Global Information Assurance Certification Paper

Archie Woodworth
30 April, 2001
GSEC Practical Assignment, version 1.2.b

Securing The Wile Modem: A Case Study on the Use of Policies, War Dialers, and Firewalls for Phone Lines

Abstract
Until recently, there hasn't been an adequate method to protect an environment against the threat posed by modems. Traditional approaches, including policies and procedures, scanning or war dialing, and removal of unauthorized modems have been somewhat effective. Nevertheless, a better method is needed to monitor or control activities taking place on the phone network.

The introduction of firewalls for telephone lines provide the capability to monitor, log, alert and terminate phone traffic based on source and destination numbers, inbound or outbound call direction, and call type (voice, modem or fax). These new devices provide businesses with an effective tool to resolve modem security issues in the never-ending quest for a secure perimeter.

Introduction
Over the last couple of years our company has been using a combination of policies and procedures, war dialers, and more recently, TeleWall a firewall for telephone lines in an attempt to control the wile modem. Until now most of the reports regarding firewalls for phone lines has been hypothetical. This paper delineates an attempt to provide practical information on the use of this technology to solve a real world problem. We're not experts by any stretch of the imagination, but we peruse volumes of material and leverage the experience and expertise of others.

It is our desire that by publishing this information, others like us, will be able to leverage and build upon the work that's already been performed.

Background
We are a medium sized manufacturing company of 4500 employees with 4 sites in 3 states, and several international sales offices. We have a distributed WAN with approximately 2800 nodes, a centralized secure remote dial-up access method, 84 known modems, and 55 fax machines.

Modem Risks
The risks modems present to organizations has already been covered in great detail, by a number of authors who are far more renowned and qualified than are we; hence we wont elaborate on this area in detail. Please refer to the Reference for links to additional information on this topic.

For those who may not be familiar with the risks we believe they can be summarized in the following points:

- Desktop systems with modems running pcAnywhere are potential entry points to your network. 1

- Desktop systems that are simultaneously connected to the Internet via an Internet Service Provider (ISP) and to the corporate LAN are potential gateways into your network. 2

To this, after having used TeleWall for a little over a year, we would add the following point:

- Any active phone line or device with a modem has the potential to be abused or become a security threat because it's simply not possible to control all of the unique, uncontrollable 'experiments' of enterprising individuals with access to a modem.

Traditional Risk Reduction Techniques
Again, other authors have already covered the tools and techniques that can be used to reduce the risks of modems; therefore, we won't elaborate in detail. However, a brief summary of best practices would include the following points:

- Implement polices and procedures regarding the authorization and use of modems.
- Attempt to control the purchase of modems or installation of DID (Direct Inward Dial) and Analog lines.
- Create an inventory of known/authorized DID and Analog lines which could be used for modems and document the "who, what, where, and why" of each modem.
- Proactively scan for active modems using a war dialer to identify unknown or unauthorized modems.
- Eliminate as many unnecessary and unauthorized modems and phone lines as possible.

Please refer to the References for links to additional information on this topic. Specifically see the paper "The Desktop Modem Threat", by Joe Livingston 3.

The Problem
Based upon our analysis, there are problems with the current methods:

1. Policies and procedures allow you to control who receives modems or analog lines and document how they should be used. However, one can't control the usage of modems once installed. 4

2. Until recently, the primary tools available for monitoring (war dialers and scanners) did not provide enough information to monitor and enforce security policies effectively.

3. War dialers and scanners covered only a portion of the picture. They identified inbound modems, but missed modems used for outbound activity and didn't provide a means to monitor real time traffic. 5

Classic Illustration

As this paper was being authored, we received a call that epitomized the problems listed above. In other words, it is difficult to enforce a policy when one can't control users and lacks sufficient monitoring capability.

Our TeleWall administrator noticed inbound modem traffic to a Direct Inward Dial (DID) analog line which was documented as belonging to an authorized fax machine. In our TeleWall security policy this particular line had been setup to allow all fax traffic and to log, alert, and allow modem traffic. When we sent someone to investigate, we found that a contractor had unplugged the authorized fax machine and replaced it with a phone cord connected to a modem on a machine in her cube. The machine was now capable of receiving inbound modem calls.

We promptly responded by:

- Attempting to call the IT contact of the contractor to find out what they were trying to do and why. (It was Friday afternoon and he was already gone for the day)
- Blocking all modem traffic to or from that particular line.
- Sending a courteous email to the individual stating our position on unauthorized modems and letting them know the activity would be blocked until they contacted us.

This incident shows that even individuals who have gone through the proper procedures to request an analog line and have received the proper authorization and training, can still circumvent all your best laid plans. Who knows what they were trying to do, it could be anything from simply testing the fax line, to attempting to setup pcAnywhere or a RAS server.

The important thing to note however, is that with a firewall for phone lines we were able to detect the security breach and them implement corrective action.

