Sample Security Policy

Purpose

The purpose of establishing this information security policy for *CORPORATION X* is to protect corporate information and computer assets while allowing: 1) e-mail communication, 2) information transfer, and 3) access to the corporate website and web-based e-commerce server between customers, corporate affiliates, and corporate users. Also, it defines policies for protecting data within the corporation and addresses the confidentiality, data integrity, availability, accountability, and responsibility issues that each employee must be aware of and comply with while working for this corporation.

Threats

1. Virus introduced by e-mail, web browsing, corporate web-site access, floppy, CD, tape, or ftp downloads.
2. Denial of service attacks from the internet to corporate servers.
3. Unauthorized login into computers by learned or hacked usernames and passwords for the purpose of reading, deleting, removing, or inserting data not approved by the responsible party of the computer resource.
4. Unauthorized network access to server and workstation computers for the purpose of reading, deleting, removing, or inserting data not approved by the responsible party of the computer resource.

5. Unauthorized physical access to corporate servers that may result in inadvertent or malicious shutoff, damage, or login access to the server.
6. Unauthorized access to data by a user because of lack of file protection.
7. Loss of data assurance (i.e., receipt of data without traceability) of confidential corporate data during network transfer.
8. Loss of data integrity (i.e., data tampered with during transmission) of confidential corporate data during network transfer.
9. Theft of disks and tapes.
10. Unauthorized tampering with network resources that can lead to the loss of the network.
11. Loss of power.
12. Lightning strike.
13. Illness of personnel that may lead to users bypassing information security for the sake of convenience.

Cost/Benefit Analysis

The calculated cost of the e-commerce server being down every minute is $______.

The calculated cost of the network being down every minute is $______.

The calculated cost of removing a virus from a single PC is $______. The cost for removing a virus from all corporate machines is $______.

The calculated cost of e-mail being down per user per day is $______.

The calculated cost of secret corporate information getting into the hands of a competitor is $______.

These are considered the primary risks due to financial loss for the following information security measures.

Confidentiality

1. Corporate servers must be located in a secure physical location with access only by authorized personnel via combination lock or access card.
2. A firewall must separate corporate computers and servers from the internet.
3. All users must have a separate user account and password that must be kept confidential.
4. Each server must have an account policy that enforces passwords to be a minimum of 6 alphanumeric characters long.
5. Each server must have an account policy that enforces password expiration every 3 months.
6. Each server must keep a password history file that saves the history of a user's passwords and does not allow reuse.
7. Users cannot share accounts.
8. All user accounts will use password-protected screen savers.

9. Users may not access another user's data without permission. Each server must have a file protection system that restricts user access to the user's own files. Exceptions include a user belonging to a group that has file access via group file permissions.
10. Users must take responsibility to protect their data.
11. All corporate confidential data must be encrypted with 128-bit encryption before being transmitted over a public communication channel (e.g., the internet, leased lines, or POTS connections).
12. All corporate confidential email must use PGP encryption. Public keys must be posted to the PKI system at the following server ldap://certserver.pgp.com. Day to day email does not have to be encrypted.
13. Financial servers and servers with highly classified corporate information must reside on a separate network that is physically separate from any corporate network that is connected to the internet.
14. No e-mail or internet access is allowed on corporate financial servers and servers with highly classified corporate information.
15. Workstations and servers behind the corporate firewall must not have a modem connection. Modem connections will be handled via an authorized dial-in server.

Integrity

1. The administrator and alternate administrator account must be the only accounts with access to all files.
2. All file transfers of highly confidential data between machines must check for the integrity of the data.
3. System files must be read-execute for users.
4. Any new data copied onto a server must be done through the server that must log the transaction.
5. All systems must have anti-virus software present that scans all disks, floppy drives, incoming IP traffic, and MS Word macros.
6. Confidential data must be encrypted during data transfer.
7. No unapproved software shall be installed on any workstation without authorization from the corporate MIS department.

Availability

1. Dial-in capability will be to a specified dial-in server that will authenticate the user.
2. Each server must have an uninterruptible power supply (UPS).
3. All servers must be available 24 x 7 x 365.
4. Access to e-mail, FTP, and HTTP services must be available 24 hours per day.
5. Each server must be in a room with controlled access.

6. The servers and workstations in the internal network must have proxy services for designated users coming in outside the firewall. Database servers may be accessed by specific IP addresses that are authorized to access the resources using FTP or HTTP. These addresses must use gateway authentication at the firewall in order to gain access to servers inside the firewall.
7. Access to servers on the internal network must be restricted by a firewall that specifies the IP address that may pass and requires authentication.
8. If IT personnel are not available during an emergency, then there will be a backup person(s) that will be assigned to the task.

Accountability

1. All account security events must be logged.
2. All confidential file access must be logged.
3. All data transfers of confidential data must use authentication between server and client.
4. All confidential data sent to another machine must have a digital signature associated with it.
5. All new software deployed on either servers or workstations must be authorized by the IT staff. A software log of installed software must be maintained.
6. All connections through the firewall must be logged.

Recovery

1. All server data will be backed up daily using incremental backups.
2. Full backups will be done once a week.
3. Archives will be done monthly.
4. Backups and archives must be stored off-site.
5. Desktop workstations will use network file services to store corporate data that should be backed up by the server.
6. Desktop workstations will have standardized configurations for each department that will include designated versions of the operating system at a specified revision level, anti-virus software, e-mail and groupware software, word processing and spreadsheet software, and other specific departmental software. An image of this software configuration will be made by MIS. This image will be pushed down to the departmental workstation in the event of operating system corruption.

Employee Responsibilities

1. Employees must adhere to the stated policy as technology changes and must make best efforts to protect data and not indulge in activities that compromise data.
2. Employees should backup any data that they feel is important that is not stored on the corporate file servers.
3. Employees must comply with the corporate information security policy.

4. Copyrighted software must be used in accordance with the software license.
5. Corporate computers cannot be used for personal purposes.
6. Corporate e-mail cannot be used for personal purposes.
7. The hardware configuration of a desktop workstation cannot be changed without approval from the MIS department.
8. Employees are prohibited from transmitting fraudulent, obscene or harassing messages to anyone.
9. Employees are prohibited from transmitting programs to anyone that have the intent of compromising information security or disrupting work.

Enforcement

1. Any reported abuses of corporate resources will be investigated. During the investigation the company may access the electronic file of its employee. If computer policy has been violated then the employee's privileges may be restricted as decided by the CIO.
2. The company will audit resources periodically to ensure that software and computer configurations comply with policy.

Education

1. Information security training will be provided by the company once a year.
2. Each employee will receive a hard copy of the corporate information security policy and must read it.

Configuration Issues

1. The corporate internal network will contain networked workstations that need to access the internet, and servers running databases, file, printer services, administrative purchase order submittal system, and expense reporting system.
2. The corporate network will have a firewall between the corporate network and internet connection.
3. Publicly accessible servers such as the web server, e-commerce server, e-mail server, and FTP server must be located on a DMZ within the firewall.
4. Mail applications must support PGP encryption as an option.
5. All computers will have anti-virus software installed.
6. Data communication between machines with confidential data must be encrypted using 128-bit encryption.
7. Network printer cards must have their default access password changed.
8. All network devices must be SNMP compliant.