GISO Practical Assignment

Information Security Officer

Assignment version 1.3 (February 7, 2003)

Securing Fire-Wall-Street Bank

Prepared by:
Ergash Karshiev

Local mentor course,
Kenosha, WI

October 3, 2003

Last Update: Saturday, October 4, 2003

1.0 ABSTRACT

This paper describes the operations of Fire-Wall-Street Bank -- a global online bank offering low-cost anywhere / anytime banking. The paper includes the following items:

* Description of the business operations of the bank
* Analysis of 3 specific risks to the security / operations of the company. The identified risks are identity theft, customer confidence loss, and DDoS attacks affecting the Internet presence
* The analysis and development of a specific policy and procedure to address one of the identified risks. The policy and procedure are focused on Identity Theft Protection.

2.0 DESCRIPTION OF FIRE-WALL-STREET BANK

(Assignment 1)

Currently the bank employs 5,000 people globally. Big part of it is a sales force expanding the bank's customer base in large cities. A global staff of 100 employees handles the IT operations.

The global infrastructure of the FWS Bank is presented in the Appendix D.

The FWS Bank was formed in 1996 (during the Internet boom period). The bank started from investment of an innovative IT company specializing in developing of secure communications software. Originally the FWS Bank employed and served students of the nearby university. Some of the banks' technologies and software were purchased by leading international banks. However, the FWS Bank has retained and improved its competitive advantage by continuously innovating and pioneering advanced financial services. The FWS Bank was able to apply its innovations much faster than the large banks who bought the same solutions from them. Larger banks could not keep up with the pace of FWS Bank due to their infrastructure complexity and internal resistance to change. The large competitors also did not want to take risks of embracing new technologies. They preferred to have small innovative banks to do it first and then just to buy tested and ready solutions from them.

This way the FWS Bank quickly increased its revenue during the 1996 -2000 period and continues successful business today. Currently, the bank's headquarters are located on a private island owned by the company. Other data centers of the bank are located in several other Islands (over the World) owned by the bank. The reasons for this geographical positioning were: diversified placement of datacenters, lower taxes, and less restricted business operations. For example, encrypted and commercial data traffic between various countries is subject to multiple and complex regulations. Local governments might decide to restrict the FWS Bank's operations or impose impossible taxes forcing the bank's relocation. Therefore, the FWS bank is a distributed country in itself. Multiple global datacenters with load-sharing and high availability capabilities ensure resistance to natural and other disasters. The bank relies on leased satellites and underground / underwater fiber communication lines for its wide Area Network infrastructure.

Another important part of the banks' infrastructure is local bank agents in multiple locations of the World (typically in populated areas). The bank agents are responsible for marketing the bank's services.

The Fire-Wall-Street Bank is an online-only bank that is trying to establish solid reputation while competing with many large traditional banks. The strong points of the bank are:

- Low infrastructure overhead allows passing the savings to the customers (no need to support multiple physical offices)

- Support for new and advanced financial services (mobile phone banking, wireless computing, integrated and simplified financial transactions, various discounts from their online service partners)

- The bank offers inexpensive wireless laptops to its customers as a membership reward and as a promotion of online wireless banking

- As a result of all of the above innovations the Fire-Wall-Street Bank has to overcome many technological challenges and face various security threats daily.

- Being innovative is the primary business advantage of the Fire-Wall-Street Bank that is hard to duplicate. Traditional banks are more conservative in adopting new technologies, they prefer if somebody else will test the waters first while they can learn from the mistakes of the brave technology pioneers. That is understandable: traditional large banks have a reputation to maintain, The Fire-Wall-Street Bank needs to win that reputation.

2.1 The Security Team

The Fire-Wall-Street Bank created their Security Team to:

1. Perform independent network and system audit
2. Conduct risk assessment

3. Develop policies (to address the risks)
4. Develop procedures (to comply with the policies)
5. Develop Enterprise Security Policy (to summarize all of the customized security best practices).

Below are the discussions and results of the security team’s work.

2.1 FWS Bank Infrastructure

The technology environment of the FWS Bank is simple and standardized. The bank's infrastructure was built recently with necessary room to grow and upgrade-ability options. The young bank does not have to deal with the old inherited infrastructure of old traditional banks. The application server infrastructure is primarily based on Intel architecture for hardware and open source software (Linux, Apache, and Snort). Leading commercial vendors are utilized as well: Dell, Cisco, Microsoft, Check Point, etc. The bank employs commercial technologies for some critical areas, but the main direction is to avoid being locked into a specific vendor. Source code availability is a requirement for most of the purchased software. Infrastructure and security applications are reviewed, complied, and tested in the company before the production deployment. Source code is necessary to protect the investment of purchasing and integrating the software if the commercial vendor is no longer in business (or acquired).

The FWS bank has several datacenters that have identical design and configuration. Each one of them can be used as a disaster recovery data center for several others. The required CPU performance and network bandwidth can be significantly increased via agreements with hardware and communication providers.

2.1.1 Network Configuration - Local Area Networks (LAN)

Diagram 1 in Appendix B shows a standard FWS Bank's LAN for a datacenter (in one of the island locations).

The design presents a balance of simplicity and redundancy in critical areas. Every datacenter relies on two independent Internet Server providers. Traffic encryption / decryption along with VPN authentication is assigned to a dedicated VPN device in a firewalled De-Militarized Zone (DMZ). The DMZ itself is made of two firewalls: external (facing the Internet) and internal (facing critical servers and LANs). The members of the DMZ are exposed to the Internet via their listening ports (like 80/tcp for HTTP, 443/tcp for HTTPS, 25/tcp for SMTP, etc.). Therefore, each member has a separate VLAN assigned on the DMZ switch. The interactions of the VLANs is strictly controlled via Access Control Lists (ACL) of the DMZ switch.

The “Networking Handbook” (by Ed Taylor) was referenced during the design of the FWSB LAN (Reference #10).

The configuration layout of a standard datacenter is listed below:

Component	**Purpose**	**Configuration**
External Firewall	Perimeter defense and Internet access	Check Point Firewall-1 NG on Hardened Red Hat Linux 9.1 (Dell PowerEdge Server: 2*2.5GHz Intel Xeon Processor, 3 GB RAM)
DMZ Switch	Connects and protects the Internet DMZ members via dedicated VLANs Also used as a central switch for the LAN of Other Production Servers and the LAN of Desktops)	Cisco Catalyst 4500 Gigabit Switch
WWW Cluster	Provides WWW services with load balancing and high availability	A cluster of 4 PowerEdge Servers (2*2.5GHz Intel Xeon Processor, 3 GB RAM) running Hardened Red Hat High Availability Cluster with Apache web server (DNS sever is integrated within the cluster)
Email Server	Provides Internet email services	Hardened Red Hat Linux 9.1 (Dell PowerEdge Server: 2*2.5GHz Intel Xeon Processor, 3 GB RAM
FTP Server	Provides Internet FTP services	Hardened Red Hat Linux 9.1 (Dell PowerEdge Server: 2*2.5GHz Intel Xeon Processor, 3 GB RAM
VPN Concentrator	Provides VPN and Internet authentication services	Cisco VPN Concentrator
NIDS + Sandbox	Intelligent Network Intrusion	Snort NIDS with proprietary

	Detection tool with Sandbox functionality (also used as and inline NIDS for the LAN of Other Production Servers and the LAN of Desktops)	Sandbox implementation Hardened Red Hat Linux 9.1 (Dell PowerEdge Server: 2*2.5GHz Intel Xeon Processor, 3 GB RAM
Internal Firewall	Internal defense and separation of critical servers and internal networks	Check Point Firewall-1 NG on Hardened Red Hat Linux 9.1 (Dell PowerEdge Server: 2*2.5GHz Intel Xeon Processor, 3 GB RAM) + 8 Gigabit NIC ports for the DMZs
NetApp Server	File Server and Backup Server for Desktops	NetApp F87 Filer (up to 576 GB of storage)
NOTE: All other servers presented on the network charts have the following configuration	All other servers	Hardened Red Hat Linux 9.1 or Hardened Windows 2003 Server (Dell PowerEdge Server: 2*2.5GHz Intel Xeon Processor, 3 GB RAM)
Desktop Department Switch	Connects and protects the Desktop department PCs	Cisco Catalyst 3500 Gigabit Switch
Standard Desktop	Provides desktop functions	Dell Dimension 2400 (2.2GHz Pentium 4, 256 MB RAM, 40 GB HDD)
Standard Notebook	Provides mobile desktop functions	Dell Inspiron 1100 (2.2GHz Pentium 4, 256 MB RAM, 30 GB HDD, DVD-R/CD-RW)
Standard PDA (for wireless banking – in pilot stages)	Provides wireless banking and PDA functionality	SONY CLIE PEG-UX40 (16 MB, Color, keyboard)

2.1.2 Network Configuration - Wide Area Network (WAN)

(Appendix D)
The Appendix D contains the WAN diagram showing any-to-any (mesh) topology chosen by the FWS Bank. This was necessary to provide maximum direct connectivity and maximum of redundant routes to recover in case of malfunctions or disasters.

