GIAC HealthCare Insurance Company

Securing Information in an Insurance Company

David H. Todd

Submitted 7/11/03

GIAC Information Security Officer (GISO) Certification
Practical Assignment Version 1.3

Abstract

This practical assignment presents an overview of the information technology and security environment of a health insurance company, GIAC HealthCare Insurance Company. Included in this document is:

A description of the company, detailing the location and working environment

An overview of the IT structure that includes a network diagram.

A brief discussion of the business operations from an IT and security perspective

Three of the most critical identified areas of risk to this of environment are reviewed. The various threats and vulnerabilities that make up the risk are also discussed, as are the consequences of the exploitation of the vulnerabilities.

An existing security policy is evaluated for one of the risks and the policy is revised to adapt it to GIAC HealthCare.

A security procedure is developed to support the revised policy.

Description of GIAC Healthcare Insurance Company

GIAC Healthcare Insurance Company (GHIC) is a small health insurance provider located in Midwestern United States that provides health insurance to small to medium size companies. The primary insurance products are HMOs and PPOs. The company has approximately 150 employees and has been in business for 17 years.

The insurance is sold by GHIC company employed agents and through insurance brokers. Claims are processed by the company in its main, and only, office which also houses all other insurance related functions as well as the Human Resources, Payroll, and Information Technology departments.

The office consists of two floors. Access to the building is controlled 24 x 7 by a security guard at the entrance. Photo identification badges must be presented to the guard upon each entry to the building and worn on an outer garment at all times when in the building. Swipe cards are required to access the work areas. Business visitors must be scheduled in advanced with the security guard and must be escorted when in the building. Personal visitors are not allowed out of the main lobby area. Trip switches on exterior exit doors annunciate at the main guard desk after normal working hours.

Most staff members have a connection to the corporate LAN. The workstations all run Windows 2000, Version 5.0, Service Pack 3. Windows Office 2000 Professional is also in use. Also, most workstations have been “ghosted” from a basic image that blocks the addition or removal of software without system administrator access. End users do not have system administration capability at their workstations.

Claims are processed in the office by accessing a third party provided Data Center. Electronic submitted claims are routed directly to the Data Center via an electronic Bulletin Board System (BBS) supported by the Data Center and do not enter the GHIC network. Checks and Explanation of Benefits statements are printed at the print center located at the Data Center.

Company employed agents, Provider Education Representatives and certain management have dial-in capability via modem to access their email accounts and corporate file servers. They are not allowed to access the Internet with this dial-in capability. No modems are utilized inside the GHIC office. The Internet is available to all internal users.

Management has kicked off the creation of a Business Continuity Plan. It is being modeled after the NIST Special Publication 800-34.[1] A Contingency Policy has been developed. This effort is currently in the Business Impact Analysis stage.

IT Infrastructure

All IT functions are supported by the Information Technology Department. Due to various stringent state and federal insurance regulations, a high level of systems availability is required at all times in order for business to be conducted in a timely manner. HIPAA Privacy and Security Rules require a high level of security surrounding electronic Protected Health Information (PHI).

For the most part, GHIC utilizes IBM X Series 225 servers.

As a general practice, all vendor supplied default passwords are removed upon installation. All other vendor default settings are reviewed for appropriateness and changed when necessary. Patches and fixes are installed on an ongoing basis after they have been proven to be generally effective and that they do not cause additional problems. Access to routers is restricted to the console located in the server room. Firewalls are set to block everything not specifically allowed.

The following a description of the infrastructure based upon the diagram in Figure 1:

- Internet Border Router – this is a Cisco 3600 series router. Set to route to the DMZ and block incoming packets that have a source address from the internal network. In addition, it filters outgoing packets that have a source address different from the internal network in order to prevent a source IP spoofing attack originating from the GHIC site, as described in CERT Advisory CA-1995-01.[2] It also blocks incoming/outgoing pings and echoes.