Our Approach

History

Going back a few years to before our company had an Internet connection, there had been quite a proliferation of analog lines and desktop modems. Virtually anyone who could justify a need to connect to CompuServe, AOL, Teltech, or any other type of bulletin board or reference service had a modem and an analog

line attached to their desktop. As you might have guessed a number of enterprising employees were also using these modems for remote access.

When we rolled out Internet access to the masses two things happened which reduced the number of installed modems significantly. First, someone realized that with the Internet, employees would no longer need access to services such as AOL or CompuServe, therefore we could remove the modems and analog lines that were used to access them. Second, we implemented a centralized authorized remote dial-up solution, which also allowed us to remove the modems and lines that were being used for remote access.

Interestingly, a number of policies that had already been developed and implemented were not being actively monitored or enforced. A brief explanation of each is included below:

COMMUNICATIONS SYSTEMS SECURITY POLICY
A high level policy that states the level of security for all communications media should be sufficient to; achieve optimum service, reliability, compatibility, protection, confidentiality and integrity of the information being communicated.

COMPUTER HARDWARE AND SOFTWARE APPROVAL POLICY
A high level policy to that states proper procedures should be followed when purchasing hardware and software. It is used to control or authorize what hardware and software can be purchased.

ELECTRONIC DATA AND NETWORK CONNECTIVITY POLICY
A high level policy which states correct procedure should be followed when any electronic data is accessed or shared, or any connection is made to, from, or within corporate network facilities or resources.

Computer Security Specification
This specification provides detailed guidance for protecting computing resources and the information they process against unauthorized access, misuse, and abuse.

Proper Internet Usage Specification
This specification provides employees with guidance necessary to facilitate their use of the public Internet in a secure and professional manner.

The relevant portions of these policies and procedures are included in full in Appendix A.

How it all began
Our journey started when someone attended a course called "How to Hack Your Network" put on by Canaudit. In his course the instructor recommended using a war dialer such as ToneLoc or THCscan (two well known war dialing programs) as a means to discover the number of modems in use in your company

As soon as we got back from the class we downloaded both of these programs and began testing them. Before we got too far along in the process we notified the Telecom department on what we were doing and asked them for a few numbers which had modems and faxes attached. With there permission, we began our testing. Of the two programs, we decided to go with ToneLoc.

Though we found ToneLoc to be relatively easy to work with, there was one quirk that we never were able to conquer. For some reason ToneLoc would often stall or lock-up during a scan. While this didn't really cause any problems, it was frustrating to fire off a scan of 200 numbers and return the next morning to find that only 15 numbers were scanned. We spent some time trying to resolve this but eventually gave up mostly because this was all extra credit work and we didn't have the time to spend on it.

Before we began a full-blown war dial, we met with the Telecom department to discuss what we wanted to do. We asked them to provide information on the prefixes and ranges of Direct Inward Dial (DID) and internal extensions in use at each of our sites. We also asked for any information they could provide documenting the extensions of modems and faxes that were currently in use, to who they were assigned, and what they were being used for.

This request turned out to be a little more work than we anticipated. We were expecting to get back 8X10 color glossies of the information we requested, instead we received a couple of hand written lists, and a few post-it notes. However, from this information we were able to identify there were roughly 3600 DID extension, 570 analog lines and 83 known modems.

Once we had this information in hand our war dial commenced. The actual dialing took about two weeks, mostly because of the locking problem.

Results
Our scans identified 36 modems, 21 of which had been identified by Telecom, and 15 of which had not and required follow-up research to identify.

Shortly after we completed the war dial, we hired a third party come in and perform a limited 2 day penetration test as part of an overall company security assessment. We provided this information to them to use as part of the assessment.

The results of this assessment indicated the following regarding the 36 modems that had been identified:

- Two modems appeared to be connect to the AS/400 (and should have been disconnected when not in use)
- Two modems appeared to be connected to routers (and should have been disconnected when not in use)
- Three modems were running pcAnywhere. Of these three, one was not turned on when they performed their assessment, one was password protected, and the third was not password protected but, didn't appear to be connected to the network.
- Three modems appeared to belong to our centralized remote dial-up system
- 26 did not provide a recognizable response and were found to be connected to Heating Ventilating and Air Conditioning (HVAC) or other equipment and used to monitor the status of fluid levels and other like metrics.

Our Response
Short Term
We immediately identified the owners of the systems with pcAnywhere installed and made sure these systems were password protected. We followed up with the Networking staff and the AS/400 operators to remind them to turn off modems when not in use.

With the information provided by Telecom and the results of our war dial, we also started to develop an inventory of analog lines and modems in use through out the company and began to determine the who, what, where, and why of the modems that had been identified. In doing so we established a procedure to follow-up with modem/DID/analog users/owners to identify the following:

- If the line is still being used, why?
- The internal person to whom the the analog line has been assigned and/or the individual who is responsible for the system the modem is connected.
- The system or device connected to the modem and the function it performs.
- The source numbers of inbound calls and destination numbers for outbound calls.
- The name of the person and/or organization who is calling or being called and the purpose.

Longer Term
We also identify two additional longer term courses of action.

