Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The Value of Risk Assessment - A Case Study

Security risk assessment is an invaluable tool in a security professional's quest to protect a company's information assets. Information Technology projects that do not go through a security risk assessment process have a greater potential of exposing a company's information assets to corruption and loss. As a security professional of a large company that has recently standardized its security risk assessment process, it is my responsibility to uncover security vulnerabilities that exist in a project, suggest possible ...

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn More

The Value of Risk Assessment – A Case Study

© SANS Institute 2003, Author retains full rights

Elton L. Pierce II

3/31/03

GSEC Practical Assignment Version 1.4b

Option # 2

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table Of Contents

INTRODUCTION **3**

PROJECT BACKGROUND **3**

BEFORE RISK ASSESSMENT **5**

APPLING THE RISK ASSESSMENT PROCESS **7**

RESULTS OF RISK ASSESSMENT **9**

SEPARATION OF TRUST ZONES 10
AUTHENTICATION AND AUTHORIZATION 14
WORKSTATION AND SERVER SECURITY 15
MONITORING, MANAGEMENT, AND PATCHING 15
BC/DR PLANNING AND DATA BACKUP 17
HIGH AVAILABILITY AND SEPARATION OF FUNCTION 18
BUSINESS CONCERNS AND LEGAL ISSUES 19
REMOTE ACCESS 21
PHYSICAL SECURITY 22
Server and Workstation Placement *22*
Facility Security *23*
Training Employee Offices *23*

LESSONS LEARNED **23**

THE IMPORTANCE OF EARLY INVOLVEMENT 23
GROUP PARTICIPATION 23
PHYSICAL SECURITY 24

CONCLUSION **24**

REFERENCES **25**

APPENDIX A – COMPLETE RISK TABLE **26**

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Introduction

Security risk assessment is an invaluable tool in a security professional's quest to protect a company's information assets. Information Technology projects that do not go through a security risk assessment process have a greater potential of exposing a company's information assets to corruption and loss. As a security professional of a large company that has recently standardized it's security risk assessment process, it is my responsibility to uncover security vulnerabilities that exist in a project, suggest possible mitigation strategies for the vulnerabilities identified, and clearly articulate any vulnerabilities that are not mitigated to those with the authority to accept them.

This paper will examine the application of the security risk assessment process to a rather complex project from the initial phases of its design prior to security risk assessment to its production state. It will discuss how risks were assessed and identified and show how the risk assessment process changed the final outcome of the project. We will also look at the impact that risk assessment had on the project and identify lessons learned.

Security risk assessment is often a tricky business. Striking just the right balance between the high price of security and business needs is not an easy task. The process is often subjective and hard to accomplish, but if implemented correctly can greatly improve the overall security posture of a company, one project at a time.

Project Background

We will be examining a project that involved a complete redesign of our company's thirty-year-old training center complex. The old training center consisted of several separate buildings. At the heart of the complex was a building that housed the classrooms, the training staff offices, and a cafeteria. Several smaller buildings that contained dorm rooms for students from out of town surrounded the main building. The complex was utilized by employees only and was protected from public access by key card activated security gates at street entrances. The offices and classrooms in this facility enjoyed un-fettered access to our companies information systems through direct connections to our core network. The complex also served as a recovery site for our company in the event of a disaster.

The way our company conducts business has changed greatly in the last several years. To accommodate these changes, our corporate training department engaged our corporate facilities and networking departments to redesign the facility to meet modern training needs. To begin with, a complete hotel would be built with all the latest amenities and services to house out of town guests. A series of brand new classrooms, meeting areas, and a large ballroom would be

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

built which would be connected to the old classroom and office building. Several of the old dorm room buildings would be demolished or converted into offices, a pub, and a restaurant. The training departments employee offices were to remain at the complex, and the facility still needed to continue to serve as a recovery center in the event of a disaster. To facilitate the ability for the complex to be sold in the future, the network and processing systems for the complex needed to be physically located on site. The most striking change of all was that this facility would be open to the public!

The United States General Accounting Office describes the security risk assessment process as, “a means of providing decision makers with information need to understand factors that can negatively influence operations and outcomes and make informed judgments concerning the extent of actions needed to reduce risk.”

The first step to successfully risk assessing a project is to determine the projects overall risk level. By doing this, projects can be prioritized so that high-risk projects can be examined ahead of lower-risk projects. To determine the overall risk level of the project, one must understand what the project is trying to accomplish, the current state of the project, the projects scope, and the projects time constraints. Examining the projects charter and project plan can help a security professional discover a lot of this information. If a charter does not exist, a quick interview with the project manager can help the security professional gather information that can be used to ascertain the projects risk level. My company also uses a small multiple-choice questionnaire with a predefined grading scheme to help uniformly determine the risk level of a project. This grading scheme can be adjusted to match the level of security your company is trying to achieve.

Assessing the overall risk level of this project was not very difficult. This project was determined to be high-risk based on the following findings:

- The complex would be open to the public.
- A third party would be contracted to run the day-to-day hotel functions.
- The overall capital expenditure of the project.
- The multiple functions of the environment and diverse connectivity requirements.
- The use of unfamiliar network technologies.

As is often the case in real life, security may not be the first consideration when a project is being developed. Unfortunately, this was the case in this project. Security was only engaged in the project after budgets had been set, initial network designs had been completed, and application vendors chosen. Several buildings had already been demolished, and the new hotel was more than halfway completed. Ideally a security professional would be involved in the initial

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

phases of the project to help identify security issues so that solutions could be budgeted for and risks mitigated prior to implementation.

Before Risk Assessment

The revamped layout of the facility consists of a new hotel that contains two wiring closets: closet A – the main hotel wiring closet, and closet B. A couple of the old dorm room buildings were converted into a pub and a restaurant. A covered walkway connects the new hotel to the ballroom and new classrooms. This new section of the training complex connects directly to the old parts of the training facility, building C, which houses the training staff offices, old classrooms, and a cafeteria. Building C also houses the main networking closet, closet C. Two other buildings remain from the old complex that function as offices and other meeting areas, building A & B. The proposed network connectivity is also shown. (See Figure 1)