- The Firewall at the Internet perimeter is a Nokia 330 running Checkpoint FW-1, v 4.1. The firewall inspects all traffic between the LAN and the Internet. It is performing stateful inspection of packets and Network Address Translation (NAT).

- A Cisco 3550 series switch handles the traffic routing to the DMZ.

- The DMZ consists of servers stripped of all services except the operating system and the specific service(s) it is running.

    - Network Intrusion Detection System running Snort 2.0 monitors the DMZ for anomalous activity.

    - Web Server running Windows IIS, version 5.0. This server does not allow any input and is for informational purposes only. It is used to advertise the company's products and provide information to insurance members, providers and the general public.

    - Email Gateway – handles Internet email traffic. McAfee Antivirus E-Policy inspects email attachments on all email entering from the Internet.

    - External DNS server – only points to the servers in the DMZ, hence information about internal computers is not available on this server.

- Cisco 6500 series Core switch – this is the main LAN switch that routes traffic on the LAN and to and from the Internet and Data Center.

- Cisco 3550 series switches handle the traffic routing to each floor in the building.

- Internal DNS Server – handles all internal DNS functions.

- Intranet Server – Windows IIS, version 5.0 – contains GHIC web pages for Human Resources as well as training and Desk Top Reference sites for GHIC operational departments. This server also runs the Tivoli Storage Manager, version 5.0, which handles all data backup.

- File/Print server – handles all printing and shared file services for GHIC. Also contains the Billing and Enrollment SQL databases.

- Lotus Notes Email Server – version 5.0.8 – handles the GHIC email services.

- Domain Controller – Windows 2000 Advanced Server is utilized as the domain architecture. Provides logon validation and private home directories.

- Back up Domain Controller - Windows 2000 OS Advanced Server is utilized as the domain architecture.

- Anti virus server – this is running McAfee Antivirus E-Policy v2.5.1 that distributes and verifies current virus definitions installed on each workstation and server.

- Remote Access Services (RAS) Server– authorizes and grants dial-up Point to Point (PTP) connection for authorized staff to access GHIC LAN resources. User authentication is via a privileged user account and password.

- The Firewall at the Data Center perimeter is a Nokia 330 running Checkpoint FW-1, v 4.1. The firewall is inspects all traffic between the LAN and the Data Center. It is performing stateful inspection of packets. Due the critical nature of the connection to the Data Center, there is a hot back up firewall that is tested on a regular basis.

- Data Center Border Router – this is a Cisco 3600 series router – routes traffic to and from the Data Center. Set up like the Internet Border Router.

Description of GHIC Business Operations

GHIC is in the business of selling and servicing health insurance to small businesses. Of utmost importance are the protection of company confidential information and the Protected Health Information (PHI) of its insured's. PHI as it pertains to GHIC is defined in the HIPAA Security Rule as "individually identifiable health information…. Transmitted by electronic media; Maintained in any medium described in the definition of ***electronic media*** at § 162.103 of this subchapter; or Transmitted or maintained in any other form or medium." [3]

Confidential Company Information and PHI will henceforth be referred to as Confidential Information. This Confidential Information is considered the crown jewels of the company and must be kept secure at all times. Access to and use of this information is protected by a combination of employee awareness training, application systems (e.g. claims, enrollment, and billing) security, and overall LAN security. Access is controlled by use of userids and passwords. The LAN and Data Center systematically force passwords to change every 60 days. Minimum password length is 7 characters. Passwords cannot be reused for 12 generations and lock out after 3 consecutive unsuccessful login attempts. A systems administrator must reset the passwords. A "challenge question" system is in place to verify the identity of anyone requesting a password reset.

The primary departments of GHIC are Sales, Enrollment, Billing, Claims, Mail Processing, Customer Service, and Information Technology.

