Case Study: My first due-diligence

SANS Security Essentials
GSEC Practical Assignment, Version 1.4b

Ken Hogan

January 2003

Table of Contents

Abstract

In this paper I will discuss the approach I took when presented with the challenge of performing due diligence on a small company XYZ with whom my company ABC expressed an interest in creating a joint venture.

I will walk you through the preparation which includes gathering information and preparing a questionnaire in advance. I will explain the results of the interview and site visit and conclude with a list of concerns and recommendations I wrote in order to help influence the company's decision.

Introduction

XYZ is made up of one hundred (100) employees of which ten (10) of them work in IT. They are a third party logistics (3PL) provider with annual revenues of $18 million and an IT budget of $250 thousand. ABC, on the other hand, is a one hundred (100) percent, wholly owned subsidiary of a large publicly owned American firm USX.

ABC's annual revenues are in excess of $5 billion with one thousand five hundred (1500) employees and eighty (80) in IT. ABC has a small division which performs third party logistics (3PL) consisting of twenty (20) employees and one (IT), which is not part of their core business, and would require a significant investment in order to become a player at the next level in the 3PL market. This division has annual revenues of $4 million.
The intent is to merge the two companies allowing XYZ to take over operations of the combined company with each company holding fifty (50) percent of the business.

This would be a one time only opportunity to interview members of XYZ.

Before - Understanding

In order to understand the task more clearly, my first objective was to find out what due diligence meant in this context. I accessed the Internet, using Google (www.google.ca) and typed in “definition due diligence”. Due diligence was explained as, “*The process of checking the accuracy of information contained in a company public statement, such as a prospectus, before recommending that company to others. Is also the act of one company investigating another company before buying its’ shares*.”[i] (Shareanalysis.com)

Based on the second part of the definition, I understood this to mean that the buyers have a responsibility to their stakeholders and themselves to perform an audit of the potential company. It should cover every aspect of the business including information technology (IT) in order to determine the risks and make an informed decision on whether or not to proceed.

Prior to my visit, a preliminary study of the overall environment was conducted by a highly respective technology company (JKL). This study focused primarily on the financial and operational aspects of the business. Their conclusion was that the joint venture would prove to be beneficial to both companies.

In addition, an interview and site visit was carried out by representatives in my company from our Information Technology (IT) department, focusing mainly on the infrastructure and the applications. Security was not involved.

The IT and JKL reports differed considerably. There were concerns surrounding the systems environment and the capabilities of this company to handle the additional capacity introduced by this merger. This represented an additional one and a half (1.5) times the current workload.

These conflicting reports sent a huge shock wave through the executive of company ABC. On one hand, you have a report from a very respectable top technology company and on the other hand one from an internal IT group.

The stage was now set for round two of the due diligence. The IT group was being asked one more time to visit with company XYZ to see if changes made by them throughout the year had significantly addressed the major concerns that were discovered in the first visit. This time, however, our CIO had changed and the new person, whom I report to, wanted security to be represented in the group.

During - Preparation

I was instructed to focus specifically on the network and physical environment. I was on my own to decide how I would prepare for it. Initially I was given no further information and one (1) week to prepare!

My first instinct was to consult our IT Internal Audit department to see if perhaps a checklist or procedure existed within the company. Surprisingly enough, it did not. They did provide me with some sample questions which they routinely ask during an audit. Of the fifty (50) questions asked, only two (2) of them were ones I might use since the majority of them were specifically financial in nature. I then turned to the SANS reading room in the hope of finding something I could use as a guideline, thankfully there was such a paper[II]. (Hartman)

Moving forward, I had two sets of documents which were made available to me. The first set of documents[1] were the result of the initial visit conducted by internal IT. The second set of documents contained an IT organization chart, a network topology, and a diagram illustrating the structure of the servers and applications which made up the computing environment at XYZ. This information is crucial and I highly recommend that you use this as a starting point for preparing your checklist as Anita mentioned in her paper "First get the background".(Hartman)

From the IT document, although it wasn't directly covering security, I was able to determine some facts concerning the overall security posture in the areas of network and physical environment for which I was responsible.

Physical Security:

1. Computer room at the facility has no door.
2. Equipment stacked one on top of another.
3. Neither an Uninterruptible Power Supply nor Generator exists.
4. No backup servers available.
5. No equipment service contract.