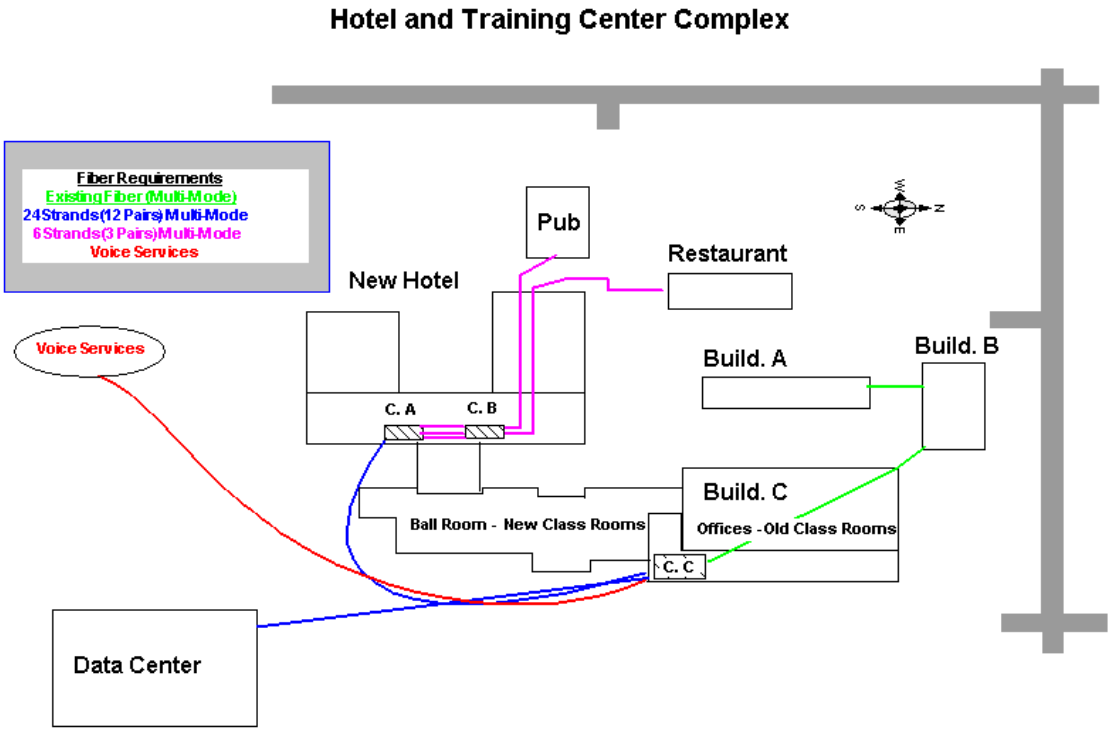

Figure 1

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The network team provided the following high-level network diagram showing the initial design of the new network. Several unfamiliar network technologies were being leveraged in this design. One of these technologies with which our company had little experience was the use of a Voice Over IP (VOIP) telephone system. (See Figure 2)

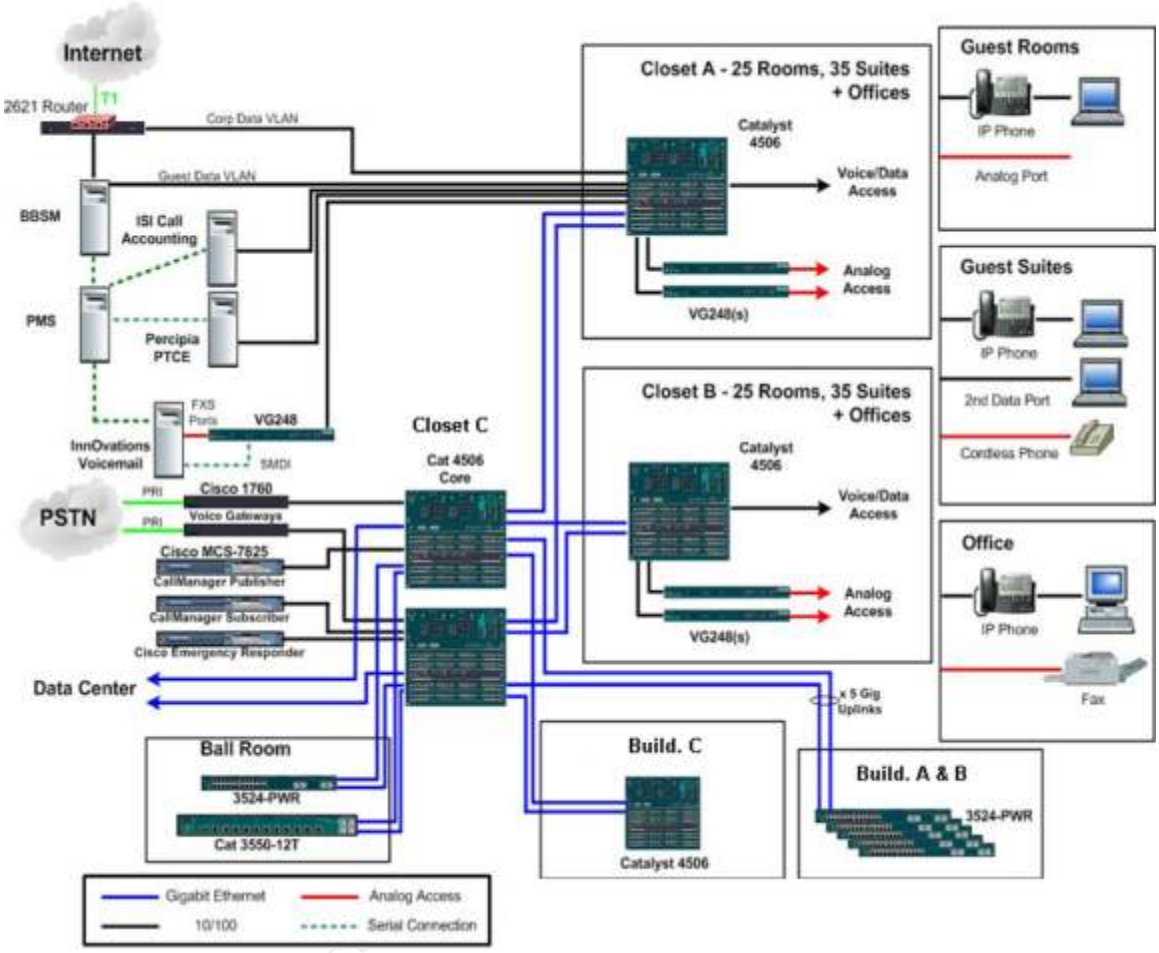

Figure 2

The following systems would be installed to provide the services needed in a modern hotel and training facility:

- **Voice Over IP Phone System (VOIP)** – A phone system that uses IP technology to digitally encode voice conversations and send them over the same network switches that the data network uses. This technology allows for the use of smart IP phones and sophisticated voice mail systems.
- **CISCO Building Broadband Service Manager (BBSM)** – A plug-and-play system for providing controlled access to the Internet from the hotel guest rooms and classrooms. **(**http://www.cisco.com/application/pdf/en/us/guest/products/ps533/c1650/ccmigration_09186a008010ba18.pdf**)**

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- **Visual One Property Management System (PMS)** – The heart of the hotel, this system is responsible for property management, sales and catering, point-of-sale management, and accounting. The PMS system interfaces with the VOIP, BBSM, key card, and others systems through a device called the COMTROLLER. (http://www.visualonesystems.com/propertymanagement.htm)
- **COMTROLLER (COMTROL)** – An interface device controlled by an Interface PC that is part of the PMS system. It controls the BBSM, VOIP, key card, and other systems through direct serial connections.
- **PERCIPIA Networks Hospitality Communication System (PERCIPIA**) – A system that manages content delivery and services that can be activated from the VOIP phone system. This system can connect to the Internet and can provide information in XML format to the IP enabled phones within the complex. (http://www.percipia.com/warper.jsp)

The majority of these systems had been chosen and purchased with very little input from the security groups within our company. Because these systems had already been purchased, we concentrated on how to implement them as securely as possible.

