



What were some of your greatest challenges in developing an alternate processing site for Pixel? What information was difficult to obtain? How did you work around the issues? Share your ideas with your classmates. Comment on other person's posts.

**10/11/2014 4:01:00 PM**

I actually have had a couple of problems breaking-into the Unit 4 assignment. The first issue had to do with what do disaster recovery sites even look like? From BizTech, Chapple (2012) discusses different kinds of sites that require specific funding and resource investments; the three primary sites briefly covered by Chapple include cold, warm, and hot (Chapple, 2012). Cold sites are basically starter sites, and contain only the bare necessities, such as power, heating, air, and network connectivity (also considered the cheapest. The next site is a warm site. A warm site goes a step further than a cold site and includes hardware and software necessary to bring operations online (by default, most systems are still offline). And finally, there is the hot site. A hot site offers the best real-time cut over, having hardware and software that are either online, or set to ready to go. While the hot site seems like a great option, it is also the most expensive. Another issue I had was power consumption; as in, how much power does the alternate site need? To solve the power issue, I went online to find servers. Finally, I came across the Dell rack mount servers. I was able to view specifications and found out that each server uses 80-400 watts, depending on the model of the server (Vertatue, 2011). So, by adding the power consumption of each server, router, and switch, I could tally up the exact power consumption required in the datacenter. Of course, I still have to add other devices such as workstations and printers to gain the total power required at the site.

#### References

Chapple, Mike. (2012/6/7). Which disaster recovery site strategy is right for you? Retrieved from <http://www.biztechmagazine.com/article/2012/06/which-disaster-recovery-site-strategy-right-you>

Vertatue. (2011/7/7). Average power use per server & desktop. Retrieved from <http://www.vertatue.com/average-power-use-server>

What is a hot issue this week in the security arena as it relates to this unit's topic? Summarize one of these issues on the message board, and respond to another person's post.

**10/11/2014 4:38:14 PM**

My article comes from Continuitycentral.com. The topic, believe it or not, is Ebola. Maclean-Bristol (2014) discusses factoring-in the Ebola infection in a business continuity plan (Maclean-Bristol, 2014). The article raises several questions, but the most important is, "What happens if your staff becomes infected?" I know for us, if particular people on the IT team became infected, it would seriously impact business flow; and the reason is because many positions, many roles, are filled by only one person. The article goes on to make points about Ebola affecting supply chains, traveling staff, and even how to deal with internal panic. One scary thought is what if the entire (or part of) company became quarantined? How would business continue? It is an interesting article, but I think many companies have addressed similar situations, such as dealing with other viruses or influenza. Nonetheless, it does bring to light the current issue of Ebola and the far-reaching ramifications of the virus...as it affects business continuity.

#### Reference

Maclean-Bristol, Charlie. (2014/10). Should we be planning for an Ebola pandemic? Retrieved from <http://www.continuitycentral.com/feature1235.html>



**10/9/2014 9:14:31 PM**

These proxy payments are pretty interesting. I'm wondering if the future of online proxy payment systems will merge with Bitcoin? I'm not sure if you're familiar with Bitcoin, but it's basically a peer-to-peer payment system...meaning there are no banks. Can you imagine that? I used the Bitcoin system once to purchase nootropics online; it was actually quite easy. I'm guessing proxy payment systems, as well as digital currency may be the wave of the future. Check out the Bitcoin site at <https://bitcoin.org/>.

**10/11/2014 2:26:58 PM**

I actually have seen exactly what you are talking about affect U.S. electronic sales. For example, Hynix, a Chinese RAM chip maker, had major fire damage last year. They did not have a business continuity plan; consequently, world-wide prices of particular types of RAM went up immediately. I can only guess if they would have implemented a warm site or hot site that RAM prices would not have spiked like they did. Check out this article: <http://www.extremetech.com/computing/166775-ram-pricewatch-memory-spikes-in-wake-of-hynix-fire-but-for-how-long>

**10/11/2014 5:02:20 PM**

I have also had a few problems with the assignment. For example, rounding up the total power consumption for the alternate site. I have been adding up the power consumption for each device (seems a little monotonous). Another issue, is of course who is going to be in charge. I've never dealt with disaster recovery or alternate sites; so I have research that issue further. I'm glad you touched on the topic of staff, because I have not gotten to that yet. I'll read the article you referenced.