2.1.3 System & Application Servers

(Appendix A and B)
A standard datacenter runs 30 Intel-based servers typically running Linux OS. A standard server has extra room for additional processors and Hard Disks (to provide potential for CPU performance increase). The servers are connected via standard high-performance switches with Check Point Firewall-1 Linux-based firewalls (utilizing isolated DMZs for sensitive or exposed network segments). Use of wireless communication is explicitly prohibited in the datacenters. Wireless services are offered outside of the datacenters.

2.1.4 Server Configurations

(Appendix A, B, and C)
Servers run under hardened configuration: only necessary daemons / services are enabled. At least two layers of protection and two-factor authentication are required to access the servers. Vendor software that cannot operate under these strict conditions is not purchased. Typically the bank does not do customization and self-support of purchased commercial software. The overall cost of self-supported solutions was found too high. The only exception is the proprietary software that the FWS Bank develops, employs, and sells commercially.

2.1.5 Servers That Support IT Infrastructure

(Appendix A, B, and C)
These servers provide DNS, DHCP, VPN, Print, Backup, and Centralized Authentication services. They are located in various parts of the network according to the design of the IT infrastructure. This creates a unique challenge for managing, monitoring, securing, backing up, and recovering these servers. The challenges are addressed via maintaining several alternative ways on handling these critical servers (remote, local, manual, etc.).

2.1.6 Primary Application Servers

(Appendix A, B, and C)
This includes web servers and financial transaction processing servers providing core services to the global customers.

Uninterrupted power supply and highly available communication lines for these servers are the other essential components for conducting business.

2.1.7 File Servers

(Appendix B, and C)
FWS bank uses AFS (Andrew File System) for better security and role-based access control. Each datacenter has two pairs of redundant file server. The first pair of serves is for daily operations, the second pair is for highly sensitive data (customer and financial information). Because the two groups of servers have different sensitivity levels, they are not allowed to connect directly and are separated by the internal firewall.

2.1.7 Backup and Recovery Infrastructure

(Appendix B, and C)
Currently the bank's data is backed up nightly on DLT tapes. Due to the non-stop operational requirement (customers do banking anytime from anywhere), the data cannot be copied directly from production servers. Instead a High-Availability Partner Server is taken off-line nightly and backed up (a mirrored copy of the production server). Of course, a disaster or an attack can have more serious impact if they happen during this backup window (since the High-Availability Partner Server is offline). This was another risk identified by the Risk Assessment (but not in the scope of this document).

2.2 Business Operations

Each customer interacts with the FWS Bank via the HTTPS Internet access. Each customer owns a personal certificate used to validate his / her identity and for VPN encryption. Customer connects to the web server (in the Internet DMZ) and authenticates. The actual financial transactions happen on the internal application server behind the second firewall layer. No customer / financial data is stored on the web server, even the web server log files are sent to a secured logging server. The customer website contains minimal amount of automation code for better security and browser compatibility.

COMMENT: How did the bank manage to stay in business while investing in training and banking equipment?
The bank saved on minimal number of security incidents and money theft compared to other banks. Customers appreciated the friendly security training because it had many good applications in everyday life. Happy customers remained loyal. They promoted the FWS Bank via the "World of Mouth" with their personal recommendation (the bank did not intentionally reward for recruiting new customers via recommendations).

3.0 RISK ASSESSMENT

(Assignment 2)

3.1 What to Protect

The bank was exposed to multiple visible and less visible risks. There were numerous attempts to illegally obtain money from the bank by various organized groups and lone criminals. Typically, it involved a form of social engineering: trusting customers were fooled into giving out their personal information that was later used in elaborate money schemes. Some customers were victimized when they lost their ATM cards or ATM receipts. Sometimes the banking credentials were stolen or eavesdropped. Malicious emails and malicious websites also were used in these schemes. In summary, the customer was often the target and the victim. Therefore, educating the customer on security became one of the bank's priorities. To make customers more motivated to take the training, the bank offered promotional discounts for those who took the training.

The critical assets and attractive targets are:

- *Money*
- *Reputation*
- *Credibility of online and wireless banking*
- *Customer identity (personal information)*

COMMENT: Who pays for the protection? The customer and the bank pay. This is difficult game: customers pay for security, so they don't lose more; cyber attackers don't pay much and can gain big money. The detection and prosecution efforts should make them pay MORE that they are willing to lose (jail time, large fines, and damaged reputation). However, the remaining challenges are: timely discovery, capturing, and prosecution of on-line criminals.

3.2 The Risk Assessment Methodology

The chosen risk assessment methodology combined quantitative and qualitative methodologies. Every vital business aspect was assessed via four independent calculations (two qualitative measurements and two quantitative measurements for each business aspect). Then the pairs of Risk Assessment data were compared (qualitative measurement #1 was compared to an independent quantitative measurement #2). This was important because Risk Analysis metrics could suffer from subjective "noise" unless every metric is confirmed independently. Obviously, the independent measurements could never match perfectly, but it provided estimates of the errors of the measurements.

3.2.1 Ensuring Completeness

The Risk Assessment Team made sure that all the significant risks were addressed, all the components were reviewed (non-critical parts can cause critical damage: like one infected PC).

The FWS Bank inspects its network regularly with vulnerability assessments scanners. All production servers run hosts-based security management software (Symantec Enterprise Security Manager). Their integrity and change process are verified via Tripwire.

The bank's staff performs a monthly inventory of the equipment and other assets to ensure that all of it is accounted for. The inventory procedure also verifies if there is any unauthorized equipment (to avoid security breach from unauthorized equipment).

3.2.2 Ensuring Correctness

The Risk Assessment Team developed alternative ways of verifying that the collected data makes sense and within a realistic range. Several parallel ways of measuring risks provide necessary "sanity checks".

The Risk Assessment Team runs several security assessment tools in parallel to correlate findings of these tools. This way potential false positives and false negatives are discovered.

3.3 Identified Risks to FWS Bank

3.3.1 Discussion

The Risk Assessment Team looked for typical and also un-conventional (often overlooked) risks. They reviewed potentials for security "ripple effects" (when several small items can pose a higher risk when creatively (or coincidentally) combined. They look for the "multiplier effect" when one little risk becomes critical if multiplied by the volume (thousands of users, millions of connections, etc.). The team also took into account risks that cannot be eliminated as they are core activities or part of human nature that is very hard to change.

The Risk Assessment Team identified that the "crown jewels" of the entire bank are financial transactions on internal application servers. However, many other significant risks were found. For example, another identified set of risks was: potential for employee's errors, negligence, or sabotage.

They also looked into new or growing risks: like wireless networks, increasing malicious Internet activity. The Risk Analysis team also tried to think one step ahead of hackers and plan for future scenarios of attacks. For example, they performed a training / study exercise with the banks managers for the topic: "What is the worst case scenario / and the best response in case of theft of large numbers of credit cards, and other personal information". Since financial transactions and distributed (and often outsourced) the banks customers can become fraud / identity theft victims even from external reasons. Besides, the upper management understood realities of technology and human nature; they did not support the proud assumption: "It will never happen to us because we are so good".

