Independent Audit Report

Conducted By

6524 Walker Street, Suite 225
Minneapolis, MN 55426
(952) 345-0642
Toll Free (866) 942-3282
Fax (800) 867-5088

US Internet

Executive Summary

The purpose of this audit was to validate the operations, policies, and procedures of the US Internet data center in compliance with the security standards set forth by the Gramm-Leach-Bliley Act (Privacy Act for Banking, Insurance, and Stock Brokers / Dealers) and the HIPAA (Health Insurance Portability and Accountability Act) Privacy and Security Regulations. The audit was performed over a four month period from August 2003 to November 2003 at the request of Kurt Lange, Vice President of Operations for US Internet.

Scope of Work

The scope of the audit was to review and observe the operations, policies, and procedures of the US Internet data center as it pertained to the Acts listed above broken down into five areas: Overall Matrix, Facilities, Security, Network, & Management. The findings of the audit and recommendations are stated below.

Overall Matrix:
Data Security Auditors uses this matrix as a quick reference guide for our clients to see specific areas that may need improvement. As you can see the range is from 5 to 0; 5 being excellent and 0 being dangerous and requiring immediate attention.

Level 5 – Excellent, achieved benchmark of security.
Level 4 – Very Good, no changes needed.
Level 3 – Standard, controls are in place and appropriate for use.
Level 2 – Improvement Needed, vulnerabilities can be exploited.
Level 1 – Improvement Required, vulnerabilities are apparent.
Level 0 – Dangerous, conditions must be improved immediately.

Item	Level	Comment
Power Supply	5	Power feeds into the building from different ends and are supplied from different sub-stations.
Uninterrupted Power Supply	5	Ample battery supply tested every two weeks, and inspected quarterly.
Backup Power Supply	5	Diesel generator on west side of building with plentiful capacity tested every two weeks, inspected quarterly.
Fire Detection	5	Vapor system equipped with a laser detection device monitors any smoke, heat, or water.

Fire Suppression	5	Fire Suppression system is FM 200 and has emergency override switches at the exits.
Building access	5	Building is locked after hours and monitored by video cameras 24 x 7 in control room.
Data Center access	5	Data Center is locked. Access is through a man-trap requiring bio-matrix and card key authentication.
Inside Data Center	5	All equipment is kept in locked racks that are monitored by control room video cameras 24 x 7.

Findings

Facilities:
The data center is located on the ground floor of the building where there are no windows or doors to the outside. There is a control room adjacent to the center that is manned 24x7. There are no sources of water above the data center or in the ceiling. The equipment power comes from two separate uninterrupted power supplies; therefore, equipment with dual power supplies are supplied power by different UPS's. The UPS's are backed up by generator power and both systems are tested every two weeks. The power equipment is well maintained by an outside electrical contractor and maintenance is performed twice a year and the batteries are inspected four times a year. The commercial power feeds to the building enter from different ends of the building and are supplied from different power sub-stations. The data center is monitored by vapor system equipped with a laser detection device which notifies the control room of any smoke, heat, or water in the data center. The fire suppression system is FM 200 and has emergency override switches at the exists.

Recommendations:
Not Applicable

Security:
US Internet has excellent security policies and procedures which are supplied to all clients. A copy of this plan is attached and all aspects of the plan have been reviewed and any discrepancies are stated in the recommendations. The building, as well as the data center, is monitored by video cameras which are observed by the control room and are taped and maintained for 30 days. Access to the building is via the front desk and all employees must display a badge and all visitors are asked to sign in and are issued a badge. All visitors are escorted when in the building. Access to the data center is through a man-trap that requires both a bio-matrix and card key checking. There is a 90 day audit trail for all accesses. All client owned equipment is kept in locked racks that only US

Internet personnel have access to. All client or third party visitors must notify US Internet prior to showing up at the data center. The client is required to submit an access list of personnel and keep it current. These visitors are escorted into the data center. All customer electronics are 3DES encrypted and only the customer has the encryption key.

Recommendations:

1) There should be a policy which requires US Internet to send every client a list of their employees and vendors that are granted access to the data center. This list should be issued quarterly and a signed copy returned to US Internet.

Network:

There are two point of presence into the building and they are supplied from two separate central offices. There is an isolated test network established for the testing of new software and patches. US Internet performs their own maintenance on network hardware and they have abundant supplies. They have a next day return for failed components and can draw on local suppliers or the Internet if needed. All separation of data and power cabling requirements were observed. US Internet uses a Virtual Private Network to transport information to their client's site.

Recommendations:

Not Applicable

Management:

US Internet has instituted the policies that ensure all employee access and equipment are returned when anyone leaves the company. There is a client specific notification and action for all clients in the CRN System, which is used to log and track problems. US Internet customizes its service level agreements to the client's needs.

Recommendations:

N/A

Special Comment:

Never before has Data Security Auditors executed an audit where the client company has received a perfect score of 5 out of 5. This rating of excellent is a solid tribute to the management and ownership of US Internet as an organization that continually invests in security and infrastructure maintaining the highest level of security for its clients.

Roger Hughes
President
Data Security Auditors