Global Information Assurance Certification Paper

5 Principles of Security

&

Where We Went Wrong

Laurie McManus
April 24, 2004

Practical Assignment v1.4b in completion of GSEC certification requirements

Abstract

GIAC Enterprise Bank &Trust has been in existence for over 100 years, and historically has trailed behind the industry in terms of technology advancements. With a "push" to capture a growing market of customer needs, GIAC Enterprise Bank &Trust rapidly made the technological jump, relying on contractors and out-sourcing for specific needs. Relying on outsourced staff, GIAC Enterprise Bank &Trust unknowingly broke the #1 principle of security's golden rule: "Know Thy System", resulting in large financial losses.

The issues that GIAC Enterprise Bank &Trust faced could easily have been avoided had management spent the time necessary to plan. Management was not prepared for the massive initiative it was about to take as a lack of technology understanding was considered not important at that time. GIAC Enterprise Bank &Trust has now addressed the need for internal security awareness and has launched an aggressive plan for physical, data and internet security, policy creation, enforcement and social engineering, but will continue to struggle until all risks and vulnerabilities have been addressed.

This document will address a summary of the initial problems and resolutions, but in no way attempts to cover all remaining vulnerabilities, not yet addressed. The growth explosion from 13 to 25 branches experienced by GIAC Enterprise Bank &Trust during the same 18 month time period as their decision for a technology leap caused needless financial losses for GIAC Enterprise Bank &Trust. A thought out plan could have ensured a smother transition, with less loss of revenue from having to dump systems and start from scratch.

Table of Contents

I. Company Background

We've only just begun

1. Who is GIAC Enterprise Bank &Trust?

GIAC Enterprise Bank &Trust was founded in 1901 and stands today as one of the fastest growing community bank in Maine. At 2.0 billion in assets, GIAC Enterprise Bank &Trust is committed to remain on top of the market.

With the induction of internet banking services, and internet access for internal employees to compete with other institutions, the need arose to offer an internet presence. Customers are now able to conduct banking business online, verifying balances, making account transfers, balancing accounts, as well as contact their service representatives via email for transactions and investment opportunities.

GIAC Enterprise Bank &Trust did not have the security concerns that faced their competition, as GIAC Enterprise Bank &Trust believed they were not accessible from the outside, as they did not have an official World Wide Web presence. GIAC Enterprise Bank &Trust network was limited to a UNIX mainframe/dumb terminal connection to users, and few departments were set up with an internal network, for ease of print and file sharing. A few stand-alone pc's were positioned within certain departments that housed individual dial up networking accesses to the internet, however, these pc's were not connected internally to the bank's network.

2. How did this happen?

In 1999 GIAC Enterprise Bank &Trust decided that in order to compete with larger, more advanced financial institutions, they would need to advance by jumping into the technology industry, to offer customers the same services as other institutions. In order to catch up, each department was given an open check book in order that they would have the opportunity to rapidly deploy new systems, believing the non-technical staff would learn how to use their own software and therefore administer for themselves. GIAC Enterprise Bank &Trust decided on a complete infrastructure upgrade from a mainframe environment to a more progressive option of installation of Windows 2000 servers and Windows 98 clients, for its 13 locations, spread out over 4 counties within the state.

With the blessing of upper management positions, this conversion was overseen by a single internal communications engineer, who was proficient with the current token ring configuration, but was lacking knowledge in installation and maintenance for networks beyond the mainframe, or personal-stand alone pc setting. Vendors were hired for this massive conversion; and all internal dumb terminals were replaced with new pcs with the Windows 98 operating system installed. Clients were impressed with the newly

improved method of file sharing that no longer relied on sneaker-net, and were excited over the new, internal only Exchange 5.5 email system.
In the absence of internal technology knowledge, the network was piecemealed together, building departmental networks individually, and then transitioned into one enterprise level network, hiring a different vendor for each migration. The only exception being 2 departments that had already been created three years prior, and their vendors required they remain separate.

Each department had knowledge of their own business needs and wants, and without any knowledge, guidance, or plan, vendors were given free reign in installing their own packages, on newly installed domain controller servers, or any server that could be discovered to have "room".