The Sales Department handles the sale of the company offered insurance products. Once a sale is completed, and the proper paperwork is submitted, the required information is passed to the Enrollment Department for creation of enrollment records of all insured members and dependents. Enrollment records are maintained in a SQL database on-site and daily uploads are made to the claims eligibility files housed at the Data Center. Sales information is also provided to the Billing Department to create the billing records. Billing is handled on a monthly basis, with staggered billing dates to spread the workload out across the month.

The Claims Department is responsible for the timely adjudication of member claims utilizing the claims system housed at the Data Center. Medical providers, via dial-up access, can submit electronic claims directly to the BBS at the Data Center over Plain Old Telephone Service (POTS). Paper based claims are keyed by the claims department directly to the claims system at the Data Center. This is accomplished utilizing IBM PCOM emulation software and a GUI front-end data entry module customized to allow easy data entry from the standard claim form. Strict Segregation of Duties (SOD) is followed in the access granted to the Claims Representatives to assure that no inappropriate access is allowed. This follows the principle of not allowing anyone that can issue a check to be able to alter the path of the check, or to create a record of an entity to which payment can be made. The claims system has a variety of edits built into the system that allows many submitted claims (electronic and paper) to self adjudicate through to payment or denial. Certain edits cause claims to suspend to a designated status. These statuses are then worked by the appropriate claims personnel to resolution or to a pending status to request additional information.

The Mail Processing center handles incoming mail, outgoing mail and microfilming. All incoming mail is sorted and microfilmed before it is released to the appropriate department. An outside vendor is used to develop the microfilm. Mail processing staff make “burns” (copies) of the microfilm upon request. Incoming billing payment mail is sorted at the Post Office by the use of specific post office boxes. Designated personnel open this mail in a controlled access room. Deposits are made daily. Any checks not deposited are locked in a safe at the end of the day. The safe is UL rated TRTL 60 (torch and tool resistant for 60 minutes).

The Customer Service Department primarily handles inquiries by members, their dependents and medical providers. Sales calls are referred to the Sales Department. Customer Service Department Representatives (CSRs) are able to access the claims system as well as the enrollment and billing databases on an inquiry basis only.

The Information Technology Department is responsible to provide all necessary information services to support GHIC.

All servers are located in a climate controlled, Halon protected room with a raised floor. The main telecommunications equipment is also housed in the server room. Moisture detectors are located under the floors. There is a redundant air conditioner specifically for the room. A Liebert Uninterruptible Power Supply allows orderly shut down of the servers in case of power failure. Access to the server room is controlled via cipher lock that records entry time and person entering. The lock on the door is keyed “off master” and is utilized for emergency access to the room. There is only a limited number of management staff with a copy of the key. Cipher codes and keys are controlled through an approval process requiring both senior management and security officer approval. Any person not specifically authorized to enter the server room must be escorted and sign in and out on a log.

LANTEL closets on each floor house the switches for the LAN on the respective floor. These closets are also controlled with cipher locks and "off master" key locks.

Most staff has access to:

Lotus Notes email
the company Intranet site containing Human Resources, training,
reference and corporate information
a variety of printers and shared files, and
the Internet for research purposes.

Access to the Enrollment and Billing databases is strictly controlled and requires management and security officer approval before the access is granted.

Sales agents working in the field as well as corporate Provider Education representatives can access the GHIC LAN via a dial-up POTS connections from company owned laptop computers. Certain other management staff also has dial-up access with their company laptops. Dial-up connectivity is handled via a RAS server.

The third party Data Center uses RACF security to control system access its environment. GHIC has established access control procedures within the company that requires documented access requests approved by management and the security officer for all Data Center, application and LAN access. Strict segregation of duties is enforced throughout the company, as is the principle of least privilege (only grant access necessary to carry out required tasks).

Paper records (e.g. enrollment, billing, and claims) are retained on-site for 60 days and then securely shipped off-site to an approved outside storage vendor.

Risk Identification at GHIC

The three most critical risks to GHIC have been identified and are as follows:

Risk #1

Release/compromise of Insured's Records

What is the risk?

