Global Information Assurance Certification Paper

Mitigating IT Security Risk Through Outsourcing
In a Mid-Sized Financial Institution

Abstract

In the Banking Industry, as in many other industries, mid-sized companies often find themselves in a quandary when trying to balance cost vs. effectiveness of technology infrastructure solutions, including security. While these companies are not large enough to build and maintain all of their systems in-house due to such factors as economies of scale, staffing restraints and budgetary limitations, they are too large to depend entirely on third parties for this support. As the use of technology in financial institutions has evolved, the exposure to security risks has increased and the Regulators have focused their scrutiny on the overall mitigation of these risks. As our company's risk assessment process was refined and we found ourselves in need of providing "high risk" services to our customers (Internet Banking) and to our employees (direct Internet access, E-mail, etc.), it was clear to both our Business management and our IT management that we could not safely and cost-effectively provide the infrastructure, security and support that would be needed in house without significant increases in staffing and the corresponding personnel issues that are associated with that level of staffing. Our ultimate solution was a hybrid approach where we made the maximum use of our own staff to develop and implement the "internal" security policies and processes combined with the use of three outside entities for three very specific functions. We selected Fiserv (an ISO 9001 compliant company) to host our Internet Banking system as they were already providing transaction processing for our customers. We selected Netsolve to provide management and monitoring of our firewall and Network Intrusion Detection Systems and we selected Bruck & Associates (BAI Security) to provide semi-annual penetration testing of our systems.

Our results have been quite favorable. In conjunction with our overall security policies, the strategy we developed has been a successful one. We have been able to accomplish 24x7 security over some very sensitive systems without the additional staff and expertise that would be needed to manage these functions in house. We have been able to leverage the knowledge of our service provider partners to help us gain an understanding of the risks present in these systems where they connect to the public network. We have been able to focus on the process rather than the technical details and that has helped us to provide a more safe and secure environment. Our internal and external auditors, as well as the Federal Bank Examiners have repeatedly reviewed our process and have found it quite satisfactory in meeting their guidelines.

Outsourcing Internet Security in a Financial Institution

Submitted By: **Raymond Wanser**
December 24, 2003
GSEC Assignment 1.4b

BEFORE

Current IT Environment

Beginning in the late 1970's, our bank was typical of other financial institutions as an early adopter of on line transaction based systems. These systems began as completely closed private networks dedicated to servicing the needs of the employees of those companies (tellers, accountant types, etc.). They then evolved to include proprietary ATM networks for serving our own customers and then evolved yet again through the 1990's into shared ATM networks to service other financial institution's customers at our ATM's as well as our own customers at other Financial Institution's machines. All of these systems had one thing in common, they relied upon secure private communication channels such as Point-to-Point circuits and frame relay technology.

Our Information Technology Strategic Plan, a document that was updated annually and approved by our Board of Directors, outlined our overall strategy to rely on proven third party providers of processing services, whenever feasible and appropriate, and to augment those services with our own IT infrastructure. Our retail account transaction processing was "outsourced" to one of the Fiserv companies, incorporating their mainframe security environment into our overall security policy. This arrangement, as were all of our third party provider relationships, was managed in adherence to our internal IT security policy and to the guidance provided in OCC Bulletin 2001-47, "Risk Management Principles in Third Party Relationships". During this time period, the vast majority of transactions were performed by employees of the bank, not directly by our customers. The two exceptions at this time were ATM transactions and so-called telephone banking transactions.

ATM transactions were enabled through our own private, frame relay network purchased through and managed by Mellon Network Services. This system provided access for our own customers to their accounts at our bank. The ATM network relied on two levels of security; the customer PIN was generated and calculated using the proprietary Atalla algorithm which was a one way cryptography methodology that relied on using pre-encoded card information combined with customer entered PIN to generate a "result". That result, calculated and stored on the host when the PIN was issued, was used to authenticate the ATM user. In addition , all of the data packets sent to and from the ATM were encrypted using DES, and later, Triple DES encryption. Since the mid-1980's, banks have recognized the value in sharing ATM locations as a way of improving availability of their service, so this private ATM Network was linked via host-to-host link with a national shared ATM network (Star System). This link allowed our customers to initiate transactions at other member financial institution's ATM's as well as allowing other financial institution's customers to use our ATM's to access their accounts. These inter-network transactions were

transported over private networks and were encrypted using Triple DES for security.