3.3.2 Future Risks

The team looked into the challenge of objectively measuring the risks (with repeatable results). They applied most applicable risk analysis methodologies and formulas (specifically for financial industry). The team focused on collecting only relevant data, which required deep understanding of the business. In summary, the team put great efforts to convert subjective interviews input into objective risk metrics (internal validation, sanity checks, parallel validation, logical lie detector-type questionnaires, comparing to similar businesses).

3.3.3 Findings

The findings of the Risk Analysis are summarized below:

1. Stolen identity or data of a security practitioner poses even higher risk. Security professionals serving the bank can be specifically targeted. They also have more control and ability to hide their malicious actions or mistakes. (The problem was later addressed via security staff training, additional monitoring, non-repudiation, and separation of duties).

2. Electronic crimes and failed promises of technology account for loss of customer confidence.

3. The FWSB' Internet presence / availability is under growing risk of attacks. This includes risks to internal operations from the Internet.

4. Technological progress in digital electronics creates new risks: Massive visual and audio data collection (via cheap and portable video / audio equipment, and data storage). Many integrated wireless portable devices are already being used for penetrating of corporate networks and spying.

5. The growing sophistication of new malicious code can exceed the banks ability to respond via traditional processes.

3.3.4 Top 3 Risks

As a result of the above Risk Analysis the team highlighted the below three primary risks:

RISK #1: Online Fraud / Identity Theft
RISK #2: Loss of Customer Confidence
RISK #3: Reliability / Safety of Internet Presence

The three primary risks and their mitigation are discussed below in more details (below).

3.3.1 RISK #1: Online Fraud / Identity Theft

Overview

The bank's biggest daily losses come from illegal activities, such as: financial fraud and customer identity theft. Obviously, the attackers are financially motivated by the money they steal (if successful). To make this prospective less attractive, a good tracking and prosecution policy is in place. This includes network and system infrastructure collecting potential forensic evidence. Cooperation with Internet Service Providers and Law Enforcement is integrated in security policies and procedures.

Threats: Online criminal activity, propagation of malicious code, sabotage, espionage

Vulnerabilities: Web/Application/OS vulnerabilities, human trust, unsecured business processes

Relevance and Potential Impact

Significant part of the banks revenue is affected by this type of crime. It also affects significant number of the banks customers. Negative publicity and actual losses had a potential to drive the bank out of business eventually.

EXAMPLE: Money theft via stolen identity
A particular ethnic-based crime organization targeted immigrants and senior citizens of the same ethnic background in large cities. The criminals would obtain identity information, and then they would ask the Bank's Help Desk to reset the victim's on-line banking password. Shortly the criminals would wire moderate amounts of victim's money to fake recipients.

These types of crimes become more sophisticated. Global online access to the financial services (via the Internet) also invites global criminal organizations. Fighting these crimes requires cooperation with global and international law enforcement organizations.

Specific Mitigation

The FWS Bank developed a policy to protect from Online Fraud and Identity Theft. The specific policy is provided at the end of this paper (see Section 5.3). The Online Banking Identity Protection Policy is well-integrated with the rest of the Corporate Security Policy.

3.3.2 RISK #2: Loss of Customer Confidence

Overview

Highly publicized cases of malicious attackers stealing large amounts of customer data and multiple cases of identity theft continuously hurt customer confidence in online banking. For small banks like FWS retaining or regaining good customer confidence is essential for the survival of the bank. This is because offering online banking services is the primary business model of the bank.

<u>Threats</u>: Negative publicity from attacks, competition, sabotage, espionage

<u>Vulnerabilities</u>: hard to use / unsecured technology, unsecured business processes

Relevance and Potential Impact

Customer confidence in online banking is very relevant to FWS Bank. Any time online banking is considered or perceived as un-secure or unreliable it affects FWS Bank and the online banking industry.

Unlike traditional banks, FWS Bank does not offer banking via multiple physical branches. Therefore, promoting convenient forms of electronic banking is essential for FWS Bank. The biggest impact from loss of customer confidence would be going out of business. That is why the bank invests heavily in user-friendly and strong security.

Specific Mitigation

FWS Bank promotes secure on-line banking via advertisement and personal recommendations of existing customers. Of course, these efforts could quickly fail, if they are not supported by real user-friendly and secure solutions.

One of the lessons learned from recent security breaches in various banks is: “Be honest and be proactive with your customers”. Whenever there is a possibility of customer data being stolen or compromised, FWS Bank notifies potentially affected customers and proactively reinstates their affected areas. Because of the financial inter-relations and outsourcing of financial processing, external factors can affect their customers. The bank proactively defends their customers is every possible way. “Not my problem” approach would be a sure way to lose customer confidence in FWS Bank.

3.3.3 RISK #3: Reliability / Safety of Internet Presence

Overview

Other significant risk to the business is unavailability of the service to the customers (especially due to malicious code and large-scale attacks like Distributed Denial of Service [DDoS] attacks or major ISP problems).

Threats: Massive attacks (DDoS, worms), unreliable ISP services

Vulnerabilities: Web/Application/OS vulnerabilities (especially Zero-Day type), vulnerable communication infrastructure (routers, switches, connections)

Relevance and Potential Impact

As with the other discussed risks, reliability and safety of the Internet presence is directly linked to the bottom line of the bank. Resilience to malicious code, security vulnerabilities, and DDoS attack is essential. Not only the bank can be kicked out of the internet by various attacks, the bank might also decide to stay disconnected from the Internet it there is a Zero-Day exploit propagating in the wild (exploiting a very new vulnerability without a known fix).

One day of unavailable services can have a catastrophic impact to the business (since upset customers could move their accounts to competitors).

Specific Mitigation

To mitigate the risks of Internet presence, the Bank implemented redundant connections to independent Internet Service Providers (Appendix A). Phone dial-up service is available as well and is sufficient to handle significant number of users.

There is also a process of performing banking transactions over the phone (with a teller or automatically). Special care was taken to validate such transactions and user identity (like enforcing hard to guess PIN numbers, tracing originating phone number to correlate the ownership of the number, etc.).

4.0 MITIGATING THE IDENTIFIED RISKS AS A WHOLE

While the three identified risks differ from each other, their mitigation efforts significantly overlap. That is why the Risk Assessment and the Security Team proposed addressing them in a coordinated / unified way. Instead of solving "Problem X" with a "Solution X", they looked at the top risks as a whole. Then they developed an integrated set of solutions. This approach was found to be more logical: many business operations, devices, and networks are highly inter-connected and mutually-dependent. Instead of protecting one business unit or one server at a time, they decided to deploy centralized and coordinated defense strategy. The integrated solutions are discussed below.

NOTE: All of the new FWSB' security policies, procedures and solutions were designed within a standard security management framework, the international standard ISO/IEC 17799. For more details see http://www.iso.ch/cate/d33441.html (Reference #2).

4.1 Implementing Multi-Layered Security (Defense-in-Depth)

(Appendix A, B, C, D)
The Defense-in-Depth approach provides multi-layered solutions to the three risks identified above. Therefore, the FWS Bank network is divided by multiple layers forming separate security zones (each populated with hosts of equivalent security requirements).

The network is not intended to provide total security to all devices due to very high costs of "total solutions". Total Security solutions also tend to be more complex. Ironically, higher complexity can lead back to lower security (more points of attack, lower reliability). Instead the FWS Bank network practices Sufficient Security based of the value of the information tied to the cost of securing it: *Solution = Information (Cost)*.

Some of general guidelines of the book "The Process for Network Security" (by Thomas Wadlow) were used in the below Defense-in-Depth solutions (Reference #3). General guidelines of the SANS T9 Training Materials were used as well (Reference #1).

4.1.1 Defense-in-Depth in Network Design

(Appendix A, B, C, D)
The FWS Bank' regional datacenter chart is presented in Appendix A. Customers interact with the Bank via the Internet (direct dial-up service is an access alternative in contingency situations). The external Internet traffic first hits the Border Router. This logical router in reality is comprised of two highly available routers connected to two ISPs for redundancy (to eliminate a single point of failure). The Border Router forwards the incoming traffic to the External Firewall. The same firewall is used to support VPN connections with external business partners (The Extranet). The firewall has separate network interfaces linked to each Border Router connecting with each ISP. This redundancy for the Border Routers and the Firewall NICs is necessary to survive DDoS attacks and ISP failures.

