Disaster Recovery and Business Continuity Plan

Created By:

Noel Richards
Sandy Smietanski
James Tanner
George Wallace

8/20/2008
Executive Summary
The occurrence of man-made and natural disasters has increased in the past few years. The nature of disasters has also changed. The impacts of disasters on companies have greatly increased and intensified thanks to technological advances, progressing globalization and the extension of the supply chain. Companies of all sizes are connected with their suppliers and customers to a much greater degree today than ever before. When a disaster occurs, it can quickly affect all those involved with the company.

As a result, management teams and corporate boards face much more pressure to make their organizations more resilient when disasters strike. This ranges from simple power outages to Category 4 hurricanes to synchronized suicide bombings. The company’s Disaster Recovery/Business Continuity (DR/BC) Management Teams’ capabilities necessary to establish that resiliency generally have ranged from absent to insufficient. This deficiency does have a high cost. A University of Minnesota study finds that 93 percent of companies that lose critical systems for more than 10 days quickly file for bankruptcy. Another study finds that 90 percent of organizations that experience a catastrophic loss of data and equipment without a business continuity plan in place go out of business within 24 months of the loss. The 9/11 Commission’s thorough investigative research concludes that the Sept. 11, 2001, terrorist attacks revealed failures in imagination, policy, capabilities and management.

The purpose of this document is to help organizations address and prevent those failures while providing all managers with a foundation on which to further develop their DR/BC thinking, strategy and processes. The purpose of this DR/BC document is not to fear the management teams, but to help enable the organization to make the most effective and cost-efficient investment in the DR/BC plan capabilities that best meet the needs of the business.

The specific objectives of this document are as follows:

- Plan and organize the Disaster Recovery/Business Continuity Team by establishing roles across departments and organizations.
- Analyze and discuss the risk, importance, and relevance of the Business Continuity process and financial impact of disasters and disaster recovery planning.
- Research, analyze, and create disaster recovery policy and procedures for various types of environments and information systems.
- Develop business continuity plan that includes policy and procedures for various types of environments and information systems through preparation, rehearsal, training, and testing to handle specific incidents to ensure business continuity.

The target audience of the plan is for all senior level executives, functional and operational managers, corporate directors, and the DR/BC Management Teams, who will benefit from its content.
Post Mortem
The Disaster Recovery/Business Continuity Team has spent considerable time and money on the business continuity plan. The plan is now implemented. The DR/BC has performed an initial recovery tests. The business needs and tightening budgets drive down the path of putting off the next DR/BC test until the current critical project is completed. By the time that project is mostly completed, the next critical project is looming overhead. Again, the DR/BC testing is delayed due to focus on meeting the demands of the business. This vicious, endless cycle can continue if the plan is never maintained.

Putting off the DR/BC plan maintenance and testing means that the company spent the initial DR/BC investment in vain. The company has wasted all that money: thousands to millions of dollars. Without ongoing testing and maintenance, history has proven time and time again that recovery is bound to fail, or at least take longer than expected as the staff wades through hundreds of small issues that would have been resolved through regular plan testing and maintenance. The bottom line is that maintaining and testing the DR/BC plan is a critical project. Without maintenance, any money spent on DR previously is mostly wasted.

Corporate executives need to be on-board with the continuous maintenance as well. All of the companies that have experienced a disaster where the DR/BC plan was driven by the CIO have had complications. The IT department is up and running, but the rest of the business is broken and in a disaster state. DR and BC are the safety nets for the health of the whole company, not just the IT department. DR/BC planning, testing, and maintenance should be driven by the CEO and board of directors as a top priority. It represents protecting all corporate assets. When DR/BC is not being driven by the CEO, all the money and time spent on DR/BC by the CIO is in vain. It is wasted as the overall corporation remains in a non-functional state in the event of a disaster.

A prime example is this:

A CEO drove DR/BC plan across their company (a large distributor with five warehouses and a central data center). This CIO didn’t have much interest in the plan, but kept the plan going as a result of the CEO’s continued vigilance. When Internet communications were cut to the central data center by an impatient back-hoe operator, the plan operated within parameters so that orders did get out by their deadlines. Some minor issues with the plan were discovered and repaired, and in the post mortem, it was determined that the plan worked. It had included the whole company, and it was the business units and employees that kept the business running while the data center was off-line. The bottom line here is that the DR and BC are only effective if driven by the CEO and board of directors across the whole company. Any money spent on DR/BC for IT alone without DR/BC for the rest of the company is wasted.
# Table of Contents

Executive Summary.................................................................................................................. 2  
Post Mortem............................................................................................................................... 3  
Table of Contents...................................................................................................................... 4  
Introduction............................................................................................................................... 11  
Backup & Restore Plan.............................................................................................................. 12  
  Good Backup Plan .................................................................................................................. 12  
  Better Backup Plan ................................................................................................................. 12  
  Best Backup Plan .................................................................................................................. 12  
  Business Impact Analysis ...................................................................................................... 13  
  Media Costs .......................................................................................................................... 13  
Data Backup Vault.................................................................................................................... 13  
Backup Types............................................................................................................................ 14  
Normal Backup........................................................................................................................ 14  
Incremental Backup................................................................................................................... 14  
Differential Backup.................................................................................................................... 15  
Daily Backup.............................................................................................................................. 15  
Copy Backup............................................................................................................................. 15  
Recommended Backup............................................................................................................. 15  
Backup and Restoring Tactics................................................................................................. 15  
Backing Up and Restoring the Registry.................................................................................... 16  
Disks vs. Tapes.......................................................................................................................... 16  
  Company Data List (E-Records)............................................................................................. 17  
  IT........................................................................................................................................... 17  
  Contacts................................................................................................................................. 17  
Backing up Files and Folders with the Backup Utility ............................................................... 17  
Backing up the Registry ............................................................................................................ 18  
Backing up System State Data .................................................................................................... 18  
Restoring Files and Folders Using the Backup Utility............................................................... 19
<table>
<thead>
<tr>
<th>Natural Threats</th>
<th>Impact Attributes/Ratings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Earthquake</td>
<td>Data</td>
</tr>
<tr>
<td>Fire</td>
<td>Wireless Security</td>
</tr>
<tr>
<td>Flood</td>
<td>Equipment Reconfiguration</td>
</tr>
<tr>
<td>Landslides/Sinkholes</td>
<td>Infrastructure Hardware Failure</td>
</tr>
<tr>
<td>Hurricane/Tsunami</td>
<td>Cable Failure</td>
</tr>
<tr>
<td>Severe Rain/Wind Storm and Electrical Storms</td>
<td>Workstation Failure</td>
</tr>
<tr>
<td>Epidemic/Pandemic</td>
<td>Printer Failure</td>
</tr>
<tr>
<td>Drought/Freezing</td>
<td>Equipment Reconfiguration</td>
</tr>
<tr>
<td>Tornado</td>
<td>Wireless Security</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IT and Technology-Based Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISP Maintenance</td>
</tr>
<tr>
<td>Server Failure</td>
</tr>
<tr>
<td>Production Equipment Malfunction</td>
</tr>
<tr>
<td>Bugs and Glitches</td>
</tr>
<tr>
<td>Workstation Failure</td>
</tr>
<tr>
<td>Cable Failure</td>
</tr>
<tr>
<td>Infrastructure Hardware Failure</td>
</tr>
<tr>
<td>Printer Failure</td>
</tr>
<tr>
<td>Equipment Reconfiguration</td>
</tr>
<tr>
<td>Wireless Security</td>
</tr>
<tr>
<td>Hand-Held Devices</td>
</tr>
<tr>
<td>Data</td>
</tr>
<tr>
<td>Data Loss</td>
</tr>
<tr>
<td>Data Corruption</td>
</tr>
<tr>
<td>Data Security</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IT Risk Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact Attributes/Ratings</td>
</tr>
<tr>
<td>Organizational Information Criticality</td>
</tr>
</tbody>
</table>
Fire .................................................................................................................. 58
Flood .................................................................................................................. 58
Landslides ......................................................................................................... 58
Hurricane/Tsunami ............................................................................................ 58
Thunderstorm ..................................................................................................... 59
Others ................................................................................................................ 59
Memo .................................................................................................................. 59
Disaster Declaration Statement ......................................................................... 60
Employees ......................................................................................................... 61
Customers ......................................................................................................... 62
Community and Media ...................................................................................... 63
Vendors and Service Contracts ......................................................................... 65
Quick Contact Information ............................................................................... 65
Computers and Servers ..................................................................................... 65
Workstations and Servers ................................................................................ 65
Shipping Computers .......................................................................................... 65
Administrative Computers ................................................................................. 65
Sales Computers ................................................................................................ 66
Research and Development Computers ............................................................. 66
Purchasing computers ....................................................................................... 66
Advertising Computers ....................................................................................... 66
Other Services and Supplies ............................................................................. 67
Production Machines ......................................................................................... 67
Blank DVD/ CD/ Cases Suppliers ...................................................................... 67
Copy and Fax Machines ..................................................................................... 67
Box Suppliers ..................................................................................................... 68
Paper Supplier ................................................................................................... 68
DigiKnight Service and Other Related Contracts Locations ......................... 68
Emergency Situations ....................................................................................... 69
Summary of Revisions: ........................................................................................................ 103
Conclusion .......................................................................................................................... 104
References .......................................................................................................................... 105
Introduction
DigiKnight Technologies is a new company in the Silicon Valley region of California (indeed it is located within miles of Electronic Arts, Lucas Arts, and Cryptic Studios.) It was founded in 2000 by its current CEO, Carlton Smith, who realized the rapidly growing potential of game distribution. DigiKnight is not a publisher, nor does it create video games, rather it contracts with major publishers to rapidly produce the physical product (games) and coordinate their shipping to stores around the world. Though a new company, it has seen its sales grow extremely quickly over the last few years.
Backup & Restore Plan

Good Backup Plan
Data protection is crucial for protecting your business's continuity. If your only data backup is on a computer and the hard disk fails or is damaged by a power surge, your business data is gone. Not to mention having paper copies of business data isn't adequate data protection. The data that is needed to carry on the business could be irretrievably lost.

Archiving business data could be a matter of the business's survival. There are two steps to archiving business data for successful data backup:

- Identifying the critical data that needs to be archived
- Using a data archiving method on a regular schedule

One can simplify the backup archiving by keeping all the files that will need to be archived on a single drive on company’s IT computer. Do a backup over the computer network, keeping the data backup files on a separate hard drive from the original files. If this isn't possible because there is a stand-alone computer, put the data backup files in a separate directory, and increase the schedule for creating physical backups.

Better Backup Plan
Storing backup tapes/disks off-site is an important step in a disaster recovery plan. One company, IT Global Inc., uses Windows 2003 Small Business Server and a DAT drive for backups. They use simple scripts with Scheduler to run an automatic backup at midnight. Even though the 20-person company has an on-site, fireproof safe rated for storing computer media, they rotate three backup tapes. The most recent full backup goes into the media safe for ready access to restore corrupt or missing files. The next most recent backup gets stored at the IT manager’s home. The third and oldest tape/disk gets stored at the off-site facility. This is one way to store backup tapes, but it is not exactly the best and safest way. Another option is to have a safe deposit box (lockbox) at the bank that the backup tapes/disks can be stored. It would require an IT staff member to drive the backup tape to the bank. The only downside to this option is that the bank is not available 24/7.

Best Backup Plan
The best backup practice should be vaulting the data. Low-budget approaches to off-site backup storage are inadequate for even small organizations. Instead, contract with a company that specializes in tape/disk storage. When shopping for an off-site vaulter, consider these options:

- Theft deterrence
- Fire protection
- Flood protection
- Environmental control
- 24-hour access

The company can dictate the contract that fits the need. The company can specify the SLA response time for the service to deliver a tape/disk from the vault to the IT department. Vaulting can also help avoid liability issues. IT managers do not have worry about tapes or disks being
stolen or lost. Even insurance companies may offer lower business insurance rates if the tapes/disks were stored in an off-site vault.

Rates for an off-site vaulting company are reasonable. A vault service can charge roughly about $5 per tape per month for storage. This is potential cheap insurance to keep the business up and running. Data is the lifeblood of any organization, and any loss of data at any level is really unacceptable. Here is why vaulting is a cost-effective precaution for the company’s data:

**Business Impact Analysis**

Take the company’s total sales and divide that number by the number of days in the year to give you the value of the day’s worth of data.

**Media Costs**

Media costs may be lower because vaults will provide the proper temperature, humidity, and handling to achieve the optimal lifetime from tapes. Analyzing the tapes to see if they produce errors is a good idea as well. Citing statistics from the Enterprise Storage Group state that up to 60 percent of backups don’t execute properly in network environments. Vaults can offer products to analyze backups across a variety of platforms and pinpoint any failures.

**Data Backup Vault**

DataVault Inc. offers BackupVault, which is a service that has many features that securely backs up the company’s systems in the event of disaster at your location. All of the data that has been backed up can be easily restored, keeping the company in business.

Their key features are:

- Choose from full-system or data-only backups. Full-system backups ensure that all system and data files are backed up on a routine schedule and provide capabilities for a full system recovery in the event of computer failure, theft, or disaster recovery. The data-only service will automatically select all of your important data files for you, but does not back up your program files. The data-only service can be easily customized by the user to include additional files, file types or directories.
- To ensure security of your data, all files are encrypted by your computer before sent and stored at DataVault’s data center using 112 bit triple DES technology.
- File versions - up to ten versions of all files are stored for easy retrieval.
- Backups can happen automatically on a schedule, can be initiated by users, or can be configured to occur in the background whenever a computer is connected to the Internet when traveling (Hands-Free-Backup TM).
- Backups are quick and efficient, even via dial-up connections.
- A ‘Heal’ feature can ‘roll back’ an entire PC configuration to a selected date in the past, to restore operation, in case of software configuration errors, some types of viruses, or other problems that can’t be easily repaired (available with full-system backup service only).
- The ability to recover lost data anywhere, at any time.

Depending on the amount of data needing to be backed up is how much the company pays:
<table>
<thead>
<tr>
<th>Account Type</th>
<th>Description</th>
<th>Backup Limit</th>
<th>Monthly Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full System Backup</td>
<td>Full backup of all your computers files, applications and system setting. Includes iHeal to restore your system and iRoam to retrieve files from any web browser.</td>
<td>10 GB</td>
<td>$39.95</td>
</tr>
<tr>
<td>Data Backup</td>
<td>Data only backup allows either automatic or manual file selection and in addition you can modify the backup set to your particular needs as required. Mapped network drives may also be included in the backup for all plans except the 4 GB level.</td>
<td>4 GB</td>
<td>$27.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10 GB</td>
<td>$39.95</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15 GB</td>
<td>$64.95</td>
</tr>
<tr>
<td></td>
<td></td>
<td>30 GB</td>
<td>$109.95</td>
</tr>
<tr>
<td></td>
<td></td>
<td>50 GB</td>
<td>$184.95</td>
</tr>
</tbody>
</table>

**Backup Types**

Like most major backup programs, the Windows Backup utility supports a variety of backup types, including:

- Normal backup
- Incremental backup
- Differential backup
- Daily backup
- Copy backup

**Normal Backup**

The most common (and default) type of backup is the normal backup. This backup type backs up all selected files and folders and clears the archive attribute on these files and folders. The purpose of clearing the archive attribute is to mark files as having been backed up, an important distinction when a normal backup is used with some of the other backup methods. Normal backups are not always the best choice for backup jobs. All files are backed up, regardless of whether any changes have occurred. This results in larger-than-necessary backups and backups and duplicate copies of identical files being stored. There is nothing wrong with this method, but it can be inefficient.

**Incremental Backup**

The incremental backup type backs up only those files that have changed since the last normal or incremental backup. An incremental backup clears the archive attribute for any files and folder it backs up. The main purpose of an incremental backup is to reduce the overall size of backup jobs. Although an incremental backup strategy ensures that backups take the least time possible, it does result in a more involved restore process. To restore the data completely, an administrator needs to restore the normal backup and then the incremental backups. This ensures that all files backed up are available again.
Differential Backup
Instead of backing up all selected files and folders, differential backs up only those files that have changed since the last normal or incremental backup took place. A differential backup does not clear the archive attribute for any files and folders it backs up. The main purpose of a differential backup is to reduce the overall size of backup jobs, although not to the same degree as an incremental backup. Although a differential backup strategy ensures that the restore process is less involved, it does result in a more involved backup process.