The first was to research cryptographic modems or handshake devices that could provide greater protection for the system running pcAnywhere. After reviewing several products we finally decided on the Challenger P2 system from Computer

Peripheral Systems as a possible means to enhance security of our dial-in modems. These are neat, inexpensive devices that connect to the analog line of a modem and operate on a LOCK and KEY principle. Any time a call is initiated that doesn't have the appropriate LOCK or KEY combination, the call gets blocked. 6

We purchased a couple of these and found they worked as advertised. Our initial thought was to implement them on the systems with pcAnywhere and maintenance modems to further control who could access them.

The second was that we needed to find a more robust scanning tool if we were going to continue scanning on a regular basis. ToneLoc worked all right, but we really needed something that wouldn't lockup. When we started our research, there were basically two products on the market PhoneSweep, from SandStorm Enterprises, Inc., and TeleSweep, from SecureLogix. Both products looked like they would do what we needed and we probably could have went with either one. That is, until SecureLogix offered to give an on-site presentation on a new product they were introducing called TeleWall that they described as a firewall for telephone lines. Needless to say, once we saw it, we were hooked.

Note at that time TeleWall was the only product of this kind on the market. Since then we believe another similar product has been introduced called the Phonewall 20 phone firewall, by Sentry Telecom Systems Inc.

Firewalls for Phone Lines

In his paper "Sorry, Wrong Number", Gregory B. White, Ph.D. provides the following excellent explanation of how Firewalls for phone lines work.

> A telephone firewall works in a similar manner to a traditional data-network firewall, except rather than filtering based on Internet addresses, the telephone firewall regulates communication based on telephone numbers. Instead of enforcing security policy based on the type of service, telephone firewalls enforce policy based on the type of call being made (i.e., voice, data or fax). This allows an organization to block traffic to or from certain numbers, or to block calls that don't follow established organizational security policies. 7

The TeleWall system consists of a management server, one or more clients, and distributed sensors that connect to the phone company side of the Private Branch Exchange (PBX) and identify calls as voice, data, or fax in real time. In addition it provides the capability to automatically enforce security policies by logging, alerting, or terminating calls based on identifying characteristics such as call type (voice, data, or fax), source or destination number, or call direction (inbound or outbound). 8

Installation and Initial Use

Our initial installation of TeleWall was performed in April of 2000. It consisted of 1 management server, 2 clients, and 8 sensors, (7 T1 and 1 Integrated Services Digital Network Private Rate Interface (ISDN PRI)) to cover the various inbound and outbound T1 lines at each site. Installation required several days because sensors had to be installed at 4 different sites in 3 states. Please refer to the diagram in Appendix B.

The only problem we can remember from the installation was caused because we ordered an ISDN PRI sensor for Site 1 by mistake. Site 1 was was the only site that had an ISDN PRI line installed, so we presumed it would need an ISDN PRI sensor. Unfortunately, we found this wasn't the case. Our current PBXs can't handle ISDN PRI lines, so we have to run them through another box (an Adtran Atlas 800) which converts them from ISDN PRI to a standard T1 which our PBX can handle. As it turned out, we had to replace the ISDN PRI sensor with a T1 sensor in order to get everything working.

For the first month we pretty much just ran the system in log and monitor mode so we could become familiar with it and configure the management server and sensors properly. We also spent time updating our inventory of analog lines and modems as new lines were being identified daily.

Once we were comfortable with the information we were receiving and our inventory list, we started adding rules to our policy to terminate or alert on different types of traffic as we identified them in reports.

Rules within TeleWall are simple to create and can be set up based on the following criteria:

Call Direction = Inbound or Outbound
Source = Any, Individual numbers, or groups of numbers
Destination = Any, Individual numbers, or groups of numbers
Call Type = Any, Modem, Voice, Fax , or Secure Telephone Unit (STU)
Time = Any, or specific time
Action = Allow or Terminate
Track = Identify, log, penetrate, realtime alert, SNMP alert, email alert
Install On = Any, or specific sensors

One to the first rules we created was to terminate incoming modem traffic to the auto attendants on our phone systems. Per the Telecom department there was absolutely no reason why those numbers should be receiving modem traffic. Unfortunately, at that time we didn't have caller ID at the corporate site; thus, we were unable to determine the origin of the calls.

Next we implemented rules to terminate voice and modem traffic to fax numbers. This caused a few problems because a few fax machines were getting categorized as modem traffic and terminated when they switch into High Speed

Fax mode. For a temporary solution we eliminated those numbers out of the rule.

This was followed by a rule that terminates outbound calls to numbers belonging to ISPs and so on.

Need for Policies

Around the time we started terminating calls, we realized we needed a policy or procedure to let employees, know there were new rules regarding modem usage. Thus, the **Procedure for Modems** procedure was developed to document the procedure for requesting a modem line, using a modem, and enforcement of modem usage. See Appendix A, for the full text of the pertinent portions of this procedure.