So called "Telephone Banking" transactions were accomplished through a proprietary, dedicated server running the IBM OS/2 Operating system and Voice Response Software from a company called Intervoice. The server connected to our host system using 3270 emulation that would mimic the keystrokes of a human operator in a very limited set of transactions. Customers had to be set up in advance by an authorized employee at the bank and the transactions were limited to inquiries and transfers between internal accounts. Security over the dial up was a simple user ID assigned by the bank and a password selected by the customer during their initial sign on.

Prior to the project, our transaction network (for non-ATM transactions) was a separate private line frame relay network with no access to public network or infrastructure. This was typical for most bank networks at this time. Our e-mail, such as it was, was primarily internal with periodic batch exchanges with our Internet E-mail Provider. These exchanges were accomplished with a dial-up account, using a product called CC-Mail (Lotus Development Corp), and were performed at regular 2 hour intervals throughout the work day. No exchanges took place after hours. Our internal LAN/WAN was made up of 80 separate LAN's connecting some 1500 PC workstations, primarily used for host access (using 3270 emulation software) and general office applications with file and print servers for storage of data. There was no direct Internet access from within the LAN/WAN. We did provide a number of stand alone PC's with dial up access to the Internet for some specific bank related activities including appraisal databases, credit agencies and investment databases.

External Forces Creating the need for change

That summarizes our network environment up until the mid to late 1990's when a number of forces were exerting pressure on our bank and banks in general to change their way of thinking and operating. Industry pressure to provide new services and delivery channels was coming from increased competition brought about by deregulation of the Financial Services Industry. Suddenly we were faced with competition from non-traditional sources (insurance companies, brokerage houses, internet only banks) and it was clear that our approach to the business had to change or we would not survive. Consumers were becoming very Internet aware and were looking for convenience that could not be provided through normal brick and mortar channels. Our own work force was becoming more mobile and that put pressure on the IT group to deliver infrastructure that would support that mobility and enhance their ability to perform their job functions, wherever they were. IT costs, especially data communication costs, were rising dramatically. It was clear we had to expand our ability to communicate electronically and that meant finding more efficient channels that could be deployed in a secure environment.

An internal task force was created to address these needs. Members of the task force came from Executive management, Internal Audit, Information Technology and the various business units in the company. The first job for the task force was to define what system functions would be implemented based on the current and foreseeable business needs. The basic goal was to come out the other end of this process with systems and infrastructure that would enable us to offer products and services to our customers that satisfied their needs for a more responsive bank and to enable our staff to take advantage of resources available outside our internal network that would make them more productive. As a financial institution, we had to pay careful attention to any Regulatory or Compliance issues related to these implementations. Internally, we placed requirements on ourselves to develop formal project plans for all implementations, to carefully examine all security issues related to the new functions and to develop all Security Policies and Procedures in accordance with Regulatory requirements as described in the FFIEC Information Security IT Examination Handbook and general industry accepted practice.

DURING

The first phase of the project was the System Selection process. This required two lengthy steps including each business unit's evaluation of the functional requirements and a complete IT Risk Assessment for each business unit addressing both existing functions and functions being added in this process. The functional requirements were developed by the operational business managers in conjunction with the IT group and Internal Audit. The IT Risk Assessment was also performed by each operational manager and was headed up by our corporate Data Security Officer. The purpose of this risk assessment, as part of our overall Information Security Program, was twofold: first, to determine the overall level of risk in information assets (data) and the technology that processes, transmits, and stores them; second, assess the risk to any nonpublic personal information involved in each department's processes as mandated by the Gramm-Leach-Bliley (GLB) Act of 1999. Each process required an evaluation of High, Medium, or Low in three areas of risk: Integrity, Confidentiality, and Availability. In addition, this assessment required that we describe any mitigating controls that tended to reduce these risks and then establish an overall risk rating for each process after taking into account the mitigating controls that were described.

When all of the functional requirements and the IT Risk Assessment were completed, the Task Force reviewed them and developed an action plan to implement the following functions and systems:

- Create a public network access point in our internal network for email and employee Internet access

- Create an Internet Banking transaction site for our Retail Banking Customers
- Develop a relationship with an outside company to provide assurance on a periodic basis that our internal network was secure from outside intrusion

In adherence to our IT Strategic Plan, the Task Force first looked for ways to leverage the use of outside providers to supplement our internal staff and to limit the need for hiring additional staff. The process involved functional RFP's sent to several companies for creation of an Internet access point in our WAN and another RFP sent to several companies with the ability and expertise to host and manage our Internet Banking Transaction site. We already had an Internet Marketing site and it was decided to leave that in place for the time being. The final project for the Task Force, finding a company to perform periodic penetration testing, was put on the back burner while the first two phases were being executed.