Daily Backup
The daily backup backs up selected files or folders that have been created or changed on the day the backup takes place. A daily backup is often used between full backups to save backup time and storage space. When this method is used, the archive attribute is not changed, so it doesn’t interfere with any existing backup procedures.

Copy Backup
A copy backup backs up all selected files and folders. A copy backup doesn’t change the archive attribute for a backed up file or folder to mark it as having been backed up. The main purpose of a copy backup is to create the equivalent of a normal backup (perhaps of a backup tape to be stored offsite) without interrupting other existing backup procedures.

Recommended Backup
Complete Normal backup at least once a week (Mondays or Fridays). The reason is that this is the only method that backs up all the files. When restoring, you only need the last tape. Differential and/or Incremental backups at least three times a week. Daily and Copy backups will be ran daily. (Any combination of backup policies can be implemented. It has been chosen that the Recommended Backup be used due to efficiency and time factors stated in the above explanations.)

Performing a restore requires the last full backup and either the last differential backup or all incremental backups between the last full backup and the current day. This allows you to completely restore all data up to the last completed backup.

It's typical to store the weekly full backup off-site each time you make a new one and to recycle them once per year. So each week, create a new full backup, and send the one from the previous week off-site for storage. This practice lets you restore immediately in minor emergencies, but you risk losing only one week of data if you suffer a major incident.

Backup and Restoring Tactics
These tactics are used for day-to-day retrieval of lost files or deleted mailboxes, disaster recovery, and/or archiving.

- Backup to a second hard disk and backup to tape.
- Keep father and grandfather copies of backup disks.
- Keep at least some of the disks offsite (possibly Intranet).
Using Backup Utility – backs up and restores operating system, application, and user data files. It can be used to schedule backup jobs, back up and restore critical System State information, and provide access to the Automated System Recovery feature.

Document backups – update records, make a calendar, or utilize the built in scheduler.

Create backup baseline – create a reference point where you know everything is working properly. It will be quicker to restore the changes from the tape. Make a written plan of who will do what in the case of an emergency incident. Create a flow chart of the sequence to retrieve data.

Use Volume Shadow Copy – allows users to access previous versions of files in shared folders when older versions need to be restored or when they simply want to compare the current an older version. It provides point-in-time copies of files on network shares, and enables you to backup open files. This should not be a substitute for a proper Normal backup.

Utilize Automated System Recovery (ASR) – this feature restores the operating system and configuration settings quickly. Applications need to be reinstalled and data needs to be restored from backup.

Backing Up and Restoring the Registry

- Back up the Registry as part of the daily automated backup or as a distinct Registry-only procedure.
- Regedit can be used to save all or part of the Registry to distinct files. It offers an Export command, which can be used to save the entire Registry, a single key, or any portion of a key to a file.
- Make a copy of the %systemroot%\System32\Config and %systemroot%\repair directories manually.
- Use Windows Server 2003 Resource Kit tools which offer command-line scripting capabilities.

Disks vs. Tapes

While tape has been the backup medium of choice for large organizations for years, a recent trend as the organization grows bigger still is to return to disk-based backup, but with a difference. Disk-based backup solutions for the enterprise are far more sophisticated than the simple scheduled copying programs used by smaller businesses, but they can also be costly.

One advantage of disk over tape is speed of access. One would have to search through a tape from the beginning to find a particular block of data, while the heads on a disk drive can go directly to a particular place on the disk.

Disks also tend to be more reliable than tape. Most users of tape backups have had the experience of a backup or recovery failure; some estimates put the failure rate at 20 percent or more. Even worse, you often don't know that a backup has failed, or partially failed, until you need it.
The move from tape back to disk is based in part on the falling prices for high capacity hard disks, and in part on the difficulty of managing and rotating the large number of tapes required in the enterprise environment.

Since recovery from disk is almost always faster, it makes sense to have yesterday's or last week's backups on disk to be easily restored across the network. It is most recommended to have disks as the backup medium.

**Company Data List (E-Records)**
- Computer Backups
- Employee Personal E-mail Accounts
- Employee Business E-mail Accounts
- E-mail Correspondence with Customers
- E-mail Correspondence with Suppliers
- Company Website Design
- QuickBooks Computer Records
- Customer Database
- Supplier Database
- Corporate Database

Contact IT during any event that affects any hardware or software.

**IT**
415-555-8352

**Contacts**
**Manager:** Alicia McKellips

<table>
<thead>
<tr>
<th>Employees</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alicia McKellips</td>
<td>415-555-0190</td>
</tr>
<tr>
<td>Luke McDowel</td>
<td>415-555-0191</td>
</tr>
<tr>
<td>Allan Smith</td>
<td>415-555-0192</td>
</tr>
<tr>
<td>Joseph Webber</td>
<td>415-555-0193</td>
</tr>
<tr>
<td>Robert Wildhorn</td>
<td>415-555-0194</td>
</tr>
</tbody>
</table>

**Backing up Files and Folders with the Backup Utility**

1. Start your Windows Server 2003 computer and log on with your Administrator user name and password.
2. Click **Start**, point to **All Programs**, point to **Accessories**, point to **System Tools**, and then click **Backup**.
3. In the Backup or Restore Wizard, click the **Advanced Mode** link to access all the Backup utility’s features. The Backup Utility window opens.
4. Click the **Backup** tab.
5. Click to expand **Local Disk (C:)**, **WINDOWS**, and **system32**.
6. Click the **Config** folder to view its contents. Click the check box next to **Config** to select the entire folder for backup.
7. In the Backup media or file name text box, type `c:\backup-config-(backup date).bkf`, and then click the **Start Backup** button. The backup date is the date that the backup was performed.
8. In the Backup Job Information dialog box, review the settings, and then click the **Advanced** button.
9. In the Advanced Backup Options dialog box, click to select the **Verify data after backup** check box. Click the **Backup Type** list arrow to view available backup options. The available backup options are Normal, Incremental, Differential, Daily, and Copy. By default, Normal is selected. Click **OK** once you have chosen the backup type.
10. Click the **Start Backup** button.
11. When the backup begins, the Backup Progress dialog box opens. After the backup is finished, click the **Report** button.
12. Close the backup *(backup number)*.log window. (The number following the name of your log file will be different every time you run a backup.)

**Backing up the Registry**

1. Click **Start, Run**. Type `regedit` and then click **OK** to open the Registry Editor.
2. Click to expand the **HKEY_LOCAL_MACHINE** key, and click the **SOFTWARE** subkey.
3. Enter a file name.
4. Verify that the Selected branch option button at the bottom of the Export Registry File dialog box is selected and that HKEY_LOCAL_MACHINE\SOFTWARE is listed in the text box. Click **Save**.
5. Regedit creates a backup file of the selected key. The procedure can be used to back up the entire Registry or just a small subset of subkeys, simply by selecting different keys or subkeys.

**Backing up System State Data**

1. Click **Start, Run**. In the Open text box, type `ntbackup`, and then press Enter. Click the **Advanced Mode** link in the Backup or Restore Wizard window.
2. In the Backup Utility window, click the **Backup** tab.
3. Click the **System State** icon to view its contents. Notice that the individual check boxes are grayed out because this utility can’t back up individual System State components. Click the check box next to **System State**.
4. In the Backup media or file name text box, type `C:\Systemstate(backup date).bkf` and click the Start Backup button. The backup date is the date the backup was performed.
5. In the Backup Job Information dialog box, click the Start Backup button. After the backup is finished, click the Close button in the Backup Progress dialog box.
6. Click **Start, My Computer**. Double-click the C: drive to view its contents.
7. Right-click the **Systemstate(backup date).bkf** file and click **Properties**. The General tab will show how large the System State backup of the system is.
8. Close all open windows.
Restoring Files and Folders Using the Backup Utility

1. Click **Start, Run**. In the Open text box, type `ntbackup.exe`, and then click **OK**.
2. In the Backup or Restore Wizard that opens, click the **Advanced Mode** link, if necessary.
3. Click the **Restore and Manage Media** tab.
4. Click to expand **File**, backup-config-(backup date).bkf, C:, Windows, and System32. The backup date is the date the backup was performed.
5. Click the **Config** folder to view the contents of the backup file. Click to select the check box next to the **Config** folder.
6. In the Restore files to drop-down list, click **Alternate location**.
7. In the Alternate location text box, type `C:\Configbackup` and click the **Start Restore** button to restore the contents of the Backup-config.bkf file to the Configbackup folder.
8. In the Confirm Restore dialog box, click **OK**.
9. After the restore process is finished, click the **Close** button in the Restore Progress dialog box. Close the Backup Utility window.
10. Click **Start, My Computer**. Double-click the C: drive, and then double-click the **Configbackup** folder.
11. Double-click **Windows, System32, and Config** to view their contents, confirming that the contents of the backup file were restored to an alternate location.
12. Close all windows.

Restoring the Registry

1. Click **File, Import** from the Registry Editor menu.
2. Locate and click your HKLMsave.reg file.
3. Click **Open**.
4. After a few moments of importing, a message stating whether the import succeeded is displayed. Click **OK**.
5. Click **File, Exit** from the Registry Editor menu.

Restore the System State Data

- **Corrupt Active Directory** – Restart the computer and choose the Directory Services Restore Mode advanced startup option. Then use the Backup utility to restore the latest System State data from backup. Restart the computer and Windows starts normally, Active Directory is automatically reindexed and updates Active Directory and the File Replication Service.
- **Restoring portions of Active Directory tree** – Use and authoritative restore. This marks specific objects in the Active Directory as the master copy and forces the other domain controllers to receive the change. To perform an authoritative restore, restart the computer in Directory Services Restore Mode, restore the most recent System State from backup, and then run the Ntdsutil utility at a command prompt in authoritative restore mode.
Natural Threats

All natural disasters can threaten the entire company. The impact from any moderate to large-scale disaster event could produce an assortment of conditions that would adversely affect health and safety of the employees, critical infrastructure expense, and the well-being of the company. These threats and threat sources impact the people, processes, infrastructure, and technologies the company needs to operate. People may be hurt or even killed; their safety is heavily at risk. The loss or damage of data, equipment, and machinery can cause the company to be inoperable. There could be potential power outages and transportation disruption. The building may become uninhabitable, and the infrastructure may be severely damaged. With these threats, customers and vendors will be greatly affected by not receiving the goods that they’ve purchased. Some recovery expectations that should be accepted is the lack of communication, limited resources (both internal and external), and displaced personnel.

Listed are the natural disasters that the company faces in the likelihood of occurrence:

<table>
<thead>
<tr>
<th>#</th>
<th>Natural Disaster</th>
<th>Occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Earthquake</td>
<td>Very Likely</td>
</tr>
<tr>
<td>2</td>
<td>Fire</td>
<td>Very Likely</td>
</tr>
<tr>
<td>3</td>
<td>Severe Rain/Wind Storm</td>
<td>Very Likely</td>
</tr>
<tr>
<td>4</td>
<td>Electrical Storm</td>
<td>Very Likely</td>
</tr>
<tr>
<td>5</td>
<td>Flood</td>
<td>Very Likely</td>
</tr>
<tr>
<td>6</td>
<td>Sink Hole</td>
<td>Likely</td>
</tr>
<tr>
<td>7</td>
<td>Landslide</td>
<td>Likely</td>
</tr>
<tr>
<td>8</td>
<td>Tsunamis</td>
<td>Not Likely</td>
</tr>
<tr>
<td>9</td>
<td>Hurricane</td>
<td>Not Likely</td>
</tr>
<tr>
<td>10</td>
<td>Epidemic/Pandemic</td>
<td>Not Likely</td>
</tr>
<tr>
<td>11</td>
<td>Wind Chill/Freezing</td>
<td>Not Likely</td>
</tr>
<tr>
<td>12</td>
<td>Heat Index/Drought</td>
<td>Not Likely</td>
</tr>
<tr>
<td>13</td>
<td>Tornado</td>
<td>Not Likely</td>
</tr>
</tbody>
</table>

*Natural Disaster Table*
Earthquake

The likelihood of an earthquake affecting the company is very likely. Earthquake activity is characterized by a sudden, unpredictable movement in the earth’s subsurface structure, usually associated with the shifting of tectonic plates that result in severe ground motion and surface deformation. A large portion of the Bay Area lies along the San Andreas Fault, which runs 800 miles up the California coast from Riverside County in the south to Mendocino County in the north. The San Andreas also has three sister faults that run through the Bay Area. Moving west to east these include the Hayward Fault, the Calaveras Fault and the Clayton-March Creek-Greenville Fault. The prevalence of these fault zones results in the frequent occurrence of earthquakes throughout the Bay area.

The number of casualties will vary with the time of day. An 8.3 magnitude quake affecting a populated area would produce many deaths and more than enough causalities. Many of the employees could become homeless, distraught, and hurt.

Serious hazardous materials incidents may occur in the city with their major rail and highway transport routes, due to natural disasters. They are present in permanent storage locations,
roadway and railway transport mediums, and long-distance pipelines. This can affect the company if employees are unable to get to work, or if they are not allowed on the roadways.

Structural collapse is a possibility depending on the size of the earthquake. Even though the building is seismically stable, other older buildings within the vicinity may have not been retrofitted. If the building or any other building were to collapse, the people, machinery, equipment, and products within the building could be potentially destroyed.

Transportation infrastructures could be damaged or completely out of service. Roadways will be temporarily closed due to ground and structural failures. Roadway clearance, emergency repairs, detours, and inspections will restrict usage during the initial post-earthquake hours. State Route 84, 92 & 238, and Interstates 680 and 880 could be damaged by strong shaking or ground failure. Rail transport and BART can become non-operational. This interruption in service will impact both freight and passengers. Necessary alternatives will have to be made in order to reroute employees and products for shipping.

Telephones likely will be overloaded by post-earthquake calls within the area and from the outside. Damage to equipment due to ground shaking and loss of electrical power will further complicate this situation. Because of shaking patterns corresponding with key facility locations, the Bay Area is likely to experience complete telephone failures. Access for repairs will be a major problem. Most cellular telephones are expected to be out of service. Cell systems rely on the landlines telephone network or microwave links to interconnect cell sites. Landlines will be disrupted, and microwave links will be subject to misalignment and antenna loss. Most two-way radios will work, but there likely will be problems caused by overloading, loss of antennae, and misalignment of microwave dishes.

With all earthquakes, utility infrastructures could become impaired. Electrical power outages are expected to be widespread. Backup generators will be running in the case of power outage. Power outages will cause problems for water systems that depend on pumps. Drinking water may have to be trucked to affected businesses. In some areas, a lack of water will hamper firefighting efforts. If water lines are broken, the building could become uninhabitable. Sewer mains may break. The main sewage treatment plant may be damaged, lose electrical power, and discharge raw sewage. With a loss of commercial power, some treatment facilities may be rendered in-operative, and pumping stations shut down. This could cause a back-up in the sewers that can affect the company’s sewer system, and be a health hazard to the employees.
Fire

Fire is the most common threat source businesses face. The company faces California wildfires that effect majority of the state every year. The likelihood of a fire is very high. A fire can threaten all aspects of the company. Fires can happen internally (electrical failure) or externally (wildfires). Either way, fire is a huge concern not only for its destructive tendencies, but also because of the potentially dangerous smoke produced.

Major fires, whether involving structures or wild land areas, may result in significant risk to life and property. Rapid moving fires in older structures, in grasslands or dense brush can quickly overwhelm firefighting efforts, resulting in possible danger to life safety. Power lines and other infrastructure may also be at risk and can be heavily damaged when exposed to major fire activity.

The most effective means of mitigating the risk from fire is effective code enforcement, fire safety inspections, and people being careful with fire. Removal of flammable vegetation in business areas can help to protect structures and provide an area of safety. The installation of fixed fire protection systems throughout the building helps to provide a suppression mechanism
for rapid intervention. Response to major fires will require mutual aid assistance from local and regional fire suppression assets and resources.