In conjunction with the Procedure for Modems, we developed a **Standard Modem Security** email that we send out anytime a new number is identified in the reports or we identify someone in violation of established procedures. In essence, the procedure states the following: (1) We have a new tool that allows us to monitor the phone system for unauthorized modem activity, (2) A potential violation has been identified, and (3) access will be terminated unless we are contacted. See Appendix A, for the full text of the pertinent portions of this email.

We also initiated the development of a Lotus Notes Modem Request database created which will become the primary means by which requests for modem lines will be submitted, authorized, and tracked. This database is now in the final stages of testing and should be rolled out soon.

Enhancements

One of the things we realized early was the need for caller ID in order to take full advantage of the features offered by TeleWall. With caller ID, you can you can terminate based on the source number of inbound calls. It's also much easier to to trace a calls origin.

In addition, we found we had a gap in coverage at our corporate site that was causing us to miss local traffic. There were two local Central Office (CO) trunks between our corporate site and the CO which handled our local traffic without sensors.

As soon as it was economically possible, we order the necessary equipment and sensors to upgrade the inbound T1 and the CO Trunks at our Corporate site to ISDP PRI. This upgrade was completed in February, of 2001 and has provided visibility to a amount of activity that we weren't even aware we were missing. Please refer to Appendix C for a diagram of our current configuration.

We've also performed two upgrades of the TeleWall system taking us from Version 1.0 to 2.1.1

Current Usage

We currently monitor TeleWall just like any other intrusion detection system. The system alerts via email on calls that look like possible intrusion attempts or that fall outside of normal operating activity. We follow-up on these with either an email if the activity was terminated (to let the individual know it wont work unless they contact us), or with phone calls and personal visits if warranted.

Our current policy has grown to include 11 rules that are as follows:

Default Rule
Allows and logs any outbound emergency numbers.

Rule 1
Terminates, logs, and alerts on any outbound calls to known ISPs.

Rule 2
Allows and logs on any outbound calls to approved modem numbers.

Rule 3
Terminates, logs, and alerts on any outbound modem calls for sites 1 and 3. We had to exclude the corporate site and site 2 because of the High Speed Fax issue noted earlier. SecureLogix has plans to fix this issue in a future release, so for now we monitor the logs and follow-up for those two sites.

Rule 4
Allows, logs and alerts on inbound modem traffic to modems connected to our site physical security systems. We generally know when calls will be coming to these systems and turn the modems on.

Rule 5
Terminates and logs on inbound fax or modem calls to specific voice lines. These are numbers that we know should not be receiving modem traffic.

Rule 6
Allows and logs inbound modem traffic to authorized modems.

Rule 7
Allows, logs, and alerts on inbound modem traffic. This rule is being used to identify modems. When we receive an alert we follow-up and either add the modem to the approved modems group in Rule 6 or add it to Rule 5 so calls are terminated.

Rule 8
Allows and logs on inbound Fax traffic to approved fax numbers.

Rule 9
Allows, logs, and alerts on inbound modem traffic to approved fax numbers. This allows us to identify and follow-up on modem calls to fax numbers that fall outside of normal usage. Most of the calls that are logged are from repeat numbers that we now recognize. We plan to create a separate rule for the High Speed faxes and then block modem traffic to all other fax numbers.

Default Rule
Allows and logs any other inbound traffic.

We average about 180 modem calls a day of which 5 on average are terminated. Typical alerts include auditors attempting to dial out from conference rooms, copier repair persons attempting to connect from fax lines, contractors attempting to connect to ISPs or their home office, employes attempting to connect to ISPs, or contractors going of the deep end as noted in our earlier example.

The important thing to note, is we get alerted as soon as the call happens and can them make a determination of the appropriate course of action.

Future Plans

We plan to populate the Modem Request database with approved modems from our inventory and roll it out along with the Procedure for Modems procedure. We also plan an awareness campaign and a grace period so everyone will be aware of the new procedures and have an opportunity to comply.

Once the grace period is up we plan to implement blocking of unauthorized inbound and outbound modem traffic where possible. There are a few instances were we will not be able to block inbound modem calls based on source. Examples of this would include call from areas that do not provide caller ID or specific pieces of manufacturing equipment which are supported by external contractors who may have to call in from anywhere at any time. Thus, we cannot effectively include all source numbers.

For instances where we can't block using TeleWall, we will investigate using the the Challenger P2 boxes to supply an additional layer of protection.

When time permits we plan to implement TeleSweep secure and integrate it with TeleWall as an added precaution.

When our budget permits we may upgrade to ISDN PRI lines at the 2 remaining sites that don't currently have caller ID.

Summary

We've come along way since we first started. We now have a good inventory of all the active modems in use throughout the organization. We've got policies and procedures ready to put in place. We have a good tool that will allow us to monitor and enforce our policy.

With these tools in place, we believe we have drastically minimized the risk associated with modems and trust others can benefit from our experience and greenhorn initiative.