In early 2000, management's fire alarm first sounded upon receipt of FDIC's notification for GIAC Enterprise Bank &Trust's first FDIC "Technology Audit" scheduled to take place 6 months from date of notification. This audit was designed specifically to address compliance with the induction of government mandates, 1999 Graham-Leach-Bliley Act.

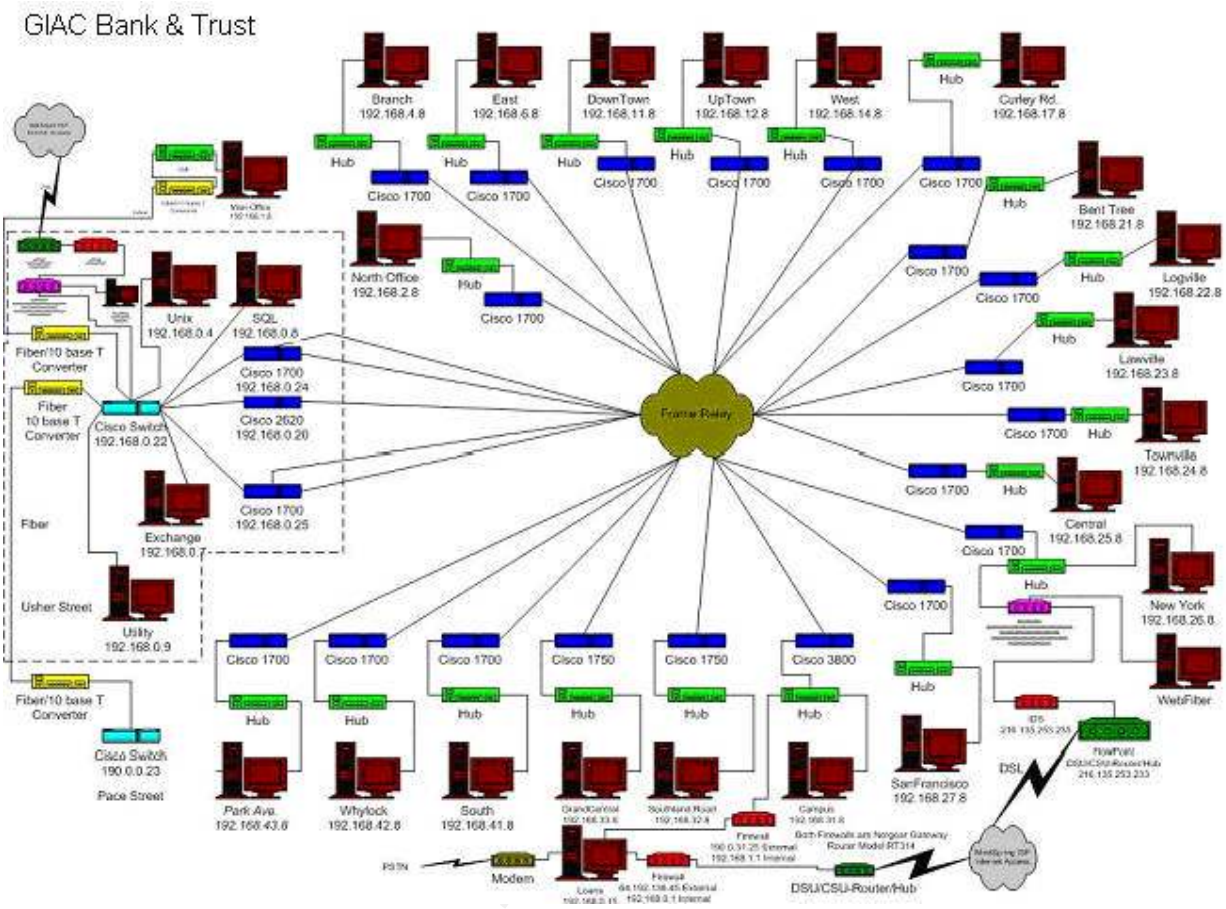
"The Gramm-Leach-Bliley Financial Modernization Act of 1999 requires companies to give consumers privacy notices that explain the institutions' information-sharing practices. In turn, consumers have the right to limit some - but not all - sharing of their information." [1]

GIAC Enterprise Bank &Trust's Audit & Risk Management department quickly created a mandatory training session for all employees, to educate them regarding the new practice of giving all customers privacy notices to explain our new practices, in compliance to The Financial Privacy Rule portion of GLB. However, GIAC ENTERPRISE BANK & TRUST was not prepared for the Safeguards Rule portion of GLB that stated,

"The Safeguards Rule requires all financial institutions to design, implement and maintain safeguards to protect customer information." [2]

Realizing their responsibility now required the ability to implement and maintain, to support this compliance, management decided to invest in hiring a network administrator, and the I.T. department was born.