Flood

Flood Hazard Areas

Flooding is likely to occur when the water flow increases at a rate that exceeds the soil’s ability to absorb it over a short period of time. Flooding may occur from locally heavy rainfall or as a result of heavy runoff being channeled into the area from distant sources along established canals and roadways.

The impact from any flooding event will vary. Injury and death associated with people being trapped in rapidly moving waterways or caught unaware during slow rate of rise conditions. This will affect all employees and truck routes going in and out of the area. If individuals attempt to forge through the submerged roadways, possible injury and death may occur. There can be damage to the critical infrastructure of the building, as well as to the roadways, bridges, and other transportation structures affecting mobility and the ability for people to evacuate flooded areas. There will be health hazards from contamination of water sources, damage to sanitation systems, and a long term presence of standing water. Although flooding incidents are generally of short duration, the need for ongoing response and long-term recovery operations cannot be
underestimated. Loss of essential flood control structures, including levees and control devices may hinder recovery efforts and pose significant problems should additional flooding occur. The city of Fremont will deploy an emergency response team with safety resources through impacted areas only. They will initiate the rescue of person imperiled or trapped by flood conditions, and initiate emergency evacuation of affected businesses.
No area is entirely free of the threat of landslides and sinkholes. Landslides can occur wherever a slope of land has become too steep. While gravity plays a part in their occurrence, earthquakes, heavy rains, water erosion, and excess weight from manmade structures, an accumulation of loose rock and mining are often the triggers behind a landslide. Landslides and Sinkholes cause an estimated one to two billion dollars in damages and kill between 25 and 50 people a year in the United States alone. They can cause extensive damage to highways and have been known to wreak havoc on structures. More and more businesses in the Bay Area are threatened by the possibility of a landslide and a sinkhole. The combination of steep slopes, weak rock material and winter rainstorms create an ideal setting for landslides.
Hurricane/Tsunami

Hurricanes are really not a potential threat to the city of Fremont. Within the last 18 years, there have only been 10 hurricanes that have pounded the California coastline. Majority of the hurricanes have turned into tropical storms by the time the hurricane moves up from the southern coastline to the city of Fremont. These tropical storms could cause severe damage to the building with high winds and heavy rain.

More than likely, the building will not be affected by a tsunami. A tsunami is possible though, and should not be disregarded. The building and employees lives could be at stake. Evacuation procedures should be followed.

Severe Rain/Wind Storm and Electrical Storms
Severe storm activity is usually seasonal and occurs with relatively predictable frequency. This can include the aftermath of a hurricane. Storm activity may include severe high winds, heavy rainfall, and massive lightning. The Bay Area is occasionally visited by severe summer and winter storms that can produce heavy rains and cyclonic winds. Although usually of short
duration, the intensity of these events can severely impact people and critical infrastructure, threatening safety of the employees and interrupting the normal flow of daily life. Strong or long-duration storms may result in various disruptions. Widespread or long-term utility outages may occur. Backup generators and UPS systems will need to be implemented if power spikes, surges, and dips occur. The company’s buildings may be damaged or destroyed due to storm impact, especially involving conditions of high wind or severe hail. Major areas of impact may include injury of employees caught in severe storm conditions and lacking adequate shelter. This would also include interruption of critical infrastructure systems due to damage and impact, and disruption of traffic flows due to reduced visibility or roadway debris. Economic losses can occur due to closed business, delay of arrival or shipment of products, and power outages. The most effective mitigation effort involves the use of effective forecasting methods, the dissemination of timely warning information to employees, and robust emergency response operations.

**Epidemic/Pandemic**
Epidemics have occurred throughout the United States in the past, and although significant advancements have taken place in medical science, there is nothing to preclude another widespread outbreak in the future. In consideration of the close proximity to the San Francisco Bay Area, the company remains at risk from epidemics. Because of increased international travel, overwhelmed sanitary systems, exposure to large concentrations of people, and emerging pathogens the threat from a major public health event is a reality.

Pandemics, which are rare in the U.S., can be expected to last anywhere from 12 – 18 months. Multiple waves (periods during which community outbreaks occur) of illness could occur with each wave lasting 2 – 3 months. Many businesses within or across regions may be affected at the same time. Customers and service providers, or vendors, will also be impacted proportionately. Rates of absenteeism will depend of the severity of the pandemic. The business may see absentee rates in the 25 – 50% range. Illness, public health measures, and self-selection issues can influence absenteeism rates.

**Drought/Freezing**
Periods of drought have followed years in which both the prevailing weather phenomena were El Nino and La Nina. Drought cycles appear to be every 7 – 11 years. During periods of drought, measures will consist of planning practices consistent with water conservation goals and various water conservation measures. There will also be increased risk of wild land fires. Static electricity may occur with buildings causing power shortages and outages.

Extended drought events present a major economic impact. It is estimated that it costs the United States between $6 billion - $8 billion annually. If the drought is long-term, potable water supplies may dwindle, resulting in the need for rationing. Long-term impacts may also include the destruction of essential ground cover, economic losses from reduced retail sales and even depopulation as residents move to areas with a more reliable water supply.

Temperatures can reach to freezing points in the Bay Area. Cold temperatures can cause pipes to burst, which can lead to a variety of problems. This could cause potential flooding in and around the building.
Tornado
No known tornado has been cited in the area within the past 10 years. Tornadoes can be prevalent from the strong winds that hurricanes can produce. There will be severe damage and destruction if a tornado would hit the building. Employees will need to follow precautionary procedures to maintain their safety. Potential casualties may occur.
IT and Technology-Based Threats
DigiKnights IT team has the goal to keep the system uptime close to 98%. This high expectation creates the need to do an analysis on the following IT and technology based threats on its hardware, software, and infrastructure: T1 line failure, server failure or damage, production line equipment malfunction, workstation failure, hard drive failure, printer problems, equipment reconfiguration, sabotage, and theft. Also data loss, bugs and glitches in software, data corruption, data security breach including internal attacks, system configuration changes, cabling issues, switches or infrastructure hardware failure, tampering or destruction, Denial of Service (DoS) to servers and phones. Wireless vulnerabilities and hand held device connectivity issues. This list may be expanded as needed but consists of the majority of issues that DigiKnights may come across.

ISP Maintenance
The threat sources for the T1 line going down include ISP maintenance, local business T1 installation, and human error. The likelihood that the ISP is going to be doing maintenance is low especially during normal business hours. Local businesses having T1 installation or maintenance is medium but the fact that their installation will affect our T1 line is low. Human error also could play a part a mistake that could easily be made to suspend service to the wrong account. If the T1 line were to go down it would affect both the employees and the customers greatly. The results of the T1 going down includes no Internet, and no telephones, however the company could still operate if a plan could be devised that would allow the company to continue business as usual with the limited internal network access. Internal email would still work as well as access to customer information. Cell phones could be used in place of the desk phones. Even though the threat level on this issue is low it will be addressed in the disaster recovery plan because T1/Internet access can and does go down and is a mission critical component. Please refer to wireless vulnerabilities for more information on how to get Internet access in times of disaster.

Server Failure
Servers can and do fail, the threats to servers come from both internal and external sources. Typically they simply need to reboot especially after updates if the problem is bigger than a reboot then it could be due to hardware but the threat to hardware is medium. The servers could be damaged if they are subject to water damage from a fire system that has been installed incorrectly. Replacing a server due to water damage would be costly and affect the company as a whole. Lost profits would result because of a loss of data, customers, and shipments. Protection from outside sources also needs to be addressed as this threat is high. This issue will definitely be addressed in the disaster recovery plan as well as the business continuity plan.
Production Equipment Malfunction
Production line equipment malfunction could be from bugs or glitches in the system, malicious workers or power failure that abruptly powers off the equipment. The likelihood that there will be a problem is pretty low even though bugs and glitches do occur with burning Cd's and DVDs. The loss for the system going down is two days. This will affect production greatly, marketing and sales tremendously, IT will be focusing on the problem for at least two days, as will the maintenance department. If the problem is serious then “We Fix’Em Inc.” will service them. On the flip side customers who purchase the games will be upset especially if they had a new game release that they are waiting to receive.

Bugs and Glitches
Bugs and Glitches in the computer systems can and do occur. Bugs and glitches are very random and minimal at best so this area won't be looked into further since the occurrences are random and few and far between. The system estimated up time is 99.8%, in addition there are well trained IT staff that are available 24x7. Planning for these occurrences is extremely difficult since software has its glitches and will be worked out as needed. The effect of bugs and glitches in the system depend upon many variables but if the system is down for two days then there will be lost productivity, lost sales, unhappy customers, and very unhappy staff.

Workstation Failure
Workstation failure could be moderate to high for a variety of reasons including but not limited to hardware or software. These threats could be internal or external. Consumers rated computer manufacturers according to their preferences which will include customer support and PC reliability, "PC World readers gave their highest praise to Apple, Canon, and Lenovo. The worst performers overall were Hewlett-Packard and Lexmark" (Bertolucci, 2007, p. 1). Digiknights owns HP's, Dell's and custom computers from Boldata. HP's are rated as worst performers, Dell's were in the middle so they are reliable but have bad customer service. Hard disk failures are one of the pieces of hardware that tend to go out on workstations. Hard disk failures have "an average of 3% vs. the estimated 0.5% to 0.9%. Disk manufacturers obviously can't test disks for a year before shipping them, so they stress test disks in high-temperature, high-vibration, high-workload environments, and use data from previous models to estimate MTTF" (Henson, 2007, p. 1). If the workstation failure is a hardware problem they are all under warranty and can be replaced. However if it is a software problem then the IT technicians can solve the issues. Workstation failure will be looked over thoroughly and added to the disaster recovery plan as there is high dependence on workstations to stay in business and be profitable.

Cable Failure
Cabling issues are an internal threat as cables are part of the internal network. Cable failure is pretty low especially on an established network. This issue has been looked at and will be skipped over on the disaster recovery plan except in instances where the cabling will need to be replaced. Instances like these it will be noted the need to replace the existing cabling and any other details as necessary.
**Infrastructure Hardware Failure**

Switches or infrastructure hardware failure is both an internal and external risk. The risk is moderate as the 10 switches have been secured with complex encrypted passwords. If the switches were to get reconfigured it would affect all network traffic and make the network more vulnerable as well. Most likely the workstations wouldn't be able to reach the servers and vice versa until repaired. This could be up to a day delayed work and lost productivity in all departments in addition to delaying shipment of product unless the production machines can operate standalone. This issue will be addressed in the disaster recovery plan.

**Printer Failure**

Printers needing a major overhaul come because printers have consumables like drums, rollers, sheet feeders, and many other parts that wear out. These threats are all internal and cannot easily be controlled. The likelihood of failure in a printer is medium depending on the age of the printers. The more pages a printer prints the more likely that the printer is going to need maintenance done to keep it working properly. Because the company has multiple printers there isn't a major concern for this issue unless it affects the high speed printers that print the users manuals. This would stop shipment completely. There is the option to use other printers but the printing would be more hands on and require more time thus slowing down productivity and as a result the customers suffer because of delayed shipments. Printer problems will be included in the disaster recovery plan with the need to inform users and route the print jobs to one of the other 13 printers until the broken printer gets fixed.

**Equipment Reconfiguration**

Equipment reconfiguration typically has to deal with changes either by a service technician, IT person or a user who has too much free time on their hands. For the most part these problems can easily be overcome and are internally based however if the network is attacked there is a possibility that the hacker will reconfigure the equipment. The probability that this would cause a major problem is pretty high. The effects would roll throughout the business and eventually affect the customers unless fixed quickly. Equipment theft is a major force in business failure and happens frequently. The source of theft is internal and easily avoidable with proper controls. Equipment sabotage is pretty low especially where DigiKnights is a fun place to work and full of great people who help others not get frustrated to the point of causing destruction. So to recap Equipment reconfiguration is high risk, equipment theft is moderate and equipment sabotage is low. For completeness all three will be included in the disaster recovery document.

**Wireless Security**

Wireless at DigiKnights was implemented and the implementation of wireless network increased the company’s vulnerability to attacks. This risk is rated as high for DigiKnights because breaking a wireless connection is fairly easy. The wireless router is secured using WPA-PSK. The router is secured and only available to make changes by directly connecting to the router. This minimizes the risk of hackers changing the settings, in addition to the direct connection required to make changes, the router also filters connections by mac address. Only employees who need access to the router will get the access desired. The exception to this rule is in times of network outages the company has broadband cards that work for select computers that need access to the Internet 24x7. This access is only activated in times of disaster. This enables the company to continue operations as needed. The loss of company wireless access would only
reduce the convenience enjoyed by employees, except for in mission critical workstations. There won't be any impact to the company, its suppliers or the customers. This issue will be addressed for completeness of the disaster recovery plan.

**Hand-Held Devices**
Hand held device connectivity issues deals with the employees who have blackberry, or other hand held devices that are granted access to company email. This service is non-mission critical and the risk medium. There are vulnerabilities with hand held devices accessing the company network. So to keep the company secure DigiKnights has implemented mobile VPN that allows the mobile users to connect to the company from any connection but still maintain a secure connection (O'Neill, 2007). Because of implementing mobile VPN the risk has been reduced to low and will not need further discussion especially because hand held device connectivity isn't mission critical. Convenience is at stake here, there may be some upset employees, but in times of disaster convenience comes last.

**Data**

**Data Loss**
Data loss is inevitable there is a high risk of this happening at DigiKnights. The threats to data loss include internal hardware, software and external hackers. However there are proper controls in place that reduce the risk of data loss. DigiKnights has regular backups as well as requires users to save company files to the network. "56% of data loss due to system & hardware problems ... Microsoft’s NTFS (used in XP & Vista) with its de facto monopoly is the worst offender. But Apple and Linux aren’t any better" (Harris, 2007, p. 1). Data loss would cause huge problems throughout the company as we are a software copying company. All of our data is electronic and losing the data would cause loss of business productivity as well as lost sales due to our games leaking out into the public. If games leaked out into the public we would be less respected and desired by the creators of game software (aka our suppliers). Data loss is a high risk possibility and will be included in the disaster recovery document.

**Data Corruption**
Data corruption does occur and is usually caused by hardware and software failure but can also occur from hackers gaining access to the file system and corrupting the files. An error test "found an overall byte error rate of 3 * 10^7, a rate considerably higher than numbers like 10^14 or 10^12 specified for components would suggest" (Harris, 2007, p. 1). The number comes to an overall byte error rate of 30,000,000 what an astounding figure! Data corruption can always occur but this subject is so detailed that we will briefly address the need to use quality hardware that has been rated with a low failure rate as implement methods to block hackers’ access to the network. Data corruption will also be addressed thoroughly in connection with hackers corrupting system files.
Data Security
Data security breaches are impossible to avoid so there is a high risk that the company’s network will be compromised. Data security breaches come from both internal and external sources. Three places that there are problems include companies being willing to break their own security standards, give access to partnering companies, and far too complacent with their security standards (Krebs, 2008). According to a study that Verizon did "In 79 percent of the cases, Verizon found that a contributing factor to the data breach was a violation of the victim's own security policies -- such as weak/nonexistent passwords -- where the company failed to follow its own rules" (Krebs, 2008). Internal attacks come from employees leaving passwords on sticky notes, or using an easily guessable password or leaving their workstation unlocked. The effect could be problematic for both the suppliers who trust DigiKnights with their software the effect on the other end depends upon if the software is deleted. If so then the impact is high on creating disks otherwise the impact is low. Denial of service is one of the many attacks that a network can have this would affect network traffic as well as telephone traffic. More implementations have been created at the switch level as well as the firewalls to stop these attacks but they still have their effects to limit or deny access to resources. Viruses are a type of data security breach, viruses cause mass destruction and millions of dollars each year, “It is estimated that PC Viruses cost businesses approximately $55 billion in damages in 2003. The same calculations in were done in 2002 and 2001, at $20-30 billion and $13 billion, respectively” (Security Statistics - Virus Statistics, 2007). The effects are big on the servers resources, bandwidth consumption and the rest of network resources. Data security breaches will definitely be included in the disaster recovery plan.
IT Risk Assessment

Impact Attributes/Ratings
The purpose of the assessment is to find vulnerabilities in the overall security posture. This will define confidentiality, integrity, availability, and the impact values of the organization. This information will allow a greater assessment of the policies, processes, standards, and the culture of the organization.