System Implementations

The outside piece of the project to create a public access point to our Internal Network for Email and Employee Internet Access was eventually awarded to NEC Business Network Solutions. The primary reason for their selection was their ability to provide support for the entire project including engineering the network design, providing direct access to the equipment needed, providing implementation services and support and providing ongoing Intrusion Detection System management and monitoring through their Netsolve affiliate.

Once the security hardware decisions were made (Cisco PIX firewall and NetRanger IDS), we began the concurrent process of developing the configurations for this hardware and the implementation of the systems that would make use of this Internet connection. An overview diagram of the Internet connection is included in this document as *Appendix A*. For E-mail, we decided to migrate away from our existing Lotus CC:Mail to Microsoft Exchange and Outlook. With the addition of Internet access, it was also decided to install a system for monitoring employee usage and restricting access to sites that were deemed to be undesirable in our corporate environment. For this purpose, we chose a system called WebSense that would allow us to perform these functions seamlessly and, at the same time, we developed an employee Internet Usage Policy that was very specific about the permissible use of the Internet on Corporate Computer assets.

For any of these implementations to be considered successful, it was imperative that the security of that Internet connection was as solid as we could make it. Although we had already decided not to host any Internet sites on our internal LAN, we knew we would still be vulnerable to significantly greater risks than when we were operating entirely on private networks. The first step in this process was to acquire a high bandwidth connection from our primary data

center to our Internet Service Provider. In addition, we acquired a second high bandwidth connection to a completely different carrier for disaster recovery purposes.

While this was underway, we began to work with Netsolve to develop the firewall policies that would be installed on the PIX 525. This was a lengthy and detailed process that was led by their security engineers and was ultimately approved by our IT management and the Task Force. Since this was a new technology discipline area for us, we relied heavily on the process developed by Netsolve that included extensive questionnaires regarding our planned use of the Internet connection. Their process was based on "deny all except for that which is specifically allowed" and, while that created a significant amount of extra work, especially in he early stages, that method has proven to be very secure. A mock up of the actual firewall policy document is included in *Appendix B* of this document. After the initial configuration was agreed upon, it was installed in the firewall and the firewall was connected to the Internet. At this point, the firewall was still physically disconnected from our internal network and only the Intrusion Detection devices and a stand alone device in both the DMZ and the internal port of the firewall were attached. Part of Netsolve's process was to expose this basic setup to the Internet and run some remote scans of the firewall to look for vulnerabilities. During this time, all activity is logged to the log host and the log files are carefully examined to look for potential problems. This period also allows the normal "hacker" activity to begin to act on the firewall so that we could determine the initial level of effectiveness.

While these steps were underway, another team was implementing the e-mail solution using Microsoft Exchange and Microsoft Outlook as the E-Mail client. Using the design specifications provided by Netsolve, we built and isolated a "DMZ" between the public network and our internal LAN. We deployed a mail relay server in the DMZ to protect our actual e-mail servers even further. In addition, we deployed an Internet URL filtering server running software called Websense.

One of the critical components of this entire exposure to the public network was the implementation of a comprehensive virus protection system behind the firewall. At the time, when we examined all of the available products that were suitable for corporate networks, we decided to deploy the McAfee Anti-virus Suite. This suite had specific modules for client workstations, NT servers, Novell servers and, most importantly, for the Microsoft Exchange Information Store. All of these server products were integrated such that the periodic updates could be performed using the same repetitive process and the individual client workstations could be set up to automatically update as well. In addition, client machines could be locked down to prevent any tampering with the AV capabilities and processes.

When we were satisfied that all of these protections were in place and working smoothly, we began the final step of connecting the internal LAN/WAN to the Internet through the firewall. Before we could set this in motion we spent another week developing our liaison functions with Netsolve. That included developing a hierarchy of potential security violations and detailing exactly what steps would be taken by the vendor and what steps would be the responsibility of the bank. This meant identifying various attack scenarios and determining whether simply reporting the activity, shunting a particular IP address, shutting down a particular port or possibly even the entire gateway would be the appropriate response for each. It also included a precisely described decision making matrix with names and phone numbers clearly identifying the responsible parties.