The crown jewels of the company are the health and enrollment records of members and their dependents and the company's confidential records. This information is primarily stored at the Data Center in electronic format, but also exists within the billing and enrollment databases, other company paper and electronic files, and microfilm.

Access to the electronic data could occur by:

Unauthorized access from within the company gaining access to the files at the Data Center or to LAN based databases and other files.

Unauthorized access to the LAN via dial up connection and gaining access to the files at the Data Center or to LAN based databases and other files.

Access to the microfilm records could occur by:

Inappropriate requests for microfilm to the mailroom for “burns” of confidential information.

Authorized mailroom employee making unauthorized copies of confidential information.

Unauthorized duplication of microfilm records at the outside developing vendor.

Access to paper records could occur by:

Mailroom or other employee making unauthorized copies of confidential information.

Copies or originals of confidential information left on a photocopier or fax machine and picked up by an unauthorized employee.

Failure to secure paper confidential information in appropriate locking containers or locking rooms at the end of day.

Failure to properly and securely dispose of confidential information.

Unauthorized access to confidential information records sent to the outside records storage company.

Why is the risk of concern and what are the possible consequences?

This risk is of major concern to the company because a large client base must be maintained to continue to stay in business and to grow the business. Compromise and/or release of PHI or other confidential information would negatively impact the company financially as well as negatively effect the company’s reputation. Lost sales as well as possible fines by government insurance agencies may occur. Release may cause public embarrassment to those individuals whose information was released or allow competitors to gain inside knowledge about the company. This could result in lawsuits against the company and loss of competitive position in the market place.

Recommended mitigation steps.

Recommended steps to mitigate the risk that applies to **all areas** listed above:

1. Perform complete personnel background checks before employment and on a regular basis after being hired.
2. Obtain a signed confidentiality statement as part of hiring.
3. Thorough security awareness training that is repeated on a regular basis.

Mitigation steps for **specific areas** listed above:

Electronic Data

1. Adhere to and strictly enforce segregation of duties procedures.
2. Strict enforcement of access authorization procedures.
3. Regular review of all staff’s system access levels.
4. Regular change of all systems’ passwords

5. Use of encryption technology for dial-up access to the GHIC LAN.
6. Use of random number generated passwords for all dial-in users. SecurId® by RSA offers this type of solution. This solution is effective by “requiring users to identify themselves with two unique factors — something they know and something they have — before they are granted access.” [4]

Microfilm Data

1. Adequate mailroom supervision including oversight of microfilm burn requests.
2. Securing mailroom at end of the workday.
3. Contract with microfilm vendor that includes a comprehensive confidentiality statement and the power to enforce it.

Paper Data

1. Adequate mailroom supervision including oversight handling of paper confidential information.
2. Stress in training and through reminders not to leave copies or originals of confidential information on photocopiers or fax machines.
3. Provide adequate containers or rooms to secure confidential information.
4. Enforce a “clean desk” policy to assure confidential information is not left on desks at the end of the workday.
5. Provide secured shredding containers for authorized disposal of unneeded confidential information.
6. Contract with outside records storage vendor that includes a comprehensive confidentiality statement and the power to enforce it

Risk #2

Power Interruption

What is the risk?

Interruption of power can occur for a variety of reasons:

Severe weather – tornado, windstorm, severe thunderstorm, winter storm
Physical cable cut – sabotage, construction error, accident
Power fluctuations – local or wide spread

Why is the risk of concern and what are the possible consequences?

Widespread loss of power is a concern to GHIC since, other than the UPS on the servers and short-term battery powered lighting, there is no alternate power source. With the BCP still in its development stages and no on-site generator, loss of power for any significant time period will have a significant impact on the day to day operations of the company. If the company cannot operate due to loss of power, new sales might be lost, claims processing will be interrupted, and billing cycles might also be delayed. If government timeliness standards in paying claims are not kept, fines may result. Goodwill with insured companies and members might be impacted.

Recommended mitigation steps.