References:

Cited References:

1. White, Gregory B., Ph. D., "Protecting the Real Corporate Network", 19 June, 1999, URL: http://www.esecurityonline.com/download/whitepaper/SL-TR-99.pdf (30 April, 2001)

2. Ranum, Marcus, J., "Thinking About Firewalls V2.0: Beyound Perimeter Security" Proceedings of Second International Conference on Systems and Network Security and Management (SANS-II), April, 1993 URL: http://pubweb.nfr.net/~mjr/pubs/think/ (30 April, 2001)

3. Livingston, Joe, "The Desktop Modem Threat", SANS Information Security Reading Room July 27, 200, URL: http://www.sans.org/infosecFAQ/firewall/modem_threat.htm (30 April, 2001)

4. Engineering Department of SecureLogix, "TeleWall System Technical Overview", 26 September, 2000, 1

5. White, Gregory B, Ph.D., "A Common Weak-Link in the Security Chain", URL: http://csrc.nist.gov/nissc/1999/proceeding/papers/p35.pdf (40 April, 2001)

6. Computer Security Peripherals, Inc., URL: http://www.cpscom.com/dsecure.htm (30 April, 2001)

7. White, Gregory B. Ph.D., "Sorry, Wrong Number",

URL: http://www.mit-kmi.com/Archives/4_7_MIT/4_7_Art5.cfm (30 April, 2001)

8. Engineering Department of SecureLogix, "TeleWall System Technical Overview", 26 September, 2000 2

Other References Used but Not Cited:

Davidson, Bob, "Telephone Network Security", December 1, 2000 Edition of Network Reliability, URL: http://www.americasnetwork.com/issues/2000supplements/20001201nr/nr20001201_security.htm (30 April, 2001)

Avolio, Frederick M., Firewalls: Are We Asking Too Much?, URL: http://www.spirit.com/CSI/Papers/fw-ask2much.html (30 April, 2001)

CCA & Associates Co., Ltd, "How Modems Compromise Network Security", Security Issues, Last modified: January 03, 2000 01:07:03 AM, URL: http://www.ccaassociates.8m.com/security.htm (30 April, 200)

Skoudis, Edward, "Tools of the Trade", URL: http://packetstorm.securify.com/docs/infosec/tools.of.trade.htm (30 April, 2001)

Threat, Minor & Maas, Mucho, "ToneLoc v0.98 User Manual", URL: http://www.textfiles.com/hacking/tl-user.txt (30 April, 2001)

Product References:

PhoneSweep, SandStorm Enterprises, http://www.sandstorm.net/phonesweep/

TeleWall, SecureLogix, http://www.securelogix.com

Challenger P2, Computer Security Peripherals, Inc., http://www.cpscom.com/dsecure.htm

Phonewall 20 phone firewall, Sentry Telecom Systems Inc. http://www.sentrytelecom.com/index.asp

pcAnywhere, Symantec, http://www.symantec.com/pcanywhere/

Appendix A Policy References:

COMMUNICATIONS SYSTEMS SECURITY POLICY

STATEMENT OF POLICY:
It is the policy of ABC to insure that the level of security for all communications media, including without limitation, telephones, computers, modems, facsimile machines, teletypes and mail service, is sufficient to; achieve optimum service, reliability and compatibility while protecting physical and intellectual assets, insure confidentiality of information, and preserve the integrity of the information being communicated.

PURPOSE:
To insure that all information being communicated outside the company is being transmitted through proper procedures.

Appendix A Policy References:

COMPUTER HARDWARE AND SOFTWARE APPROVAL POLICY

STATEMENT OF POLICY:

Capital requests, standard and non-standard purchase requisitions and evaluations for computer hardware and software need to be approved prior to obtaining a project/purchase order number. All computers and all software need approval except:

1. Hardware that is used solely to "Functionally Control" a piece of equipment or is on the approved list of equipment hardware.

Definition of Functionally Control: The operations required to make the piece of equipment perform the actions to be able to produce product.

PURPOSE:

1. To allow for effective support and maintenance / upgrades.
2. To ease integration of data/information and minimize training expenses.

Appendix A Policy References:

ELECTRONIC DATA AND NETWORK CONNECTIVITY POLICY

STATEMENT OF POLICY:

It is the policy of ABC Corp Inc. (ABC) to ensure correct procedure is followed when any electronic data is accessed or shared, or any connection is made to, from, or within corporate network facilities or resources. Connections to ABC network facilities or resources shall be allowed only after receiving appropriate Corporate Business Systems management approval. ABC shall provide and support these facilities or resources for work-related use only. Any non-compliance with the appropriate procedure shall constitute a violation of this policy.

PURPOSE:

To achieve optimum service, reliability and compatibility, throughout ABC's network infrastructure.

To protect physical and intellectual assets and ensure security and confidentiality of information.

To preserve the accuracy and integrity of information being communicated.

To address corporate responsibilities regarding the use of ABC property.

Appendix A Policy References:

Computer Security Specification

1.0 Purpose
The purpose of this specification is to provide detailed guidance for protecting ABC computing resources and the information they process against unauthorized access, misuse, and abuse. This specification supplements the ABC Information Protection Policy.

2.0 Scope
This document is applicable to all employees, contractors and suppliers of ABC who use computer hardware, software or applications to create, manage, process, maintain or distribute ABC information assets.