II. Network Layout



Each branch/location is configured in a star topology, utilizing Ethernet connections to a switch, which is then connected to a router, and is connected to the operations center via frame relay.

Campus locations (indicated in the diagram with a dotted line) are connected via fiber backbone, and are centrally located within a four block radius.

III. 5 Principles of Security

A. Know Thy System

Know thy system is the first of 5 principles of security, which is most likely the most important. Know thy system is the concept of understanding what is connected to the network, how it is configured, what is its purpose, and what its needs are. With the many implications of knowing and understanding a systems/network/business process need, the other principles of security will follow suite. Knowing and understanding all the given systems on a network will give the business understanding of the vulnerabilities/threats that their system is vulnerable to.

"In order to know whether your systems are secure or have been compromised, you must know the services that are running on your systems and which ports they have opened up. Attackers connect to systems via these ports and then compromise the underlying services to get access to the computer. Knowing what those access points are is critical" [3]

1. What we did wrong

GIAC Enterprise Bank &Trust relied solely on the suggestions of contractors/vendors to plan and deploy the network and system setup. With no one the wiser, servers were not secured, nor were they part of a patch management system to ensure they were updated against vulnerabilities. Every few servers were installed by a different vendor or contractor who did not follow an established guideline for security purposes, as no guidelines were established. Each had their own beliefs on the configuration for a server, including what services should be turned on and open ports. With an eye on decreasing cost, workstations were purchased based on "deal of the week", from local warehouse type sales, and included Windows 98 SE, as the operating system. Each system was installed "out of the box"; what ever home-use type software was included, remained on the system. Individual copies of Norton Antivirus was purchased and installed, but not configured correctly to update definitions. Once the internet was available to users, downloaded games, web-shots screen savers, web radio, chat, etc, was reaching epidemic proportions, as no means of control or management of systems were in place, the network administrator was reduced to desk side support, leaving the servers unmanaged, in an attempt to keep all users working.

2. How we have corrected

GIAC Enterprise Bank &Trust first recognized the growing need for desk side support and approval was made to increase the I.T. department to include a help desk analyst and two desk side support technicians, to manage 300 client pcs.

"New layers of security are ineffective without intelligent management infrastructure."[4]

A more drastic change finally took place a year later upon GIAC Enterprise Bank &Trust's recognition that main systems were unstable and crashing, along with an unstable network that was up and down on an hourly basis and realized the need for investing on the means to get the technology growth under control. The I.T. department then began to grow with the hiring of an I.T. Director with experience in financial institutions.

Under the guidance of the new I.T. director, replaced existing client hardware for a more stable, business grade hardware that includes a more secure operating system (Windows XP), forcing users to log on to the network, has also forced a standardized security settings (no users have the ability to download/install applications without the written knowledge of I.T.) – to pass through an authentication method that will ensure this new software does not interfere with security settings on the workstation. Client workstations have been configured with Norton Anti-virus enterprise solution that manages virus definition updates and system scanning on a regular basis. Systems have also been installed via an imaging process that ensures all pc's have the basic system software and configuration that includes Microsoft's SMS and Norton Anti-virus, to allow for managed care, and removes user's ability (rights) to make changes. This solution also gives the network administrator an easier solution to verify the health of all managed client systems. Coupled with written and published acceptable use policies, social engineering is beginning to take shape, as users are now forced to follow password guidelines that include password complexity, 90 day forced changed, and a policy that remembers the last 18 passwords used. Client systems were further secured via group policies and administered through active directory.