## **Business Continuity Planning – The Alternate Processing Site**

When there is an outage of some or the entire IT system infrastructure, a company may be unable to survive without quickly recovering. A business continuity plan or BCP is, therefore, an important part of any security policy.

During normal operation, all IT functions are carried on by dedicated infrastructure. When a disaster strikes that interrupts IT functions, the alternate processing site (or just the alternate site) is brought online to carry mission critical operations. The alternate processing site's routine maintenance, activation, and deactivation are all part of a carefully constructed business continuity plan.



## Outcomes

**After completing this unit, you should be able to:**

- Analyze a business's operations to identify mission critical applications.
- Outline the process for implementing an alternate site.
- Describe routing, naming, and addressing issues for an alternate site.
- Define the steps for doing a walk-through for bringing up the alternate site.
- Develop the most cost-effective design for the alternate site.
- Plan for cutting over to and cutting back from the alternate site.

**Course outcome(s) practiced in this unit:**

**IT540-3:** Develop a computer network disaster recovery plan.

## What do you have to do in this unit?

- Complete assigned Reading.
- Complete the Learning Activity.
- Participate in Seminar or complete Alternative Assignment.
- Participate in Discussion.
- Complete unit Assignment.

## Read

Read Chapter 4: "Risk Management," in *Principles of Information Security*.

## Terms

**Risk management:** The process of identifying vulnerabilities in an organization's information systems and taking carefully reasoned steps to ensure the confidentiality, integrity, and availability of all the components in the organization's information system.

**Risk identification:** The process of examining and documenting the security posture of an organization's information technology and the risks it faces.



**Risk control:** The process of applying controls to reduce the risks to an organization's data and information systems.

**Information security:** Understand the threats and attacks that introduce risk into the organization

**Asset valuation:** The process of assigning financial value or worth to each information asset.

**Management and users:** Play a part in the early detection and response process; ensure that sufficient resources are allocated

**Information technology:** Assist in building secure systems and operating them safely.

**Clean desk policy:** A policy requiring employees to secure all information in appropriate storage containers at the end of each day

**Likelihood:** is the probability that a specific vulnerability will be attacked

**Risk Determination:** For the purpose of relative risk assessment, risk *equals* likelihood of vulnerability occurrence *times* value (or impact) *minus* percentage risk already controlled *plus* an element of uncertainty

**Residual risk:** The risk that remains to the information asset even after the existing control has been applied.

**Vocabulary provided by:** Mattord, H. J. & Whitman, M. E., (2012). Principles of Information Security, 4th ed. Boston, MA: Course Technology.

## Seminar

Attending live Seminars is important to your academic success, and attendance is highly recommended. The Seminar allows you to review the important concepts presented in each unit, discuss work issues in your lives that pertain to these concepts, ask your instructor questions, and allow you to come together in real time with your fellow classmates. There will be a graded Seminar in Units 1 through 5 in this course. You must either attend the live Seminar or you must complete the Seminar alternative assignment in order to earn points for this part of the class.

### Option 1: Attend Seminar:

- Discussion on what a business continuity plan is
- Types of alternative processing sites



- Tips for Unit 4 Assignment

### **Option 2: Alternative Assignment:**

You will benefit most from attending the graded Seminar as an active participant. However, if you are unable to attend you have the opportunity to make up the points by completing the alternative assignment.

### **Assignment Instructions:**

Complete the following research assignment. Submit your answers in a single word document to the Dropbox.