Network Security:

1. Dialup modems to three (3) EDI Vans.
2. Local area network using Ethernet with a Star topology.

Defense in-Depth:

1. No Business Continuity/Disaster Recovery plan exists.

My next step was to study the application/server design and the network topology diagrams[2] in order to understand their environment and to formulate my questions.

[1] See appendix A
[2] See appendix B

According to the documentation provided by XYZ, the basic structure of the network was network-centric. Their warehouses were connected centrally to the data center which housed all the application/data servers. This design makes the remote locations fully dependant on the host site to run their operations.

Each remote location is similarly equipped. They have a router connected to a switch supporting a Radio Frequency (RF) controller wireless access point (WAP) hosting several wireless handheld RF-devices, a local file server, several printers and pc workstations, a Radio Beacon WEB server, and a warehouse management server running Radio Beacon (RBT). Each of the three (3) remote locations also uses a Simplex server for building access control and timecards.

Since the remote locations are fairly close in proximity, they are using different means of connecting depending on their distance. Site A is using a wireless bridged connection via Entana (www.entana.com). Site B uses a fiber-optic connection as a local area network (LAN) extension. Finally, Site C is using a private point-to-point T1 connection from Bell Nexxia, through a firewall and routers to the host site.

Manufacturing customers, whose products are being warehoused at XYZ, are connected via the internet through a firewall to the FTP server. This allows them to receive reports and file updates, have their own connection to the value added networks (Vans) to submit orders for processing and receive order confirmations from XYZ.
The host site (XYZ) is comprised of thirteen (13) servers[3] from different manufacturers.

This information enabled me to start preparing my questionnaire[4]. It gave me a good idea of what to look for in terms of improvement since the last visit as well as what questions must be asked regarding security.

I decided that I would design my questioning to discover the following about XYZ:

1. A general sense and feeling of their attitude with regards towards security.
2. A better understanding of their environment from a security perspective.
3. What methods were in place to protect their environment?
4. Were there any significant risks to us in the proposed merger?

It was important to remain flexible with the questioning since we would be provided with updated information on the day of the meeting. This information could have an impact on questions that were based on past documents.

[3] Refer to Appendix B for diagram following first site visit
[4] Refer to Appendix C for Questionnaire

The day before the meeting, we convened a meeting of the four (4) representatives to discuss each other's approach. We prepared an agenda, and reviewed each other's questions to make sure we did not run the risk of redundancy or rhetoric.

The intent of the others was primarily to revisit the previous concerns and review what changes had occurred since the last visit.

Meeting day:

A good friend of mine always says, "If you fail to plan, you plan to fail".

The meeting commenced and after the introductions, we were presented with a set of new documents for the network topology and the new architecture and applications in use[5]. Each of us took a few moments to study the new designs, making the necessary adjustments to our questions.

I proceeded with my questions starting with the Network Security, General topic[6]. I learned that there was only one person responsible for network administration and they didn't have a person to back him up. I realized at this point that the person I most needed to speak with was not in the meeting. I asked that he be made available to me later in the day, and it was arranged. Seventy-five (75) percent of the critical business (Orders) are conducted through electronic data interchange (EDI), ten (10) percent over the Internet, and the remaining fifteen (15) percent via Fax, Email, and telephone. The company processes twelve thousand (12,000) orders per month consisting of one hundred fifty thousand (150,000) items and the Help desk handles four hundred (400) events per month with an average turnaround of twenty-four (24) hours.

For the remaining topics, under network security, I deferred them until later on when I could speak with the Network Administrator. I filled in answers to the questions that were answered on the network diagram.

I skipped over to the Environment Security, General topic[7]. I discovered that there was a security audit performed by an independent consultant in the past year. I was told that nothing serious was found and unfortunately I could not have access to the report. I also learned that there were no company security policies/procedures/guidelines in place.

Normal business hours were Monday to Friday from 8am until 11pm and intrusive system maintenance was performed on the weekend when required. I noticed on my way in to the building that the front door was unlocked. No one was responsible for receiving visitors and pass cards were not required.

[5] Refer to Appendix D, "New" Hardware and Applications Diagram
[6] Refer to Appendix C, p.17
[7] Refer to Appendix C, p.19

Access to the warehouse required a pass card. Exits were clearly marked yet there were no apparent signs of evacuation procedure maps on the walls.