Appling The Risk Assessment Process

After accessing the overall risk level of the project and gathering information about its current state, it was time to identify vulnerabilities that existed in the project design. Our company uses a risk assessment report and databases to document the vulnerabilities that exist in a project. The security professional begins by attending project meetings and builds a report that contains security issues that have been identified. These risks are communicated to the project members and sponsors throughout the life of the project and are updated in the risk assessment database.

The report contains following sections:

- **Executive Summary** – Describes the project in non technical language and identifies the open risk issues with minimal detail
- **Project Information** – Describes the project name, purpose, sponsor and manager.
- **Overall Risk Level Statement** – A statement describing the overall risk of the project as determined by the initial risk assessment questionnaire and interview.
- **Open Issues** – Lists security vulnerabilities that have been identified in the project that may not be resolved prior to production. Provides the risk level assigned to an issue and a target date for resolution.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- **Resolved Issues** – Lists security vulnerabilities that have been identified in the project that have been resolved prior to production. Provides the risk level assigned to the issues and how they were mitigated.
- **Signature** - Signatures are solicited that affirm the credibility of the report and acceptance of risks associated with the project.

During the project life cycle, issues can be resolved and moved from the open issues section of the report to the resolved section. A week or two prior to production, the report is finalized and issues that have not been resolved are given target dates for completion. Officers of the company must accept the open issues through signature before the project can move into production. Risks that are not going to be mitigated are also noted and accepted through signature.

This project contained an intermediate phase that allowed some risks to remain open even though the network and technologies listed above were being used. The complex would be opened to company employees several months prior to being opened to the public. I will refer to these phases as the private and public openings.

Identifying security risks that exist in a project can be a difficult task. I spent several months meeting with the project team, which consisted of representatives from our corporate facilities department, network team, voice systems team, and the third party contractors who would run the hotel. Most of this time was spent discussing the various systems that would were being installed and documenting requirements for their use. I used our company's security policies as the backbone of the process as well as best practices and security training I have received over the last few years to help identify issues. As issues were uncovered, I would discuss them with other members of my security team and come up with possible solutions to help mitigate the issues. For complex issues such as installing a CISCO PIX firewall bundle, I would engage senior members of our corporate security team. We worked closely with the network team to help reengineer the network design and create appropriate trust zones.

Issues are added to the report using the following format. (See Example, Table 1)

- **No.** – Issue Number.
- **Issue Description** – A brief description of the security vulnerability that exists in the project.
- **Risk** – A brief description of how the vulnerability could be leveraged to cause data corruption, loss of data, or downtime.
- **Recommended Mitigation Strategy** – A possible strategy to help lessen or eliminate the vulnerability from the project.
- **Risk Level** – A high, medium, and low scale used to identify the importance of correcting the risk based on likelihood of an attacker to leverage the vulnerability and impact to the company's information assets.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table 1

Open Issues				
No.	**Issue Description**	**Risk**	**Recommended Mitigation Strategy**	**Risk Level**
2.	The Percipia Core Server utilizes an operating system that is out of date (Linux 7.1) and unsupported by our company. Linux is not a company approved standard OS.	Operating systems that are out of date may not contain the latest security patches and updates to prevent the server from malicious attacks. This server will obtain data directly from the Internet.	Determine who will support and update the operating system on this server. Apply all available security patches for the OS.	HIGH

Note: Many fields that would normally be included in our company's official report have been removed for clarity.

To help identify security vulnerabilities that may be more harmful if leveraged by an attacker, issues are given a high, medium, or low risk level ranking. Determining the risk level of an issue is often a judgment call between how easily the vulnerability can be exploited, the likelihood that the vulnerability will be leveraged by an attacker, and the amount of damage that could be caused if it were.

As an example, the above issue was give a high risk level due to the our company's lack of experience with the Linux operating system, the fact that this system would connect to the Internet to retrieve data, and where the system was located in the network design.

A complete listing of the issues identified for this project through the security risk analysis process can be found in Appendix A.

Results of Risk Assessment

From a security point-of-view, there were many problems with the initial network design mainly due to the different requirements the complex was trying to fulfill. Initially the network group had not included anything except an IOS firewall on a router to protect the network from the Internet. The design relied heavily on Virtual LAN technology to segment different trust zones, and the network was also going to remain directly connected to our core network through existing firewalls.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The risk assessment process helped identify several issues with the project that can be broken down into the following categories:

- Separation of Trust Zones
- Authentication and Authorization
- Workstation and Server OS Security
- Monitoring, Management, and Patching
- DR/BC Planning and Data Backup
- High Availability and Separation of Function
- Business Concerns and Legal Issues
- Remote Access
- Physical Security

Lets examine the issues that were uncovered in these categories and discuss how they impacted the project.

Separation of Trust Zones

Our company utilizes a trust level scale to categorize different types of users and systems into different groups. By doing this, guidelines can be put in place describing what security barriers are required when connections are made to our network. The trust levels are: untrusted, minimally trusted, semi trusted, and trusted. Prior to the redesign of the training complex, it had been categorized as a trusted environment due to the fact that it was only used by employees and had physical security measures in place such as gated entry and security guards to protect the network and its users. The redesign changed all of that. The complex now involved a mix of several different user categories:

- **Untrusted Public Guests** – Non-employees that resided in the guest rooms and utilized the training and meeting rooms.
- **Semi Trusted Third Party** – Contractors that had been contracted to run the hotel day-to-day functions.
- **Trusted Employees** – Employees of our company that had offices located in the training center and conducted employee training at the facility.