Confidentiality: By restricting access and disclosure to authorized individuals and restricting access to unauthorized persons and groups. Systems that deal with confidentiality take the form of access control systems such as passwords, key cards, and identifiable information.

Integrity: Integrity in a security model deals with data preservation. Information that is entered must stay the same or it can no longer be relied upon. Whether the data originally entered is right or wrong, it has to stay consistent. This also deals with being able to identify the source and destination of data, to verify that the message was never intercepted by others. Systems that deal with this are commonly seen in emails. Digital signatures and message privacy protocols.

Availability: Availability is a measure of how accessible the data is. Data that is not available when it is needed is no better than not having the data to view. Organizations that depend on their data cannot survive if the information is unavailable. Systems that help maintain availability are commonly setup for redundancy. Power backups (UPS), RAID configurations for servers, and data backups all help maintain an organization’s availability. By providing copies of documents, power when fluctuations arise, and backups of data on a regular schedule.

Impact values:
High – This impact value defines what is critical to the business or the worst case scenario. If any of the following services go down for an extended period of time, two or more days, it would be detrimental to the business. These services include loss of customer's product information, communication with the customer, and non-planned shutdown of machinery. Loss of these services could cause loss of clients, missed deadlines, and would cause a significant loss of income.

Medium - This impact value defines what would cause significant damage to the business. If any of the following services go down for twenty-four to forty-eight hours it might have an unfavorable effect to the business. These services include loss of customer's product information, communication with the customer, and remote access to servers. Loss of these services would cause agitated clients.

Low - This impact value defines what would temporarily disrupt business. If any of the following services go down for twenty-four hours or less it might have a negative effect on the business. These services include loss of customer's product information, communication with the customer, and remote access to servers. Loss of these services could cause client complaints.
Organizational Information Criticality

This section discusses the perceived impact of the loss of confidentiality, integrity, or availability in regard to the information types stored, processed, and transmitted within specific denoted systems of the DigiKnight organization.

Information Matrix

<table>
<thead>
<tr>
<th>Information</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee</td>
<td>H</td>
<td>M</td>
<td>L</td>
</tr>
<tr>
<td>Financial</td>
<td>H</td>
<td>M</td>
<td>L</td>
</tr>
<tr>
<td>Legal</td>
<td>M</td>
<td>M</td>
<td>L</td>
</tr>
<tr>
<td>Customer’s Data</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>HR Information</td>
<td>H</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>High Watermark</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

Organizational Information Criticality Matrix

Employee Information:
- Social Security Numbers
- Addresses
- Financial Information.

Financial Information:
- Bank Account Information
- Credit Card Information
- Payment History

Legal Information:
- Policies that deal with copyright
- Trade secrets
- Legal documents

Customer’s Data
- Game data

HR Information:
- Items that would deal with staff and legal matters. (Harassment policies, time off, salary, employment history.)
## System Information Criticality Matrix

<table>
<thead>
<tr>
<th>Server Name</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Noo</td>
<td>HIGH</td>
<td>HIGH</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>Klumclot</td>
<td>HIGH</td>
<td>HIGH</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>Fronkblumb</td>
<td>HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>Foltcloo</td>
<td>HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>Blump</td>
<td>HIGH</td>
<td>HIGH</td>
<td>LOW</td>
</tr>
<tr>
<td>Hidotgrog</td>
<td>LOW</td>
<td>LOW</td>
<td>HIGH</td>
</tr>
<tr>
<td>Mong</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>LOW</td>
</tr>
<tr>
<td>Bomphbomph</td>
<td>HIGH</td>
<td>HIGH</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>Brugbone</td>
<td>HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>Pobhead</td>
<td>HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>Funkug</td>
<td>HIGH</td>
<td>HIGH</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>Doozfrolt</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
<td>HIGH</td>
</tr>
<tr>
<td>Jultfumble</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>Gulfhead</td>
<td>HIGH</td>
<td>HIGH</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>Huzz</td>
<td>HIGH</td>
<td>HIGH</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>Dookob02</td>
<td>HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>Dookob01</td>
<td>HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>Nulf</td>
<td>HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>Bunphboog</td>
<td>LOW</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>Frunkdoof</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
<td>HIGH</td>
</tr>
<tr>
<td>Bumunt</td>
<td>HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>Ghunph</td>
<td>HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>Gunbfug</td>
<td>MEDIUM</td>
<td>HIGH</td>
<td>LOW</td>
</tr>
<tr>
<td>Nok</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
<td>LOW</td>
</tr>
<tr>
<td>Foobdok</td>
<td>MEDIUM</td>
<td>HIGH</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>Mump</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>Oar</td>
<td>HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>Uzi</td>
<td>HIGH</td>
<td>HIGH</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>Scooby</td>
<td>LOW</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
</tbody>
</table>
**Maximum Tolerable Downtime (MTD)**

The maximum tolerable downtime (MTD) is the amount of time a company can tolerate the outage of certain asset or entity. The following departments MTD are defined as followed:

<table>
<thead>
<tr>
<th>Department</th>
<th>MTD</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT</td>
<td>30 minutes</td>
<td>infrastructure critical</td>
</tr>
<tr>
<td>Maintenance</td>
<td>30 minutes</td>
<td>infrastructure critical</td>
</tr>
<tr>
<td>Shipping</td>
<td>12 hours</td>
<td>mission critical</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>12 hours</td>
<td>mission critical</td>
</tr>
<tr>
<td>Sales</td>
<td>12 hours</td>
<td>mission critical</td>
</tr>
<tr>
<td>Administration</td>
<td>24 hours</td>
<td>critical service</td>
</tr>
<tr>
<td>Marketing</td>
<td>48 Hours</td>
<td>primary service</td>
</tr>
<tr>
<td>Security</td>
<td>48 hours</td>
<td>primary service</td>
</tr>
<tr>
<td>Research and Development</td>
<td>60 hours</td>
<td>secondary service</td>
</tr>
</tbody>
</table>

**Maximum Tolerable Downtime**

These department maximum tolerable downtime where determined by it need to keep the company operational, and continue making profit. The following departments are defined as:

- The information technology (IT) department is Infrastructure Critical. This department is responsible for the upkeep and repair of computer and computer related devices. The loss of this department would cause loss of clients, missed deadlines, and significant loss of income.
- The maintenance department is infrastructure critical. This department is responsible for the upkeep, repair of product machinery, and is present/on call 24/7. The loss of this department would cause loss of clients, missed deadlines, and significant loss of income.
- The shipping department is a mission critical. This department prepares the product for shipment, and receives supplies and materials for the production of the physical product. This would cause loss of clients, missed deadlines, and significant loss of income.
- The manufacturing department is a mission critical. This department manages the re-supplying machinery, and helps prevents non planed downtime. This would cause loss of clients, missed deadlines, and significant loss of income.
- The sales department is a mission critical due to its contacts with stores nationwide, and operates closely with the shipping department to ensure the prompt, on time delivery of products to stores. In the event of downtime this would cause missed deadlines, and would cause a significant loss of income.
- The administration department is a critical service due to its responsibility for oversee the day-to-day operations, and make officiating executive decisions. In the time event of downtime this may cause loss of deadlines, and agitated employees within the company.
- The marketing department is a primary service that performs constant endeavors to find and maintain contacts. In the event of downtime this would cause nothing detrimental to the organization.
- The security department is a primary service. This department maintains the physical security of the facilities. The loss of this department would cause an employees to feel unsafe, and our facility to be unguarded.
The research and development team is a secondary service. The focus of this department is primarily on researching improvements of production systems. This would not cause any loss if department experiences downtime, but we would like to get it up in a timely manner.
Warm site

Warm Site Pros:
- Redundancy built into DigiKnights which is headquartered in the bay area where there is high risk of disasters occurring and affecting the company operations.
  - 2 servers and 5 backup computers would stored off site.
- Down time from 10 hours to 2 days or less.
- Second location could be used for business functions, and off site backups.
- Cost to have the warm site could be reduced by purchasing or renting a small building.
- Completely customizable to DigiKnights needs.

Warm Site Cons:
- Increased overhead costs
  - Initial costs go up to setup and maintain a warm site but when a disaster hits the costs are much less because business can continue.
- If both the main location and the warm site are affected by the disaster then the company is out of luck until they can get a location and equipment.

Recommendations:
- High speed connection of 7 megabits per second is recommended.
- Implement off site backups by using the encrypted VPN tunnel to a SCSI drive on one of the servers at the warm site.
- Use the warm site for business functions, and testing the disaster recovery plan.

"The way you decide to equip your disaster recovery site will be a function of your available resources and the criticality of your IT operations. In order to decide between hot, warm, or cold sites, it is crucial to perform an analysis of your disaster recovery needs" (Chickowski, 2005). A warm site is one of four business continuity options. The four business continuity options include mirrored, hot, warm and cold. Each of the four business continuity options will each be briefly
described as follows: A cold site is essentially an empty building that would require purchasing new equipment or relocating old equipment after the disaster, as well as setting up the infrastructure. A hot site on the other hand is a working second location and would only be feasible if a company has the time and resources to invest in a second location. A mirrored site is a duplicate copy of the servers in a secure, vaulted rack that limits entrance to DigiKnight IT personnel. The vault protects the servers from the environment. A warm site is somewhere in the middle, it is like a work in progress. The costs become effective and will only take a few days or less to get the data and essential components running for DigiKnights.

<table>
<thead>
<tr>
<th>Site Type</th>
<th>Capital Costs</th>
<th>Hardware/Software</th>
<th>Networking/Communications</th>
<th>Setup Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirrored</td>
<td>High</td>
<td>Full</td>
<td>Full</td>
<td>Minimal</td>
</tr>
<tr>
<td>Hot</td>
<td>Medium/High</td>
<td>Full</td>
<td>Full</td>
<td>Hours</td>
</tr>
<tr>
<td>Warm</td>
<td>Medium</td>
<td>Partial</td>
<td>Partial or Full</td>
<td>Days</td>
</tr>
<tr>
<td>Cold</td>
<td>Low</td>
<td>None</td>
<td>None</td>
<td>Days/Weeks</td>
</tr>
</tbody>
</table>

The differences between off-site options

Each of the four business continuity options have advantages and disadvantages, however the warm site will be the primary focus. "A warm site provides many of the same benefits, but the data is not refreshed as often. Generally, the data replication routine can occur anywhere from once every 24 hours to once a week. The data transfer often takes place through a high-speed data connection. In the event of a disaster, the warm site would provide day-old data" (Donnelly, n.d.). A warm site is being proposed because it is a half way medium in cost and complexity. In addition a warm site is completely customizable to DigiKnight like the other options.

The essential components of a warm site include servers, workstations and machines at a separate location. DigiKnights does regular backups, the regular backups will allow DigiKnights to minimize data loss and down time. The backups will not catch every file because there will always be a day delay in between backups, but planning for the disaster will allow DigiKnights to minimize the effects of the disaster on the business operations.

The system, data and application functionality will be the primary parts of the planning for a warm site. An additional component that will be proposed is the recommendation to store the servers off site, while still retaining 24x7 access to them. Offsite storage is very secure; For example the service from Another9 provides fire protection, security access with notification, in an underground building that protects the servers from the environment. Be advised offsite storage is the Cadillac version of a warm site and will cost much more than a warm site. "Companies that go to this level of disaster preparedness are rare; a high level of competence and forward thinking is required [to] plan, build and maintain it" (Types of Disaster Recovery, n.d.). Off-site storage is recommended but would be costly to implement. The best option for DigiKnights is a warm site with servers that could provide relief from a disaster. The backups would be sufficient to update the servers located at the warm site and would allow the company to continue business. Business continuity in this section of the paper refers to the bare minimum to operate. Although the warm site being proposed is not the ideal working situation it would provide the essentials to continue business operations such as selling, creating, and shipping the
video games and owner’s manuals after a disaster. Many disasters could affect the main location and planning before the disaster occurs will minimize the effects on DigiKnight's success as a business. DigiKnights warm site would provide the needed applications, programs and files that are necessary to create disks. Business continuity even after a major disaster would keep customers who purchase the games happy.

The Plan:
The warm site will consist of a networking infrastructure (high speed connection, one router, wiring to 10 computers (for expansion or computers brought from DigiKnight after a disaster), as well as the wireless functionality mentioned in the IT and Technology based threats section). In addition there will be heating, cooling, and other working utilities, five computers, one high speed printer, two servers, one firewall, a VPN tunnel and an old disk replicator machine. The machines that have been chosen will be assigned to the infrastructure critical and mission critical departments. The assignments will be as follows: The two necessary servers and one computer for the IT department, one workstation for maintenance, one for shipping, one for manufacturing, and one for sales. The workstations can also be drop in style so if other departments need to use the computers they can when the computers are not in use. Wireless access would allow managers or a predefined set of people bring company laptops or personal laptops for use after a disaster. IT would have close supervision of those using laptops and access would be restricted after DigiKnight recovers from the disaster.

The servers would have the following services and applications available: active directory (a close replica of the company as of the latest backup), file shares, print server, customer and supplier data, and images of the games. The equipment and servers should be safer in the warm site. The idea is to have the two servers connected 24x7 to the main location via a high speed Internet connection and protected access through a VPN tunnel with firewalls at each end. There will be anywhere between 10 hours up to two days downtime to get all data back to the most current setup. Theoretically the servers would be up and running in a matter of hours because the servers and data are being backed up daily. The only work required would be to do a restore of the most current backups to the servers; this would enable the data to be the most current.

During normal business operations the machines will remain in standby except as needed. The location is relatively close, so the building can be used for meetings, practice drills for the disaster recovery plan as well as any other need. Because the machines will be in very minimal use the IT department will have them setup to wake on LAN so updates can be installed remotely. The updates to the computer will keep the computers current with the most current software patches and virus definitions. In addition to the data replication that will occur weekly to the standby servers. To provide high security behind the high speed connection the warm site will need a firewall, a VPN tunnel for communication between the warm site and the main location. Keeping the computers up to date will minimize downtime in the event of a disaster. The costs of the warm site can be allocated to the meetings and events held there so the costs won't always be for a "disaster."

Outsourcing the warm site to another company would be the optimal solution but would cost much more than having our own IT department setup and maintain the warm site. The cost to lease a building is a minimum of $2.20 per square foot so if it is possible to find a small building
for rent it would cost 1,200 square foot building would come to $2,640 a month. Heating, cooling, and other electrical costs would be minimal since the five workstations would be on standby until they did update once a month. This power scheme would save power by not producing as much heat. Also the thermostat would be set at a much lower temperature because the building would be in standby use until needed for a disaster or other event. The computers would come from DigiKnights old computers before upgrading. Depending upon our contract with Dell, HP, and Boldata we could keep five of the nicest computers before upgrading, it might cost some money but would most likely be cheaper than going out and buying five new ones that will just sit and get outdated, unless in the case of a disaster. A similar thing can be done once a printer becomes old but still working good, DigiKnight can relocate a high speed printer to the warm site.

The location of the building is also important to analyze especially because a close building would be nice and convenient for access purposes. Yet if a disaster hit that affects the whole bay area it would be nice to have the warm site far enough away that the disaster wouldn't affect the building. As mentioned before the cheapest leases go for $2.20 a square foot but an average lease goes for much more some leases are up to $17 a square foot.

At this point it is important to not lose perspective and totally reject the idea of having a warm site. Disasters aren't cheap but it is much cheaper in the long run to plan ahead. Planning ahead pays because many people and businesses will charge more after a disaster. In addition most disasters only affect certain regions and the suppliers or customers will expect to have their regular orders.
Hot Site Solution
A hot site is a duplicate center located in a remote location. The remote location itself will be located at several miles away from 2725 E. Technology Ave. Freemont, CA. The location is equipped hardware and software in the event of a disaster.

The sales at DigiKnight have been very promising over the past five years. The game publishers that have done consistent business with DigiKnight are large vendors and keeping their business is crucial. Part of the appeal that many of the companies see in DigiKnight is that it rapidly produces their physical products for them. In the event of a disaster DigiKnight would not be able to produce physical product and keep track of sales. Losing the business of Electronic Arts, Nintendo, Capcom and Ubisoft may mean the end of a successful era at DigiKnight. Many of these issues can be circumvented by being well prepared for various disasters. A hot site is a strong solution for DigiKnight, below the details and proposals are described in detail.