Moving along to the topic of W2K/Novell servers it was revealed that the Network Administrator was also the System Administrator. Access control was maintained by Active Directory using Group policies. A new anti-virus server was put in place and vulnerability scanning was being performed by a third-party service called Insight Manager (Compaq/Hp). Patch deployment to clients and servers was being performed by software called Sitekeeper® from Executive Software. All users on the network were using standardized images on their workstations, which were locked down and had anti-virus clients. No documented change management procedures existed. Personal computers were allowed to connect via Citrix from home.

Account administration of local accounts was handled by the Security Administrator. Notification of the request came from web server software called HelpDesk™ from Parature, Inc. This software left an audit trail of each request. Systems were not monitored to capture security violations and there were no requirements to change passwords on a regular basis. Users required their own account and did not share accounts.

IT was responsible for security. Neither employees nor non-employees (i.e. consultants, 3rd party vendors) were required to sign a confidentiality agreement. Consultants were used on a regular basis in IT. There are two people on call at all times, one for business application problems and one for network/hardware/security related incidents. Only one person had access to the administrator accounts.

In the afternoon we visited the computer room and I had my opportunity to talk to the network administrator to conclude my questioning. The computer room had a door with a combination lock. This combination was known only to the administrator, the IT Manager and the Business Analyst. All of the servers were housed in storage cabinets with cable management systems and independent power bars. There was air-conditioning, smoke and fire detectors, and a sprinkler system containing water. The servers were all equipped with sensors to detect if it was too hot. In the event of an air-conditioning failure, they were programmed to shut down, sound an alarm, and send an email to the person on-call. The systems were monitored by software called Whatsup® from R.B.Hall Associates and notify the on-call person immediately if a problem is detected.

There remained only one modem in use to dial-out for one customer on the IBM value added network (VAN). The modem had the auto-answer feature turned off.

Switches were primarily HP Procure and routers were Cisco and they used a combination of Dynamic Host Configuration Protocol (DHCP) and static IP addresses. For internal remote locations that weren't behind firewalls the routers

were configured to disallow cross-pollination. Unused ports on the switches were not blocked. The intention, eventually, was to change all switches to those supporting access blocked by media access control (MAC) address. This would prevent unauthorized connection to the local area network (LAN).
Static port assignment was kept manually in a spreadsheet by the network administrator. The LAN was monitored for collision-detection rates.

Access to the Internet was available internally to all users. There was a proxy server in place preventing access to undesirable sites and providing management with usage reports. Remote access to the local network was provided via the Citrix® MetaFrame® Secure Access Manager.[III] Although two-factor authentication was supported using tokens or pins, XYZ was using only single factor authentication with logon id and password. There was no intrusion detection system in place therefore the firewall was being used to record Internet traffic.

I asked the question of how the file transfer between the two (2) sites connected via Entana wireless was protected and was informed that they were using the WPA encryption standard. Not being familiar with this standard, I browsed the Internet and found the following explanation;"Wi-Fi Protected Access (WPA) is the latest security standard for users of computers equipped with Wi-Fi wireless connection. It is an improvement on and is expected to replace the original Wi-Fi security standard, Wired Equivalent Privacy (WEP). WPA provides more sophisticated data encryption than WEP and also provides user authentication (WEP's user authentication is considered insufficient). WEP is still considered useful for the casual home user, but insufficient for the corporate environment where the large flow of messages can enable eavesdroppers to discover encryption keys more quickly"[IV] (SearchMobileComputing.com).

Additional information gathered at the beginning of the meeting uncovered new servers which hadn't been taken into account in my question list. XYZ had added an Intranet to their fold which was built using Extensible Markup Language/Extensible Stylesheet Language (XML/XSL) and was available to internal users only and bookmarked by department for insurance of separation of duties.

Analysis of systems and network logs was not being performed on a regular basis to look for violations or outside attempts of gaining access to the network.

This concluded the meeting. It was time to summarize our findings into a document to be presented to the executive committee.

After – Conclusion

At first, it was extremely difficult for me to put the content into perspective from a small to medium business (SMB) viewpoint since I had never worked in this environment. In actual fact and irregardless of the size of the company, the point I was trying to determine was the risk to the business that was being created by the conditions of the information technology environment.

It was obvious that company XYZ had improved their security stature since the first visit and they had made a serious attempt to increase their protection of the perimeter from outside attacks. The additions of the anti-virus mail server to protect the mail from SPAM and viruses as well as the conversion to a virtual private network (VPN) connection to the VAN site were excellent choices in strengthening the network. The inclusion of a proxy server reduced the risk of productivity loss of employees and the ability of unwanted outsiders viewing or gaining system information when users cannot visit questionable sites.