Vulnerability/baseline analysis was run on all existing servers, to get an overview of the current configurations & vulnerabilities. Servers were then secured based on newly established guidelines for configuration, followed by installation of service packs, and security patches. Servers have also been installed with Norton Antivirus Server application as well as SMS to ensure ease of patch and upgrade management, in an effort to co-inside with Microsoft's recent election to release patches once a month, the implications could cause catastrophic proportions, if a system is left vulnerable for too long.

An IDS was installed, and is currently vendor monitored, with daily reports emailed to GIAC Enterprise Bank &Trust on activity. This was the best solution, at this time, on the view of cost savings for hiring and training a new employee was not an option. The vendor has contact numbers in the event an incident arises. The previous "home" level firewall was replaced with a more robust firewall, designed for a business environment.

3. Future

In the near future, guidelines will continue to be modified, enhanced and monitored for their complexity or ease of compliance, and changes will be made accordingly.

Patch management have been established in a simple spreadsheet layout that identifies changes/updates/upgrades for all servers. Vulnerability testing guidelines have been issued and include a rotation schedule that ensures all servers are current on patches and security updates. GIAC Enterprise Bank &Trust is investigating industry offerings of patch management software. Vulnerability testing will continue on all systems on a rotation schedule.

B. Least Privilege

"The principle of least privilege states that you give an entity the least amount of access it needs to do its job and nothing more. This principle applies to systems and users of those systems."[5] Principle of least privilege is the concept of not allowing users or equipment access to other equipment/users/data. The more restrictive the access is will compensate in a more secure and the less chance of a possible for accidental (or not-so accidental) mistakes. The concept is to start with nothing & grant only as needed. This concept is not limited to data access, but to physical accesses as well.

1. *What we did wrong*

In the initial environment, decision makers, lacking the knowledge of the importance of only allowing what is needed, opened access to all users, vendors and guests.

In an effort to avoid restrictions, users shared their passwords/key/ with co-workers, contractors and vendors who may not have their own, or have forgotten their password. It was discovered that users who were no longer employed with the bank still had active accounts. When investigated, users reported that they *"used that id, because I needed to get to a secured page that no one but her had accesses*."

The process of revoking an access only upon abuse, neglect, termination (IF reported), or audit findings was the normal procedure.

2. *How we have corrected*

Since all accesses were granted by default, GIAC Enterprise Bank &Trust first invested months educating users on the need for stricter security for compliance requirements, however, acceptance of this level of change has proven quite a challenge in revoking accesses. Users have become offended, believing the new "I.T. Department thinks we're all thieves."

GIAC Enterprise Bank &Trust has installed physical card accesses to buildings, departments, and rooms, where a person may only enter with correct accesses. Although this hinders access to some, this by no means eliminates the problems where others will open the door, for an unauthorized user or a co-worker who "forgot" their

badge. Only through continual education, documentation (guidelines) and training, and enforcement, will this issue become more manageable.

GIAC Enterprise Bank &Trust has also initiated written guidelines & created forms to document system accesses in account generation, termination and changes. System owners must be made aware of who has access by authorizing access to each user.

3. Future

GIAC Enterprise Bank &Trust will continue to define, modify, train and monitor the success of these guidelines; however social engineering will continue to take a growing role.

C. Defense in Depth

"The approach of layered, defense-in-depth policy, procedures and tools is well accepted as best practice for information security." [6]

Defense in Depth refers to "build(ing) successive layers of protection around anything that we are trying to protect." "Using a Defense in-Depth strategy does not make it impossible to get to your core resources"[7]

A Defense in-Depth strategy will not guarantee no-one can or will reach the item protected, but it will hopefully slow them down, until their attempt can be noticed and stopped. Multiple "layers" of defense is the concept of ensuring the best possible configuration is in place. As in the concept of peeling an onion, we can only hope that each layer will bring about a bit more of a challenge to go forward. With any luck, the attacker will go elsewhere, where they don't have to work as hard. What follows is a brief overview of the 5 minimum layers for a defense in-depth strategy, and how GIAC Enterprise Bank &Trust implemented them.