Not only did the datacenter core network need to be protected from the untrusted users, the hotel processing systems and customer data needed to be protected as well. The following issues were defined on the risk assessment report to identify these risks. (See Table 2)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table 2

Resolved Issues				
No.	**Issue Description**	**Risk**	**Recommended Mitigation Strategy**	**Risk Level**
1.	The hotel and training complex contains several processing systems that contain data that must be protected from improper access and tampering.	An attacker could retrieve customer personal data or launch an attack against our company or other external networks from within the hotel and training complex.	Install a PIX firewall bundle to separate processing systems from general guest access. Install a PIX firewall to separate management traffic for the hotel processing systems from the data center core. Require all guest and classrooms to access the Internet or our company's network through the CISCO BBSM. When accessing our company's network, the user traffic must pass through our company's external VPN concentrator.	HIGH
2.	Firewalls can be configured with weak rule sets.	Incorrect firewall configuration could allow an attacker to gain access to sensitive data.	Configure the hotel network firewalls with appropriate rule sets to allow only essential network traffic between the various VLAN's according to our company's standards.	HIGH

After meeting with the project team to discuss these issues and their importance, the network team agreed to install a CISCO PIX firewall bundle and segmented the network into the different security zones using the firewall and VLAN's. Firewall rules sets were configured on each interface that restricted access between the different network segments. (See Figure 3)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

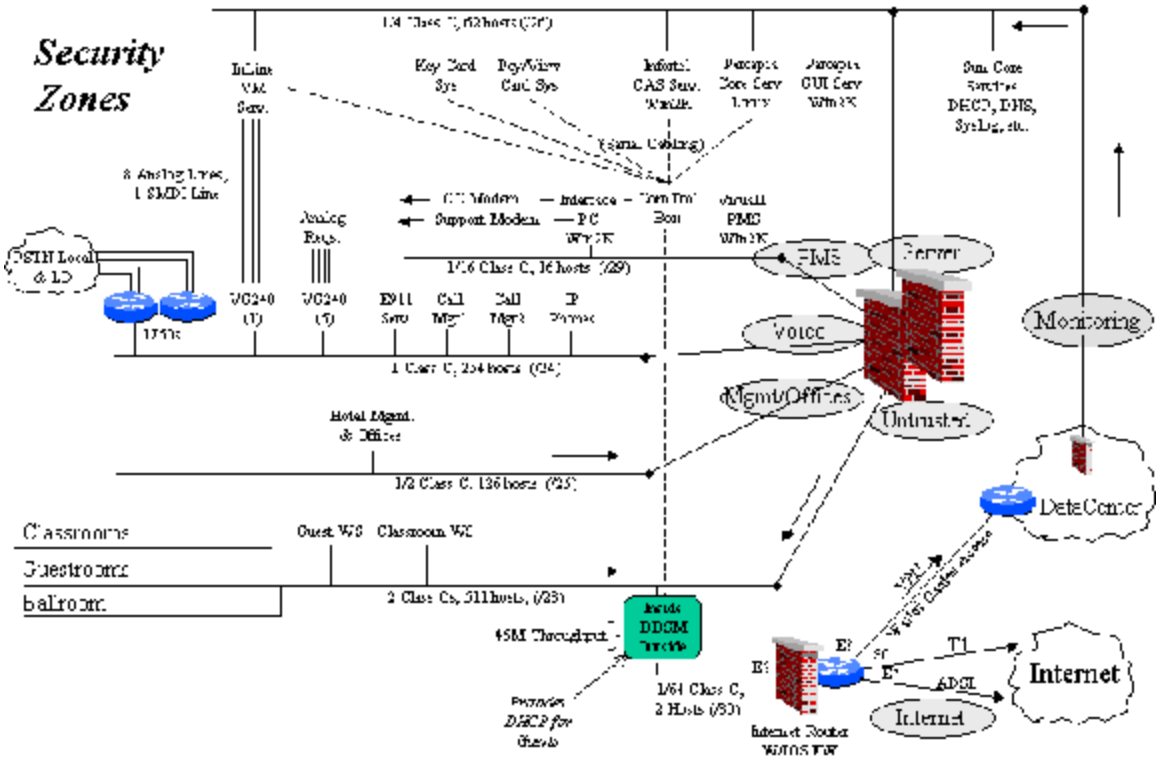

Figure 3

Here is a description of the various network security zones and their trust level:

- **Untrusted VLAN** – This network segment allows users in the new and old classrooms, the guest rooms, and the ballroom and meeting rooms to access the Internet through the BBSM. An Internet router with IOS firewall rule sets and the BBSM protect this segment from the Internet. This segment is considered untrusted.
- **Management/Offices VLAN** – This network segment is for the workstations that are needed for the day-to-day function of the hotel. This includes point-of-sale terminals, check-in workstation, and hotel office computers. The rule sets on the firewalls are configured to allow traffic from this network segment to the PMS network segment and to the untrusted network for Internet connectivity. This segment is considered semi trusted.
- **Voice VLAN** – This network segment is used for the IP phones and call manager systems. The rule sets on the firewall are configured to allow traffic from this segment to access the Server segment for voice mail and IP phone information. This segment is considered minimally trusted.
- **PMS VLAN** – This network segment is reserved for the Property Management System, file and print server, and authentication systems needed by the Management/Offices VLAN users. Firewall rules sets are

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

configured to allow only the Management/Offices segment and the Monitoring Network segment to access this segment. This segment is considered semi trusted

- **Server VLAN**– This network segment houses the voice systems for the hotel. Only the Voice VLAN is allowed to interact with this network segment through firewall rule sets. The PMS system interacts with the systems located on this segment through the COMTROL interface device. This segment is considered semi trusted.
- **Monitoring VLAN** – A separate VLAN also exists that connects the training center network to the data center through another leg on the firewall for monitoring and management of the servers at the complex. Only specific monitoring and management traffic is allowed between this segment and the datacenter core network. This segment is considered semi trusted.

These network segments are distributed throughout the complex. (See Figure 4)