Pros:
- Minimal loss of operations.
- There will be a duplicate of all the central servers.
- Less costly than a fully mirrored site.
- The offsite can have operations restored within one to four hours.
- Nearly complete backups of all user data.
- Allows for disaster recovery testing.

Cons:
- While this is the most thorough solution it is expensive.
- Aside from the cost of implementation the cost of maintenance can be high.
- The amount of time that the hot site can be used after a disaster may be limited by the vendor.
**Recommendations:**

Outlined below are the recommendations for the hot site. As financial resources are the main issue surrounding this solution for DigiKnight there are numerous suggestions to save company resources.

This solution will incorporate all of our systems to minimize down time and reduce the associated costs with lost time. This plan will require us to duplicate all the resources used within the three buildings. The most crucial part to duplicate for the hot site is the central servers located in building 3 within the IT department. To maintain effective business continuity it will also be necessary to have the ten administrative computers, the twelve sales computers, the three research and development computers, four shipping computers, the three purchasing computers, the five advertising department computers, and the ten IT computers.

Choosing what hardware and software to have ready onsite is vital to continuity. However to save money not all hardware has to be exactly duplicated and it is possible to downgrade some of the hardware.

The **four central servers** need to remain identical to the ones on location. The monitors can be downgraded to save money. The specifications for the machines at DigiKnight are as follows:

- Dual 3.2 GHz Processors, 4 GB of RAM, 3 X 500 GB Hard Drive (configured to RAID 5), Windows Server 2003, Dual Gigabit Network Cards and 15 Inch Monitors.

The **ten administrative computers** do not need to be identical to the ones located on location at DigiKnight. These machines are generally used for very basic things such as word processing and various spreadsheets. Our vendor for the administrative machines is Compaq and they can be contacted to use alternative video cards. A lesser video card can be used because these machines do not require intensive video processing. Alternate monitors can be used at the hot site as well. The specifications for the machines located at DigiKnight are as follows:

- 2.2 GHz Pentium 4 Processors, 1024 MB of RAM, 100 GB SATA Hard Drive, Built-In Video Card, Gigabit Network Card, 17 Inch Monitors and Windows XP.

The **fifteen sales computers** do not need to be identical to the ones on location at DigiKnight. These machines are mainly used to store sales data. Three of the machines do not need to be replicated at all due to the fact that they are not in use by any staff or for any storage. Nine of the machines are used by the sales staff and last three machines are used as a local database for sales members. Our vendor for the sales machines is Dell and they can be contacted to use alternative video cards. A lesser video card can be used because these machines do not require intensive video processing. Alternate monitors can be used at the hot site location. The specifications for the machines located at DigiKnight are as follows:

- 2.7 GHz Pentium 4 Processors, 1024 MB of RAM, 200 GB SATA Hard Drive, Built-In Video Card, Gigabit Network Card, 21 Inch Monitors and Windows XP.

The **three research and development computers** do not necessarily need to be identical to the ones on location at DigiKnight. These machines run CAD software which is graphic intensive.
All three of these machines were custom built for DigiKnight by Boldata Technology. In the event of a disaster research and development will not be a top priority. While research and development is important to DigiKnight and ensures the company’s place in the market it can be put off until the permanent site is restored. However, it is necessary to keep backup all of the information and data from research and development. All of this information must be kept current at the offsite location so that no research or data is lost. The specifications for the machines located at DigiKnight are as follows:

- 3.2 GHz Pentium 4 Processors, 2048 MB of RAM, 450 GB SATA Hard Drives, Quatro Pro Video Cards, Gigabit Network Cards, Dual 21 Inch Monitors and Windows XP.

The four shipping computers should be kept close to the current specifications because they are vital to the business, insofar as they help prepare and track shipments originating from the company. If these machines are not available at the necessary given moments the time and money lost would lead to huge financial losses for DigiKnight. Our vendor for the shipping machines is HP and they can be contacted to use alternative video cards if it is found financially necessary. A lesser video card can be used because these machines do not require intensive video processing. Alternate monitors can be used at the hot site location. The specifications for the machines located at DigiKnight are as follows:

- 2.0 GHz Pentium 4 Processors, 512 MB of RAM, 50 GB SATA Hard Drive, Built-In Video Cards, Gigabit Network Cards, 17 Inch Monitors and Windows XP.

The three purchasing computers do not have to be identical to the ones on location at DigiKnight. These machines deal with the purchasing of raw supplies which are used in production. Our vendor for the purchasing machines is HP and they can be contacted to use alternative video cards. A lesser video card can be used because these machines do not require intensive video processing. Alternate monitors can be used at the hot site location. The specifications for the machines located at DigiKnight are as follows:

- 2.0 GHz Pentium 4 Processors, 512 MB of RAM, 50 GB SATA Hard Drives, Built-In Video Cards, Gigabit Network Cards, 17 Inch Monitors and Windows XP.

The five advertising department computers do not have to be identical to the ones on location at DigiKnight. These five machines are used to find additional retail outlets to distribute the products to and to find new publishers who wish to use DigiKnight to produce their games. All five machines only need internet access and office applications. Our vendor for the advertising machines is HP and they can be contacted to use alternative video cards. A lesser video card can be used because these machines do not require intensive video processing. Alternate monitors can be used at the hot site location. The specifications for the machines located at DigiKnight are as follows:

- 2.0 GHz Pentium 4 Processors, 512 MB of RAM, 50 GB SATA Hard Drive, Built-In Video Cards, Gigabit Network Cards, 17 Inch Monitors and Windows XP.
The **ten IT department computers** need to be very much like the ones at location at DigiKnight. The IT computers keep all the other computers for the entire company up and running. These machines are fast and powerful and need to remain so at the hot site. The specifications for the machines located at DigiKnight are as follows:

- 3.2 GHz Pentium 4 Processors, 1024 MB of RAM, 100 GB SATA Hard Drives, Built-In Video Cards, Gigabit Network Cards, 21 Inch Monitor and Windows XP.

### The Hot Site Plan

#### The Company

4Service Inc. located in Los Angeles, Agoura Hills and Las Vegas. Los Angeles is close enough for business continuity without excessive delay but it is far enough away so that certain disasters would not affect the Los Angeles area in many circumstances. The location is secure and DigiKnight’s mission critical applications will be kept running. They are responsible for supplying their data center which will make our servers available to the internet 24 hours a day, 7 days a week and 365 days a year.

4Service Provides:
- 8 Tier-One Backbone Providers under one roof (Intelligent Routing)
- High Capacity Fiber Optic Sonet Ring Network
- Cisco Switches & Routers
- Strong SLA’s with **99.99% Uptime guarantee in writing**
- Redundant Back up Power
- 24-hour Monitoring by Network Operations Center
- Pro-Active Support Service

**Other Benefits:**
- Critical Data is secured in data vaults over multiple redundant remote locations.
- Choice of encryption level.
- Flexible backup scheduling and data retention settings.
- On call support technician and a dedicated account manager.

This solution is one of the strongest possible for DigiKnight. This solution starts at $3,000.00 a month. DigiKnight employees will need to be trained in emergency response procedures and drills to the hot site will need to be practiced to ensure that everyone is comfortable with handling various situations. The first cost figures may seem startling or excessive but they can be nothing compared to the business and money lost during down time due to being ill prepared for disasters.
Recovery Management Teams

Determine if Management Team will meet at the command center or proceed directly to the recovery site.

- Call the Crisis Communication Command Center to arrange access and set-up if it is an internal site, or make reservations for the external site.
- If determined that Recovery site will be activated, alert appropriate contact and arrange access.
- Determine and assign team leads for core recovery teams (damage assessment, administration and recovery teams).

Assess potential domino effect (upstream/downstream interdependencies) on business customers, partners, and vendors. Contact your Business Resiliency Manager to establish bridge line call if necessary.

- Administration and Support
- Sales, Purchasing, and Shipping
- Production and Manufacturing

Assign Damage Assessment Team, if appropriate

- Ascertain injuries and fatalities.
- Provide results of damage assessment.
  - Perform an inspection of the property. Compile a complete description of damage, including damage to the buildings, equipment, and inventory. After itemizing, set damaged property aside for examination. If immediate disposal of any property is required, it is advisable that photographs or other documentation be retained in order to identify all items destroyed.
- Address any special insurance issues.
  - Review coverage with Insurance Agent/Claim Representative. Some items that may help with the claim process are historical sales records, income and expense information as shown in recent profit and loss statements and income tax returns, records of extra expenses incurred to resume business operations after a covered loss (this may include temporary rental space, temporary equipment rental, and moving expenses), receipts/records for damaged inventory, and other business records that may help project what profits might have been had a loss not occurred.
- Work closely with civil authorities.
- Estimate expected duration of outage.
- Determine work-in-progress issues.
- Provide ongoing recovery status reporting.
- Keep Management Team informed of progress.
- Escalate any issues.
- Document recovery actions taken during recovery process for post-event debriefing and discussion.
Assign Administration Team, if appropriate

- Notify Corporate Insurance of incident and track all expenses incurred during the recovery process of insurance claim follow up.
- Direct the retrieval of items stored off-site.
- Implement telephone redirection procedures.
- Coordinate travel requirements.
- Perform redirection of mail.
- Obtain needed office supplies, special forms, and other supplies.
- Maintain a record of all expenses incurred during the recovery process and provide to Management Team.
- Provide ongoing recovery status reporting.
- Keep Management Team informed of progress.
- Escalate any issues.
- Document recovery actions taken during recovery process for post-even debriefing and discussion.
- Contact USPS, UPS, FedEx, and DHL to hold all mail until further notification as to where to redirect.

Contact Information

**Department/Management Contacts**

<table>
<thead>
<tr>
<th>Department</th>
<th>Name</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td>Mark Saunders</td>
<td>415-555-0180</td>
</tr>
<tr>
<td>Sales</td>
<td>Diane Ford</td>
<td>415-555-0200</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>Linda Kraemer</td>
<td>415-555-0150</td>
</tr>
<tr>
<td>Research &amp; Development</td>
<td>Carlton Bowden</td>
<td>415-555-0100</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Michael Winters</td>
<td>415-555-0400</td>
</tr>
<tr>
<td>Marketing</td>
<td>Michael Churchill</td>
<td>415-555-0160</td>
</tr>
<tr>
<td>Shipping</td>
<td>Kenneth Gilliam</td>
<td>415-555-0130</td>
</tr>
<tr>
<td>Security</td>
<td>Brett Kelcey</td>
<td>415-555-0170</td>
</tr>
<tr>
<td>IT</td>
<td>Alicia McKellips</td>
<td>415-555-0190</td>
</tr>
</tbody>
</table>

**Floor Warden/Safety Coordinators**

**Building 1**

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rod Hatherly</td>
<td>415-555-0181</td>
</tr>
<tr>
<td>Bea Holdeman</td>
<td>415-555-0182</td>
</tr>
<tr>
<td>Kendra Bell</td>
<td>415-555-0184</td>
</tr>
</tbody>
</table>

**Building 2**

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Natasha Love</td>
<td>415-555-0202</td>
</tr>
<tr>
<td>Anne Mcloskey</td>
<td>415-555-0104</td>
</tr>
<tr>
<td>Owen Mill</td>
<td>415-555-0162</td>
</tr>
</tbody>
</table>

**Building 3**

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lance Addams</td>
<td>415-555-0144</td>
</tr>
<tr>
<td>Katelin Griffin</td>
<td>415-555-0143</td>
</tr>
<tr>
<td>Bell Rosenberg</td>
<td>415-555-0141</td>
</tr>
</tbody>
</table>
DigiKnight Employee Hotline
1-800-555-1234
Follow the prompts on the line to obtain information specific to the incident or issue. This line is to keep employees informed of the incident status and actions to take.

HR Hotline
1-800-555-6789
This is an alternate number when unable to contact Management during an incident. Employees can call to report their safety in the event they can’t reach, or be reached by, their manager.

Communications Representative
Mary Jane Rogers
415-555-0166
Refer all Media requests and questions to your local communications representative.

IT
415-555-8352
Call IT if you lose a laptop or Blackberry, or have any other computer security incident.

Security
415-555-3852
Call security to report an emergency.

State Farm Insurance for Business Needs
Corporate Headquarters:
1 State Farm Plaza
PO Box 8105
Bloomington, IL 61710-0001
Phone: 309-766-2311

State Farm Insurance Agent (Local):
Norm Epperson
Address:
38970 Blacow Rd. Suite D
Fremont, CA 94536-7380
Phone: 510-796-5911
Mailing Address:
Fremont, CA 94537-8105

State Farm Insurance Agent (Distance):
Tim Rosene
Address:
720 Robb Dr. Suite 109
Reno, NV 89523-3733
Phone: 775-826-5554
Fax: 775-826-5557

*See Warm Site Recovery for recovery location.
Business Retail and Service

- Business owners get comprehensive protection for buildings, business personal property, loss of income and business liability. Policies designed for owners and operators of retail, wholesale, and service businesses. Optional coverages are also available.
- For businesses that need $1 million or more of liability protection, State Farm’s Commercial Liability Umbrella Policy offers broad coverage at a sensible price.
- Business owners with employees need Employment to cover claims for harassment, discrimination or wrongful termination. It is specifically designed to help protect the insured and their business in the event an employee brings a suit or administrative charge.
- Technology Services Errors and Omissions Liability protect specific types of businesses that provide their customers with technology services. This coverage can help protect the insured from liability arising from mistakes, whether real or alleged.
- Accountants Professional Liability covers certain accountants and related businesses which are protected from claims alleging a negligent act, error or omission in the performance of professional accounting services.
- Under the Miscellaneous Errors and Omissions Liability, specific customers are protected from liability arising from a negligent act, error or omission in the performance of their professional service. An important benefit of this product is coverage for legal defense costs. Even when found innocent, the legal costs can be substantial.
- The business will need workers’ compensation insurance to protect employees who are injured on the job and to comply with workers’ compensation laws.
- State Farm Business Auto Insurance provides comprehensive coverage against damage or liability claims involving a business vehicle. This insurance provides coverage for a wide variety of vehicles such as delivery vans, tractor-trailers, utility trucks, and private passenger vehicles. Coverage options include liability, medical payments coverage, personal injury protection, comprehensive, collision, emergency road service, car rental and travel expenses, uninsured and underinsured motor vehicle coverage, death, dismemberment and loss of sight, and loss of earnings coverage.
- If the community participates in the National Flood Insurance Program, then flood insurance policy can be purchased through a State Farm agent. Most flood insurance is written through the Nation Flood Insurance Program (NFIP), which is administered by the Federal Emergency Management Agency (FEMA). State Farm services policies through an arrangement with FEMA. A flood insurance policy normally takes 30 days from the date of purchase to go into effect.
Precautionary Measures to Take to Reduce Risks

Business Safety

 Business Equipment

 Use surge protection devices. Properly installed electrical service meter surge protection devices (SPDs) used in conjunction with individual plug-in SPDs offer a high level of protection for your buildings and business equipment.

 Install lightning protection system. A qualified contractor should install a lightning protection system.
  o Local lightning protection contractor:
    Hart & Associates, Inc.
    Lowell H. Hart
    Phone: 888-551-4278
    www.lightning.org

 Fire Prevention

 Equip the building with an automatic sprinkler system or dry chemical system. When properly installed and maintained, this system provides 24-hour fire protection. Should a fire start, the system will activate and release a water or chemical spray in the area of the fire, suppressing it until the fire department arrives. Often, a sprinkler/chemical system totally extinguishes a fire. It is important that the system be professionally inspected on a regular basis.
  o Arrow Fire Protection
    3330 Seldon Ct. Suite 1
    Fremont, CA 94539
    Phone: 800-478-2766
    Fax: 510-70-8649
    Email: CustomerService@ArrowFire.com
    http://www.arrowfire.com/home.php

 It is important that the building has the right type, size and number of fire extinguishers. Contact the nearest fire protection equipment supplier or fire department to ensure that we have the protection we need. A quality extinguisher will be either UL-listed or FM-approved. A professional fire equipment supplier should periodically inspect the extinguishers to verify they are still operational. See fire department contact information.