At this point we were ready to activate the connection between the Internet and our internal LAN/WAN. Our end users still did not have an Internet browser installed on their workstations so we were only really enabling the e-mail link to the outside world. Our company policy required that any employee who needed Internet access would have to obtain written approval from his/her manager defining the business need for that access. When that authorization was in place and the employee read and signed the newly developed Internet Usage Policy, the IT department would install the appropriate browser on that employee's workstation.

The second big project that was running concurrently with the Internet connection was the development and deployment of an Internet Banking web site for processing a limited set of transactions for our Retail Banking customers. The Task Force had already decided that trying to put up a web site on our own that was capable of performing the transactions we needed and the interfaces to our host systems was not feasible either financially or from a resource perspective. So, as was our strategic direction outlined in our Strategic Plan documents, we sought this service from outside providers. While we sent out Requests for Proposal to three companies, it was clear that, since Fiserv already processed our host based customer transactions, it would make sense to use their Internet Banking solution if it met our business objectives. As we expected, they already had the interfaces built into their host systems and several of their customers were already using both the host based and web based systems simultaneously. We still made a careful evaluation of the offerings from all 3 vendors but ultimately decided that all other things being essentially equal, we would save considerable time and money by using Fiserv.

We were, of course, very concerned about the security of the Web site so our first criteria for evaluation of the system was security. The system we selected was built on a platform from Hewlett Packard called the HP Virtual Vault. At that time, it was considered one of the most secure platforms, based on a TCSEC (www.itsecurity.com/dictionary/tcsec.htm) B2 Trusted version of the HP UX 10 OS. In addition, the system was protected by a firewall that was equipped with a sophisticated Intrusion Detection System that was monitored 24/7. As a

supplement to our due diligence, the vendor received an independent certification from the TruSecure (www.trusecure.com/index.shtml) organization, as further testament to the layers of security around the web site. The application that was running on this platform was the industry standard Net Bank, which was, at that time, the premiere Internet Banking application on the market. It provided a complete set of customer initiated transactions including account inquiries, transfers between internal accounts and on-line bill payment provided by Check Free.

In designing the web site, we had considerable flexibility in page sequencing and page layout as well as various options related to security. We had to select such security options as user ID and password schemes, encryption levels, sign up methodology and transaction sets. We opted for features that leaned more toward security sometimes at the expense of convenience. For example, it would have been easier to allow automated customer signup but we opted for the more secure system that required a bank employee to verify all initial sign up information and to contact the customer directly with their initial password. We also opted to require 128 bit encryption which, at that time, created some problems for customers needing to update their browsers prior to using the system. We also opted for longer passwords, with a requirement for at least one number to be included in the minimum 8 character password. As we finished the design and building of the web site, we elected to use a three tier approach to the rollout. First a small group of 15 of the project team members, who had accounts at the bank, would be the initial beta test of the system. These members were selected based on their ability to really exercise the various components of the system. This phase of the testing lasted 60 days and was designed to find and correct as many problems as we could. After the changes necessitated by the first phase were implemented, the second phase of the implementation was begun, and the system was opened up to all bank employees (around 1,000) to sign up and use for 30-45 days. This phase was designed to fine tune the system and make sure that people who were not involved in the project had the chance to exercise the system. After this phase, we were ready to begin rollout to select customers who had already expressed a desire for the system and finally after another 30 day period, we opened the system up to general customer sign up.

The third part of the project, also running concurrently with the other two phases, was the development of a relationship with an independent outside organization for the purpose of performing periodic penetration testing of both our internal LAN/WAN Internet access point and our Internet Banking site. To that end, we interviewed 4 firms that were recommended by our External Auditors and looked at their ability to provide the services we needed, their track record with other companies, their flexibility in designing a testing program and, of course, their pricing. When the evaluation was completed, we selected BAI Security as the vendor of choice and began to develop that relationship. The initial work with BAI involved getting our network engineers and NetSolve's engineers to work