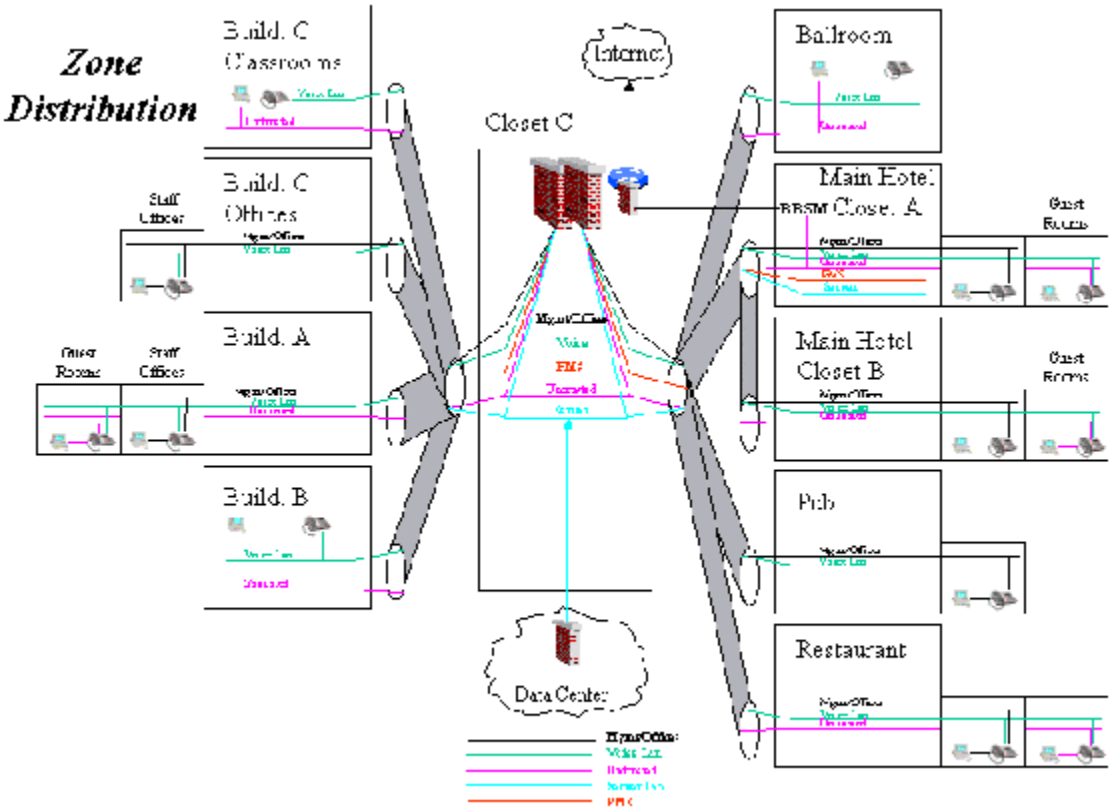

Figure 4

Employees that need to access our companies processing systems must use a VPN client on their workstation from the Untrusted or Management/Offices VLANS, exit through the CISCO BBSM, and enter our companies network through an already existing external VPN concentrator DMZ. (See figure 3) All

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

connections back to the core network except for those allowed for monitoring and management are considered untrusted.

Authentication and Authorization

To facilitate authentication and authorization and to build an environment that could be separated easily from our internal systems, a separate authentication repository was needed for the complex. Because the PMS application and workstations require the Microsoft Windows operating system, I suggested that a Windows 2000 Active Directory running in native mode with strict group policies should be utilized to authenticate users. To insure that our company's policy regarding user ID and password requirements was being followed, a password policy issue was added to the report. An issue was also included to address security within the PMS database system. (See Table 3)

Table 3

Resolved Issues				
No.	**Issue Description**	**Risk**	**Recommended Mitigation Strategy**	**Risk Level**
3.	The Visual One application requires a domain for authentication that should be separate from our enterprise Active Directory.	Combining the hotel domain with the enterprise AD may allow unauthorized access to internal systems.	Create a separate Active Directory domain for the hotel complex and configure it according to our company's security policies. Separate this network from our company's core network appropriately. Migrate any current workstations to the new network/AD.	HIGH
5.	User accounts could be configured with weak passwords.	Weak password policies can lead to unauthorized access.	User accounts must follow our company's current policies for password length, expiration, complexity, etc.	HIGH
11.	The Visual One application uses a database to store sensitive data.	Users who access the Visual One system should not be granted direct access to the database. Such access could lead to data compromise.	Secure access to the Visual One data store by configuring application and administration ID's for the database. Allow only the application and database administrators to make changes to the database. Make sure authentication passwords adhere to our company's policies.	MEDIUM

An active directory was created and configured to meet the password policy requirements. The PMS system database was configured with unique

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

application and administration ID's. Users were only given appropriate levels of access to file shares.

Workstation and Server Security

To aid in securing the workstations and servers, our company standardized certain versions of operating systems and developed standard builds, complete with security templates, that detail what components are allowed to be installed and enable security settings. These builds dictate base OS patch levels and include antivirus clients. Standard builds and security templates had already been completed for the SUN Solaris and Microsoft Windows operating systems. To help insure that the standards would be followed in this project, the following issues were captured on the risk assessment report. (See Table 4)

Table 4

Resolved Issues				
No.	**Issue Description**	**Risk**	**Recommended Mitigation Strategy**	**Risk Level**
10.	Workstations, and POS's that have not been secured may be used to gain unauthorized access to the Visual One application.	Unsecured workstations are vulnerable to various attacks that could lead to unauthorized access of the hotel and training center internal systems.	Workstations connecting to the hotel and training center network should be secured per our company's standards. Security recommends use of our company's standard workstation loads.	MEDIUM
12.	Operating systems are vulnerable to security issues unrelated to the Visual One server application.	Vulnerabilities in the configuration of the base OS can lead to data corruption and downtime.	Use our company's approved server load and apply appropriate security templates.	MEDIUM

As the systems were being built for the hotel and training center complex, standard loads and security template were applied.

Monitoring, Management, and Patching

Several issues were identified in the area of Monitoring, Management, and Patching. Due to the late involvement of security in the process and an aggressive production date, a couple of these issues would not be completed before the hotel and training center complex's private opening. (See Table 5)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table 5

Open Issues				
No.	**Issue Description**	**Risk**	**Recommended Mitigation Strategy**	**Risk Level**
2.	The Percipia Core Server utilizes an operating system that is out of date (Linux 7.1) and unsupported by our company. Linux is not a company approved standard OS.	Operating systems that are out of date may not contain the latest security patches and updates to prevent the server from malicious attacks. This server will obtain data directly from the Internet.	Determine who will support and update the operating system on this server. Apply all available security patches for the OS.	HIGH
3.	Solutions for monitoring and management for various security related systems such as Firewalls, Antivirus, Security Event Logging (Syslog), and Network Intrusion Detection systems have not been agreed upon and installed.	Without proper tools and systems in place to manage and monitor virus activity, intrusion detection, authentication activity, and firewall maintenance, intruders could compromise data without being detected.	Identify which teams should be involved and design solutions that include documentation on how various security monitoring systems will function in the new Hotel and Training Center environment.	HIGH

As a result of Issue # 2, our company created a standard load and security template for Red Hat Linux 8.0 that includes a base OS patch level. Our security operations team worked with the project team to determine how security monitoring would take place. The infrastructure design was flexible enough to allow for the installation of a core services server that functions as a drop point for security logs and antivirus updates. A network intrusion detection device was also installed to help protect the hotel and training center network form intrusion.