 Smoke detectors don’t put out fires, but they do provide early warning that may allow escape from the building. Detectors are laboratory tested to ensure that they meet certain safety and performance standards. For battery-operated units, test and replace the batteries on a regular basis. Some detectors may be powered by the building’s electrical system and may also have a back-up battery. These units should be tested regularly. See fire department contacts.
There are a variety of flammable or combustible liquids that are used within the business, such as cleaners, solvents, adhesives, etc. Flammable liquids give off vapors that may travel with the natural airflow. These vapors may explode when ignited by a spark, such as a faulty electrical switch or a flame from a water heater pilot light. Store flammable liquids in their original container or in a UL-listed safety can. Allow plenty of ventilation when using flammable liquids to reduce the risk of fire and injury or illness from breathing the vapors. Limit the amount of flammable liquids stored on the property.

**Employee Safety**

- Machines in the workplace can pose operating hazards. From minor cuts and abrasion to serious lacerations, exposure to machine operations can be detrimental to life, health and productivity. Machinery should be equipped with guarding and employees be trained to use them. Employees should be trained in the start up, operation and shutdown procedures of all equipment. All equipment should be inspected for possible operating hazards before each use. Questionable equipment should not be used and should be reported to management. Unavoidable circumstances and complications can occur with the machinery. Employees should be trained in service and maintenance of machinery and lockout/tagout procedures.

- Chemicals and solvents in the workplace can create hazardous conditions. Some combinations of common cleaning chemicals can cause serious life threatening conditions. A designated storage place for chemicals should be used. Labels on the products must be read, as well as the Material Safety Data Sheets (MSDS). MSDS are sheets provided by a supplier that lists important information about the product such as chemical content, physical characteristics, health hazard and what to do after exposure, fire and explosion hazards, reactivity, cleanup procedures and the personal protective equipment that should be worn while working with the chemical.
  - [www.MSDSonline.com](http://www.MSDSonline.com)

- When workplace hazards cannot be eliminated or reduced, personal protective equipment may be necessary. Personal Protective Equipment (PPE) does not eliminate a hazardous situation. It can simply create a protective barrier between the employee and the hazard. Equipment can be in the form of safety glasses or goggles, gloves, boots, hearing protection, hardhats, and/or respirators. Employees that are required to wear PPE are to be properly fitted and trained.

- It is important that employees are educated on the proper positioning of all elements within an employee’s workspace. Make sure that proper ergonomics are followed, practice proper techniques when lifting items, and emergency procedures are followed correctly.

**Preventing Slips, Trips, and Falls**
- Maintain adequate lighting in parking areas, on sidewalks, and in stairways.
- Gutters should not drain water from the roof onto walkways or into parking areas.
- Reported spills should be cleaned up quickly.
- Repair or replace torn carpets, rugs, loose or missing floor tiles, or any other flooring materials.
- In parking lots, potholes or uneven surfaces should be repaired.
- Install handrails on stairways and ramps in accordance with local building code requirements. Handrails should be stable and securely fastened. Consider using non-slip surfaces in stairways, steps, and ramps.
- Uneven surfaces, large cracks, or bumps in the sidewalk should be repaired. Remove obstructions from walkways. The lawn sprinkler system should be turned off and drain the system when the temperature nears freezing.
- An incident-reporting procedure will be developed and all employees and managers will be trained on how to use it. A manager will be on duty whenever possible, emergency phone numbers will be posted on the company’s Intranet, keep first aid kits handy and ready for use, investigate all incidents, and keep a record of those incidents. Incident reports should be written to aid documentation and should include who was injured, dates, and circumstances. Management should review all incident reports.
  - Incident Investigation Report
- When the power goes off for extended periods of time, backup emergency generators are very beneficial. The correct generator size is determined by the business’s need in emergencies. Permanent Standby Generators are to be installed as part of the electrical system and provide power to the building wiring. An automatic switch prevents the generator from back-feeding power into the utility lines and protects the generator from damage when power is restored. It should only be installed by a licensed electrician. The city building department must inspect the switches and wiring. When the installation is complete, the local utility should be notified a back-up system is in place.
  - Licensed Electricians and Backup Generators
    - Mission Valley Electric, Inc.
    - Phone: 510-745-8847
  - City of Fremont, Planning Division
    - 3300 Capitol Ave. Building A
    - Fremont, CA 94538
    - Phone: 510-284-4000
http://www.ci.fremont.ca.us/CityHall/Departments/Planning.htm
**FEMA**

In times of countless disasters a company must be ready for anything. We have already defined what natural threats are of concern to our company. Now we must address what resources we have access to, and what processes does the company have to follow to get these resources.

One of the greatest resources a company can have in case of nature disasters is FEMA. “The Federal Emergency Management Agency (FEMA) is an agency of the United States Department of Homeland Security. The purpose of FEMA is to coordinate the response to a disaster which has occurred in the United States and which overwhelms the resources of local and state authorities.” (Wikipedia, 2008)

**Services Provided by FEMA**

The services provided by FEMA are not determined whether or not there is a disaster, but do you qualify for them? To qualify for assistance from FEMA the company needs two things. One, the company losses must have occurred in area covered by a disaster declaration. Secondly, you must file for a claim with your insurance company.

**Available Disaster Assistance**

**Disaster Assistance Available From FEMA**

When addressing what FEMA can do for the company or an individual may be limited, but its possibilities are great. FEMA provides three categories:

- Housing needs
  - Temporary housing
  - Repair
  - Replacement

Permanent housing construction

- Other than Housing needs
  - Disaster related medical, dental, funeral and burial cost.
  - Clean-up times; clothing; household items; tools required for job; education materials.

- Additional Services
  - Crisis Counseling
  - Disaster unemployment assistance
  - Legal services
  - Special Tax consideration
Disaster Loan Available From Small Business Administration
The U.S. Small Business Administration (SBA) can provide federal subsidized loans to repair or replace homes, personal property, or business that sustained damage not covered by insurance. There are three types of disaster loans:

- **Home disaster loans:** This loan provides homeowners and renters to repair or replace disaster-related damages to home or personal property.
- **Business physical disaster loans:** This loan provides business owners to repair or replace disaster-damaged property, including inventory, and supplies.
- **Economic injury disaster loans:** This loan will provide capital to small businesses and to small agricultural cooperatives to assist them through the disaster recovery period.

Disaster Assistance From Small Organizations and Agencies
This section provides a list of agencies that may be of assistance for selected disaster. This list does not provide any agencies in our location. The majority of the numbers are in Central America and Eastern America. Although, this doesn’t mean that these agencies wouldn’t be of assistance to our organization.

Possible Risks Defined by FEMA
The possible risks defined by FEMA are not only natural threats, but human made threats as well. This will not cover procedure in which the company should protect it equipment, or data. This will cover the procedure, guidelines, and policies in which to save life. This will prepare the company for surviving and responding to disasters. The disaster is listed as followed:

**Heat**

**Overview:**
- Preparations

These are modifications that our company can perform that would keep the employees safe of heat exhaustion, and help preserve the safety of our equipment and product. With the implementation of storm windows all year will employee time of putting up, and prepares your company for any unexpected events.

For more information please see link: [http://www.fema.gov/hazard/heat/heat_before.shtm](http://www.fema.gov/hazard/heat/heat_before.shtm)

**Earthquake**

**Overview:**
- Six ways to plan ahead

FEMA covers the six ways to plain ahead that defines the following: hazards, safe places, education, disaster supplies, emergency communication, and helping the community. All of these six steps have supplies, procedures, and helpful information allowing individuals survive such disasters. For more information please see link: [http://www.fema.gov/hazard/earthquake/eq_before.shtm](http://www.fema.gov/hazard/earthquake/eq_before.shtm)
Fire

Overview:
- Smoke Alarms
- Escaping the Fire
- Flammable Items
- Heating Sources
- Matches and Smoking
- Electrical Wiring
- Other

This will inform of technology, procedures, policies, practices, and signs one should be aware of incase of a fire. For more information please see link: http://www.fema.gov/hazard/fire/fire_before.shtm

Flood

Overview:
- Preparations

This will inform of technology, procedures, practices, and signs one should be aware of incase of a flood. For more information please see link: http://www.fema.gov/hazard/flood/fl_before.shtm

Landslides

Overview:
- Before Landslide or Debris Flow
- Warning signs

This will inform the effects of a landslide or debris flow, how to minimize this hazard, and inform individuals of the signs of landslides. For more information please see link: http://www.fema.gov/hazard/landslide/ls_before.shtm

Hurricane/Tsunami

Overview:
- How to protect yourself from Tsunami
- Preparations for hurricane

This will inform the corporation of measurements that should be taken before a hurricane, and terms, what to do before and after, and what can result be form a tsunami. These measurements should be implemented into practices and policies. For more information please see link: http://www.fema.gov/hazard/hurricane/hu_before.shtm
http://www.fema.gov/hazard/tsunami/index.shtm
Thunderstorm
Overview:
- Preparation for a thunder
- Guidelines
- Things to avoid

This will inform the corporation of guidelines to follow, how to prepare for thunder, and what should you avoid. This will not address the effect on machinery, and should be considered when implementing these policies, procedure, and guidelines. For more information please see link: http://www.fema.gov/hazard/thunderstorm/th_before.shtm

Others
Overview:
- Dam Failure
- Hazardous Material
- Nuclear Explosion
- Terrorism
- Volcano
- Tornado

These hazards may not be as important as the other hazards, but these hazards should be taken into consideration as well. FEMA provides inform of technology, procedures, policies, practices, and signs one should be aware of in these typed of events. For more information please see link: http://www.fema.gov/plan/index.shtm

Memo
To: Shelley Keating  
From: George Wallace  
Date: July 6, 2008

In times of countless disasters a company must be ready for anything. We have already defined what natural threats are of concern to our company. Now we must address what resources we have access to and what processes does the company have to follow to get these resources.

DigiKnights Inc. is still considered a small organization with limited resources. We are reliant on various different originations functionality to get our product made and shipped. So with this information in mind I strongly believe that considering FEMA into our disaster recovery plan for these specific reasons:

- **Business physical disaster loans**: This loan provides business owners to repair or replace disaster-damaged property, including inventory, and supplies.
- **Economic injury disaster loans**: This loan will provide capital to small businesses and to small agricultural cooperatives to assist them through the disaster recovery period.
The importance of these two specific reasons is in time of need our corporation could use this to cover damages that our insurance does not. This will allow a greater chance of recovery, but a greater edge on the other competition as well.

In conclusion, with the environment changing and the difficult of small businesses surviving, these options that I presented will not only allow better survivability and an edge on our opponents.

**Disaster Declaration Statement**
In case of disaster please address one of the following example documents. If none of the documents match the any of the issues then create statement that would fit the situation. The following Disaster Declaration statements are as followed:
Increasing productivity to be a Digital Knight in shining armor to get the games in the hands of the gamers.

Dear Friends and Colleagues,

In light of the recent disaster that has affected many of our daily lives. DigiKnight Technology Inc. would like to extend our deepest sympathies to everyone affected by this disaster. Our employees and their families are an important part of our company, and we will be happy to support you in any way we can.

A representative will contact you personally with detail of the disaster, and how this will affect DigiKnights Technology Inc. In case anyone feels that they need more support than can be provided by DigiKnight Technology Inc. please contact the following numbers:

- Red Cross Helpline: 1-800-RED-CROSS
- Government Relief Helpline: 1-800-WHATS-GOINGON

While we firmly believe that these actions are in the best interest of all involved. Again, we want our employees and their families to know they’re not alone.

Sincerely,

Carlton Smith
Digiknights Technology INC. Founder and CEO
To our valued customers:

We would like to take this opportunity to thank you for the support you’ve given Digiknight Technology over the years. Through all our ups and downs, we’ve always been proud of our loyal customers. That’s what makes our recent actions so difficult.

In light of recent events DigiKnight Technologies Inc. is unable to continue production and shipping of its products. These events were caused by <Enter Event>. A full assessment of the situation is still under way, and a representative will contact you again within 24 hours with a full update. If you have any concerns about your order please contact our sales representatives.

While we firmly believe that these actions are in the best interest of all involved. Again, we want to extend our sincerest thanks to everyone for their understanding.

Sincerely,

Carlton Smith
Digiknights Technology INC. Founder and CEO
Community and Media

[Insert Date]

[Insert Logo]

Increasing productivity to be a Digital Knight in shining armor to get the games in the hands of the gamers.

Dear community,

I want to take this opportunity to thank you for your hard work and dedication in supporting us in our time of need. You have never failed up to help us meet our obligations, but we understand help from the community can only go so far.

It has recently come to our attention that that <Enter Disaster> has affected us greatly. Due to these events Digiknight Technology Inc. Will be unable to continue manufacturing and shipping it products to our customers. Until a full assessment of all systems we cannot make a decisive decision when we will be fully operational.

Digiknights Technology Inc. will keep everyone notified of situation. If you contact us during business hours we will be happy to answer any questions concerning this incident. We will also be contacting customers and keeping them posted every step of the way.

Again, we want to extend our sincerest thanks to everyone for their understanding and support.

Sincerely,

Carlton Smith
Digiknights Technology INC. Founder and CEO
Legal and Regulatory Notification

[Insert Date]

[Insert Logo]

Increasing productivity to be a Digital Knight in shining armor to get the games in the hands of the gamers.

[Dear whomever],

In light of this new [legal or regulatory] notification Digiknight Technology Inc. We will not be able to continue manufacturing and shipping games. These regulations are:

[insert Quote]

If you contact us during business hours we will be happy to answer any questions concerning this recent issue. We will also be contacting customers and keeping them posted every step of the way.

Until these regulations are met we will not be able to continue producing and shipping our games. While we firmly believe that these actions are in the best interest of all involved. Again, we want to extend our sincerest thanks to everyone for their understanding.

Sincerely,

Carlton Smith
Digiknights Technology INC. Founder and CEO
Vendors and Service Contracts

Quick Contact Information

<table>
<thead>
<tr>
<th>Computer Vendors</th>
<th>HP</th>
<th>Boldata</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell</td>
<td>3000 Hanover St.</td>
<td>Bold Data Technology, Inc.</td>
</tr>
<tr>
<td>One Dell Way</td>
<td>Palo Alto, CA 94304-1185</td>
<td>Dba BOLData Systems</td>
</tr>
<tr>
<td>Round Rock, Texas 78682</td>
<td>USA</td>
<td>48363 Fremont Blvd.</td>
</tr>
<tr>
<td>(1 – 800 – WWW - DELL)</td>
<td>(800 – 262 - 6672)</td>
<td>Fremont, CA 94538</td>
</tr>
</tbody>
</table>

Computers and Servers

Workstations and Servers
The Servers and IT department computers keep all the computers running at DigiKnights and provide backups. The ten IT department computers and four servers have been purchased from Dell. There is a current and standing service contract between DigiKnights and Dell which expires every year on December the 29th. This contract is renewable every year without changing any of the contract terms. The contract includes same day service if the request comes in before 3:00 PM. Otherwise the contract guarantees service the next day for computer replacements and repairs. The contact number if needed is 42368131588-DKG and each of the purchased computers is numbered with the serial DGK12389-#. The number symbol corresponds with the number of the computer at DigiKnight, which there are twenty five of. If customer support is needed for these machines 1-888-555-5897 can be called to reach a representative.

Shipping Computers
The four shipping computers help prepare and track shipments originating from DigiKnights. These workstations have been purchased from HP. The service contract for these machines is provided through HP and includes 24 hour service, three hundred and sixty five days a year service. The contract number if needed is DGK – 13548253. The contract between HP and DigiKnights expires every year on the 22nd of February without changing any of the contract terms. All of the computer serial numbers start with DGK55879-#. The number symbol corresponds with the number of the computer at DigiKnight, which there are twenty two of. If customer service is needed for any of the machines 1-888-555-5237 can be called for assistance.