with the BAI staff to lay out the network and develop the plans for the scope of the penetration testing. Our objective was to do an initial test prior to opening up either our local LAN/WAN Internet connection or the Internet Banking site to production activities. Once BAI understood our environment, they spent a week designing the initial "attacks". BAI's process goes as far as determining if an attacker could do damage but does not actually do any damage. For the first test, we agreed to inform the host organizations and our third party IDS monitoring service that we were going to test and that the tests would take place some time within a two week period. We did, however, notify these vendors that future tests would be done unannounced but reiterated that no actual damage would be done during the process. The pre-implementation testing actually went very well. Because we had already engaged outside vendors to configure and deploy the firewall and IDS for both locations, these systems were very securely configured with all of the obvious protections in place. As a result of the initial test, we discovered some minor problems in our LAN/WAN firewall configuration and some vulnerabilities on two of our DMZ devices. After those were corrected, we went through the battery of testing again and passed without exception.

At this point, the Project Task force determined that we were ready to go live with all phases of the project and we sought and received executive management approval for that step.

AFTER

The post implementation period was divided into two distinct tracks; the business track, charged with reviewing the business outcomes of the newly implemented systems and the security track, charged with monitoring and managing the newly outsourced security functions. The business side was fairly straight forward and involved customer surveys for our Internet Banking functions and business process reviews for our internal system upgrades. These tasks were mostly managed by the business side while the security issues were left to the IT group working with Auditors and Regulatory Agencies.

During this post-implementation period we fine tuned some very important processes that were developed during the project. Specifically, the interface with the vendors providing network security monitoring and management became the focal point. We had already developed communication channels and written policies and procedures for dealing with security incidents, but these had to be continually reviewed and modified as the environment changed. It quickly became apparent that the public network was becoming a more dangerous place each day so we established a daily routine of reviewing security logs in addition to the instant alerts we were receiving for more serious events. This process, over time, gave us a clearer picture of the real threats versus the casual "script kiddies" that are so prevalent on the public network. In addition to our ongoing

monitoring of the public access points, we elected to perform semi-annual penetration tests using BAI. These tests would be performed unannounced and the results would be shared with our Internal Auditors as well as becoming a part of our annual examination by our Federal Regulatory Agency (OCC).

As the initial post implementation period passed, we performed a formal evaluation of the results versus the initial expectations as it pertained to the business solution and the security solution. The business activities were accomplished without exception and the resultant customer service and process improvements have definitely had the desired effect. From the security standpoint, we met our initial criteria of; (1) deploying these functions in a manner that would meet all the guidelines and standards of the industry and regulators, (2) use third party providers, wherever possible, to provide expertise that we could not provide internally without substantially increasing our staffing and costs and (3) develop a relationship with a different third party to periodically verify and monitor the activities of the original providers. Our regulators and auditors have examined our process, the third party processes and the penetration test schedule and findings and have given us high marks for the comprehensive approach we took. Our process, which included a complete formal IT Risk Assessment was used as an early model by the Regulators to demonstrate a sound process to other banks and financial institutions. Our Board of Directors and Executive Management were pleased with the outcome because we were able to deliver some sorely needed system enhancements safely and securely (or at least as safely and securely as we could reasonably accomplish) without increasing our bottom line expenses to any substantial degree. Our operations employees were pleased because they were now able to use the new capabilities to streamline their functions and our sales staff (bank branches) were pleased because their customers had new capabilities that were very desirable and would make their sales efforts easier in the future. For these reasons, we deemed the project had met all of the significant objectives.

In closing, while we developed and implemented a reasonably secure system, it is clear that there is no bullet proof system. Hackers and others are constantly upgrading their skills and tools and we continue to work with the Netsolve security engineers to upgrade our ability to detect and stop these attacks. We continue to train our employees so that they recognize “social engineering” scenarios as well as the importance of following all the recommended policies and procedures related to security. We require annual updates to our End User Computing Policy and an annual recertification by all employees. This whole security process is ongoing and has become a vital piece of corporate life in the modern world.