Table 6

Resolved Issues				
No.	**Issue Description**	**Risk**	**Recommended Mitigation Strategy**	**Risk Level**
8.	Improper use of the Visual One solution.	Could lead to compromises of private guest information.	Log administrative and user access to the Visual One SQL server and review them regularly. Tie systems into the central audit logging initiative and follow our company's logging requirements.	MEDIUM

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

9.	Maintain Visual One application and W2K OS service packs and hotfixes.	Vulnerabilities to applications and operating systems are often corrected in patches and hotfixes.	Document a service pack/hotfix update plan for the Hotel processing systems.	MEDIUM

Security logging was enabled on all servers through the operating system security template. The Visual One server and voice systems were added to our company's current service pack/hotfix update plans. (See Table 6)

BC/DR Planning and Data Backup

One of the requirements outlined by the third party contractors responsible for managing the hotel was that customer data regarding reservations as well as accounting information needed to be retained for a period of seven years. As mentioned earlier, the facility also needed to double as a recovery site in the event of a disaster. To make sure these requirements were addressed, the following issues were added to the report. (See Table 7)

Table 7

Open Issues				
No.	**Issue Description**	**Risk**	**Recommended Mitigation Strategy**	**Risk Level**
4.	A design and backup system is needed for the Visual One SQL server and various Voice system servers that exist in the hotel and training complex.	Lack of a backup can lead to the inability to recover from a malicious intrusion or virus out break in the environment and may violate data retention laws.	Design a local backup solution that will backup the Visual One SQL server and voice systems. This system should include a tape retention scheme that meets the customer guidelines.	HIGH
6.	The hotel and training center will double as a recovery site for our company should a disaster occur.	The hotel and training complex is considered an untrusted area due to it being open for reservations of training and hotel rooms to non-employees.	Create a DR Mode document describing how the network and various areas such as the ballroom and classrooms will be reconfigured in the event of a disaster. Describe in the document different security measures that will be taken to secure the DR Mode areas physically as well as electronically from the rest of the hotel complex.	MEDIUM

Issue # 4 remained open because, even though a backup system was designed for the complex, the tape retention scheme had not been finalized prior to the private opening. Our company already utilized a third party vendor for off site storage, so an agreement was made with this group to add the data from the hotel complex into the retention rotation.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

To address the need for part of the complex to double as a recovery site in the event of a disaster, Issue # 6, the network team designed a solution that isolated the ballroom with switches that could be reconfigured in the event of a disaster to have direct connectivity back to our data center. A plan was created that documented how this reconfiguration would take place and how the ballroom would be physically secured from public access should the recovery site be needed.

A business continuity plan and disaster recovery plan was also needed for the hotel processing systems themselves. The following issue was added to the report to address this risk: (See Table 8)

Table 8

Resolved Issues				
No.	**Issue Description**	**Risk**	**Recommended Mitigation Strategy**	**Risk Level**
13.	A BC/DR plan needs to be created detailing steps to ensure disaster recovery for the Hotel processing systems.	Lack of a BC/DR plan could lead to mistakes in data recovery during a disaster.	Document a BC/DR plan for the hotel management and voice systems.	MEDIUM

A plan was created that outlined a manual process that would be used so that the complex could continue to function if a system outage occurred. A plan was also created that discussed how backups would be utilized to recover from a disaster. Both of these plans were put in place prior to the private opening.

High Availability and Separation of Function

High Availability and Separation of Function issues are often hard to address when working on a project. Finding the right balance between costs and high availability is often problematic. The following issue addressed the risk involved with having one server house the account repository and the database for the PMS application. No plan was put in place to mitigate this issue and it was ultimately accepted through the signature process. (See Table 9)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table 9

Open Issues				
No.	**Issue Description**	**Risk**	**Recommended Mitigation Strategy**	**Risk Level**
5.	The current design requires the Visual One SQL server to function as an AD domain controller, file server, and Visual One SQL server.	Housing multiple applications on one physical server increases the severity of impact if the server is compromised.	Separate the Visual One SQL and File server from the AD domain controller.	MEDIUM

The need for a system to be highly available is dependant upon the importance of the system and the ability for business to continue while it is unavailable. The following issue was added to the report to address high availability. It requests that a component failure impact analysis document be created for the processing systems in the complex. By requesting that this documentation be created and communicated to the project sponsors, I was able to raise awareness of this issue and resolve it without having to list every component in the report. This also allowed the project team to define its own level of availability requirements without having them mandated by security. (See Table 10)

Table 10

Resolved Issues				
No.	**Issue Description**	**Risk**	**Recommended Mitigation Strategy**	**Risk Level**
7.	The current Visual One and voice systems are not highly available. The Interface PC does not contain redundant components.	Designs that contain single points of failure can lead to increased downtime and security breaches.	Complete component failure impact analysis documentation for the environment. Security recommends creating a highly available server design using servers that employ redundant hardware on critical systems such as the Visual One SQL server and the Interface PC per customer availability requirements.	MEDIUM

A component impact failure analysis document was created for this project and it was shared with the project sponsors so that they would be aware of failure points in the design.

Business Concerns and Legal Issues

Sometimes complex issues arise that are not exactly security issues but require mitigation strategies that involve security. A rather large one that occurred in this

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

project is identified below. The department that conducts the employee training in the old training center was not included in the project until the network was close to being converted to the new design. (See Table 11)

Table 11

Open Issues				
No.	**Issue Description**	**Risk**	**Recommended Mitigation Strategy**	**Risk Level**
1.	A migration plan to determine how employee training will be carried out on the new hotel and training center network has not been finalized.	The training department offices and server are needed to support training at the conference center. Changes in how the users access the server and data center from the new training complex network may impact how they do business. Opening of the complex to public access changes the training center trust level, requiring changes to current business processes.	In the intermediate state, segment the training department offices from the rest of the complex using a key card activated doors and leave them directly connected to the data center core network. Install temporary switches in the ballroom and various classrooms to allow our company's trainees to access the training server and core network directly (without a VPN client). Create a migration plan to be put in place before the public opening of the complex that details how training will take place, where the training server will be located, how VPN access will be managed for trainees, how the training department offices will be connected, etc.	HIGH

If the training offices had been converted to the new network design, they would have been required to use VPN clients to access our companies internal systems as well as their own training server through the external VPN concentrator DMZ. From the training employees point of view, this was an unfair requirement and would require major changes in how they conducted business. A compromise was made; key card readers were installed on all door ways leading to and from the training offices and the training department offices were allowed to remain on the old network switches that connected directly back to the core network. However, whenever the trainer leaves their office and utilizes a classroom that is available to the public, they are required to utilize VPN clients to access our company's core network.