3.0 Requirements
3.2 COMPLIANCE

This specification applies to all employees and contractors of ABC. It also applies to all ABC computer systems, computer-based tools, computer applications and network components, to the extent permitted by the technology involved, business risk, cost of conversion and complexity of change.

Individuals who intentionally violate the word and/or intent of this specification shall be subject to disciplinary action up to and including termination, in accordance with HR Corrective Action guidelines.

3.11 PROTECTING EXTERNAL NETWORK CONNECTIONS

DIAL-UP
Dial-up access into ABC computer systems shall be secured to prevent unauthorized access to stored data and connected networks. The chosen method for securing ABC dial-up shall be robust and highly resistant to unauthorized penetration.

INTERNET
Concurrent connection with an ABC network and the public Internet is prohibited unless the Internet access is processed through the ABC-owned and controlled security firewall. For example, employees shall not access the public Internet directly via modem from their workstation.

Connections between the ABC network and the Internet shall be protected by a robust, tested and maintained security firewall. The firewall shall be diligently monitored to detect security breaches, penetration attempts and any unusual network activity.

Appendix A Policy References:

Proper Internet Usage Specification

1.0 Purpose

This specification is intended to provide ABC employees with guidance necessary to facilitate their use of the public Internet in a secure and professional manner.

2.0 Scope

All PC users who utilize the Internet.

3.0 Requirements

EXPECTATIONS:

All traffic to and from the Internet shall travel through the approved ABC firewalls. The firewalls present secure points of entry into the ABC network and essentially form funnels through which all Internet traffic shall pass. The firewalls and their associated servers enforce ABC security policies and access control decisions for traffic coming from or going to the Internet. Any activity which bypasses the ABC firewalls shall be authorized, in writing, by CBS management, and shall be secured against external threats to the ABC network.

SAFEGUARDS:

The Internet is a collection of technologies (e.g., computers, communication links, local area networks and transmission protocols) that form a huge communication backbone that spans the globe. **None of these components can be considered trusted.** In addition, there are inherent vulnerability's in these components that are routinely exploited over the Internet. As a result, ABC regards the Internet as an unsecured network.

ABC protects its internal network from the known exposures associated with the Internet through the use of security firewalls. The firewalls allow ABC employees access to the Internet while restricting access from the Internet into ABC's internal network.

Concurrent connection with the ABC network and the Internet is prohibited unless the Internet access is controlled through ABC's firewalls. Necessary business activities which are incompatible with the ABC firewalls shall be approved in writing by CBS management, and shall be secured against threats to the ABC network.

Activities that bypass gateway security protections are prohibited because they expose the internal network to uncontrolled security risks.

Appendix A Policy References:

Procedure for Modems

1.0 Purpose
To establish written guidelines for the protection of modems against unauthorized telecommunications access to ABC's network

2.0 Scope
This documents the procedure for requesting a modem line, using a modem, and enforcement of modem usage.

3.0 Tasks and Responsible Function

3.1 **New Modem Requests**

3.1.1 All requests for new modems lines shall be submitted to Corporate Security for review and approval.

3.1.1.1 Requests shall include individual and/or department requesting a modem.

3.1.1.2 Reason for connection.

3.1.1.3 Destination name(s), location and phone numbers the modem will be connecting to outside of ABC and phone numbers that will be connecting to ABC.

3.1.2 Corporate Security will inform the appropriate site telecommunications technician when a modem request is approved.

3.1.3 Phone numbers not provided to Corporate Security will be blocked by ABC's telecommunications firewall until applicable information is received.

3.1.4 A strong password must be used when using any remote access systems, ie. (PC Anywhere).

3.1.4.1 Passwords should be 7 characters in length, and include special characters, ie. (! @ # $ % ^ & * : +)

3.1.5 Users shall notify Corporate Security with any changes to their original approved list of numbers.

3.1.6 Corporate Security must be notified when a modem is no longer needed.

3.1.6.1 Corporate Security will notify the appropriate telecommunications technician to remove the number from the PBX system.

3.2 **Enforcement**

3.2.1 The Corporate Security department shall monitor compliance to this specification.

3.2.2 Periodic scans shall be conducted to ensure only authorized modems are present and secure passwords are being used.

3.2.3 In the event a security breach is detected, Corporate Security shall disconnect any compromised and/or noncompliant device.

4.0 Application

This procedure shall be followed when requesting a modem line, using a modem and enforcement of modem usage.

