts remote calls, verifies the user and then hangs up and calls the user back at the authorized number. Logical access (for example, firewalls, routers, and password controls) is maintained by the IT department. These controls are tested on a periodic basis by performing penetration testing from both within the internal network and from the Internet. Identification and authentication is accomplished through the combination of a user ID and one time password. Remote access to and use of the computing resources are restricted to authenticated users.		

Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Business to Business E-commerce	Illustrative Controls for Service Providers
			The remote access to and use of the computing resources are restricted by the implementation of an authentication mechanism of identified users and resources associated with access rules. User IDs and passwords are stored in an encrypted database with the associated encryption key stored off line.
C.1.7 The entity has procedures to prevent customers, groups of individuals, or other entities from accessing other than their own private or sensitive information.	Customers are required to enter a user ID and password to access personal information and orders. A challenge word or phrase (for example, favorite sport or music – not a word that is easily identifiable such as mother's maiden name) is stored on the system in the event a user forgets or misplaces a password. The authentication process allows the user to access only information relevant to that particular user. Other methods are in place to detect users attempting to guess another password or if a brute force attack is under way. If such an attack is detected, the system will disconnect from the user and report the security breach for follow-up.	All access to customer accounts is restricted to the customer through the use of a unique digital certificate associated with each customer. Customer sessions between the browser and e-commerce systems are protected to avoid other users from hijacking a customer's session (for example, use of unique digital certificates or cookies checking for random unique identifiers before the start of each session).	One-time passwords and/or smart cards restrict all system access from outside the entity, other than for customary e-commerce transactions through the Web page. The use of strong authentication and authorization procedures are in place. The authentication process allows the user to access only information relevant to that particular user. Other methods are in place to detect users attempting to guess another password or if a brute force attack is under way. If such an attack is detected, the system will disconnect from the user and report the security breach for follow-up. Customer Web sites hosted by the ISP are prevented from intercepting messages not addressed to them. Packet filters are implemented on the ISP Internet Gateway Routers using Access Control

Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Business to Business E-commerce	Illustrative Controls for Service Providers
			Lists (ACLs) according to the ISP firewall policy. Anti-spoof filters are used on the routers to prevent spoofing of trusted sources. Additional ACLs are used to control customer access to only their network segments. The various LAN segments are firewalled from the rest of the networks.
C.1.8 The entity has procedures to prevent dial-up access during active local area network session(s).	If an employee of the entity attempts to use a dial-up connection to access the Internet (rather than use the network connection), the system will drop the network connection until the dial-up session is terminated. The session address will be transmitted to the security officer for follow-up.		
C.2 The entity maintains system configurations that minimize security exposures.	Company management routinely evaluates the level of performance it receives from the ISP which hosts the company Web site. This evaluation is done by evaluating the security controls the ISP has in place by an independent 3rd party as well as by following up with the ISP management on any open items or causes for concern.	Management maintains relationships with all critical vendors (for example, firewall, operating system, and routers). Meetings are held on a routine basis to discuss current system configuration(s) and the impact any known security incidents may potentially have on the company configuration. All configuration changes must be documented approved by the security team after a discussion with vendors and authorization given by the CIO.	The service provider meets with its technology vendors on a regular basis (for example, SUN, Cisco, and Microsoft). Identified vendor security issues are documented and conveyed to the vendor to the appropriate level of management, depending on the severity of the exposure and risks associated with its planned or current deployment in the network. All vendor security issues are associated with agreed upon time frames and followed up on by an ISP representative.

	Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Business to Business E-commerce	Illustrative Controls for Service Providers
C.3	The entity minimizes or eliminates unneeded network services (port numbers).	The entity reviews on a monthly basis all services offered by the system (for example, FTP, Telnet) and eliminates those not needed.	A listing of the needed server services (for example, telnet, FTP, HTTP) is maintained by the IT department. This list is reviewed by company management on a routine basis as to its appropriateness for the current operating conditions. A port scan is done at least monthly and compared to the approved list. Any variations are reported to management within twenty-four hours for follow-up.	
C.4	The entity updates software to optimal versions and patches.	The entity has relationships with all key systems vendors and is notified when via email when a new update is available.	The IT department maintains a complete listing of all software and the respective level and patch. Management meets (via email, telephone, or in person) with its technology vendors on a regular basis to ascertain current software release and patch levels and the associated security issues. Management then makes a determination with consultation from vendors as to the optimal software release and patch level.	On a month basis, the service provider obtains notification from the software vendors the current release, version number and patch level. With consultation and information from reputable outside security information sources (for example, Computer Security Resource Clearinghouse, Computer Incident Advisory Council) management makes a determination as to optimal software and patch level based on the current operating environment.
C.5	The entity utilizes 128-bit encryption to protect transmissions of user authentication and verification information over the Internet from unintended recipients.	The entity utilizes 128-bit encryption for all transmission of private of confidential information, including user ID and password. Users are also encouraged to upgrade their browser to the most current version to avoid any possible security problems.		

	Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Business to Business E-commerce	Illustrative Controls for Service Providers
C.6	The entity protects internal systems from viruses.	The company maintains anti-virus software on its systems, updates its virus signatures at least monthly, and takes reasonable precautions to protect both its systems and the customer's computer from viruses during the e-commerce session.	In connection with other security monitoring, management participates in user groups and subscribes to services relating to computer viruses. Daily the server downloads the most current virus definitions and any updates are then automatically "pushed" to users as they log on. Any viruses discovered are reported to the security team as well as an alert created for all users notifying them of a potential virus threat.	Management subscribes to several services relating to virus and other malicious codes. The service provider's systems run two separate virus scanning programs at all times that are updated daily. Internal users are required to run a full scan on their local machines once a month.
C.7	The entity implements programming standards and conducts software testing to ensure Web pages using active content technologies (for example, example, Java applets, Active X, Java Scripts) are not susceptible to security weaknesses.	The company's systems development methodology describes the software development and maintenance processes and the standards and controls that are embedded in the processes. These include programming and testing standards.	Current policy prohibits the copying of applets, scripts, or other active content from other sites. All pages and other programs are placed on a staging server for testing before being placed on the main server. Management subscribes to current security publications that evaluate these technologies.	

	Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Business to Business E-commerce	Illustrative Controls for Service Providers
C.8	The entity protects against its unauthorized access to customer or other remote systems.	The company requests the customer's permission before it performs any diagnostic or inventory on the customer's computer.	Scanning, sniffing or other methods of gaining access to remote users' systems is prohibited. Any access to remote customer or supplier's systems is clearly communicated to the remote user as to need and purpose before such access takes place.	Management has policies and procedures that prevent its employees from accessing the customer's computer without expressed authorization from the customer. The customer should receive notification that the host wants to enter the customer's computer. The customer can then give or reject permission.
C.9	The entity limits physical access to firewalls, servers and other critical system(s) to authorized personnel.	Physical access to the servers and related hardware (for example firewalls, routers) is controlled and monitored by video surveillance.		
D	**Monitoring/Performance Measures**			
D.1	The entity has procedures for monitoring the security of its e-commerce systems.	The Information Security group uses the following monitoring tools: COPS – this software provides a snap shot of the system which is analyzed on a monthly basis. Tripwire – a real time monitor which is used to detect intruders. SATAN -- this software is run monthly and provides a security analysis of the system. In addition the group maintains and analyzes the server logs.	Commercial and other monitoring software (COPS, SATAN, ISS) is run on a routine basis. The report outputs from these programs is analyzed for potential weaknesses and threats to the systems. Changes are made due to the information contained in these reports and with the consultation and approval of management.	

	Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Business to Business E-commerce	Illustrative Controls for Service Providers
D.2	The entity has procedures in place to keep its security policy current.	The entity subscribes to publications and user groups specific to its industry and application in order to receive the most current security information. On a monthly basis the Webmaster reports to the CIO any weaknesses perceived in the system. The entity management reviews this report for follow-up and resolution.		
D.3	The entity has procedures in place to test its security incident policy and update it as needed due to technology changes, changes in the structure of the e-commerce system(s), or information gained from tests of its plan.	Weekly IT staff meetings are held to address current security concerns and their findings are discussed at quarterly management meetings.	Senior management reviews the security policy on a biannual basis and considers developments in technology and the impact of any laws or regulations.	
D.4	The entity has procedures in place to test its disaster recovery plan as it relates to the entity's security policy and update this plan as needed due to technology changes, changes in the structure to the e-commerce system(s), or information gained from tests of its plan.	The Information Security group maintains a disaster recovery plan that contains configurations, contingencies and other documentation. This plan is reviewed at least annually or when any major changes are made to the system. A listing of major suppliers is also maintained along with an emergency implementation plan. Mirrored sites are also updated when any configuration changes are made to the infrastructure.		
D.5	The entity has procedures in place to effectively monitor and act upon security breaches.	All system logs are monitored and evaluated on a routine basis. Monitoring software is in place that will notify the IT manager via email and pager should any incident be in progress. If an incident occurs a report is filed within twenty-four hours for follow-up and analysis. Customers are directed to an area of the Web site to post a message about security breaches or possible breaches as soon as they become concerned. These customer comments are followed up within twenty-four hours for evaluation and a report is issued back to the customer and CIO or the customer may contact the Incident Response hot line by telephoning 888-911-0911 24X7.		