There was also some disagreement on whether or not the third party contractors responsible for running the day-to-day functions of the hotel had completed the proper clauses and schedules stating that they would protect the company's assets appropriately. The following issue addressed this situation. (See Table 12)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table 12

Resolved Issues				
No.	**Issue Description**	**Risk**	**Recommended Mitigation Strategy**	**Risk Level**
6.	Third party contractors currently have access to our company's networks and some processing systems. Third party contractors will be managing the hotel and training complex.	Third party contractors may not be contractually obligated to follow our company's security policies or protect our company's data/networks.	Have the third party contractors complete a Schedule L. A Schedule L is a part of the contract with the vendor that states that they will follow our company's policies and protect our company's assets, with some sort of liability clause if they don't.	HIGH

After having our legal department review the contract, it was determined that the correct schedule had been included.

Remote Access

The PMS system required the use of a credit card processing modem connection as well as a support modem in the event that the vendor needed to help remedy a problem with the database or application. The following issue was added to the report to address this requirement. (See Table 13)

Table 13

Resolved Issues				
No.	**Issue Description**	**Risk**	**Recommended Mitigation Strategy**	**Risk Level**
4.	The Visual One Interface PC requires two modem connections. One for credit card processing and another for vendor support issues.	Modems can allow unauthorized access to core systems, bypassing security barriers that have been put in place, possibly allowing compromise of internal systems.	Follow our company's policy regarding modems. Complete appropriate exceptions where needed. Power the modem off and disconnect the phone line when not in use. Only enable the modem for support reasons. Only allow outgoing call initiation and require authentication when connecting.	HIGH

Our company has strict policy defining the use of modems in our network designs. Exceptions are required that must be approved by upper management before a modem can be installed. The credit card vendor provided a special modem to protect the credit card transactions. A second modem was configured for support that was connected to a dial-out-only line. A process was created to

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

document how the modem would be enabled in the event of a problem and describing how the connection would be initiated from our network.

Physical Security

What about physical security? As you can see there are very few issues directly related to physical security on my report. Most of the projects that I deal with do not require a lot of thought about physical security because the processing systems reside in a datacenter, but this project has many areas where physical security is needed. The following list describes physical security measures that were taken to protect the hotel and training center network and employee assets from the public.

Server and Workstation Placement

All servers and network gear are housed in locked closets, out of reach from the general public. The following list defines where the servers are located and the physical security measures put in place to protect the assets:

- **Closet A** - Closet A is the main wiring closet in the new hotel. It is a small room about 5' X 5' that is located inside a maintenance/storage room. It houses the switches for the south wing of the hotel, the CISCO BBSM, The PERCIPIA voice servers, and an Interface PC that controls the COMTROL device. These systems needed to be located near the COMTROL system due to serial cable length restrictions. These assets are protected from access by locks that exist on the maintenance room door and the closet door.
- **Closet B** - Closet B is the smallest of all the wiring closets and contains the switches for the north wing of the hotel. It is about 3' X 3' and is also located inside another maintenance/storage room. It is protected from access by locks that exist on the maintenance room door and the closet door.
- **Closet C** - This closet is the most secure section of the old complex. It contains network switches and routers that connect the hotel and training center complex back to the datacenter and to the phone company. It is a 15' X 12' area that contains battery backup systems and all the processing systems that do not need serial connections to the COMTROL device. This includes the PMS database server, the PIX firewall devices, some of the voice systems, and the core services server. These assets are protected from access by a key card activated door and are monitored by security guards that exists at the datacenter.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Workstations exist at the front desk for check in, in the hotel offices for accounting and supply management, and at the pub and restaurant as Point-Of-Sale stations. They connect back to the processing systems through closet A & B. (See Figure 1)

Facility Security

Since opening the complex to the public, the key card access gates that used to surround the complex were removed. However, the complex is monitored by video surveillance from the security guard desks at the datacenter, as well as hotel security guards provided by the third party contractor.

Training Employee Offices

To protect employee offices and their datacenter direct network connections from access by the public, key card activated locks were installed on all doors leading to and from employee offices. The majority of these offices exist in the old training complex building C. (See Figure 1)

Lessons Learned

While researching and developing this project I learned a number of things, including the importance of early involvement, group participation, and about physical security issues.

The Importance of Early Involvement

As mentioned earlier in this paper, security was not engaged in this project until after many Information Technology decisions had been made. Since we were not included, the technologies chosen to provide the services in the complex were not examined in great detail. In my next project, I plan on being involved early in the projects life cycle, however the project manager is ultimately responsible for getting security involved in their projects.

Group Participation

As you can tell, this project involved several departments spread across several different lines of business. Unfortunately, even though the executive level over the training department was driving the project, the managers of the training department were reluctant to participate. Security issues such as the need to use a VPN client to access the core network from the classrooms and physical security restrictions placed on the employee offices were not raised until after the project team had agreed upon solutions. Requiring a VPN client for students also proved to be a complicated issue. A process had to be defined for how

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

students that did not already possess a VPN ID and client software could be provided with one for training. In the future I will examine the scope of the project and make sure all the necessary groups are involved so that all the requirements are examined.

Physical Security

Many issues around physical security were not raised through the security risk assessment process. This is due to my lack of knowledge on how to deal with physical security and to a lack of involvement from our corporate physical security team. I would like to learn more about physical security, and plan to attend more training classes.

Conclusion

Through the process of security risk assessment, this project underwent many changes. My team was able to identify may security risks and offer solutions such as: A firewall bundle was purchased to help segment different trust zones within the network, security templates were installed, servers were physically protected from direct access, disaster recovery plans were developed, and monitoring and management solutions were created. Without security risk assessment, many of these security improvements may not have been implemented, leaving the company's network and customer data vulnerable to attack.

Although there were considerable costs involved with mitigating the security vulnerabilities in this project, these costs are minor compared to the losses our company could incur due to a compromise of customer data.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

Alberts, Christopher and Dorofee, Audrey. Managing Information Security Risks, Pearson Education, Inc., Boston, MA, 2002.

Cisco Systems. "Cisco Building Broadband Service Manager". URL: http://www.cisco.com/application/pdf/en/us/guest/products/ps533/c1650/ccmigration_09186a008010ba18.pdf (31 March 2003).

General Accounting Office. "Information Security Risk assessment". November 1999. URL: http://www.gao.gov/special.pubs/ai00033.pdf (31 March 2003)

Percipia Networks. URL: http://www.percipia.com/warper.jsp (31 March 2003).

Tipton, Harold and Krause, Micki. Information Security Management, Auerbach Publications, Boca Raton, FL, 2000.

Visual One. URL: http://www.visualonesystems.com/propertymanagement.htm (31 March 2003).