1. Security policy

"Security Policy protects both people and information."[8]

A security policy should be created to guide others on the correct or acceptable use of systems and accesses. A security policy should be easy to follow for all employees and should include acceptable use, as well as consequences of non-compliance. The security policy should be able to apply to the best and worst employee, without bias.

a. What we did wrong

GIAC Enterprise Bank &Trust did not create a security policy beyond the initial mainframe systems. Users were instructed to keep their passwords to themselves, but this policy was not enforced. Only the "root" password was kept private, however, all

users that 'needed' this level of access utilized the same password. Individual root access accounts were not created. From the department head to the computer operator, a total of 6 users had full root-level access. The only audit in place could identify a date & time the root account was used, but no identification as to who was using it. This security policy was not sufficient in addressing network, physical accesses and data security.

b. How we have corrected

GIAC Enterprise Bank &Trust has created, approved and is enforcing new security policies that monitor compliance from all users, for all systems. The initial UNIX system is in works to be replaced with a more robust and secure system, and will be managed and audited by a new core system group, which will monitor system accesses. No two users will access the system utilizing a "master" password.

Auditing is now being utilized for system access, changes, etc., on not only the UNIX system, but also on Windows 2000 servers, network routers, firewall and IDS.

c. Future

GIAC Enterprise Bank &Trust will continue to define, modify, train and monitor the success of these guidelines.

2. Password strength & assessment

Passwords should be designed & enforced in a manner that will ensure data protection. Guidelines have to be written and users have to be trained to understand the guidelines, as well as having explanation of failure to comply.

a. *What we did wrong*

Security was not explained to users. Most users were able to "cancel" from authorizing on the network, & most used weak passwords on mainframe accesses. Users also shared passwords with peers. No repercussion would come from an infraction of following the rules, and users did not develop an understanding of the need to protect passwords. Passwords strengths were never tested to ensure compliance.

b. *How we have corrected*

Password complexity has been enforced, coupled with a force-change at 90 day intervals, not allowing the same password for 18 cycles. During training/re-education sessions, users are given easy to remember methods of password creation (for example – using the first character in a favorite quote) which has encouraged users to be original in their passwords. Training users to understand the requirements, along

with published guidelines have helped users understand and to protect their identities & passwords.

c. *Future*

GIAC Enterprise Bank &Trust will continue to educate and enforce password complexity, and has plans to implement regular testing utilizing password crack software.

3. Incident handling

"Incident handling is an action plan for dealing with intrusions, cyber-theft, and denial of service, fire, floods and other security-related events." "Incident handling is that planning is essential to the success of a strong incident handling foundation."[9]
An incident could be in any form, deliberate or accidental changes or deletions from within a network, and also includes all forms of disaster or any type of compromise of internal data. An incident handling plan is to possibly prepare for the worse. As no one can possibly plan for any and every form of incident, in preparing a plan, it is in hopes that if an incident arises, we'll have a starting point, and hopefully avoid panic, lessening the severity of the incident.
.

a. What we did wrong

GIAC Enterprise Bank &Trust has not enacted any type of plan or documentation in the event of an incident with the exception of the mainframe contingency/disaster recovery plan. For all other servers/routers, switches, firewall, etc. have been treated with a "fix if/when it breaks". This has caused us numerous wasted hours while trying to recover from a crashed system. No method of tracking the cause of the crash other than hardware issues. Systems had not been monitored for attacks, or unauthorized accesses.

GIAC Enterprise Bank &Trust did not have a disaster recovery site, or plan (beyond recovering the mainframe only). When an issue/incident arose, a backup tape will be inserted into the mainframe, records restored, and processing continues.

b. How we have corrected

GIAC Enterprise Bank &Trust is in process of creating a new disaster recovery plan, which will include a departments' needs (which server to recover first). A new DR site has been purchased and remodeled to house needed equipment, and equipment is in process of installation. A business continuity specialist has been hired, who is managing the progress of the DR process. An incident handling plan is in process that will include logging and a section for each server/service/department that will give detail on handling an incident, as well as documentation for configuration settings.

c. Future

GIAC Enterprise Bank &Trust will have regular DR testing, to ensure the success of all systems and processes, and will continue to update documentation. Incident logs will be monitored for completion, and for reoccurring events, that may be a signal of a more serious issue.