Appendix A Policy References:

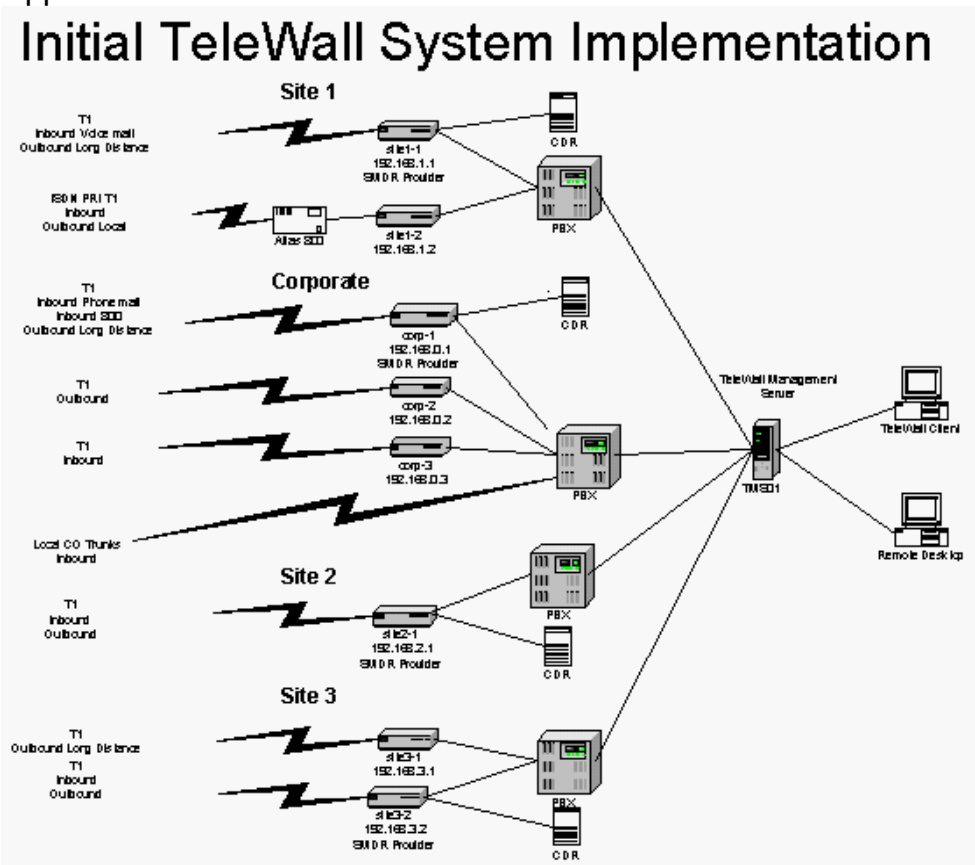
Modem Security Email
Corporate Security recently deployed a new telephone firewall monitoring tool that will allows us to protect against unauthorized telecommunications access to ABC's network. Unauthorized modems connected to networked computers can provide connectivity internally for outsiders such as hackers. This new system, TeleWall, will also allow us to identify and block various call types, ie. (voice, modem, fax) as they happen.

Current reports indicate that you have either initiated and or are receiving modem calls. To ensure that uninterrupted service is maintained, please list all modem numbers you connect to outside of ABC. Your list should also include company name and reason for connection. If you receive modem calls from the outside, please list the number and company you receive calls from and reason for connection.

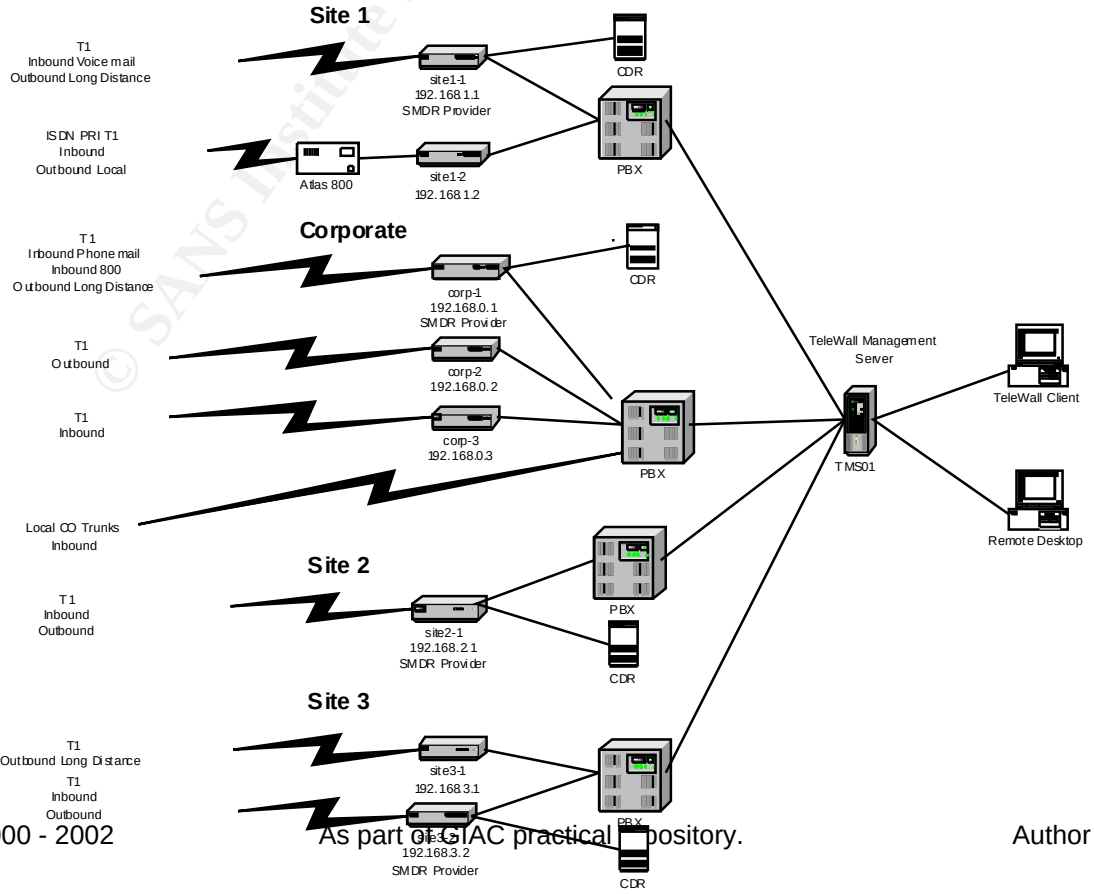
Numbers not given to Corporate security will be blocked until information is received. Thank you for your prompt attention to this matter.

If you have any questions you can contact your helpful security administrator.

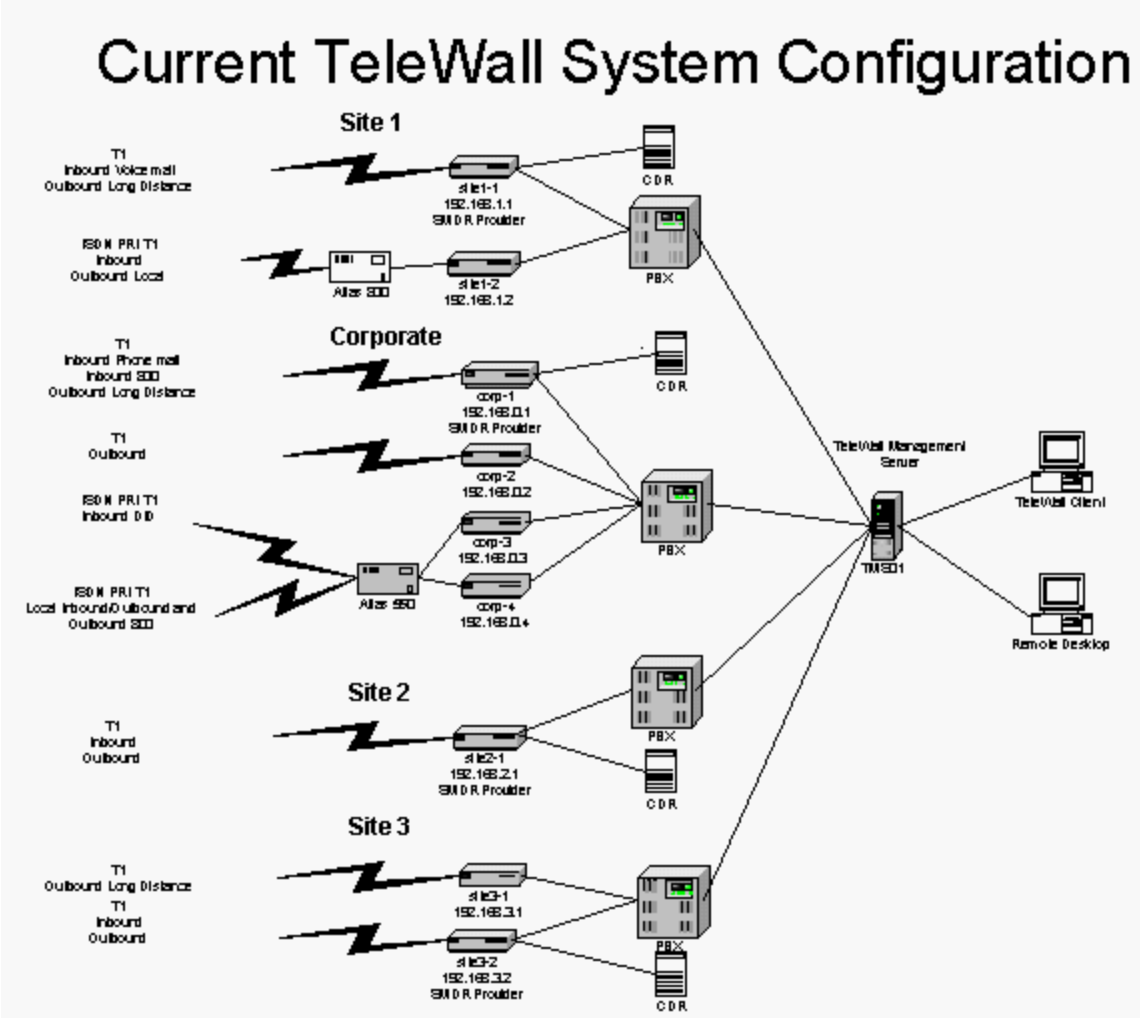
Appendix B



Initial TeleWall System Implementation



Appendix C



Current TeleWall System Configuration