The Network Intrusion Detection device (NIDS + Sandbox) serves as an additional layer of security between the Internet DMZ and the Internal DMZ areas. This device analyzes the incoming and outgoing traffic for signs of attacks. It also plays the external transactions in a virtual computer (Sandbox) for signs of malicious / suspicious behavior before sending the traffic to the internal firewall. The trade-off is in some delay of the transactions and occasional "false positives" – blocking legitimate transactions. Fortunately, the device can be custom-configured in its Learning Mode. It can also be manually updated / configured at any time.

In addition to this, the Fraud Department utilizes sophisticated IDS and Pattern Monitoring systems constantly inspecting other areas of the bank's network. The financial transactions ("the crown jewels") are constantly monitored via Artificial Intelligence software analyzing financial patterns to detect new behaviors. For example, if a money-conscious customer starts buying untypical expensive items, the Fraud Department would call for verification. Special precautions are taken to protect this type of information (to prevent abuse and privacy violations).

4.1.2 Defense-in-Depth in Firewall Policies

Traffic from the Internet is never allowed to reach the internal firewall directly. Any incoming connections can only reach the DMZ servers and only on the listening ports they serve. Every other access from the Internet is blocked.

Here are some general firewall rule creation policies that were developed:

Rule 1: Anything that is not explicitly permitted is denied

Rule 2: Only minimal necessary set of ports / protocols and hosts are allowed (Example: Whenever source and/or destination are known, a specific firewall rule is created to for the known source and/or destination only)

Rule 3: Advanced firewall security techniques should be deployed whenever possible (Example: IP anti-spoofing rules, advanced packet inspection, protocol analysis, etc.)

Rule 4: All Internet connections terminate within the Internet DMZ (not allowed reaching anything else beyond the designated Internet DMZ servers).

4.1.3 Defense-in-Depth in Customer Access

A special set of procedures was enabled to protect the new customer setup. Before mailing the access credentials, the bank had to know the identity of the recipient and enter it into the access card. Password shared between the customer and the bank can be eavesdropped, stolen, or replayed. Unfortunately, biometric properties cannot be changed and can be eavesdropped and replayed. Therefore, biometric technology was not utilized in this case.

The found solution was in creating a digital identity software / hardware combination that was mailed to new customers (containing user certificate and secure ID card in an inexpensive integrated device). Upon receiving the package, the new customer would call FWSB Help Desk for the rest of the activation procedures.

4.1.4 Wireless PDA Banking Pilot Program

Currently the FWS Bank is pioneering Anywhere-Banking PDA service offering. The chosen wireless PDA is SONY CLIE PEG-UX40 (16 MB, Color, and keyboard). This wireless PDA banking program is deployed as part of testing and mitigating risks of wireless banking.

This is a small wireless PDA banking device. The bank found it cheaper to buy and provide this standard and secured (hardened) device instead of trying to support online banking for multiple configurations of customers' PDAs. The device unlocks via password authentication. A local bank specialist would visit a new customer to conduct initial setup and training. The cost of hardware & software can be much lower than the cost of the recovery from banking fraud. Also, improved overall security and standard equipment provided additional savings. The Pilot Program customers were happy to get the secure wireless banking device for free. Convenience of banking from anywhere was an additional bonus.

In contrast, competing banks who were introducing wireless banking via cell phones suffered from interface limitation and lack of standards: the cell phone interface happened to be very limited. Supporting multiple phone models, vendors, and configurations is very difficult.

FWS Bank plans to start providing this wireless PDA banking device in 2004. Functionality and connectivity integration potentially carries a lot of security problems and challenges. Therefore, the chosen direction was to stay with a specific tightly controlled hardware and software configuration of PDA.

Besides, the FWS banking PDA could be used for other PDA functions that are considered less risky. Such functions could be optionally enabled.

4.2 Monitoring Requirements (and Customer / Employee Privacy)

The growing threats of identity theft and other illegal abuse of online banking services forced the bank's management to take countermeasures. Since the attacks vary and improve continuously, a proactive and flexible (scalable) set of solutions was needed. In order to detect early stages of attacks proactive monitoring of transactions was implemented. One of the biggest challenges was correlating and verifying electronic transactions with physical events and people. For example, one hacker could initiate multiple transactions from various places and overload / corrupt the system. The early warning system would detect and block these events (a real customer cannot and should not initiate multiple parallel transactions). The fraud monitoring AI software solved this problem to some extend.

4.3 Maintaining System and Financial Integrity

Integrity assurance is one of the proposed solutions for addressing of the identified risks. The integrity of the systems and financial assets will be assured via business processes (double accounting, inventory, audits) and via technology tools (like Tripwire). The proposed integrity solutions are discussed below.

4.3.1 Double Accounting and Tripwire Integrity Verification

The Risk Assessment Team identified that the "crown jewels" of the entire bank are financial transactions on internal application servers. Therefore, the Security Team developed an advanced security solution described below: Double Accounting with Integrity Verification.

The double accounting solution is presented in Appendix A. The idea is to process the same transactions (in parallel) on two very different (and presumably secure) platform running the same application that were developed separately. Any pairs of transaction that do not match are discarded. The two different platforms are not likely to have the same vulnerabilities. Therefore, it would be very difficult to hack both platforms and make them produce the same fake transaction output. This Double Accounting technique should also help to catch programming errors in the application code,

Both application servers (UNIX and Windows 2003) have separate NICs and reside in separate DMZs. Both application servers are continuously verified with Tripwire for file integrity. Tripwire agents are installed on all servers of FWS Bank. They take integrity snapshots every hour and submit the results to the Tripwire Management Server.

The double accounting practice is a technique of conducting financial transactions in parallel via independent systems, software, and processes. This situation can potentially double the cost of transactions as well. However, in can reduce risks of fraud (except when the two different methods are susceptible to the same fraud technique or type of error). Double accounting can reduce risk of fraud based on system compromise. It is less likely that two different systems (utilizing different platforms, architecture, and applications) would suffer from the same attack.

However, upcoming “super-worms” and “hybrid-threats” might be able to penetrate even this defense. The strong argument in favor of this double accounting system is: not only attackers have to break two very different systems, but they also have to break them in the same controllable way, so the fraud on System 1 will match the fraud on alternative System 2 (the results must match to be committed as a valid transaction).

4.4 Identity, Authentication, and Passwords (fighting identity theft and attacks)

The Risk Analysis found that the weakest link of the user Identity Protection is the users themselves (trust, unprotected personal data, and malicious code). That is why customer security training and awareness was proposed as a necessary part of the solution.

The new version of Security Policy added the requirement for security training of customers and staff. Special effort was made to deliver simple security solutions since they require less training and more likely to be followed.

4.5 Improving Business Continuity / Disaster Recovery

While Business Continuity and Disaster Recovery were not highlighted amongst the three primary risks, they remain as one of the necessary security layers in the proposed

“Defense-in-Depth” models. At some point, all preventive security measures can fail, nothing can replace a clean and valid backup then.

* The Risk Analysis found that some parts of critical data are not being backed up frequently enough. This could have resulted in a very high financial loss in case of a disaster.

* In a separate case the backup frequency was sufficient, but the backup tapes were removed from the tape robot only weekly (to be taken to an off-site location). Therefore, there was a risk of data loss (up to one week of data) if the tape robot is consumed by a disaster.

* Another finding: in some cases mission-critical data was stored on laptops without backup and without encryption.

These cases were addressed quickly due to the good understanding of the new Corporate Security Policy by management and employees.

4.6 Customer & Employee Security Training / Awareness

The bank does not deny membership to any eligible person. There are no discrimination restrictions. By growing the customer base the bank gets more people who un-intentionally (or intentionally) could violate the banks' security policy. There are customers of very different backgrounds and education level. The goal was to protect the bank and abiding customers from potential violators. A series of training sessions were established (with training handouts).