Upon completion, documentation manuals will be kept up to date with a change management log, showing changes/updates to all systems, in the event of a disaster, to expedite recovery.

4. Information Warfare

> "*Information warfare is the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries.*"[10]

In a defense strategy, information warfare is the plan or ability to protect or ensure data's integrity. This can be approached not only in defending the information from attack, but to secure those that access the data, cannot manipulate, corrupt or destroy the data in an effort to misrepresent the company, users, or customers.

a. What we did wrong

Users were under the impression that if the computer printed out the information, it had to be true. Users had yet to understand the concept of data integrity.

Users were not educated on the integrity of what they read on the internet may not be correct. Users were not familiar with the mass information stores that were now at their disposal. GIAC Enterprise Bank &Trust did not prepare users to validate information. As users were not restricted to productive business web sites, the bank was beginning to be increasingly bombarded with spam, as users were readily giving their email addresses over the web, at any location that requested it.

b. How we have corrected

Systems are being created to test internal data integrity, coming from our current mainframe system.

Web management software has been installed, and users are being restricted from unproductive surfing. This has cut down on internal user's problem of sharing the "latest & funniest" picture on the web, as well as erroneous information.

c. Future

CB & T will continue to investigate and develop guidelines to assist in data integrity.

5. Web security

a. As Defined for the purpose of this abstract

"Security is no longer simply a matter of hardening your Web Server; you must design security into your applications and browsers as well."[11]

Previous understanding of web security encompassed the concept of hardening a web server. This concept no longer applies, as not only are the web servers at risk, but web applications are at a high risk, due to their increase in use. A simple web research project for information can return damaging scripts embedded within a web server's response. This could have been at the result of the web server previously being compromised, with no visible indication; the client could download embedded code, and infecting their own pc's, and consequently the company's network.

b. As defined for GIAC Enterprise Bank &Trust

As GIAC Enterprise Bank &Trust has launched an internet presence on the World Wide Web, we have chosen at this time to opt for outside web hosting. Internet content is updated, managed, maintained and secured at the hosting company. Future plans indicate a possibility of launching an intranet, to be hosted internally for employees, and depending on the success, the possibility of internal hosting for internet presence will be considered.

In the interest of securing browser and internet connectivity, security has been increased in client browsers, by not allowing automatic downloads of internet scripts (applets, java, etc.). This does on occasion render a client unable to open a web page or access a web application until the script can be checked & possibly downloaded to clients on an as-needed basis, based on job requirements.

D. Prevention is ideal; detection is a must

"As long as your network is connected to the Internet, there's no way to prevent every attack. Therefore, you must not only deploy multiple layers of protection, but also have mechanisms in place that allow you to detect an attack before serious damage has been caused."[12]

1. What we did wrong

Prior to the introduction of the web to GIAC Enterprise Bank &Trust, the only "foreseeable" risk to guard against was from internal users accessing fellow employee's accounts. The idea of protection of the mainframe system was limited to the concept of physical security, and preventing "non-authorized users" from accessing "root-level" access to the mainframe. Auditing was active in the ability to recognize when one employee looks at the checking/savings account of another employee, but other risks were not noted.

With the introduction of the internet to GIAC Enterprise Bank &Trust, the mainframe group mistakenly believed that if someone was not "plugged" into the local network, the data was not at risk.

2. How we have corrected

GIAC Enterprise Bank &Trust has implemented security controls in an attempt to prevent access, and has also implemented audit logs on servers, routers and firewall. An IDS (intrusion detection system) has been installed that is out-sourced managed with contacts in the event of an issue. GIAC Enterprise Bank &Trust has increased staff to monitor/review audit logs collected from all devices, in order to monitor for unauthorized accesses. Systems are now in place to assist in detection.

3. Future

GIAC Enterprise Bank &Trust will continue to modify detection systems to possibly lower security risks.

E. Access Points

Access Points refers to any means that can be used to get inside. Defense of access points would be a hardening to encompass physical and logical means. On the physical side, shutting down unused ports of a switch & ensuring the switch is behind locked doors. On the logical side, this would be in closing unused ports on a firewall or server.

1. What we did wrong

GIAC Enterprise Bank &Trust had no prior understanding of security issues when implementing their LAN. As Windows was decided as the backbone operating system

for the company, software was chosen based on the compatibility with windows. As software was purchased, the vendor was granted access to the network server to load their software. No thought was given to securing a software package or in ensuring the security of the server after software installation. Servers were originally installed using a "default" install selection, and no critiquing took place.

As departments joined the LAN, if a particular department had individual access to the internet, this was added in. After all departments were connected to the LAN, GIAC Enterprise Bank &Trust discovered over 15 separate internet connections. Only 3 were "known" DSL connections. The remaining 12 connections consisted of individual pc's where an individual's job responsibility required internet access, so management would take it upon themselves to purchase a modem, connect to a pc & sign up for individual ISP connection "for their department". As users were added to the enterprise network, so was their dial up access.

Upon the induction of the internet to the bank, users quickly demanded a means to reach their systems from home. Hence the VPN access was implemented, without prior planning, guidelines, or security in place.

2. How we have corrected

GIAC Enterprise Bank &Trust has hired a wan communications manager that is proficient in managing point to point access. He has developed and implemented ACLs (router based access control lists), and is able to monitor for unauthorized activity across the wan. In addition to the ACL lists, he is disabling unused switch ports, closing unused ports and protocols in the firewall. Since all client pc's had been replaced with a new company standard pc that did not include a modem, all dial up and DSL connections to the internet have been disconnected, with the exception of a single entry point that forces all inbound & outbound traffic through the upgraded firewall. The Communications manager was able to disconnect all unauthorized analog phone lines, to ensure users couldn't purchase a modem & "plug in".

With the installation of a more robust firewall solution, a superior VPN was structured. Users must read and sign a policy of acceptable use, as well as VPN home pc minimum standard policy prior to being granted VPN access. VPN access is based on business need, with expressed written consent from upper management and approval from the newly developed I.T. Steering committee.

3. Future

Policies have been written and users will continue to be educated.

IV. Conclusion:

GIAC Enterprise Bank &Trust realizes that the surface has just been slightly scratched in securing our network, and there are many areas of improvement. This document recognizes only those items that were considered first in the interest of lowering the highest risks, in the shortest amount of time.

With the ever growing threat from internal as well as external sources, GIAC Enterprise Bank &Trust has charged forward to protect it's assets with the implementation of a security staff that will monitor, analyze, develop and improve it's network security.

References:

[1] Author unknown. In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act. Federal Trade Commission http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm

[2] Author unknown. SafeGuards Rule: The Gramm-Leach Bliley Act. Federal Trade Commission. http://www.ftc.gov/privacy/glbact/

[3] Cole, Eric. "How to Secure Your company" ComputerWorld. June 26, 2003. http://www.computerworld.com/securitytopics/security/story/0%2C10801%2C82515%2C00.html

[4] Samoun, Gilles. "Thou Shalt Not…" SC Magazine; March, 2004: 29

[5] Cole, Eric. "How to Secure Your company" ComputerWorld. June 26, 2003. http://www.computerworld.com/securitytopics/security/story/0%2C10801%2C82515%2C00.html

[6] McCreary, Larry. "A Proven Paradigm for Best Practices in Information Security" 14 April, 2003 http://www.itsecurity.com/papers/securecomp2.htm;

[7] Cole, Eric; Fossen, Jasson; Northcutt, Stephen; Pomeranz, Hal. SANS Security Essentials with CISSP CBK, Version 2.1, Volume1 SANS Press; April 2003. 294

[8] Committee Authors. "GIAC Basic Security Policy Version 1.35" September 5, 2000; pp 3 http://www.remainsecure.com/whitepapers/policy/basicpol.pdf

[9] Cole, Eric; Fossen, Jasson; Northcutt, Stephen; Pomeranz, Hal. 461

[10] Dr. Ivan Goldberg: "Institute for the Advanced Study of Information Warefare" http://www.psycom.net/iwar.1.html

[11] Cole, Eric; Fossen, Jasson; Northcutt, Stephen; Pomeranz. Hal 532

[12] Cole, Eric. "How to Secure Your company" ComputerWorld. June 26, 2003. http://www.computerworld.com/securitytopics/security/story/0%2C10801%2C82515%2C00.html

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event