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Appendix A – Complete Risk Table

Open Issues				
No.	**Issue Description**	**Risk**	**Recommended Mitigation Strategy**	**Risk Level**
1.	A migration plan to determine how employee training will be carried out on the new hotel and training center network has not been finalized.	The training department offices and server are needed to support training at the conference center. Changes in how the users access the server and data center from the new training complex network may impact how they do business. Opening of the complex to public access changes the training center trust level, requiring changes to current business processes.	In the intermediate state, segment the training department offices from the rest of the complex using a key card activated doors and leave them directly connected to the data center core network. Install temporary switches in the ballroom and various classrooms to allow our company's trainees to access the training server and core network directly (without a VPN client). Create a migration plan to be put in place before the public opening of the complex that details how training will take place, where the training server will be located, how VPN access will be managed for trainees, how the training department offices will be connected, etc.	HIGH
2.	The Percipia Core Server utilizes an operating system that is out of date (Linux 7.1) and unsupported by our company. Linux is not a company approved standard OS.	Operating systems that are out of date may not contain the latest security patches and updates to prevent the server from malicious attacks. This server will obtain data directly from the Internet.	Determine who will support and update the operating system on this server. Apply all available security patches for the OS.	HIGH
3.	Solutions for monitoring and management for various security related systems such as Firewalls, Antivirus, Security Event Logging (Syslog), and Network Intrusion Detection systems have not been agreed upon and installed.	Without proper tools and systems in place to manage and monitor virus activity, intrusion detection, authentication activity, and firewall maintenance, intruders could compromise data without being detected.	Identify which teams should be involved and design solutions that include documentation on how various security monitoring systems will function in the new Hotel and Training Center environment.	HIGH

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

4.	A design and backup system is needed for the Visual One SQL server and various Voice system servers that exist in the hotel and training complex.	Lack of a backup can lead to the inability to recover from a malicious intrusion or virus out break in the environment and may violate data retention laws.	Design a local backup solution that will backup the Visual One SQL server and voice systems. This system should include a tape retention scheme that meets the customer guidelines.	HIGH
5.	The current design requires the Visual One SQL server to function as an AD domain controller, file server, and Visual One SQL server.	Housing multiple applications on one physical server increases the severity of impact if the server is compromised.	Separate the Visual One SQL and File server from the AD domain controller.	MEDIUM
6.	The hotel and training center will double as a recovery site for our company should a disaster occur.	The hotel and training complex is considered an untrusted area due to it being open for reservations of training and hotel rooms to non-employees.	Create a DR Mode document describing how the network and various areas such as the ballroom and classrooms will be reconfigured in the event of a disaster. Describe in the document different security measures that will be taken to secure the DR Mode areas physically as well as electronically from the rest of the hotel complex.	MEDIUM

Resolved Issues				
No.	**Issue Description**	**Risk**	**Recommended Mitigation Strategy**	**Risk Level**
1.	The hotel and training complex contains several processing systems that contain data that must be protected from improper access and tampering.	An attacker could retrieve customer personal data or launch an attack against our company or other external networks from within the hotel and training complex.	Install a PIX firewall bundle to separate processing systems from general guest access. Install a PIX firewall to separate management traffic for the hotel processing systems from the data center core. Require all guest and classrooms to access the Internet or our company's network through the CISCO BBSM. When accessing our company's network, the user traffic must pass through our company's external VPN concentrator.	HIGH

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

2.	Firewalls can be configured with weak rule sets.	Incorrect firewall configuration could allow an attacker to gain access to sensitive data.	Configure the hotel network firewalls with appropriate rule sets to allow only essential network traffic between the various VLAN's according to our company's standards.	HIGH
3.	The Visual One application requires a domain for authentication that should be separate from our enterprise Active Directory.	Combining the hotel domain with the enterprise AD may allow unauthorized access to internal systems.	Create a separate Active Directory domain for the hotel complex and configure it according to our company's security policies. Separate this network from our company's core network appropriately. Migrate any current workstations to the new network/AD.	HIGH
4.	The Visual One Interface PC requires two modem connections. One for credit card processing and another for vendor support issues.	Modems can allow unauthorized access to core systems, bypassing security barriers that have been put in place, possibly allowing compromise of internal systems.	Follow our company's policy regarding modems. Complete appropriate exceptions where needed. Power the modem off and disconnect the phone line when not in use. Only enable the modem for support reasons. Only allow outgoing call initiation and require authentication when connecting.	HIGH
5.	User accounts could be configured with weak passwords.	Weak password policies can lead to unauthorized access.	User accounts must follow our company's current policies for password length, expiration, complexity, etc.	HIGH
6.	Third party contractors currently have access to our company's networks and some processing systems. Third party contractors will be managing the hotel and training complex.	Third party contractors may not be contractually obligated to follow our company's security policies or protect our company's data/networks.	Have the third party contractors complete a Schedule L. A Schedule L is a part of the contract with the vendor that states that they will follow our company's policies and protect our company's assets, with some sort of liability clause if they don't.	HIGH
7.	The current Visual One and voice systems are not highly available. The Interface PC does not contain redundant components.	Designs that contain single points of failure can lead to increased downtime and security breaches.	Complete component failure impact analysis documentation for the environment. Security recommends creating a highly available server design using servers that employ redundant hardware on critical systems such as the Visual One SQL server and the Interface PC per customer availability requirements.	MEDIUM

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

8.	Improper use of the Visual One solution.	Could lead to compromises of private guest information.	Log administrative and user access to the Visual One SQL server and review them regularly. Tie systems into the central audit logging initiative and follow our company's logging requirements.	MEDIUM
9.	Maintain Visual One application and W2K OS service packs and hotfixes.	Vulnerabilities to applications and operating systems are often corrected in patches and hotfixes.	Document a service pack/hotfix update plan for the Hotel processing systems.	MEDIUM
10.	Workstations, and POS's that have not been secured may be used to gain unauthorized access to the Visual One application.	Unsecured workstations are vulnerable to various attacks that could lead to unauthorized access of the hotel and training center internal systems.	Workstations connecting to the hotel and training center network should be secured per our company's standards. Security recommends use of our company's standard workstation loads.	MEDIUM
11.	The Visual One application uses a database to store sensitive data.	Users who access the Visual One system should not be granted direct access to the database. Such access could lead to data compromise.	Secure access to the Visual One data store by configuring application and administration ID's for the database. Allow only the application and database administrators to make changes to the database. Make sure authentication passwords adhere to our company's policies.	MEDIUM
12.	Operating systems are vulnerable to security issues unrelated to the Visual One server application.	Vulnerabilities in the configuration of the base OS can lead to data corruption and downtime.	Use our company's approved server load and apply appropriate security templates.	MEDIUM
13.	A BC/DR plan needs to be created detailing steps to ensure disaster recovery for the Hotel processing systems.	Lack of a BC/DR plan could lead to mistakes in data recovery during a disaster.	Document a BC/DR plan for the hotel management and voice systems.	MEDIUM

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 21st, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced