**BACKGROUND**

Omega Research is a rapidly growing research and consulting firm. They have a single main office located in Reston, VA and three small branch offices located in San Diego, CA, Salem, OR, and Kansas City, MO. Omega is not currently involved in e-commerce or business-to­business relationships.

Two weeks ago, Omega experienced a significant loss of proprietary data (estimated value $550,000.00) that was stored electronically in an Oracle database in their main office in Reston. The data was unrecoverable and backups were not being routinely maintained, so no restoration was possible. Although he has no hard evidence, Omega’s CTO believes that the loss resulted from deliberate deletion of files by a systems administrator from the Kansas City office that had been “let go” several weeks prior to the loss. Needless to say, the CTO has been tasked to “get things under control.”

You have been hired as a consultant to develop a comprehensive plan for improving the company’s recovery posture in order to prevent future outage of Omega’s critical systems and network resources. Your guidance and observations will eventually be used to develop a long-term procedural and policy solution for Omega Research. The CTO has stepped up to the plate and made the commitment to do whatever it takes to address these issues.



Baseline Network Infrastructure

* Omega leverages AT&T Managed Internet Services for each of its office locations.
* Omega owns and manages the border routers for each of their office sites.
* Offices in Reston, San Diego, and Kansas City receive full T-1 service.
* Offices in Salem receive 256k F-T1 circuit service.

Systems

**Business processes provided by AIX Environment**

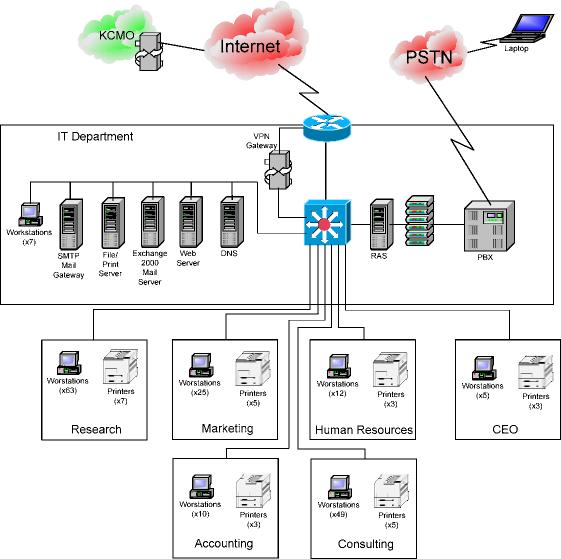
1. Financial
2. Reporting
3. Data Warehouse

LAN

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Vendor** | **Services** | **Address** | **Phone** | **Contacts** |
| IBM | Tape Library  TSM Server | 522 South Rd  Poughkeepsie, NY 12601 | 214 451-7747 | Steve Barretta |
| SunGard | Recovery services for server environment | 401 N Broad St.  Philadelphia, PA | 877 456-3966  215 351-1300 | * Don Meltin (Test Coord.) * Jack Fabrianni (Acct. Rep) * Lincoln Balducci (Resource Coord.) |

**BASELINE ARCHITECTURE**

**Local Area Architecture (Reston Office)**



**AIX Environment**

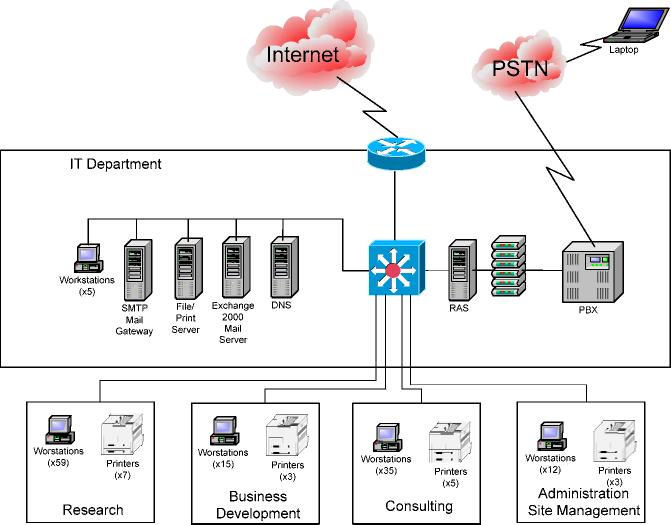


* Perimeter protection provided by screening router. Configured for dynamic packet filtering using reflexive Access Control Lists (ACL’s).
* Remote access is provided to employees while at home or on travel through PPTP VPN, and, dial-up RAS offered by a Microsoft Windows NT 4.0 Server ®.
* All servers in the Reston office have been centrally located to a data center.
  + The Reston data center supports a 5-keypunch combination lock that is required to have access to the room. That combination is shared with all IT personnel and is infrequently rotated.
  + The data center is controlled for humidity through HVAC purification.
  + The data center is controlled for temperature with isolated HVAC services.
  + The data center is not on a raised floor to control static electricity.
  + The data center does not have a site-wide UPS. Each server and network equipment supports their own mini-UPS.

* Internal Omega E-mail is supported by a Microsoft Exchange ® 2000 mail server running on a Microsoft Windows ® 2000 Server. Omega has installed an SMTP mail gateway to support Internet mail exchange.
* Omega is the registered owner of [omegaresearch.com](http://omegaresearch.com) and maintains a DNS Server at the Reston facility for name resolution supporting Omega users and to allow Internet access to publicly accessible information (web and e-mail).
* Web hosting services are provided on a Microsoft Windows ® 2000 Server running Internet Information Services (IIS).
* X.500 directory services are available through Active Directory although their implementation is relatively immature – they are operating in a mixed environment.
* Server and client o/s environments have not been routinely patched.
* Reston office printers are all network connected.
* The IT Department is responsible for management of the networks and networked resources at the Reston facility. They manage more than 170 workstations and 6 servers performing the functions previously described.
* Client machines consist of Microsoft Windows ® 95, 98, NT Workstation 4.0, 2000, and XP. Mac operating systems include OS/8 and OS-X, Panther.
* Productivity applications have not been standardized. Some user communities enjoy Corel OfficeSuite ® while others appreciate Microsoft Office ®. There are various editions of these packages installed on client machines.

**BASELINE ARCHITECTURE**

**Local Area Architecture (San Diego Office)**



* The San Diego is essentially a mirror of the network architecture provided at the Reston facility.
* Differences:

o San Diego does not host a web server.

o San Diego does not support VPN or RAS connections.

o There are fewer employees working out of the west coast office. The local IT staff consists of one engineer who manages all networks and networked resources within the San Diego office.

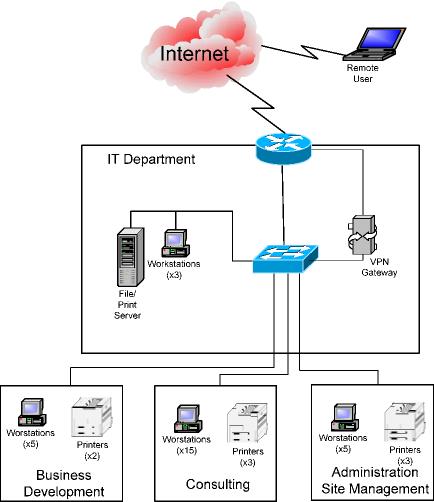
o There are less than 50 client machines in San Diego with similar configurations as the main office.

o All servers have been located in a spare office in San Diego.

* There is not a controlled access restriction like in the main center.
* The office is not controlled for temperature, humidity, or static.
* There are no redundant power supplies.

**BASELINE ARCHITECTURE**

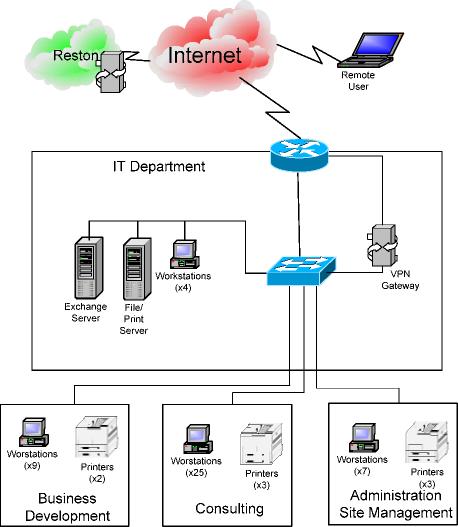
**Local Area Architecture (Salem Office)**



* Salem is a small site with only 30 workstations configured in much the same way as the rest of the company.
* Sale supports a single combined shared file and print server hosted on a Microsoft Windows ® NT 4.0 Server.
* Mail services are obtained through the San Diego office, using mailboxes set up on the San Diego Exchange Server.
* There are no publicly available networked resources at the Salem office.
* Remote access to Salem’s infrastructure is provided to mobile and home employees using VPN client to gateway connectivity.
* Salem has an IT staff of one engineer that manages all networks and networked resources at this site.
* All servers have been located in a spare office in San Diego.
* There is not a controlled access restriction like in the main center.
* The office is not controlled for temperature, humidity, or static.
* There are no redundant power supplies.

**BASELINE ARCHITECTUREARCH**

**Local Area Architecture (Kansas City Office)**



* Kansas City is very similar in size to the Salem office with the exception that Kansas City runs a Microsoft Exchange ® 2000 server for mail services.
* Kansas City has a local system administrator for support.
* All servers have been located in a spare office in Kansas City.
* There is not a controlled access restriction like in the main center.
* The office is not controlled for temperature, humidity, or static.
* There are no redundant power supplies.

Figure 1 - Main Application Equipment List



**CONSIDERATIONS**

**Networking and Systems Administration**

1. Access to any site LAN automatically guarantees access to the entire WAN. This means that user accounts authenticated in the Salem office have immediate access to resources in San Diego, Kansas City, and Renton.
2. User accounts and access restrictions are independently managed by each office’s system engineer. There is not a common user policy – rules concerning how passwords are created an enforced, cycled, aged, lockout, user account retention, and so on, are created and maintained per office.
3. There is no formal backup and disaster recovery policy at any site. Backups are decentralized. Off-site rotation only happens at the Reston office. Salem currently performs DASD to DASD backups without Tape copies being made.
4. The local system administrators at the satellite offices take all direction from the central office and are not authorized to make boundary router changes. They do not have authority to change anything without central IT approval. They have no site specific budget; they have full accountability for their LAN’s.
5. All machines run antivirus software although local IT staff infrequently maintains their definition files and relies on user intervention to perform file updates. No machine has spyware protection.
6. There is no dedicated program for training employees on avoiding threats like, say, Phishing.
7. Firewall logs, host packet analysis, application logs, event and error logs are generally ignored across the board.

**Business Requirements**

1. The organization is growing rapidly in spite of recent events.
2. Their strength is in developing business within the local market and providing on-site consulting services. The research end of the business is the well-spring from which they draw their competitive edge, but Omega is realizing that consolidating the research workforce adds synergy to their efforts, and reduces unnecessary overhead.
3. They plan to continue down that road. As a result, local sites will expand their consulting workforce and research will continue to be consolidated at the Reston and San Diego facilities. As this trend continues to develop, access to the research data stored at the east and west coast facilities becomes critical. Additionally, they cannot afford a similar loss of proprietary information as was recently experienced....and they know it could have been much worse.

**Known Environmental Risks**

1. The San Diego office is located in a 20-year earthquake zone. Once every 20 years, it estimated that a 6.0-Richter scale earthquake or greater will strike the facility, likely causing damage to the facility/computer equipment; management assumes losses to computer assets could be estimated at 20%. As a countermeasure, the company has purchased insurance with $18,000.00/year annual premiums that increase 5% every year.
2. The Reston office is located in a 500-year flood zone. Once every 500 years, it is estimated that a flood will strike the facility likely causing damage to the facility/computer equipment; management assumes losses to computer assets could be estimated at 40%. The company has opted to not purchase insurance. Annual premiums would run approximately $25,000.
3. The Kansas City office suffers a significant tornado event once every five years. When the tornado hits, severe electrical disruption affects the equipment and the office suffers 10% losses on computer assets. The company pays $14,000 in annual insurance premiums.

Appendix A.

**Balance Sheet**

|  |  |  |  |
| --- | --- | --- | --- |
| **Reston** |  | **Book Value** | **Actual Value** |
| 81,290 45,690 27,390 13,330 | 17,250  9,450  4,309  0 |
| Networking Equipment Server Equipment  Workstation Equipment Peripherals |
|  | TOTAL: | 167,700 | 31,009 |
| **Kansas City** |  |  |  |
| Networking Equipment |  | 12,700 | 11,900 |
| Server Equipment |  | 4,009,250 | 3,400,000 |
| Workstation Equipment |  | 18,200 | 13,400 |
| Peripherals |  | 4,433 | 0 |
|  | TOTAL: | 4,044,583 | 3,425,300 |
| **Salem** |  |  |  |
| Networking Equipment |  | 4,300 | 0 |
| Server Equipment |  | 3,600 | 0 |
| Workstation Equipment |  | 7,200 | 500 |
| Peripherals |  | 4,433 | 0 |
|  | TOTAL: | 19,533 | 500 |
| **San Diego** |  |  |  |
| Networking Equipment |  | 81,290 | 17,250 |
| Server Equipment |  | 45,690 | 9,450 |
| Workstation Equipment |  | 27,390 | 4,309 |
| Peripherals |  | 13,330 | 0 |
|  | TOTAL: | 167,700 | 31,009 |

Appendix B.

The Business Impact Interviews

Bill Hermann - We are a service-based company and our ability to take in and book cash is critical. Without solid cash flow or expenses increase exponentially in the very short period of time. In addition our cash position which I monitor through the SAP system allows us to manage our treasury and short-term funding. I would estimate within two days we would have to borrow money which could increase our costs and overhead.

Tiffany Sabers – The I.T. organization is in a period of transition when it comes recoverability. Implementation of SAP was very expensive, time-consuming, and drawn out. We have built-in a level of redundancy to sustain production should any number of things fail within a data center itself. However we are not in as good a shape as we should be to protect your organization to the entire data center become unavailable for any significant period of time. Several factors come into play when considering the recovery of a central system such as SAP. The availability of the technology we've chosen at our recovery vendor has been a challenge to say the least. SunGard needs to acquire and fund the appropriate IBM servers that we use to run the SAP application. Secondly there is for a terabytes of production data that needs to be recovered from tape once a disaster is declared. The recovery activity using the current tape library technology on the floor is estimated to take 3 to 4 days barring any problems. For tape to be a viable option going forward we need to upgrade to higher speed higher density devices and media to meet the needs of the business which is another capital expense. I think we all knew and accepted the risk of having to retool with the implementation of SAP. Now that time has come and this exercise is crucial to determine the proper recovery strategy and technology to meet the business needs.

John Sampolous - I agree with Bill that our finance structure is key. Since we don't make anything physical our business model relies on our cash position. I will say though without having finance information available we may begin borrowing on the second day of an outage. The way the SAP system works without current data we will be a day behind at the time of business start the second day. We're certainly capable of maintaining business function but will begin to lose $3-$500,000 per day in interest alone. The bottom line is treasury function that is maintained via a finance module within SAP is critical from our standpoint.

Linda Okonieski - from a purely operation standpoint we are currently dead in the water if we can't get to our schedules and billing information for the persons in the field. We generate a quarter million dollars in revenue a daily basis to our service organization. So if there is a hard fail of the SAP system we stand to have issues in two functional areas. The first and most obvious is that if we cannot invoice our clients in a timely manner or cash flow will diminish significantly at the end of the first week. The second concern is his longer-term and related to legal and contractual ramifications if we could not maintain business as usual as quickly as possible. In our business customer confidence and brand value are priceless and need to be protected. So if we are unable to quickly recover we could very well lose future business that could affect our viability of the company.

Nate Brown - Linda hit the nail on the head, we need to ensure that we have the right people in the field generating income through billable hours and we need to continue to collect for their work. So I would say the schedule and billing within the SAP system ranks very high for me. And to add to Windows last point customer confidence is how we've been able to maintain a preferred vendor status with most of these companies where we do business, so many chink in the armor could cost us a significant amount of business.

Sandy Ales - Without access to the SAP system we can’t sell services we can’t deliver. Most of our customers rely on us to be able to find and supply the appropriate consultant/resources as quickly as possible. Since we are one of several preferred service providers we will begin to miss out on new contracts and renewals to our competition. Our reliance on up to date information affects 30 to 40% of our short-term contracts and their ability to compete or longer-term assignments for our higher value personnel. Since we converted from our old system last year we had become completely reliant on the SAP application.

Tyler Amdahl - We have built-in on site redundancy for the SAP system, but we are still negotiating a new contract with SunGard services for a recovery configuration at the hotsite. Given the amount of data that is involved with the SAP system we are looking at 12 to 16 hours minimum recovery.

Rachid Chad – The SAP system is designed/architected for failover capability. Unfortunately the production system implementation is currently around $14 million dollars. There is no economy of scale for full redundancy or real-time failover. There are several options worth considering if anyone the recovery time objectives that we all agree to. I can say that they will not be cheap so we will need to understand the costs were relating to an outage from the business perspective to enable us to construct the proper recovery strategy.

Reyes Emme – If you were to ask the employees they would rank getting their paychecks on time as a number one priority. However the fact is that by self insuring our payroll funding for a week to 10 day period we could provide estimated payroll and then rectify many issues once we're back up and running. We in HR also have or long-term concerns should an outage extends for more than a few days and began to affect our brand value. The reason to be quite honest is that we attract the best consultants partly based on their perception of our technical abilities as an organization.

Fionna O'Connor – The audit and compliance areas are not affected in the short term should an outage occur. However, timing is everything. Should the outage occur during the close of SOX testing on the ramp above financial reporting to the board we could have issues with the regulators will.

Jackson Davis - We have an all-in situation with the SAP system. We are completely reliant on the system availability for day-to-day operation. The risk we have with the prolonged outage is that we will begin to incur penalties for our accounts payable since we have been able to migrate to a just-in-time payment practice. I am also concerned that we may not have the proper documentation to manually operate should the system be unavailable. I think however this exercise turns out several of our departments need to go back and designed some contingency plans should the data center be unavailable to us. The penalties for late payment would be 10% of $100,000 per day.