4.7 Legal Compliance International and Internet-related laws; Prosecution of hacking and identity theft

FWS Bank has customers in many countries. The Bank has to comply with financial, security, and privacy laws in those countries. To simplify this international compliance the Bank developed its policies using the safest common denominator for operating in those countries. That means the policy chooses the strictest (most secure) option in each case so in can apply everywhere.

There are cases when financial laws of one country are in direct disagreement with laws in other country. Example: some countries require protecting customer privacy (even at high cost) other countries might require disclosure of customer financial data to their government. In controversial or conflicting cases the bank considers economic, political, and international factors when deciding whether or not to operate in a particular country.

Tracking and prosecuting attacks originating form the Internet was found to be difficult. Today's spoofing, relaying, and hiding techniques made tracking and prosecution more challenging. The FWS Bank cooperates with international security organizations and business partners in tracking Internet attacks.

The following Section 5 provides policies and procedures to address the identified RISK #1: Online Fraud / Identity Theft.

===

5.0 POLICY DEVELOPMENT -- ONLINE BANKING IDENTITY PROTECTION

(Assignment 3)

NOTE: The following policy was developed specifically for this assignment. Therefore, this policy does not have external references.

The below sections address the identified RISK #1: Online Fraud / Identity Theft.

Section 5.1 describes the original policy on that subject (before the Risk Assessment described in this paper).

Section 5.2 evaluates the original policy for any gaps discovered by the above Risks Assessment.

Section 5.3 provides a new (improved) version of the same policy that addresses the newly discovered risks.

Finally, Section 5.4 describes a related Online Banking Identity Protection Procedure.

5.1 Original FWS Online Banking Identity Protection Policy

(In effect since 01/01/1995)

Purpose (Orig.)

Online banking is the key service offered by FWS Bank. This Identity Protection Policy is aimed to protect private information of customers and employees during online banking. Cases of violation of this policy should be examined with necessary administrative, disciplinary, and/or legal actions. Accepting this policy is required for all of the Bank's customers and employees (prior to accessing the FWS Bank's network).

Definition (Orig.)

This policy defines Online Banking as: The ability to perform FWSB' financial transactions utilizing telecommunications services.

In this context, Identity Protection is defined as a set of measures and technologies to safeguard personal private information up to the sufficient level.

The specific definition of the sufficient level of protection will change (and will depend on real risks affecting the users). Therefore, the sufficient level of protection will change with time.

Background (Orig.)

The objectives of the FWS Bank's Identity Protection Policy are:

1. To assist users in safer Online Banking
2. To protect the Bank's assets (confidentiality, integrity, and availability)
3. To manage risks of financial losses due to security breaches / security incidents resulting form Identity Theft
4. To comply with all applicable laws.

Scope (Orig.)

This policy covers Identity Protection for all types of Online Banking services offered by FWS Bank:

* Online Banking via the wired Internet
* Online Banking via dial-up services (phone lines)
* Online Banking via private network connections

Policy Statement (Orig.)

The following guiding principles outline the Online Banking Identity Protection Policy:

1. Identity and personal data of customers and employee must be protected from theft and modifications. Maximum effort should be taken to prevent disclosure or eavesdropping of this information during all stages (transmission, processing, archiving, etc.). The only exception is in cases when a disclosure is required by applicable laws (like in cases of investigation).

2. The personal identity information is used for creation of online access accounts and for verification purposes. The personal identity information should nod be exposed or used for any other purpose.

3. The personal identity information should not be stored in high-risk systems, like servers accessible from the Internet, publicly available systems, etc.

4. Any software and hardware that violates this Identity Protection Policy should not be used.

5. Management and staff of FWS Bank should be trained on secure handling of personal identity information.

6. Customers / Employees utilizing Online Banking service must sign their agreement form of Appropriate Use Policy (that includes rules for handling of personal identity information).

7. Employees utilizing FWSB computer accounts should be guided by the same principles.

Responsibilities (Orig.)

* The *Upper Management* of the FWS Bank has ultimate responsibility for secure and safe Online Banking service.

* The *Security Group* formulates security policies and standards.

* The *Corporate IT* team implements the above policy upon approval of the Upper Management.

Action (Orig.)

The following specific actions are necessary for implementing the Identity Protection Policy.

The steps #1 and #2 should be performed at least quarterly (or after any significant security infrastructure change). The other steps (#3 - #7) should be checked for compliance by assigned Corporate Security members at least daily.

1. A Security Manager should be assigned to oversee security compliance of the Online Banking according to the FWS Bank's Policies, Standards, and applicable laws.

2. A formal Risk Analysis Process should be performed for Identity Protection compliance in procedures, applications, and network components. Risk mitigating controls and procedures should be developed as well.

3. The confidentiality and integrity of data transmitted via Online Banking connections should be protected. 128-bit SSL encryption (or better) is required.

4. Users should be advised and discouraged from using software and hardware known for violation privacy and handling personal information insecurely.

5. Whenever users discover facts of leaking of personal information (or errors), they should immediately report this to the Corporate Security of FWS Bank.

6. Corporate Security of FWS Bank should proactively monitor any applicable international laws related to identity protection. Any cases of conflict with this Identity Protection Policy (and The Corporate Security Policy) should be reported to upper management. Significant changes in the related laws might require modifications to this policy.

7. Corporate Security of FWS Bank should proactively search the Internet resources for any signs of stolen proprietary information of the FWS Bank (including identity information of FWS Bank). If such information is found, they should consult Law Department of FWS Bank for further actions.

==============================

5.2 Evaluation of the Original Online Banking Identity Protection Policy

(Was performed during 01/12/2002 – 31/12/2002)

(All changed or added parts are marked with *Italicized Font*)

Purpose (Eval.)

This section still meets the requirements of the new Corporate Security Policy. No changes were applied here.

Definition (Eval.)

The Definitions section was not changed in the new policy for Online Banking Identity Protection.

Background (Eval.)

The background of the FWS Bank's Identity Protection Policy remain the same.

Scope (Eval.)

The scope of the Online Banking services offered by FWS Bank has expanded. The new policy also covers "*Online Banking via wireless Internet (802.11a, b, g)*" as a new technology being requested and accepted by the bank's customers.

Therefore the new scope was added as follows:
* *Online Banking via wireless Internet (802.11a, b, g)*

Policy Statement (Eval.)

The following new principles were added in the Online Banking Identity Protection Policy:

8. Wireless banking is only allowed utilizing the below or better security configurations:

> ** Wireless 802.11b or 802.11g protocols with WPA security enabled*
>
> ** If WPA security is not supported, WEP security is allowed instead (with the highest possible level of encryption, but not lower than 128 bits)*
>
> ** The wireless implementations should be hardened to minimize risks and information leaks (like: SSID broadcasts should be disabled)*
>
> ** Multi-layered access controls should be put in place to further improve wireless security and to make hacking more difficult (access controls by MAC addresses, by shared passwords, and user certificates)*

Wireless security considerations were partially based on the following reference material: (Reference D.) Wireless Network Security: 802.11 (11/2002) by NIST: http://csrc.nist.gov/publications/nistpubs/800-48

The password and account reset procedures existed from the beginning. However, the account management principles were not integrated into the old corporate policy. Therefore, the new statement about account management was added.

14. All computer accounts are managed per guidelines of the Access Controls section of the ISO/IEC 17799 security standard.
(Reference #2)

Responsibilities (Eval.)

The Identity Protection policy compliance was not audited and enforced before. Therefore, the implementation of the policy was not completely successful.

For that new addition for the Responsibilities was created:
** The Corporate Audit team is responsible to audit for compliance with this policy at least annually.*

Action (Eval.)

Actions related to handling identity protection in wireless environment were added:

8. Users utilizing wireless access for FWS Banking should receive sufficient training on secure use of wireless devices (Examples: enabling encryption, personal firewalls, good password procedures, etc.).

9. Corporate Security of FWS Bank should conduct regular wireless audits of the FWS Bank Datacenters for unauthorized / unsecured wireless installations.

10. User certificates already utilized in FWSB' (wired) online banking should be integrated into the wireless authentication and encryption mechanisms of the wireless PDAs (currently in pilot stages). The user certificates should be used for standardized identity validation across wired and wireless media.

Actions on better password and account management were added as well:

11. Password and account management procedures should be reviewed for compliance with this Identity Protection Policy. The procedures should be updated accordingly.

==============================

5.3 New Online Banking Identity Protection Policy

(In effect since 01/01/2003)

NOTE: All changed from the previous version or added parts are marked with *Italicized Font.*

Purpose (New)

Online banking is the key service offered by FWS Bank. This Identity Protection Policy is aimed to protect private information of customers and employees during online banking. Violations of this policy should be investigated with necessary administrative, disciplinary, and/or legal actions. Accepting this policy is required for all of the Bank's customers and employees (prior to accessing the Bank's network).

Definition (New)

This policy defines Online Banking as: The ability to perform FWS financial transactions utilizing telecommunications services.

In this context, Identity Protection is defined as a set of measures and technologies to safeguard personal private information up to the sufficient level.

The specific definition of the sufficient level of protection will change will depend on real risks affecting the users. Therefore, the sufficient level of protection will change wit time.

Background (New)

The background and objectives of the FWS Bank's Identity Protection Policy are:

1. To assist users in safer Online Banking
2. To protect the Bank's assets (confidentiality, integrity, and availability)
3. To manage risks of financial losses due to security breaches / security incidents resulting form Identity Theft
4. To comply with all applicable laws.

Scope (New)

This policy covers Identity Protection for all types of Online Banking offered by FWS Bank:

* Online Banking via the wired Internet
* Online Banking via dial-up services (phone lines)
* Online Banking via private network connections
** Online Banking via wireless Internet (802.11a, b, g)*

Policy Statement (New)

The new Corporate Security Policy is based on the ISO/IEC 17799 security standard. This Online Banking Identity Protection Policy is a subset of the Corporate Security Policy. Therefore, it is must comply with the ISO/IEC 17799 security standard where applicable. Identity Protection is addressed (from various viewpoints) in ISO/IEC 17799 Chapters 6-12 (Reference #2).

All ISO/IEC 17799-compliant principles from the old policy are preserved and listed below. New related requirements of ISO/IEC 17799 were added: specifically from the section 12.1.4 (Data protection and privacy of personal information) of the ISO/IEC 17799 security standard. See Corporate Security Policy for details.

The following guiding principles outline the Online Banking Identity Protection Policy:

1. Identity and personal data of customers and employee must be protected from theft and modifications. Maximum effort should be taken to prevent disclosure or eavesdropping of this information during all stages (transmission, processing, archiving,

etc.). The only exception is in cases when a disclosure is required by applicable laws (like in cases of investigation).

2. The personal identity information is used for creation of online access accounts and for verification purposes. The personal identity information should nod be exposed or used for any other purpose.

3. The personal identity information should not be stored in high-risk systems, like servers accessible from the Internet, publicly available systems, etc.

4. Any software and hardware that violates this Identity Protection Policy should not be used.

5. Management and staff of FWS Bank should be trained on secure handling of personal identity information.

6. Customers / Employees utilizing Online Banking service must sign their agreement form of Appropriate Use Policy (that includes rules for handling of personal identity information).

7. Employees utilizing FWSB computer accounts should be guided by the same principles.

8. Wireless banking is only allowed utilizing the below or better security configurations:

> ** Wireless 802.11b or 802.11g protocols with WPA security enabled*
>
> ** If WPA security is not supported, WEP security is allowed instead (with the highest possible level of encryption, but not lower than 128 bits)*
>
> ** The wireless implementations should be hardened to minimize risks and information leaks (like: SSID broadcasts should be disabled)*
>
> ** Multi-layered access controls should be put in place to further improve wireless security and to make hacking more difficult (access controls by MAC addresses, by shared passwords, and user certificates)*

Responsibilities (New)

* The Upper Management of the FWS Bank has ultimate responsibility for secure and safe Online Banking service.

* The Security Group formulates security policies and standards.

* The Corporate IT team implements the above policy upon approval of the Upper Management.

** The Corporate Audit team is responsible to audit for compliance with this policy at least annually.*

Actions (New)

The following specific actions are necessary for implementing the Identity Protection Policy.

The steps #1 and #2 should be performed at least quarterly (or after any significant security infrastructure change). The other steps (#3 - #7) should be checked for compliance by assigned Corporate Security members at least daily.

1. A Security Manager should be assigned to oversee security compliance of the Online Banking according to the FWS Bank's Policies, Standards, and applicable laws.

2. A formal Risk Analysis Process should be performed for Identity Protection compliance in procedures, applications, and network components. Risk mitigating controls and procedures should be developed as well.

3. The confidentiality and integrity of data transmitted via Online Banking connections should be protected. 128-bit SSL encryption (or better) is required.

4. Users should be advised and discouraged from using software and hardware known for violation privacy and handling personal information insecurely.

5. Whenever users discover facts of leaking of personal information (or errors), they should immediately report this to the Corporate Security of FWS Bank.

6. Corporate Security of FWS Bank should proactively monitor any applicable international laws related to identity protection. Any cases of conflict with this Identity Protection Policy (and The Corporate Security Policy) should be reported to upper management. Significant changes in the related laws might require modifications to this policy.

7. Corporate Security of FWS Bank should proactively search the Internet resources for any signs of stolen proprietary information of the FWS Bank (including identity information of FWS Bank). If such information is found, they should consult Law Department of FWS Bank for further actions.

8. Users utilizing wireless access for FWS Banking should receive sufficient training on secure use of wireless devices (Examples: enabling encryption, personal firewalls, good password procedures, etc.).

9. Corporate Security of FWS Bank should conduct regular wireless audits of the FWS Bank Datacenters for unauthorized / unsecured wireless installations.

10. User certificates already utilized in FWSB' (wired) online banking should be integrated into the wireless authentication and encryption mechanisms of the wireless PDAs (currently in pilot stages). The user certificates should be used for standardized identity validation across wired and wireless media.

11. Password and account management procedures should be reviewed for compliance with this Identity Protection Policy. The procedures should be updated accordingly.

==============================

5.4 Password / Account Reset Procedure for Customers

(Assignment 4)

(In effect since 01/01/2003)

This procedure is a part of the new Online Banking Identity Protection Policy that states:

11. Password and account management procedures should be reviewed for compliance with this Identity Protection Policy. The procedures should be updated accordingly.

Purpose (Proced.)

Abuse of password / account reset procedures can be exploited by cyber criminals in Identity Theft schemes.

This procedure is designed to provide a safe ways for password and account reset for online banking customers of FWS Bank. The procedure has built-in mechanisms against Identity Theft. The purpose of the procedure to provide password and account reset mechanism with a practical set of checks and balances to minimize risks of user impersonation and account abuse.

* The below Checklist is activated upon a phone call or email from a customer requesting password / account rest
* If the user is successfully validated, the reset is performed by a Help Desk representative over a secure connection to the authentication server
* The Help Desk representative must confirm his / her identity via certificate-based authentication before the reset actions can be performed
* The authentication server access and functionality by Help Desk representatives is restricted to the scope necessary for their duties.

Scope (Proced.)

The procedure covers password and account rest requests from the bank’s customers. The procedure affects:
* Customers requesting password and account resets
* The Help Desk of FWS Bank performing the procedure according to the below Checklist
* The Fraud Department of FWS Bank monitoring recently reset accounts for suspicious activity

Procedure (Proced.)

Note that users are able to change their passwords and cancel their accounts remotely via valid authentication. The below procedure is only for cases when the password is lost, or forgotten. The sequence and the details of the below procedure will be changed periodically to prevent Identity Theft via replaying a well-known procedure.

The Password / Account Reset Validation Checklist
(When requested via phone or email)
NOTE: All email communication must be digitally signed on each end (with the user certificate and the Help Desk certificate).

	Steps	**Results**	**Comments**
1. □	Record the name (and username) of the requester and validate if the name is listed as a customer of the bank (if the name is valid, go to the Step 2)	The reset procedure cannot continue if the name is not confirmed and/or spelled incorrectly	Initial identity verification
2. □	Ask the requested to connect to the FWS Bank's authentication server via HTTPS (from PDA or PC) and to present the user's certificate (If the certificate is valid, go to the step 3)	If the certificate is not validated properly or cannot be found, go to the Step 3.	This is the most preferred way, since user is responsible for proper protection and handling of their FWS Banking certificate
3. □	If the user certificate validation did not work, ask the user to confirm: * The date of the initial account creation * The account number * The secret word provided by the user initially (you can assist with a hint on the category)	If all three validations in this step were successful, go to the step 4.	The procedure intentionally avoids using SSN since this information is often stolen, or could be stolen during these steps. Instead, other unique user information is validated. For the validation steps use the user information and keywords stored in the account database.
4. □	The password or account can be reset at this stage. However, the account will remain under fraud inspection for 30 days for any suspicious activity. The Fraud Department of the bank will call the user's home number to	Reset the account to a temporary (hard to guess) password and communicate it to the user. The user will be forced to change the password upon his/her first logon. The user has 24 hours to do so. Otherwise,	**Validation:** a reset automation script (used by Help Desk at this step) will enable the reset account to be available for 24 hours (for the user logon and password change). Help Desk and Fraud Department are notified via email when the first

	verify the first transaction after the reset.	the account is locked.	user logon is performed. They are also notified if there was no logon within 24 hours (to inform that the account is locked at that point).

Responsibility (Proced.)

* The Help Desk of FWS Bank is responsible to answer the customer calls regarding password and account reset.

* The users are responsible to keep their FWS Bank certificates securely.

* The Fraud Department of FWS Bank is responsible for monitoring the newly reset account s fro suspicious activity.

Revision History (Proced.)

Version 1.0.
In effect since 01/01/2003

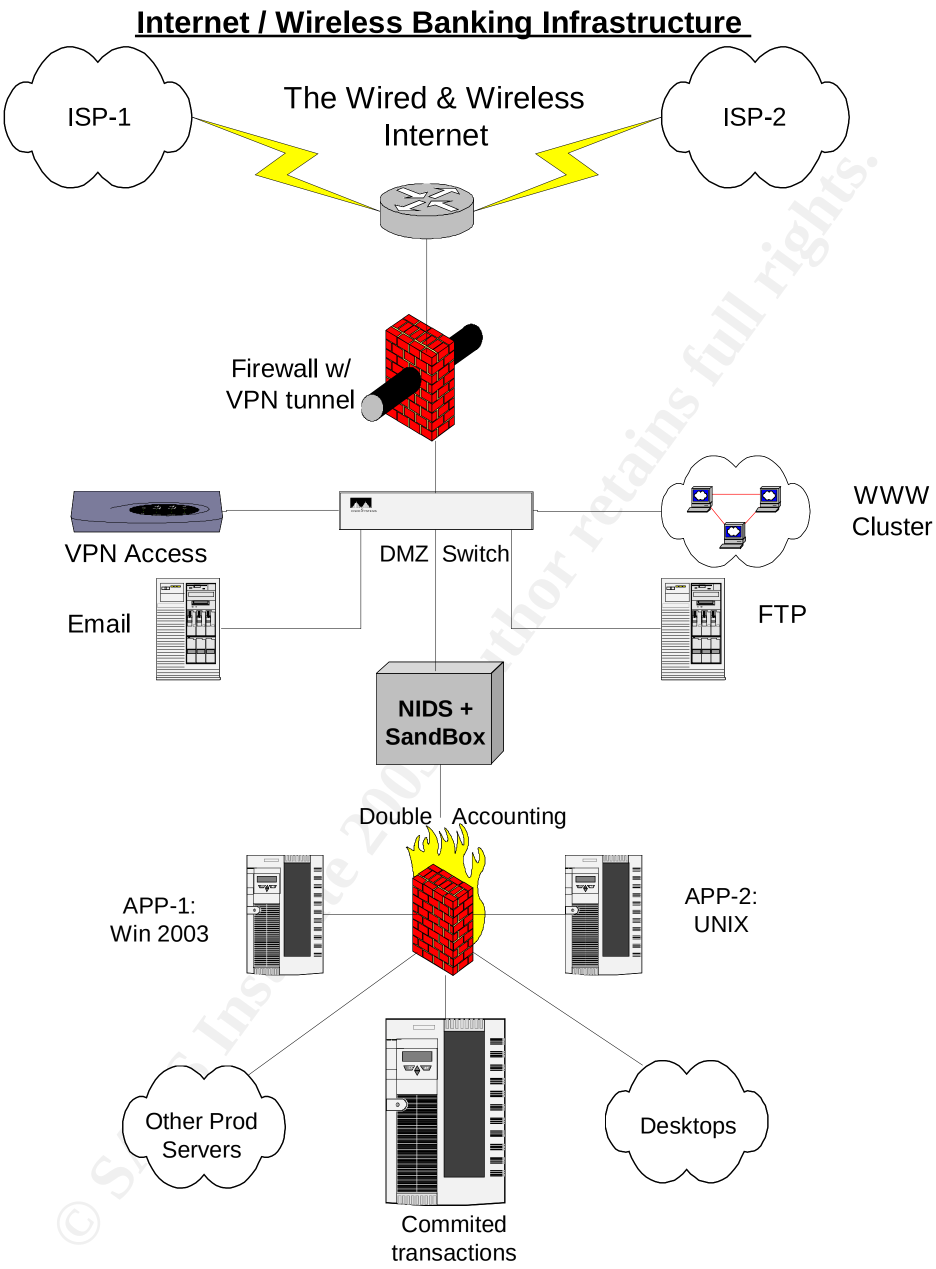
Reference (Proced.)

* Online Banking Identity Protection Policy: *"14. All computer accounts are managed per guidelines of the Access Control section of the ISO/IEC 17799 security standard. See Corporate Security Policy for details."*

* ISO/IEC 17799, security management standard: http://www.iso.ch/cate/d33441.html (Reference #2).

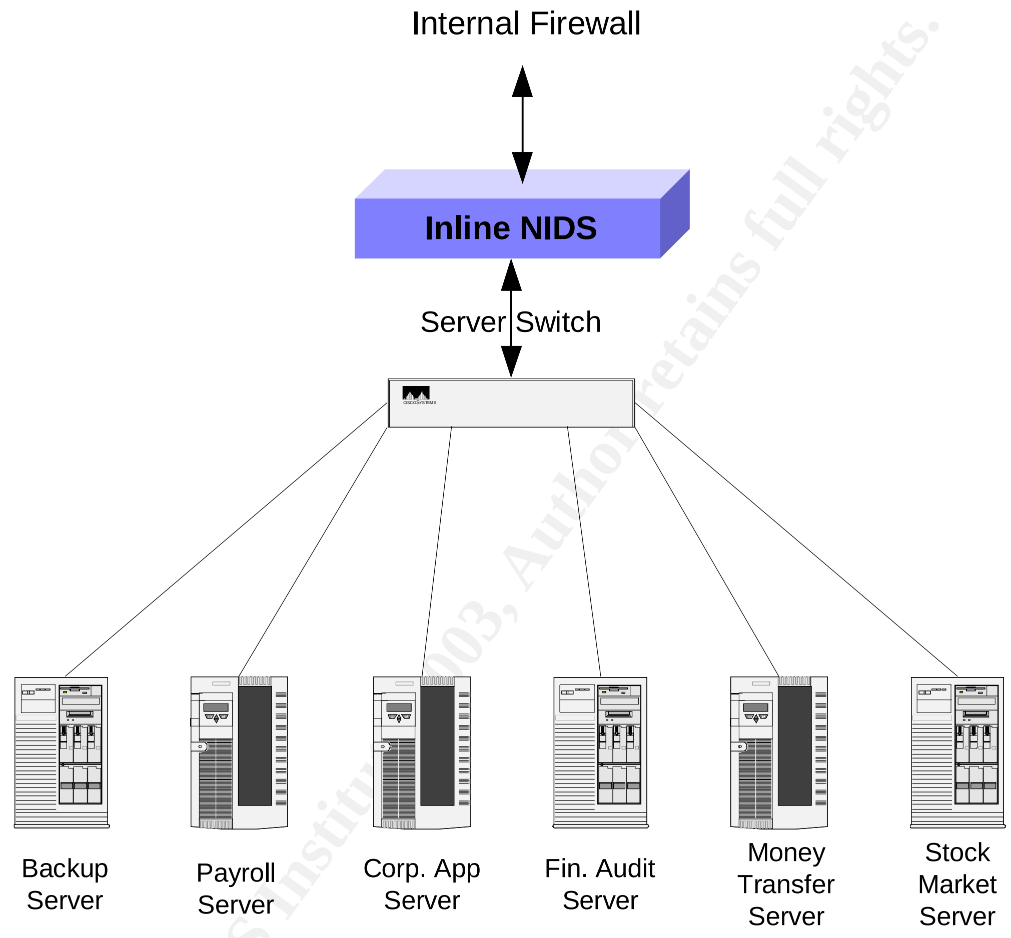
The following network diagrams are referenced and discussed in the above sections.

6.0 APPENDIX A – FWS BANK' DMZ ARCHITECTURE

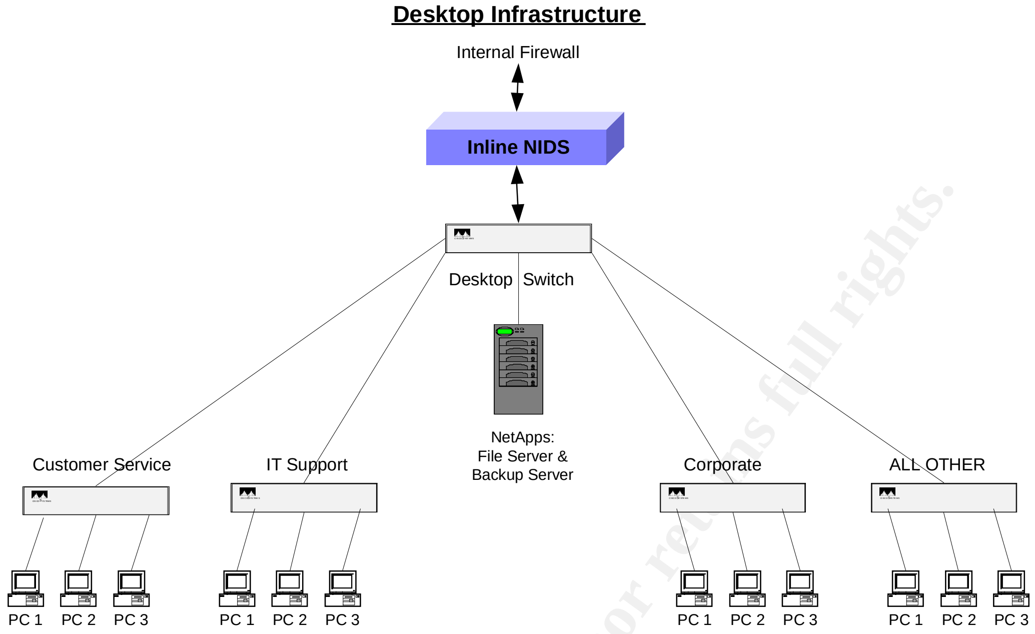


7.0 APPENDIX B - FWS BANK' PRODUCTION SERVERS

Other Production Servres

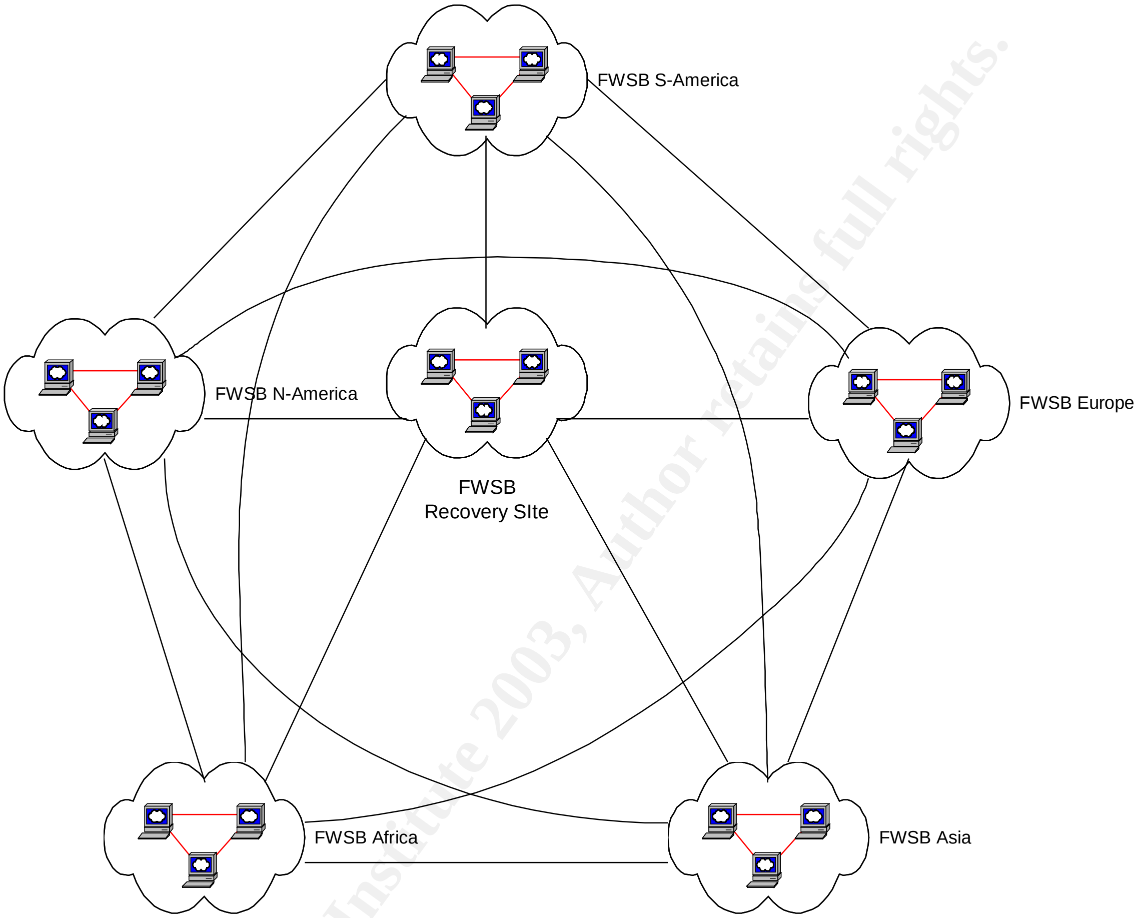


8.0 APPENDIX C - FWS BANK' DESKTOP INFRASTRUCTURE



9.0 APPENDIX D - FWS BANK' WAN CONFIGURATION

Global WAN of FWS Bank (Mesh Topology)



10. REFERENCE

10.1 Publications

The following references were used in preparation of this document (as well as partially referenced in the document):

1. SANS Track 9 – Information Security Officer Training (Study materials)

2. * ISO/IEC 17799, security management standard: http://www.iso.ch/cate/d33441.html.

3. Wadlow, Thomas: The Process for Network Security (2000), ISBN: 0-201-43317-6

4. Peltier, Thomas: Information Security Risk Analysis (2001), ISBN: 0-8493-0880-1

5. Toigo, John: Disaster Recovery Planning (2000), ISBN: 0-13-084506-X

6. Prosise, Chris and Mandia, Kevin: Incident Response: Investigating Computer Crime (2001), ISBN: 0-07-213182-9

7. Zwicky, Elizabeth; Cooper, Simon; Chapman, D. Brent: Building Internet Firewalls (2000), ISBN: 1-56592-871-7

8. Goncalves, Marcus: Firewalls Complete (1998), ISBN: 0-07-024645-9

9. McClure, Stuart; Shah, Samuil; Shah, Shreeraj: Web Hacking (2003), ISBN: 0201761769

10. Taylor, Ed: Networking Handbook (2000), ISBN: 0-07-135451-4

10.2 Online Resources

A. SANS Reading Room: www.sans.com/rr

B. CERT Coordination Center: www.cert.org

C. Security Focus: www.securityfocus.com

D. Wireless Network Security: 802.11 (11/2002) by NIST: http://csrc.nist.gov/publications/nistpubs/800-48