These additions, coupled with the firewall already in place, and the avoidance of using the internet between locations certainly made the site more secure. The usage of the WPA encryption standard for the wireless communications and protection of the wireless access points using a combination of sequence hopping and MAC address verification also bolstered the environment.

These points lower the risks by reducing the potential for vulnerabilities of threats from the internet through exposure.

My overall sense and feeling was that the attitude of XYZ towards securing their organization was changing and they were prepared to take the steps necessary to continue in this direction.

Following are a list of concerns which I brought forward to the internal group in order to finalize our paper which was to be presented to the senior executive.

<u>Concerns:</u>

1. The dependency on one individual to perform network and system administration. This was a very high risk situation, since internal protection did not exist and the System administrator had unlimited system access and his actions were not audited[V] (Bianco).

2. No documented BCP/DRP procedures were in place. This environment was extremely complex requiring interaction between several servers. The threat of an extended loss of power combined with the lack of backup power support at the host site certainly made this concern a significant risk.

3. Sarbanes-Oxley. This law was enacted in the US for publicly owned companies having very stringent rules associated with it which does not allow for non-compliance. An internally designed IT Controls self-assessment was performed on XYZ by me, indicating that a lot of work would have to be done to comply with this regulation.

4. An overall lack of awareness and understanding of the need for security in the internal computing environment as a whole.

    a. No company security policies/procedures/guidelines were in place enabling employees to know what they can and cannot do.
    b. No requirement for changing passwords, leaving them susceptible to being hacked because the passwords were cracked.
    c. No logging on the servers for violations and no audit trails providing little understanding as to what may be occurring on their systems.
    d. No requirement for signing confidentiality agreements by insiders or outsiders making it extremely difficult to take legal action against individuals if this becomes necessary.
    e. No IDS units to detect if intrusions were being attempted and whether or not they were being successfully stopped.
    f. No change management procedures to help raise awareness of occurrence and to document methods of safe removal if problems arise.
    g. No daily review of logs to look for suspicious events which may have occurred against the network or on the servers.

5. There was a false sense of security on the part of XYZ believing that they were secure because the perimeter was protected from attackers. It is common knowledge in the industry that more than seventy-five (75) percent of attacks emanate from within. Since there is no definite fact stating whether external or internal vulnerabilities were more serious, then they should be treated as being equally important.

6. None of the remote locations had a backup connection to the network in the event the primary connection failed as they were entirely dependent on the network for their operation this was a risk.

7. Lack of an Incident response procedure and incident detection in order to defend against serious attacks, leaving XYZ with the inability to deal with such an issue if one arose.

8. Backup media is currently being taken home by employees for safe keeping.

Recommendations:

1. Institute a central logging server and have violations reviewed daily by someone other than the System Administrator and make sure that he doesn't have administrative rights to this machine.
2. Implement a documented change management control procedure requiring management to review and authorize any changes that will take place.
3. Document an IT disaster recovery plan to identify areas of concern and design and implement architecture to satisfy the minimum business requirements.
4. Draw up a standard confidentiality agreement and have it signed by all personnel and consultants who have access to the systems.
5. Invest in an independent IT security risk assessment. This should include a penetration test to establish a baseline assessment of network security as seen from the outside. Perform network and vulnerability scans to determine whether all the necessary patch levels are in place and if all unnecessary services are turned off. Also verify if all unneeded IP ports are closed and proper access control lists are in place.
6. Draft a copy of IT Security Policies and Procedures and communicate them throughout the organization. Policies should cover topics such as Acceptable Use, Email, Internet, Physical Security, Password, Workstation, Portable computing, Remote access, and sanction definitions for policy violations.
7. Print hard copies of router configurations, group policy definitions, and system settings and give them to IT management before and after every change.
8. Institute a password policy requiring regular password changes and define group policies to automate and enforce it.
9. Invest in some form of backup connection like ISDN for each remote location.
10. Contract an outside firm like Iron Mountain to provide offsite storage services.

At the final meeting, we met with our VP to prepare the executive summary for the senior executive committee. We were each asked to provide our opinion on whether or not we felt that there was a significant risk for ABC to proceed with the joint venture.

Since a highly effective security program must be sponsored from the top down[VI] (Doll,Rai,Granado) and armed with the knowledge that, at ABC, we haven't attained this level, I was very careful in my criticisms of this environment. I didn't want to end up with a "Do as I say, not as I do" situation.

I basically stated the following:
"I believe that the overall risk to ABC of proceeding with this venture was minimal. The environment was reasonably protected from outside threats. Vulnerability management and patching controls are well managed. Providing the number one risk of one security/network administrator is addressed and moving forward the company strives to improve their internal protection and processes, this alliance could proceed. They should also promote security awareness and training throughout the company. In addition, all financial controls required by Sarbanes-Oxley would have to be addressed immediately in order to meet the date of December 2004 from our IT Internal audit department".

Lessons Learned

Looking back, I realized that I focused on the operational aspects of the environment, like running the warehouses and taking and filling orders. I did not pay enough attention to the business side, mainly the financial applications, whatsoever. With the introduction of Sarbanes-Oxley, financial applications are the most important applications to look at, since its entire raison d'etre surrounds financial controls and reporting. Although it was not evident at the time, whether or not Sarbanes-Oxley would apply, it illustrates to me that you have to look and question outside of the box ensuring that you have a complete picture of the entire computing environment.

I realized why there are probably no standard checklists available since preparation of the questionnaire was based entirely on documents provided by the company under study. This makes every situation unique requiring different questions for each one. A good base of questions to draw from is necessary to ensure and prompt you while building your own.

.

Appendix A

XYZ – Equipment

Risk Description

- All apps PC based
- Mix of desktops and servers
- Mix of manufacturers IBM, Compaq, Dell
- No one standard configuration
- Mix of NT4 & W2K servers
- Aging equipment (> 3 years old)
- RAID technology not implemented on all servers
- Applications spread across many servers
- Novell 5 server used for main application
- No backup servers
- Citrix used for one client / internal user remote applications access
- No equipment service contract
- MS Exchange used for email
- WEB server using Microsoft IIS
- One firewall before Internet
- WEB hosting utilized on public side
- Current systems shared by all 3 XYZ companies
- Telephony shared by all 3 companies
- System capacity / performance measured on some servers

XYZ – Environment

Risk Description

- Daily file backups performed
- Weekly entire system backup performed on Novell server only
- No documented backup/recovery or BCP/DRP procedures
- No system documentation
- Computer room
    - Dirty and covered in dust
    - No security
    - Wires hanging everywhere
    - No door
    - Equipment stacked
- No UPS or generator
- System passwords are changed only when someone leaves
- Dialup to 3 EDI Vans

Appendix B

Hardware & Applications Diagram

Checkpoint Firewall PC

MS Exchange Server Compaq, W2K	Web Server Compaq, W2K, IIS, VB, FXPRO, Verisign	FTP Server IBM, W2K MS products	Apps/Data Server Compaq, Novell 5

CITRIX Server Dell, W2K	Print 2000 Server Compaq, W2K	Crystal Rpts Server Compaq, W2K	EDI Server Compaq, W2K

App. 1 Server Compaq, W2K	App. 2 Server Compaq, W2K	App. 3 Server Compaq, W2K	UFMS Server Compaq, W2K

W2K = Windows 2000 Server; VPN = Virtual Private Network;
RPS = Redundant Power Supply; MD = Hardware mirrored disk drives;
R5 = RAID5

Appendix C

Security Due Diligence Questionnaire

Network Security:

GENERAL:

1. How many people are responsible for network management?
   Do they have backups?
2. What percentage of the critical business (i.e. Cust. Orders) depends on
   a. Internet?
   b. EDI Asset + modems?
   c. Faxes?
   d. Private network?
   e. Other? Specify:
3. Are there any other network devices not shown in the diagram?

ROUTERS/FIREWALL(S):

1. Are there any additional routers involved?
2. What is the type and level of the O/S?
3. Are all non-used services disabled or deleted?
4. How often are patches applied?
5. What ports/services are opened inbound? Outbound? Printout of configuration?
6. Who has access to the Network administrator account?
7. How often is the password changed for admin account?
8. How does admin access the router/firewall for changes?

MODEMS:

1. Who is responsible for attaching modems to the network?
2. Is the auto-answer feature disabled?
3. What happens if a modem is unusable?
4. Are all communications dial-out?
5. What is the speed of the dialup modems to the vans?