This risk can be mitigated by the implementation of the BCP. In addition, an onsite generator capable of powering most, if not all, of the building should be considered. An alternate warm or hot site may also be considered to allow continued operation under this risk as well as for other risks that would make the building unusable.

Risk # 3

Lack of hardware redundancy

What is the risk?

There is no backup for the Core Cisco switch.

Why is the risk of concern and what are the possible consequences?

If this switch were to fail, there will be loss of connectivity to the LAN and the WAN (Data Center). If the LAN/WAN access is lost for any significant time, only manual processes will be in place. New sales will not be completed, enrollment records will not be built and claims will not be paid. Email will be unavailable. This may cause loss of goodwill, loss of new sales, interruption of billing cycles, and impact the claims processing. If government timeliness standards in paying claims are not kept, fines may result.

Recommended mitigation steps.

Steps to mitigate this risk are to implement the BCP, keep a back up switch on-site or enter into a service level agreement with a vendor to replace the switch in a short time period.

Evaluate Security Policy

The policy being evaluated in Appendix B is based on a policy taken from the author's company policy manual. The policy address Confidentiality of Information (Risk #1).

Purpose: The purpose is clearly stated, outlining why the policy has been established ("to protect confidentiality of information") and what issue it is meant to address ("prevent unauthorized disclosure, alteration or destruction of such confidential information").

Background: The background is alluded to in the "Guidelines" section, discussing that information is "particularly sensitive for technical, personal or business reasons". However, the policy does not further stress the importance of why the policy is important to the company. Further detail in this area is in order.

Scope: How confidential information exists is clearly outlined and employees are charged with protecting it. The policy then alludes to providers, suppliers and vendors complying with the policy in the "Responsibilities" section. These entities should be more clearly discussed in the scope of the policy.

Policy Statement: The policy statement within the "Guidelines" section is very broad stating that access to confidential information is restricted and should be protected. However, how any of this should occur is not discussed. No actions are specified on how the information is restricted or how it is protected.

Responsibility: Responsibilities are limited to vaguely directing management to maintaining the confidentiality and security of information and systems, and for communicating handling requirements (whatever they are!) to their staff, providers, vendors and suppliers. These same employees, providers, suppliers and vendors are charged with complying with this policy. It could be inferred that management is responsible for the security of systems ("Management is responsible for maintaining the confidentiality and security of information and systems"), which certainly goes well beyond the scope of this policy. Other than the reference to management, there is no specific mention of who is responsible for putting the policy in place. There is also no assignment of who can draft, review, approve, or modify the policy.

Action: Action is limited to charging management, along with Human Resources, to be accountable for investigating issues of non-compliance, and taking appropriate action (whatever that is). No direction is given on what is supposed to be done, and "issues of non-compliance with the policy" is too broad of a statement since the policy never clearly defines what can be considered a breach of the policy. No statement as to when investigations should commence is made.

Revise Security Policy

Policy Title: Confidentiality of Information
Policy #: 306
Original Effective Date: 11/01/1999
Department: Human Resources
Document Owner: Director, Human Resources & Administrative Services
Document Approver: Vice President, Human Resources & Administrative Services

Revision History

Date	Description	Approval Initials
09/30/1999	Draft, to be reviewed by Vice President, Human Resources & Administrative Services	

11/01/1999	Original policy issue	XYZ
06/30/2003	Revision to clarify policy	XYZ

Purpose: The purpose of this policy is to provide guidance in protecting the confidentiality of the information maintained by GHIC relating to its operations, services, employees, subscribers and their family members, providers, suppliers and to prevent unauthorized disclosure, alteration or destruction of such confidential information.

Background: The necessity to respect the privacy of the company's members and the change of legal requirements surrounding the protection of information has necessitated the expansion of GHIC's Confidentiality Policy to further address the proper handling of confidential information.

Scope: This policy applies to all GHIC employees, providers, suppliers and vendors who have access to GHIC confidential information. This information may exist in any form, including verbal, paper, electronic or microfilm/fiche. Information that is considered confidential must not be disclosed, altered, or destroyed in an unauthorized manner.

Policy Statement:

GHIC, in the course of doing business, acquires and maintains information pertaining to subscribers, providers, patients, prescription drug usage, employees, services, operations, claims systems, financial data, and other corporate matters. Selective information obtained from these sources is classified as confidential when such information is considered to be particularly sensitive for technical, legal, personal or business reasons.

Confidential information can exist in any form including verbal, written, microfilm, microfiche, electronic media or electronic CRT display. Information that is confidential must be kept confidential at all times, regardless of the form in which it exists. It is the responsibility of employees who have access to confidential information in any form to protect it and use it only as authorized.

Examples of confidential information include, but are not limited to:

Medical Records
Provider Credential Records
Demographic Data
Company Financial Data
Systems Security Setups
Enrollment Records
Claims History
Human Resources Records
Social Security Numbers
Physical Security Setups

Access to confidential information is restricted to employees of the Company on a need-to-know basis. Such information should be protected from unauthorized disclosure, use, alteration or destruction by either accidental or intentional means.

Employees must not allow anyone to gain access to confidential information under their control unless that entity is authorized to access this information. Employees must never allow anyone to use their individual system access to access system based confidential information. Employees must maintain a clean desk policy at the end of each workday. Paper based confidential information no longer needed must be destroyed (shredded or placed in locking shredding containers).

Non-employees are only granted access to GHIC confidential information on a strict need to know basis. All initial access requests must be in writing and approved by appropriate GHIC management and the Security Department. In addition, a current GHIC Confidentiality Agreement must be on file.

Responsibilities:

The Director of Human Resources and Administrative Services owns this policy. He/she can create and modify this policy. Upon approval by the Vice President of Human Resources and Administrative Services, the Director may implement or modify the policy. All GHIC management, employees, providers, suppliers and vendors who have access to GHIC confidential information must abide by this policy. Management is charged with communicating the requirements of this policy to their employees. Management and the Security Department are charged with enforcing the provisions of this policy.

Enforcement:

Any known or suspected breach of this policy discovered by an employee must be reported immediately to his/her supervisor. A breach is considered to be unauthorized disclosure, alteration, or destruction of confidential information. The Security Department, along with appropriate management, will investigate the situation. Sanctions against employees will be imposed as covered in the "Security Violation Level and Corresponding Actions" policy.

Any known or suspected breach of this policy discovered by a non-employee, is to be reported directly to the Manager of Operations. An investigation by the appropriate management and Security Department personnel will be conducted. Violations by employees will be addressed as discussed above. Violations by outside entities connected to GHIC will be pursued under the terms of the current signed Confidentiality Agreement.

Develop Security Procedure

Procedure Title: Reporting and Investigation of Inappropriate Release of Confidential Information
Procedure #: SSO 028
Original Effective Date: 07/06/03
Department: System Security
Document Owner: System Security Officer
Document Approver: Manager, System Security

Revision History

Date	Description	Approval Initials
06/16/2003	Draft, to be reviewed by Manager, Systems Security	
07/06/2003	Initial issue of documentation	ABC

1.0 OBJECTIVE

The objective of this procedure is to document the steps to follow to report and investigate a suspected inappropriate release of Confidential Information.

2.0 SCOPE

System Security Department
GHIC Management
GHIC Staff

3.0 REFERENCES

Confidentiality of Information - Policy 306
Security Incident Report
Security Violation Level and Corresponding Actions – Policy 101

4.0 SUMMARY

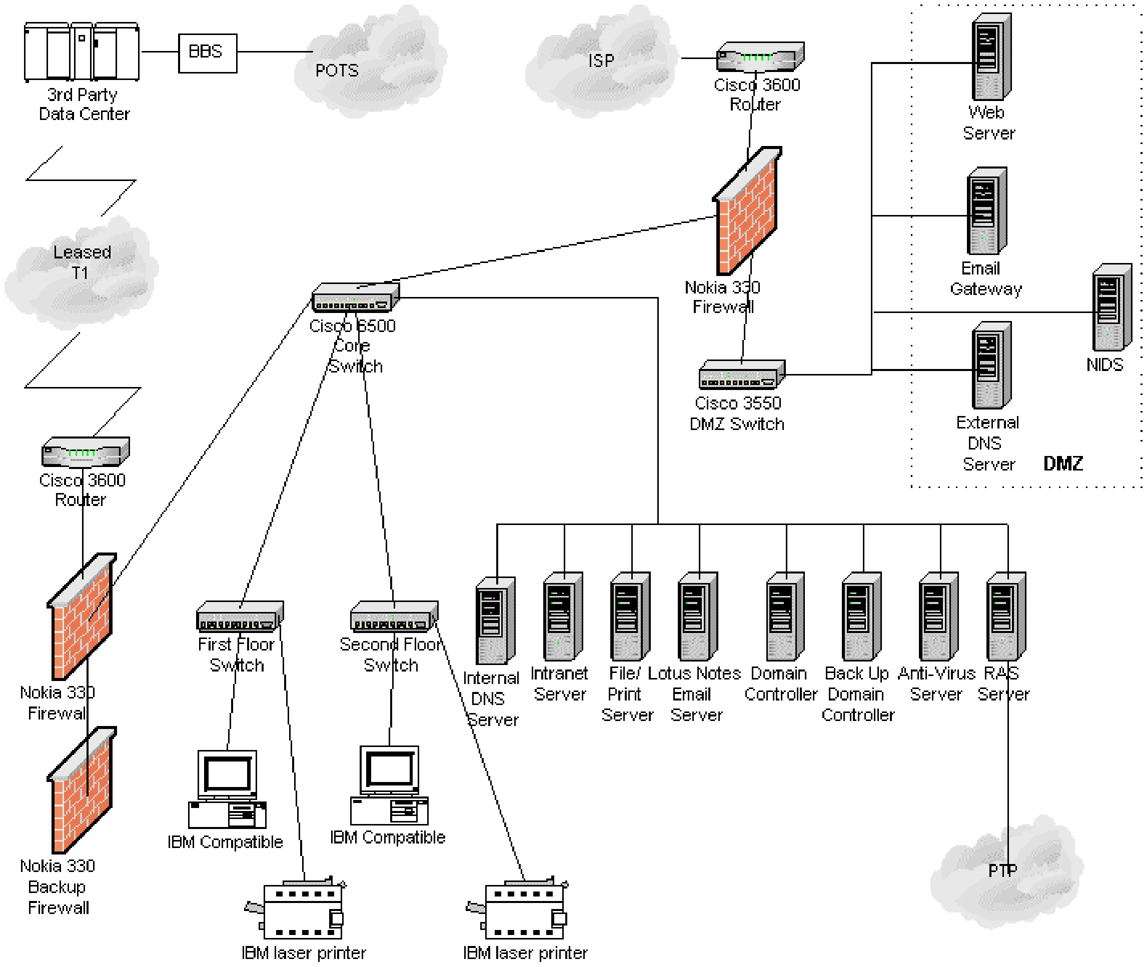
This procedure outlines the process to follow to ensure that any suspected inappropriate release of confidential information is properly reported and investigated. This is to guarantee that an appropriate response is taken to mitigate the incident and, if necessary, to properly counsel any identified employee who may have caused the incident to occur.

5.0 PROCEDURE

- ♦ If an employee suspects that a breach in the handling of confidential information has occurred, he/she must immediately report the incident to his/her supervisor. Outside entities reporting a potential breach are to be directed to the Manager of Operations.
- ♦ The supervisor/manager initiates a Security Incident Report to document the circumstances surrounding the incident. This report must include:
  - ❑ the time and date of the incident
  - ❑ a description of the incident
  - ❑ who was involved in the incident

- where the incident occurred
    - who reported the incident
    - who documented the incident
- The Security Incident Report is forwarded to the Security Department for action.
- A Security Department representative will review the report. Questions may be posed to the employee who reported the incident and/or the manager who completed the report. Outside entities involved in and/or reporting the incident are contacted as needed. If an employee caused the incident, the Security Department representative will then interview the individual(s) involved. All interviews will be conducted in a private office and are strictly confidential.
- If the release of information was due to a systems malfunction, the Manager of Information Technology is immediately contacted with details of the incident. This department in conjunction with the Security Department will investigate any systems an/or applications involved to determine the root cause of the incident. Corrective actions will be taken and details will be provided to the Security Department for documentation.
- The Security Department representative will complete the Security Incident report with results of the investigation and any actions taken. Any follow up actions that are necessary are also documented and these actions are assigned to the appropriate person. Follows up actions are tracked through to completion. All of this information is logged to a Security Incident Tracking database for tracking and auditing purposes. A monthly report is generated from the Security Incident Tracking database and provided to Senior Management.
- If the investigation reveals that Confidential Information has been mishandled, the following steps are followed:
    - If information is released outside the company, the Security Department will contact the person or entity that received the information. They will be asked to securely return the information. The confidential nature of the information will be emphasized along with the legal ramifications surrounding the mishandling of the information.
    - If information is inappropriately released within the company, the employee(s) that have received the information will be contacted. They will turn the information over to the Security Department representative.
    - Any employee that causes a breach will be counseled by their respective management as outlined in the "Security Violation Level and Corresponding Actions" policy.

Appendix A: Network Diagram



Appendix B: Sample Policy

This sample policy is from the author's company and has been sanitized for use in this paper.

Policy Title:		**Confidentiality**	
Number:	306	**Original Effective Date**	November 1, 1999
Section:	Employee Relations	**Revision Date**	
Sponsor:	Human Resources	**Approved By:**	Vice President, Human Resources & Administrative Services

Purpose: To protect the confidentiality of information maintained by the Company related to its operations, services, employees, subscribers and their family members, and to prevent unauthorized disclosure, alteration or destruction of such confidential information.

Guidelines: The Company, in the course of doing business, acquires and maintains information pertaining to subscribers, providers, patients, prescription drug usage, employees, services, operations, claims systems, financial data, and other corporate matters. Selective information obtained from these sources is classified as confidential when such information is considered to be particularly sensitive for technical, personal or business reasons.

Access to confidential information is restricted to employees of the Company on a need-to-know basis. Such information should be protected from unauthorized disclosure, use, alteration or destruction by either accidental or intentional means.

Confidential information can exist in any form including verbal, written, microfilm, microfiche, electronic media or electronic CRT display. Information that is confidential must be kept confidential at all times, regardless of the form in which it exists. It is the responsibility of employees who have access to confidential information in any form to protect it and use it only as authorized.

Responsibilities:

Management is responsible for maintaining the confidentiality and security of information and systems controlled by the company and for communicating the requirements of handling such confidential material to their staff as well as applicable providers, vendors, and suppliers with whom they do business.

Employees, providers, suppliers, and vendors who have access to confidential information are responsible for complying with this policy.

Accountability:

Management, with assistance from Human Resources, is accountable for investigating issues of non-compliance with this policy and for taking the appropriate action.

References:

[1] National Institute of Standards and Technology, Special Publication 800-34
http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf

[2] CERT® Advisory CA-1995-01 IP Spoofing Attacks and Hijacked Terminal Connections
http://www.cert.org/advisories/CA-1995-01.html

[3] Final Standards for Privacy of Individually Identifiable Health Information
http://www.hipaadvisory.com/regs/finalprivacy/501.htm

[4] RSA SecurId® Authenticators product description.
https://www.securehq.com/images/rsa/SID_DS_0601.pdf