Complete research on Alternative Processing Sites. Why are they important? What benefits do they offer a company? How do Alternative Processing Sites relate to Business Continuity Plans?

Your paper should be 3-4 pages of content, in APA format and cite all references used. Submit to the Seminar Dropbox.

#### **Part 1:**

Is a firewall needed? 0–10

How about remote access? 0–10

What is the physical security provided at the hosting company?

0–10

#### **Part 2:**

1. The report is complete and contains all of the 11 sections as indicated in the assignment description. Each section contains substantive material appropriate to the section.

0–15

2. The report correctly identifies mission critical services provided by the alternate site.

0–15

3. The report correctly identifies non-mission critical services that deliberately are not provided by the alternate site. Apps deemed



non-critical are a judgment call on the instructor's part.

0-15

4. The design of the equipment at the alternate site is complete and accurate. It correctly incorporates all data security aspects required to secure the site.

0-15

5. The hand-off process is completely and accurately documented.

0-15

6. The hand-back process is completely and accurately documented.

0-15

Consider the LAN for a small 100-person business, Pixel Inc. The business occupies one floor in an office building. Everybody has a computer on his or her desk, and there are servers for the Web, file & print sharing, email, database, and a small 3D render farm, a rack of 20 dual processor Xeon® servers running Red Hat® Linux that generates the actual high-resolution video animations that Pixel produces for its clients. The desktop systems consist of Apple Mac Pro desktops running Mac® OS X Leopard® for the creative staff, and Windows Vista® PC computers for general use. The servers are Windows Server 2008 running Microsoft Exchange®, Web server, and file and print service.

Consider the LAN for a small 100-person business, Pixel Inc. The business occupies one floor in an office building. Everybody has a computer on his or her desk, and there are servers for the Web, file & print sharing, email, database, and a small 3D render farm, a rack of 20 dual processor Xeon® servers running Red Hat® Linux that generates the actual high-resolution video animations that Pixel produces for its clients. The desktop systems consist of Apple Mac Pro desktops running Mac® OS X Leopard® for the creative staff, and Windows Vista® PC computers for general use. The servers are Windows Server 2008 running Microsoft Exchange®, Web server, and file and print service.

**The network has the following additional specifications:**

- The network is all TCP/IP based.
- The network is based on Cisco routers and switches.
- All desktop computers include email, Web, database access, and office productivity software.
- Creative users also have multimedia authoring software installed.
- All server and critical network equipment is in a secure server room.
- Printers are located around the office area.



- The multimedia department uses high-end workstations for video rendering and animation.
- A load-balancing dual firewall connects the network to the Internet.

**Security Policy:**

- All email must be secure so it cannot be inadvertently sent to the wrong party or intercepted.
- All network resources and equipment must be password protected.
- Company equipment may not be used for personal business.
- All Windows-based PCs must run approved anti-virus and antispyware programs.
- All servers and desktops should run host-based intrusion detection software.
- Clients may use the Secure FTP (SFTP) server to send or receive multimedia files but under no

circumstances should one client be able to view the files of any other client.

- The mail server must be configured not to forward email that originated on the Internet.
- Password aging must be enforced on all servers and desktops.
- All server configurations must be readily available to rebuild a failed system.
- Offsite backup is required, with 24/7 access to that location.
- All employees will demonstrate they understand the security policy.

**There will be a security officer who reports directly to the CEO of Pixel.**

Be sure that you capture the following information in your report:

- List of mission critical applications, list of non-critical applications dropped
- List of equipment needed at alternate site
- A plan to install equipment at the alternate processing site
- A Plan for updating alternate processing site software during normal operation
- Documentation showing a simple rack diagram and a network diagram
- Network configuration info (IP, DNS, MX)
- Power consumption estimates
- Bandwidth estimates
- Information security architecture (firewalls, VPNs)
- Plan for cutting over to the alternate plan
- Plan for cutting back to the main site (a.k.a. hand back)