References

FFIEC, "FFIEC Information Security IT Examination Handbook", Dec 2002
http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html#infosec (10 Dec, 2003)

OCC, OCC Bulletin 2001-47, "Risk Management Principles in Third Party Relationships", Nov 2001
http://www.occ.treas.gov/occ_current.htm (9 Dec, 2003)

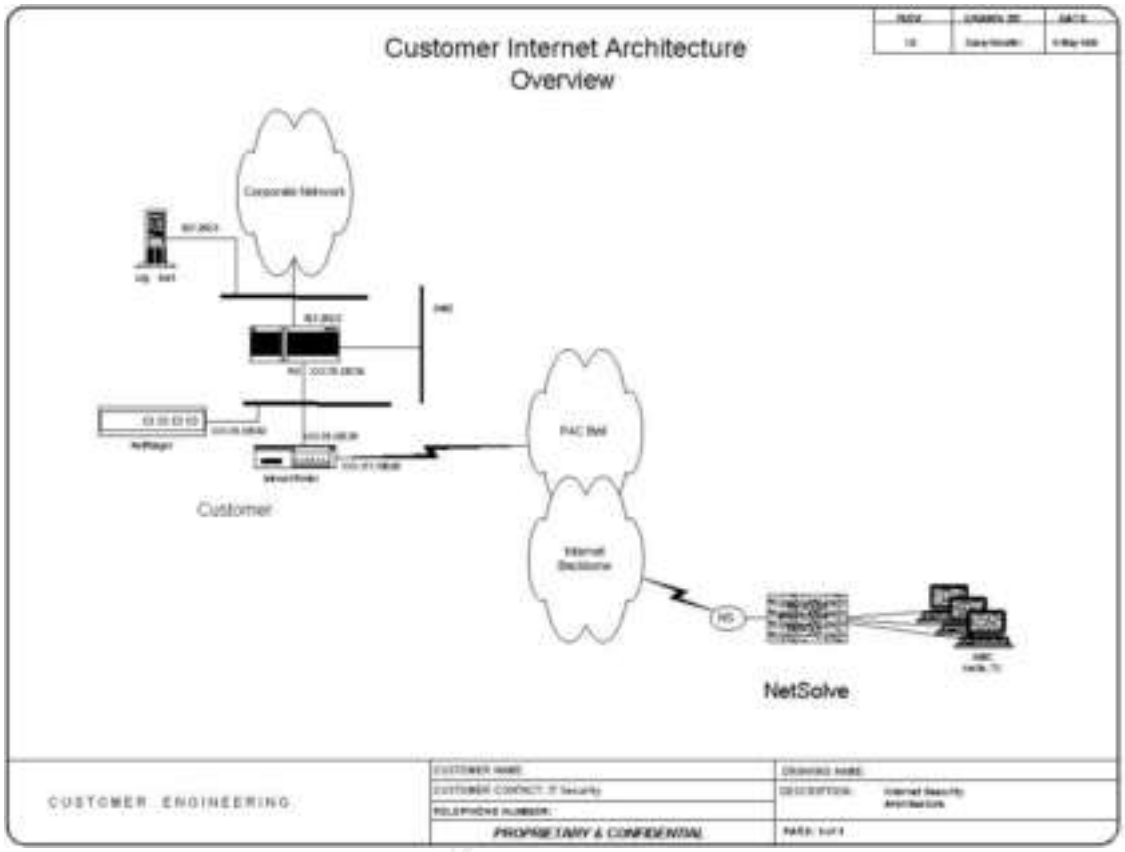
HP Atalla, "Atalla Network Security Hardware"
http://www.atalla.com (23 Dec 2003)

Intervoice Web Site, "Intervoice Technology solutions for financial institutions"
http://www.intervoice.com/solutions/industries/financial/ (20 Dec 2003)

US Senate, "Gramm-Leach-Bliley Act of 1999", Nov 1999
http://www.senate.gov/~banking/conf/confrpt.htm (23 Dec 2003)

BAI Internet Site, "BAI Security Penetration Testing Overview"
http://www.baisecurity.net/auditing.asp (9 Dec 2003)

Appendix A



Appendix B

ProWatch Secure Access Policy

for

Company

Appendix B

Table Of Contents

Section **Title** **Page**

Abstract: **16**
1.0: Access Policies at Points of Monitoring **16**
1.1: Point of Monitoring A - San Mateo 16
1.1.a: Network Address Translation tables 16
1.1.b: Address Mapping Assignments 17
1.1.c: External Network Traffic allowed to the DMZ Network 17
1.1.d: External Network Traffic allowed to the Internal Network 17
1.1.f: Internal Network Traffic allowed to the DMZ Network 18
1.1.g: DMZ Network Traffic allowed to the Internal Network 18
1.1.h: External Network Traffic Explicitly Blocked Due to Registered Attacks 18
2.0: Points of Contact 19
3.0: Procedures **20**
3.1: Initial **20**
3.1.1: Yellow Alarms 20
3.1.2: Red Alarms 20
3.2: After the 1st week of service **20**
3.2.1: Yellow alarms 20
3.2.2: Red alarms 20
A: APPENDIX **21**
A.1: Internet Engineering Task Force Assigned Port Numbers **21**
A.2: Sources of Information on Computing Security **21**
A.2.1: CERT 21
A.2.2: Bugtraq 21
A.2.3: RISKS Forum 21
A.2.4: Ping of Death 21
A.2.5: Microsoft Internet Explorer bug 21

Appendix B

Abstract:

This document details the access policy for Company at each of it's ProWatch Secure points of monitoring. Also included is a point of contact list and a summary of the procedures followed by NetSolve in resolving monitored alarms.

1.0: Access Policies at Points of Monitoring

This section contains a summary of the currently implemented Internet security policy for Company. Questions about the current security policy and/or change requests should be directed to the NetSolve ProWatch Secure NMC at 1-XXX-XXX-XXXX.

Company has the following points of monitoring:

Point of Monitoring	*External IP address(es)*	*Internal IP Address(es)*	*Description*
San Mateo	999.999.150.95	999.99.125.33	Cisco 2524 Ethernet 0
	999.99.125.34	10.7.252.2	PIX
	999.99.125.62	n/a	NetRanger

1.1: Point of Monitoring A - San Mateo

The following table details the IP address space that will be recognized as internal addresses at this point of monitoring.

IP address	*netmask*	*Network*
10.0.0.0	255.0.0.0	Internal
192.168.0.0	255.255.255.0	DMZ

1.1.a: Network Address Translation tables

Internal and DMZ traffic directed to the Internet

The following IP address pool is available for dynamic address translation as shown:

Internal Source IP	*DMZ IP Address*	*External Translated IP Address*
10.0.0.0 255.0.0.0	n/a	999.99.125.37-999.99.125.61 999.99.125.36 (PAT)

Internal traffic directed to the DMZ

The following IP address pool is available for dynamic address translation as shown:

Internal Source IP	*DMZ Translated Address*
n/a	n/a

Appendix B

1.1.b: Address Mapping Assignments

External traffic directed to the Internal network

The following internal IP addresses have been statically translated as shown:

Internal IP Address	*External Translated IP Address*	*Comment*
10.7.252.16	999.99.125.35	mail hub
192.168.0.2	999.99.125.61	HTTP server

External traffic directed to the DMZ

The following DMZ IP addresses have been statically translated as shown:

DMZ IP Address	*External Translated IP Address*	*Comment*
n/a	n/a	

DMZ traffic directed to the Internal network

The following internal IP addresses have been statically translated as shown:

DMZ IP Address	*DMZ Translated IP Address*	*Comment*
n/a	n/a	

1.1.c: External Network Traffic allowed to the DMZ Network

The following table details the TCP/IP services allowed from the external network to the internal network at this point of monitoring. Anything not listed in the following table is denied.

Protocol	*Port*[1]	*Source IP Address*	*Destination IP Address*
n/a	n/a	n/a	n/a

1: Refer to http://www.internic.net/rfc/rfc1700.txt for a list of official port assignments.

1.1.d: External Network Traffic allowed to the Internal Network

The following table details the TCP/IP services allowed from the external network to the internal network at this point of monitoring. Anything not listed in the following table is denied.

Protocol	*Port*[1]	*Source IP Address*	*Destination IP Address*
SMTP	TCP/25	any external IP address	999.99.125.35
HTTP	TCP/80	any external IP address	999.99.125.61

1: Refer to http://www.internic.net/rfc/rfc1700.txt for a list of official port assignments.

Appendix B

1.1.e: Internal Network Traffic allowed to the External Network

The following table details the TCP/IP services allowed from the internal network to the external network at this point of monitoring. Anything not listed in the following table is denied.

Protocol	*Port*[1]	*Source IP Address*	*Destination IP Address*
any	any	any internal IP address	any external IP address

1: Refer to http://www.internic.net/rfc/rfc1700.txt for a list of official port assignments.

1.1.f: Internal Network Traffic allowed to the DMZ Network

The following table details the TCP/IP services allowed from the internal network to the external network at this point of monitoring. Anything not listed in the following table is denied.

Protocol	*Port*[1]	*Source IP Address*	*Destination IP Address*
n/a	n/a	n/a	n/a

1: Refer to http://www.internic.net/rfc/rfc1700.txt for a list of official port assignments.

1.1.g: DMZ Network Traffic allowed to the Internal Network

The following table details other, nonstandard network traffic not covered by previous listings.

Protocol	*Port*	*Source IP Address*	*Destination IP Address*
n/a	n/a	n/a	n/a

1.1.h: External Network Traffic Explicitly Blocked Due to Registered Attacks

The following sites have been explicitly blocked from sending any traffic from the external to the internal network at this point of mon itoring.

Network address	*Netmask*	*Reason for Block*
none	none	n/a

Appendix B

2.0: Points of Contact

NetSolve ProWatch Secure will contact the following Company contacts in resolving monitored alarms:

Type of contact	*Hours*	*Contact*	*Phone*	*Pager*
security contact	24/7	Jim Jones	650-555-1212	650-555-2222
alternate security contact	24/7	Paul Revere	650-555-3333	650-555-4444
administrative contact	24/7	George Washington	650-555-5555	650-555-6666
customer premise equipment	24/7	Abe Lincoln	650-555-7777	650-555-8888

Company will contact NetSolve via the following for policy change requests and security related issues in general:

Primary contact during business hours

Bill Bradley
Charles Barker - Alternate

After hours contact should be initiated through the ProWatch Secure Network Management Center

The following are other security services related contacts at NetSolve that are directly responsible for the Company account:

Name	*Title*	*number*	*pager*
Bill Bradley	Network Engineer	800-555-1111	800-555-2222
Charles Barkley	Network Engineer	800-555-3333	800-555-4444
Michael Jordan	Project Implementation Manager	800-555-5555	800-555-6666
Patrick Ewing	Engineering Manager	800-555-7777	800-555-8888
Network Management Center		800-999-9999	

Appendix B

3.0: Procedures

3.1: Initial installation (first two weeks)

3.1.1: Yellow Alarms

Customer will be contacted via phone, pager or email in the event of yellow alarms in order to verify that traffic should be denied or allowed. This will allow for revision and fine tuning of security policy.

3.1.2: Red Alarms

Customer will be notified of a red alarm after the alarm has been analyzed and steps initiated to resolve the source of the alarms. All red alarms during this period will be discussed via conference call with the primary contact. The customer will be provided with alarm description, alarm resolution if available, and a recommendation on what further actions to take to secure the network from future alarms. Follow up actions will be taken and daily reports will be made.

3.2: After the 1st 2 weeks of service

3.2.1: Yellow alarms

Customer will be notified via conference call and reports at the end of every month of yellow alarms and the resolution of the alarm if available. This notification will be presented in the form of a monthly report and a conference call to determine if any changes need to be made to the policies..

3.2.2: Red alarms

The customer has decided that all red alarms shall result in immediate shunting of the source IP address for a minimum of 72 hours and the immediate contact of the person listed as the primary contact. Notification of red alarms and resolutions shall also be delivered at the end of the month along with yellow alarms in the monthly report and conference call.

Appendix B

A: APPENDIX

A.1: Internet Engineering Task Force Assigned Port Numbers

Please refer to the URL `http://www.internic.net/rfc/rfc1700.txt` for a comprehensive list of Internet Engineering Task Force (IETF) assigned port numbers.

A.2: Sources of Information on Computing Security

Please refer to any of the following sources for additional information regarding computing security.

A.2.1: CERT

The Computer Emergency Response Team (CERT) archive contains security tools as well as security advisories detailing operating system bugs, detected attacks, and the related precautions and/or resolutions. Connect to the URL `ftp://ftp.cert.org/pub/cert_advisories` for listing of current advisories as well as instructions on how to join the mailing list.

A.2.2: Bugtraq

This mailing list acts as a forum for discussing details of security holes as well as the merits of available solutions and work-arounds. Send subscription requests to `bugtraq-request@fc.net`.

A.2.3: RISKS Forum

RISKS is available as a mailing list (send subscription requests to `risks-request@csl.sri.com`) and as the `comp.risks` newsgoup on USENET

A.2.4: Ping of Death

Information on the Ping of Death attack can be found at the following URL :

`http://www.sophist.demon.co.uk/ping/index.html`

A.2.5: Microsoft Internet Explorer bug

Information on the Microsoft Internet Explore bug can be found at the following URL :

`http://just4u.com/webconsultants/dig824.htm#bugs`