SWITCHES/HUBS:

1. Who is responsible for managing switches/hubs?
2. What types of switches/hubs are being used for LAN?
3. Are unused ports being blocked?
4. Is LAN monitored for collision-detection rates?
5. Are you using DHCP or fixed ports?
6. If fixed ports, who manages assignment, how?
7. Are there any wireless devices on the LAN?

INTERNET:

1. How many internal users have remote access to systems via the Internet?
2. How many external users have remote access to the systems via the Internet?
3. How many levels of authentication are performed?
4. What methods are used? (username-password; certificates; tokens)
5. Do System administrators perform remote support of systems via the Internet?
6. How are network intrusions detected?
7. What incidents have been encountered in the past 12 months?

FTP Server:

1. Does this server have all unused services disabled/deleted?
2. Are file transfers using encryption?

Environment Security

General:

1. Has there been an IT Security Audit performed in the last 24 months?
    a. By whom? Report available? Major findings?
2. Are there IT Security Policies/Procedures in place?
3. What are the normal hours of business?
4. How do employees access the building?
5. Is access to the building logged after hours?

Computer Room:

1. How is access controlled to the CR?
2. Are there fire detection devices?
3. Are there sprinkler systems?
4. Is there air-conditioning?
5. Are there uninterruptible power supplies on critical systems?

W2K/Novell Servers:

1. How many System Administrators are there?
2. How are accesses controlled?
3. Is there Antivirus software on the servers?
4. How is patch management performed?
5. How are new Microsoft vulnerabilities detected?
6. How many general users have access to the systems?
7. Is there AV software on the Client PC's?

Account Administration:

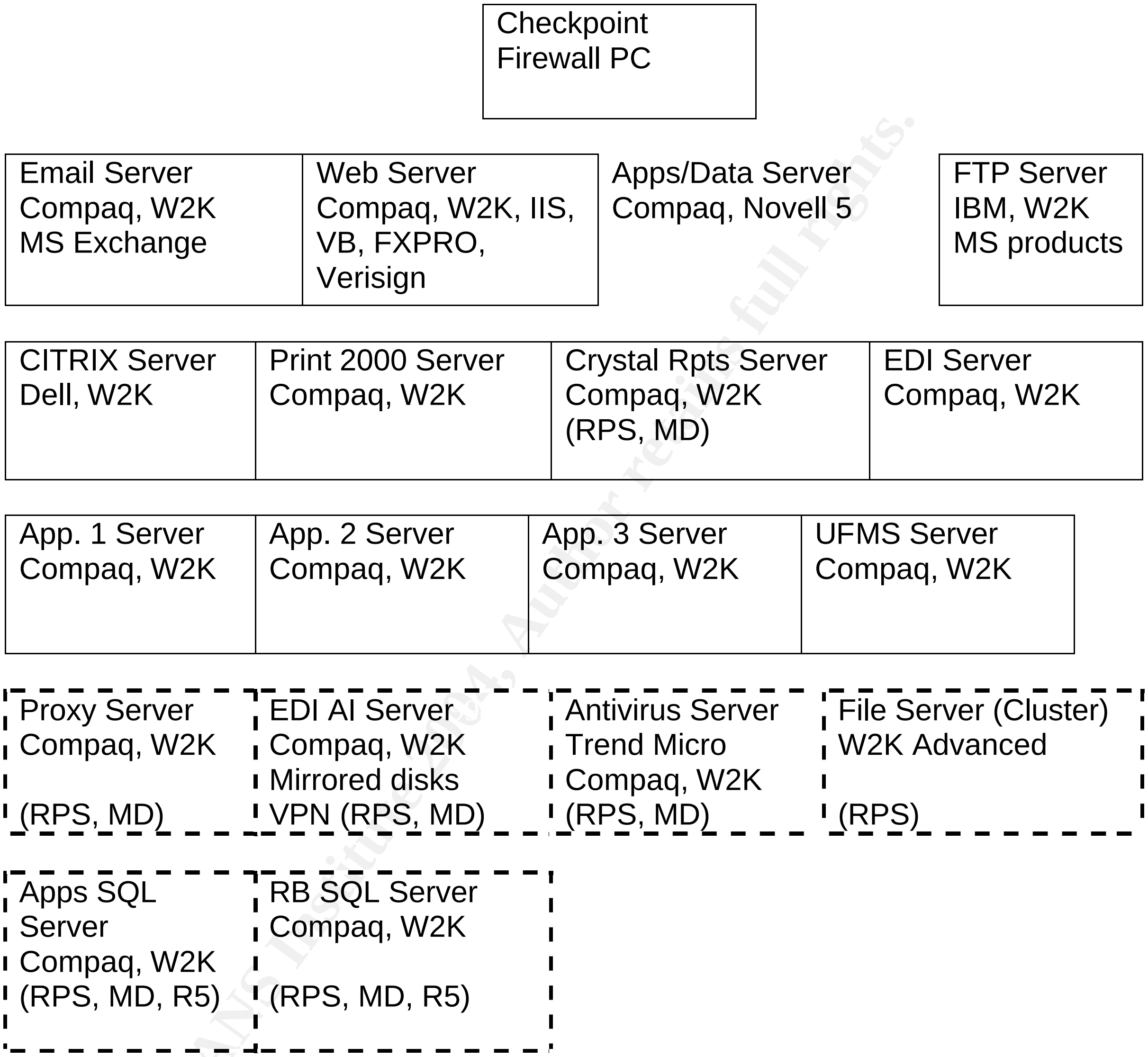
1. How is account creation/modification/deletion performed?
2. Is there an audit trail?
3. Are systems monitored to capture security violations?
4. Are passwords forced to change periodically?
5. If the answer to #4 is yes, what is the expiration interval?
6. What is the minimum password length required?
7. Do users share IDs/Passwords?

IT Personnel:

1. Does security fall under IT? Which role is responsible?
2. Are IT personnel required to sign a non-disclosure/confidentiality agreement?
3. Do you use contractors/consultants frequently?
    a. Are they required to sign non-disclosure/confidentiality agreements?
4. How many staff are required to perform after hours support?
5. Do all IT personnel with system administration access have another person with equivalent authorities?

Appendix D

“New” Hardware & Applications Diagram



Checkpoint Firewall PC

Email Server
Compaq, W2K
MS Exchange

Web Server
Compaq, W2K, IIS, VB, FXPRO, Verisign

Apps/Data Server
Compaq, Novell 5

FTP Server
IBM, W2K
MS products

CITRIX Server
Dell, W2K

Print 2000 Server
Compaq, W2K

Crystal Rpts Server
Compaq, W2K
(RPS, MD)

EDI Server
Compaq, W2K

App. 1 Server
Compaq, W2K

App. 2 Server
Compaq, W2K

App. 3 Server
Compaq, W2K

UFMS Server
Compaq, W2K

Proxy Server
Compaq, W2K
(RPS, MD)

EDI AI Server
Compaq, W2K
Mirrored disks
VPN (RPS, MD)

Antivirus Server
Trend Micro
Compaq, W2K
(RPS, MD)

File Server (Cluster)
W2K Advanced
(RPS)

Apps SQL Server
Compaq, W2K
(RPS, MD, R5)

RB SQL Server
Compaq, W2K
(RPS, MD, R5)

W2K = Windows 2000 Server; VPN = Virtual Private Network;
RPS = Redundant Power Supply; MD = Hardware mirrored disk drives;
R5 = RAID5

References

[I] (ShareAnalysis.com); URL: http://www.shareanalysis.com/asp/learning/glossary.asp

[II] (Hartman) Hartman, Anita; Security Considerations in the Merger/Acquisition Process; August 11, 2001; SANS Practical Assignment, p.1;
Question 1 Network Security MODEMS taken from Appendix A
Questions 4,5 Environment Security General; Question 1 Computer Room;
Questions 4,5,6,7 Account Administration all based on questions found in Appendix A;

[III] Citrix; Citrix Systems Inc.; URL: http://www.citrix.com/site/PS/products/product.asp?familyID=19&productID=184

[IV]SearchMobileComputing.com; Glossary; Wi-Fi Protected Access; URL: http://searchmobilecomputing.techtarget.com/gDefinition/0,294236,sid40_gci887323,00.html

[V] (Bianco); Bianco, David; “Admins’ Dirty Little Secret”; p.55; Information Security magazine, October 2003 edition.

[VI] (Doll,Rai,Granado); Mark W. Doll, Sajay Rai, Jose Granado; Ernst & Young; defending the digital frontier – A Security Agenda; p.123; John Wiley & Sons Inc; ISBN 0-471-22144-9