Administrative Computers
The administrative computers at DigiKnight are used only by administration for word processing and spreadsheets. All of these machines have been purchased from Compaq. The service contract for these machines is provided through HP and includes 24 hour service, three hundred and sixty five days a year service. The contract number if needed is DGK – 13548253. The
contract between HP and DigiKnights expires every year on the 22nd of February without changing any of the contact terms. All of the computer serial numbers start with DGK55879-#. The number symbol corresponds with the number of the computer at DigiKnight, which there are twenty two of. If customer service is needed for any of the machines 1-888-555-5237 can be called for assistance.

Sales Computers
The sales computers at DigiKnights are used by the sales staff and mostly contain sales data for DigiKnight. There are currently fifteen sales workstations purchased from Dell. There is a current and standing service contract between DigiKnights and Dell which expires every year on December the 29th. This contract is renewable every year without changing any of the contract terms. The contract includes same day service if the request comes in before 3:00 PM. Otherwise the contract guarantees service the next day for computer replacements and repairs. The contact number if needed is 42368131588-DKG and each of the purchased computers is numbered with the serial DGK12389-#. The number symbol corresponds with the number of the computer at DigiKnight, which there are twenty five of. If customer support is needed for these machines 1-888-555-5897 can be called to reach a representative.

Research and Development Computers
The research and development computers are high performance systems capable of running CAD software. There are currently only three purchased systems from Boldata Technology. Boldata Technology provides a service contract that covers sending maintenance personnel onsite Monday through Friday between the noon and five. The contact number if needed is DGK1161. This contract expires every three years on the 9th of March. These three machines have the serial number DGK - #. The number symbol corresponds with the number of the computer at DigiKnight. Boldata can be reached at 1-888-555-1497.

Purchasing computers
The three purchasing computers at DigiKnights deal with the purchasing of raw supplies which is used in production. There machines were purchased from HP. The service contract for these machines is provided through HP and includes 24 hour service, three hundred and sixty five days a year service. The contract number if needed is DGK – 13548253. The contract between HP and DigiKnights expires every year on the 22nd of February without changing any of the contact terms. All of the computer serial numbers start with DGK55879-#. The number symbol corresponds with the number of the computer at DigiKnight, which there are twenty two of. If customer service is needed for any of the machines 1-888-555-5237 can be called for assistance.

Advertising Computers
There are five advertising computers which find retail outlets to distribute products to and find new publishers who wish to use DigiKnights to produce their videogames. All advertising workstations have been purchased from HP. The service contract for these machines is provided through HP and includes 24 hour service, three hundred and sixty five days a year service. The contract number if needed is DGK – 13548253. The contract between HP and DigiKnights expires every year on the 22nd of February without changing any of the contact terms. All of the
computer serial numbers start with DGK55879-#. The number symbol corresponds with the number of the computer at DigiKnight, which there are twenty two of. If customer service is needed for any of the machines 1-888-555-5237 can be called for assistance.

Other Services and Supplies

Production Machines
All of the production machines at DigiKnight are custom built so there is no immediately replacing them. There are no serial numbers on the production machines. The machines at DigiKnight are serviced by the onsite maintenance staff. We Fix’Em Inc. provides repair services in the event that the onsite maintenance staff is unable to fix the production machines. We Fix’Em may be reached at 1-888-555-0567 and if needed the service contract number is WFDK4898.

Blank DVD/CD/Cases Suppliers
The Tech Geek is the main supplier located at 48965 Warm Springs Boulevard, Fremont, CA 94539 and can be called at 1-800-456-0825. Currently Disc Makers at 7905 North Route 130, Pennsuaken, NJ 08110-1402 is the secondary supplier of disks and disk accessories they can be called at 800-468-9353 toll free or 856-663-9030. Disk Makers also has a company website at http://wwwdiskmakers.com. In the case of an emergency there are two additional disc makers Dub-It Media Services and ISSI Business Solutions. Dub-It Media Services is located at 1110 North Tamarind Avenue, Hollywood, California 90038 and be called at 1-888-99DUB-IT or 323-993-9570. ISSI Business Solutions is located at 22122 20th Avenue SE #152 Bothell, WA 98021 and can be called toll free at 1-800-660-3568 or 425-483-4801.

Should there be an issue receiving DVD, CD or disk cases from Tech Geek, Dub-It media services, ISSI business solutions or Disk Makers DigiKnights will use Megalodan multimedia. Megalodan is located at 518 Washington Street, Ashland, OR 97520 and can be called toll free at 888-234-2283 or at 541-201-5324. The website address is http://megalodon.com. They provide mid height tray packs, tall tray packs, jackets, folders, specialty jackets, mailers, jewel cases, portfolios, retail boxes, software boxes, multi-disc set packaging, bulk CD, Mini and other recordable media.

Copy and Fax Machines
All of the copy and fax machines located at DigiKnight are covered by Office Equip Inc. The service contract states that service will be provided during normal working business hours. Office Equip will send out new units to replaces working ones and DigiKnights is responsible to send back broken units to the Office Equip. The last known information shows that the last contract expired on November 7th, 2007. However the contract number for all the office equipment is OEIDKG-125. All the serial numbers to the copy and fax machines at DigiKnight are DGK191 as assigned by Office Equip and they can be reached at 1-888-555-1576.

In the case of an emergency if Office Equip cannot fulfill the needs of DigiKnight HP should be used to replace machines. HP sells home and office printers as well as home and office faxes.
DigiKnight also has a current standing service contract with DigiKnight to help facilitate service. HP can be called at 1-888-555-5237. The website can be accessed [http://www.HP.com](http://www.HP.com) from which a live representative or technician can be reached. The website also contains email forms for users with questions or issues.

Box Suppliers
The primary box supplier for DigiKnight is Customized Packaging Solutions Inc. Their mailing address is 8333 24th Avenue, P.O. Box 278060, Sacramento CA 95826. No phone number for Customized Packaging Solutions Inc. In the event of an emergency The Packaging House Inc. is the secondary supplier for packaging software and they are located at 6330 North Pulaski Road, Chicago, Illinois 60646-4594. The Packaging House Inc. can be called at 800-966-1808.

For an additional source for software packaging Magellan Packing can fulfill the needs of DigiKnight. Magellan provides software packaging in CD/DVD cases and wallets, manuals, any components that need to be packaged with software such as cables and a distribution channel. This solution would provide sales through retail outlets or directly to customers through courier or regular post. Magellan can be reached at +1 (408) – 324-0620.

Paper Supplier
JC Paper is the current provider for paper for box inserts. JC Paper is located at 47422 Kato Road, Fremont, CA 94538 and can be called at (510) 413 – 4700. There is no known service contract currently between DigiKnight and JC Paper. In the event of an emergency Ace Paper Company can be used to keep business running normally by providing paper, commercial paper, industrial paper and paperboard products in rolls or sheets. Ace Paper Company is located at 2835 East Washington Boulevard, Los Angeles California 90023-4216 and can be called at (323) 268-1900.

DigiKnight Service and Other Related Contracts Locations
Certain records are only available through hard copies which include the following: employee contracts, computer service contracts, machine service contracts, software service contracts, office equipment service contracts, records of store distribution sales receipts, distribution contracts with publishers which legally allow production, building blue prints, machine blueprints, machine manuals, employee hiring records, corporate handbook, corporate phonebook, local phone book, supply purchase receipts, advertising prints, company authorized photos, customer lists, OSHA compliance data, EPA information, accounting files, tax records and manufacturer provided computer manuals.

The following data lists are available through computerized records: optical media computer backups, employee personal e-mail accounts, employee business e-mail accounts, e-mail correspondence with customers, e-mail correspondence with suppliers, company website design, QuickBooks computer records, customer database, supplier database, corporate database and customer payment information including credit card transactions.
Emergency Situations
The Fremont Police Department recommends dialing 9-1-1 if you smell fire or smoke, to get help for someone who is hurt, if you see someone getting hurt, if you see a crime in progress, if you’re not sure you have an emergency. 911 should be contacted as soon as possible after an emergency or disaster. Below the contact information for local emergency services including the closest emergency room, the closest urgent care, local fire stations, several police contacts, hazardous materials services and search and rescue services is provided. However in the case of an emergency 911 should be contacted because it may very well save lives.

Damage Assessment Team
Mark Saunders Manager of Administration:
Mark Saunders should be the first member of the Damage Assessment Team to be contacted in the event of an emergency. During normal operation hours the office number should be called first. During non operational hours the home or cell phone number listed below should be contacted. If the land lines are not operational or an emergency has occurred that would not enable Mark to be at his desk then the cell phone number should be called next. If you have any non emergency questions Mark may be reached at the email address below.

Office Number: 415-555-7841 ext: 0180
Cell Phone Number: 415-555-7842
Home Number: 415-555-7843
Home Address: 4333 E. Monica Drive, Fremont CA 94538
Email: MSaunders@DigiKnights.com

Alicia McKellips Manager of IT:
Alicia McKellips should be the second person contacted in the event of an emergency if Mark Saunders cannot be reached. During normal operation hours the office number should be called initially. During non operational hours at DigiKnights the cell phone number listed below should be contacted. If the land lines are not operational or an emergency has occurred that would not enable Alicia to be at her desk then the cell phone number should be contacted next. If you have any non emergency questions Alicia may be reached at the email address below.

Office Number: 415-555-8352
Cell Phone Number: 415-555-7844
Home Number: None Provided
Home Address: 5789 Dales Street, Fremont CA 94538
Email: AMckellips@DigiKnights.com
**Carlton Smith CEO:**
Carlton Smith should be contacted in the event of an emergency regardless of order and in the event that Mark Saunders and Alicia McKellips cannot be reached Carlton Smith should be contacted third for damage assessment. During normal operation hours the office number should be called initially. During non operational hours at DigiKnights the cell phone number listed below should be contacted. If the land lines are not operational or an emergency has occurred that would not enable Carlton to be at his desk then the cell phone number should be contacted next. The pager number and home number can be contacted next if all the other numbers fail to reach Carlton.

Office Number: 415-555-7841
Cell Phone Number: 415-555-7844
Pager Number: 415-555-7845
Home Number: 415-555-4746
Home Address: 7772 N. H Street, Freemont CA 94538
Email: CSmith@DigiKnights.com

**Crisis Management Team**

**Mark Saunders Manager of Administration:**
Mark Saunders should be the first member of the Crisis Management Team to be contacted in the event of an emergency. During normal operation hours the office number should be called first. During non operational hours the home or cell phone number listed below should be contacted. If the land lines are not operational or an emergency has occurred that would not enable Mark to be at his desk then the cell phone number should be called next. Mark will be the first person to contact emergency services and civil authorities should they be needed. Mark is proficiently trained in CPR and assisting injured persons. If you have any non emergency questions Mark may be reached at the email address below.

Office Number: 415-555-7841 ext: 0180
Cell Phone Number: 415-555-7842
Home Number: 415-555-7843
Home Address: 4333 E. Monica Drive, Fremont CA 94538
Email: MSaunders@DigiKnights.com

**Linda Kraemer Manager of Manufacturing:**
Linda Kraemer should be second member of the Crisis Management team to be contacted in the event of an emergency if Mark cannot be reached. During normal operation hours the office number listed below should be called first. During non operational hours the home or cell phone number listed below should be contacted. If the land lines are not operational or an emergency has occurred that would not enable Linda to be at her desk then the cell phone number should be called next. Linda will be the first person to contact emergency services and civil authorities should they be needed if Mark Saunders is for any reason unable to do so. Linda is proficiently
trained in CPR and assisting injured persons. If you have any non emergency questions Linda may be reached at the email address below
Office Number: 415-555-6161 ext: 0150
Cell Phone Number: 415-555-7177
Home Number: 415-555-7178
Home Address: 98714 N. 103rd Avenue, Fremont CA 94538
Email: LKramer@Digiknights.com

Evacuation and Shelter Leaders
Michael Winters and Michael Churchill will be responsible for leading employees through evacuation procedures, locating shelter sites and assisting them to shelters. After shelter information is released Michael Churchill and Michael Winters will also find transportation methods to the site.

Initially Michael Churchill should be contacted first and Michael Winters will assist with evacuation and shelter efforts. During normal operation hours the office number listed below should be called first. During non operational hours the home or cell phone number listed below should be contacted. If the land lines are not operational or an emergency has occurred that would not enable Michael Churchill to be at his desk then the cell phone number should be called next. Michael Winters should be contacted if all attempts to contact Michael Churchill fail.

Michael Churchill
Office Number: 415-555-0160
Cell Phone number: 415-555-3977
Home Number: 415-555-3978
Home Address: 544 S. Glendale Avenue, Fremont CA 94538
Email: MChurchill@DigiKnights.com

Michael Winters
Office Number: 415-555-0400
Cell Phone Number: 415-555-3971
Home Number: 415-555-3972
Home Address: 56987 N. Sienna Street, Fremont CA 94538
Email: MWinters@DigiKnights.com

Emergency room
From DigiKnight Washington Hospital Healthcare is the closest 24 hour emergency room. Washington Hospital provides services such as 24-hour emergency care. The center also includes childbirth and family services, cardiac surgery, catheterization and rehabilitation, nutritional counseling. Outpatient surgery, pulmonary function, crisis intervention and respiratory care are provided 24 hours a day. Washington Hospital provides rehabilitation services involving cardiac, physical therapy, occupational therapy, speech and stress care.
Additionally social services, laboratory, medical imaging, level II nursery and hospice care are provided but not 24 hours a day.

**Washington Hospital Healthcare System can be found at:**
2000 Mowry Ave. Fremont, CA 94538  
Main Phone Number: (510) 797-1111  
Information line/Community Relations Department: (510) 791-3417  
Email: feedback@whhs.com

**Driving directions** to the Washington Hospital from the center of 94536 are as follows:  
On Greenwood Dr. drive toward Arlene Ct. and turn right on Arlene Ct. Drive 0.1 miles on Arlene Ct. and turn left on Peralta Blvd (CA-84). Drive 0.1 miles on Peralta Blvd (CA-84) and turn right on Paseo Padre Pkwy. Drive 0.8 miles on Paseo Padre Pkwy and turn left on Mowry Ave. Drive 0.3 miles on Mowry Ave and arrive at Washington Hospital. The total distance is 1.3 miles and in ideal driving conditions the total driving time should take five minutes.

**Urgent Care**
An urgent care center may be required in case of an emergency. Appointments are not needed to see a physician. An urgent care center is appropriate when medical attention is needed but injuries are definitely not life threatening. Urgent care centers are able to treat medical problems that are not emergencies but do require care within twenty four hours. If an ailment is not life threatening it may take medical care away from patients at emergency rooms that require that care.

The Fremont Urgent Care Center of the Palo Alto Medical Foundation (PAMF) is the closest urgent care center to DigiKnight. The hours for the location are Monday through Friday, 8 a.m. to 8 p.m., Saturday, Sunday and Holidays, 8 a.m. to 5 p.m. In ideal driving conditions traveling by car should take approximately 6 minutes.

**PAMF can be found at:**
3200 Kearney Street  
Level 1, Building 2  
Fremont, CA 94538  
Main phone: 510-490-1222

**Driving directions** to the Fremont PAMF from the center of 94536 are as follows:  
On Greenwood Dr. go toward Arlene Ct., turn right on Arlene Ct. Drive 0.1 miles on Arlene Ct. and turn right onto Peralta Blvd.(CA-54). Drive 1.4 miles on Peralta Blvd and turn right on Kearney St. Drive 0.1 miles and arrive at PAMF urgent care.
Fire Stations
The ten closest fire stations to DigiKnight are listed below. The administrative Fremont fire station office is located at 3300 Capitol Ave, Fremont, CA 94538. The mailing address for the City of Fremont Fire Department is P.O. Box 5006, Fremont, CA 94537-5006. The email address for the City of Fremont Fire Department is fremontfire@ci.fremont.ca.us.

- Fire Station 1: 4200 Mowry Ave., Fremont, CA 94538
- Fire Station 2: 37645 2nd Street, Fremont, CA 94536
- Fire Station 3: 40700 Chapel Way, Fremont, CA 94538
- Fire Station 4: 1000 Pine Street, Fremont, CA 94539
- Fire Station 5: 55 Hackmore Lane, Fremont, CA 94539
- Fire Station 6: 37412 Fremont Boulevard, Fremont, CA 94536
- Fire Station 7: 43600 South Grimmer Boulevard, Fremont, CA 94538
- Fire Station 8: 35659 Fremont Blvd. Fremont, CA 94536
- Fire Station 9: 39609 Stevenson Place Fremont, CA 94539
- Fire Station 10: 5001 Deep Creek Road Fremont, CA 94555

Hazardous Materials
The Fremont fire department is the Certified Unified Program Agency otherwise known as CUPA, for all of the businesses in the city of Fremont. The mailing address for CUPA is P.O. Box 5006, Fremont, CA 94537-5006. To contact the City of Fremont by phone call 510-494-4282 or email abarraza@ci.fremont.ca.us.

According to the city of Fremont website CUPA consolidates the following environmental programs: Hazardous materials management plan and inventory (HMMP) and the hazardous materials business plan (HMBP), Risk Management Program (RMP) and underground storage tank (UST) program. CUPA also consolidates the Spill prevention, control and countermeasure plan (SPCC) for aboveground petroleum product storage, hazardous waste generators and on-site hazardous waste treatment.

CUPA must be contacted for hazardous materials reporting when one of the following thresholds are reached, 55 Gallons of Liquids, 200 cubic feet of Gases or 500 pounds of Solids.

For fire extinguishing systems it is suggested that the following be available, fire extinguishers, a fire hose and foam with nozzles/hose.

Wash Station, Safety Showers, Cartridge Respirators, SCBA Units. It should also be indicated prior to an event to CUPA which of the above are available for use in case of an emergency.

**Police Department**

The Fremont Police Department can be reached by phone at 510-790-6800 and faxed at 510-790-6831. The Police Department is located at 2000 Stevenson Boulevard, Fremont, CA 94538. The Chief of Police is Craig Steckler and he may be reached by email at csteckler@ci.fremont.ca.us. For emergency situations 911 should be dialed. According to the City of Fremont website the Police Department is responsible for safeguarding of citizens’ lives and property, the preservation of constitutional rights, and neighborhood problem solving. Other Police Numbers and email addresses for the city of Fremont:

- Capt. Frank Grgurina phone number: 790-6911 email: fgrgurina@ci.fremont.ca.us
- Capt. Richard Lucero phone number: 790-6818 email: rlucero@ci.fremont.ca.us
- Capt. Robert Nelson phone number: 790-6815 email: rnelson@ci.fremont.ca.us
- Animal Services, Sgt. John Dauzat phone number: 790-6630 email: jdauzar@ci.fremont.ca.us
- Communications Unit, Lt, Gus Arroyo phone number: 790-6988 email: garrote@ci.fremont.ca.us

**Search and Rescue**

There are several search and rescue operations in the immediate area surrounding DigiKnight. The Bay Area Search & Rescue Council provides communications and other services for search and rescue teams throughout the Bay Area.

California Explorer Search and Rescue (Cal-ESAR) is a wilderness search and rescue team which responds to searches and other types of emergencies throughout all of California. They are also a charter member of the Bay Area Search & Rescue Council. The main office is located at 205 DeAnza Boulevard #30, San Mateo California 94402. Cal-ESAR can be reached by phone at 650-340-4779. This is a volunteer team based in San Francisco Bay area. Cal-ESAR can be reached at pr@calesar.org. They should be contacted first for search and rescue operations.
DIGIKNIGHT SHELTER-IN-PLACE POLICY AND PROCEDURES

What is sheltering in place? Sheltering in place consists of staying indoors to protect from chemicals, floods or other hazards that could be problematic. “Shelter in Place is used across the country as a protective action for the public. But even before formal sheltering in place was common, examples of the effectiveness of staying indoors during chemical emergencies exist... [One of such examples comes from] Labarre, LA in 1961 A 30 ton chlorine releases immediately surrounded the house of a young family. After about 15-20 minutes, the father panicked and carried his young son outdoors. The rest of the family stayed inside. The family and the father survived, but the young boy died from the chlorine exposure he received outside” (Shelter in Place Information Center, n.d.). What if a major disaster happened during normal business hours? DigiKnight wants to protect all within its premises from any danger.

This portion of the disaster recovery and business continuity plan will define where emergency supplies are located and what should be done to take shelter on DigiKnight company facilities. This policy in no way supersedes authorities in fact it is quite the opposite. If the city of Fremont, California is providing instructions that supersede what this document says then employees should follow city leaders, while still exercising caution of course. DigiKnight is very much aware of the employees and that they each have needs that extend to family and friends.

Shelter-in-place triggers include first and foremost advisement from the public authorities to stay put, and the following types of emergencies that DigiKnight could incur:

- Chemical emergency
- Severe Wind/Rain Storm and Electrical storm
  - Downed Electrical pole
- Epidemic pandemic
- Shoot out at a neighboring business

The procedures can vary depending upon the emergency type. However the basics will be the same. For example people will still need access to water, lights, and a space to rest. DigiKnight has some basic supplies on hand for sheltering in place. These supplies consist of bottled water, water purification tablets, flashlights, fresh batteries (AA), battery operated radio & batteries, tape, plastic for all windows and doors, blankets & pillows, some clothes, and some non-perishable food. Once these items are gathered and maintained by the manager of administration or in his absence the manager of manufacturing, they are both on the crisis management team the supplies will be stored in closets in each building. For more information on the crisis management team please see crisis management team as referred to in their identifying section. Please refer to image # Building 1&2 and image # Building 3 for specifics on the location for each closet. The image also includes the water plan, and what the city and maintenance team have passed on to the disaster recovery team. These two images include all utility closets, circuit breaker panels, power lines, gas, electric, and water lines.
Quick Reference for Crisis Management Team:
First point of contact: Michael Churchill's contact numbers Office Number: 415-555-7841 ext: 0180, Cell Phone Number: 415-555-7842, or Home Number: 415-555-7843
Second Point of Contact: Linda Kraemer's contact numbers Office Number: 415-555-6161 ext: 0150, Cell Phone Number: 415-555-7177, or Home Number: 415-555-7178

Checklist for Any Shelter in Place:

- Activate the shelter in place plan by sounding an alarm.
- Gather everyone into the emergency assembly area. Each buildings has an area for gathering and sheltering in place.
- Check to see that every employee is accounted for and OK.
  - The administrative assistant will call the roll to make sure that every person is present.
- Close the business, and change phones to mention that the business is sheltering in place.
- "If there are customers, clients, or visitors in the building, provide for their safety by asking them to stay – not leave. When authorities provide directions to shelter-in-place, they want everyone to take those steps immediately. Do not drive or walk outdoors" (Evacuation Plans and Procedures eTool: Evaluating the Workplace, n.d.).
- If there is danger of explosion cover all windows with plastic, and lower blinds to minimize the glass from coming into the building.
- Encourage customers, employees and visitors to call their family or close friend to let them know everything is OK.
- Communicate regularly with employees.
- Pull out supplies as needed from the emergency kits.
  - Make sure there are enough provisions to care for all present.
- Listen to the radio, internet news or TV for continued updates on the situation.
- Stay put until further notified by authorities or reports from the media state that all is clear.
- After hearing that all is clear
  - Uncover vents and windows
  - Turn on ventilation systems
  - Go outside
- Deactivate the shelter in place plan.

Why leave the building so quickly? Wouldn't the building continue to be a safe place? "With tight buildings, any vapors that may have entered the structure during its exposure to hazardous vapors will leave the building very slowly. Chemicals that have [ab]sorbed onto building surfaces will also gradually desorb. If an occupant remains in the building without radically increasing the air exchange rate, exposure to the hazardous chemical will continue and dosage of that chemical will increase" (Shelter in Place Information Center, n.d.).

Specifics for Individual Types of Shelter in Place:
The following sections include specifics for case by case shelter in place disaster responses.
Chemical Emergency
DigiKnight has a neighbor business that creates chemical gases, the employees need to be trained to watch the area for problems, and however, the authorities will be the primary people to contact DigiKnights regarding chemical spills. DigiKnight's crisis management team will turn off all air ventilation, and tape with plastic covering. If there are dangers of explosion the windows will also be covered with plastic. After authorities state that all is clear the employees will be evacuated from the building. Then the plastic will be removed quickly, and the ventilation will be turned on to reduce any chemicals that entered the building.

Severe Wind/Rain Storm and Electrical Storm
Electrical storms cause major damage through lightning strikes. Fires and damage is caused because of the lightning. The best place to be is inside as long as there is proper grounding. If the lightning is far away and not causing damage nearby then under precaution it might be possible to not require all employees to shelter in place. The vents will not need to be taped or shut off.

Downed Power Pole
If the downed power pole has blocked traffic, started a fire or caused a major reason to shelter in place and not go home then by all means DigiKnight will be there for its employees.

Epidemic/Pandemic
If there is a major outbreak of a disease then DigiKnight would heed the counsel given from authorities to minimize impact on its employee’s by sheltering in place and DigiKnight's crisis management team will turn off all air ventilation, and tape with plastic covering.

Shoot Out at Neighboring Business
If and when a shootout occurs for the safety of the customers and employees shelter in place will be provided. Following the general shelter in place guidelines as mentioned above.
Layout – Building 3
Assembly Sites
- A pre-determined temporary meeting location where employees are to assemble when notified to evacuate their workplace, generally to take headcount and/or perform roll call.

During Business Hours:
If there is a building incident and the building needs to be evacuated, all employees should vacate the building and report to designated assembly site. Everyone is to leave the site/location and go to the Primary Assembly Site unless instructed to go to the Secondary Assembly Site.

Primary Assembly Site – The designated Assembly Site

- Starbucks
- Secondary Assembly Site – Where employees are to assemble when gathering at the Primary
- Assembly Site is not feasible or safe. This location should be farther away than the primary site.
- Chester’s Steakhouse

Activities at the Assembly Site:

- Take roll-call; verify all employees’ status and safety.
- Gather initial recovery team.
- Determine work in process and identify business priorities.
- Establish the times of the next critical deadlines.
- Identify the key contacts that should be called ASAP and advise them of the situation.
- Determine what travel options are available for staff to commute to recovery site.

Safety Coordinators along with management will account for all staff members and notify emergency personnel of those staff members whose whereabouts are unknown. Department Managers report to Assembly Site, take a head count and verify safety of personnel.

If it’s determined by management to invoke the Business Continuity Plan, management will review the roles and responsibilities for identified staff members. Specific tasks and procedures have been documented in the plan.

<table>
<thead>
<tr>
<th>Primary Assembly Location Address:</th>
<th>Corner of Technology Ave &amp; Central Ave, Fremont, CA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Assembly Point:</td>
<td>Starbucks</td>
</tr>
<tr>
<td>Secondary Assembly Location Address:</td>
<td>201 E. Jefferson St., Fremont, CA</td>
</tr>
<tr>
<td>Secondary Assembly Point:</td>
<td>Chester’s Steakhouse</td>
</tr>
<tr>
<td>Primary Contact Name:</td>
<td>Michael Churchill</td>
</tr>
<tr>
<td>Primary Contact Number:</td>
<td>415-555-0160</td>
</tr>
<tr>
<td>Primary After-Hours Contact Number:</td>
<td>415-555-3978 – Home</td>
</tr>
<tr>
<td></td>
<td>415-555-3978 – Cell</td>
</tr>
<tr>
<td>Alternate Contact Name:</td>
<td>Michael Winters</td>
</tr>
<tr>
<td>Alternate Contact Number:</td>
<td>415-555-0400</td>
</tr>
<tr>
<td>Alternate After-Hours Contact Number:</td>
<td>415-555-3972 – Home</td>
</tr>
</tbody>
</table>
After Business Hours:
Using call trees, managers, supervisors, and leads will notify employees when and where to report to work. Employees may also call the DigiKnight Employee Hot Line (1-800-555-1234) to receive information.

If the employee is not available, the caller will ask for a number where the employee can be reached.

If it’s determined by management to invoke the Business Continuity Plan, management will review the roles and responsibilities for identified staff members. Specific tasks and procedures have been documented in the plan.

Emergency Wallet Card

**EMERGENCY INSTRUCTIONS**

*If at work:*
- Evacuate as instructed
- Report to your designated assembly/safe haven location

*If primary worksite is unavailable upon arrival:*
- Go directly to assembly/safe haven location

*During non-work hours:*
- Call DigiKnight Emergency Hotline 1-800-555-1234 for status updates
- Follow instructions from management or Emergency Hotline

**EMERGENCY CONTACTS:**
- Security: 415-555-3852
- IT: 415-555-8352
- Emergency Fire/Police: 911
- Local Police: 510-790-6800

**KNOW...**
- How to notify:
  - Fire Department
  - Police Department
  - Security

- Your recovery plan before the need arises
- How to evacuate your area and register your status at assembly/safe haven location
- Directions to your assembly/safe haven and recovery locations

**DO NOT...**
- Use elevators or go to the roof
- Open hot doors
- Run in stairwells
- Enter an evacuated building until instructed to do so
- Make statements to the media

**DIGIKNIGHT**

Business Resiliency

**EMERGENCY WALLET CARD**

**TO REPORT AN EMERGENCY, CALL**

SECURITY:
415-555-3852

DIGIKNIGHT EMPLOYEE HOTLINE:
1-800-555-1234

**KEEP THIS CARD WITH YOU AT ALL TIMES**

CONFIDENTIAL AND PROPRIETARY TO DIGIKNIGHT.
FOR INTERNAL USE ONLY.
LOCATION INFORMATION

Primary Assembly/Safe Haven
Starbucks

Secondary Assembly/Safe Haven
Chester’s Steakhouse

Recovery Location
Greater than 3 days:
201 W. Broad St.
Building 4
Modesto, CA 95350

DIGIKNIGHT EMPLOYEE HOTLINE: 1-800-555-1234
Follow the prompts on the line to obtain information specific to the incident or issue.

HR HOTLINE: 1-800-555-6789
Alternate number when unable to contact Management during an incident.

MANAGEMENT CONTACTS

Mark Saunders 415-555-0180 (w)
415-555-7842 (c)

Dane Ford 415-555-0200 (w)
415-555-3070 (c)

Linda Kraemer 415-555-0150 (w)
415-555-7177 (c)

Carlon Bowden 415-555-0100 (w)
415-555-3042 (c)

Michael Winters 415-555-0400 (w)
415-555-3072 (c)

Michael Churchhill 415-555-0160 (w)
415-555-3077 (c)

Kenneth Gilliam 415-555-0130 (w)
415-555-7899 (c)

Brett Kelsoy 415-555-0170 (w)
415-555-7863 (c)

Alicia McKelips 415-555-0190 (w)
415-555-7844 (c)

MISCELLANEOUS INFORMATION/CONTACTS

Floor Warden/Safety Coordinator:
Building 1:
Rod Hatherly 415-555-0181
Bea Foldsman 415-555-0182
Kendra Bell 415-555-0184

Building 2:
Natasha Less 415-555-0202
Anne Molokey 415-555-0104
Owen Mill 415-555-0162

Building 3:
Lance Addams 415-555-0144
Karin Griffin 415-555-0143
Bell Rosenberg 415-555-0141

IT:
415-555-8352
If you lose a laptop or Blackberry or have any other computer security issue.

Communications Representative:
Mary Jane Rogers 415-555-0166
Refer all Media requests and questions to your local communications representative.
Evacuation Route – Building 1

Digiknight Building One – Evacuation Route
Natural Disasters

Earthquakes

Things to know and do before hand
An emergency kit should be prepared with non perishable food items (canned food, sugar, chips, rice, peanut butter, etc.), water, flashlights, portable battery operated radio, batteries, medicines, first aid kit and clothing.

All the safe spots throughout DigiKnights should be located and checked periodically. Safe spots include spaces under sturdy desks and tables or against interior walls. Alternatively there are places to avoid in the case of an earthquake, which includes spots near mirrors, hanging objects, fireplaces and tall, unsecured furniture. Water heaters, major appliances, heavy furniture, hanging plants, mirrors, picture frames will need to be properly secured. Roofs, walls and foundations will need to be checked regularly for stability.

To ensure that everyone is safe a buddy system will be implemented. Generally each person will be responsible to locate two other members within their area and if that person cannot be found one of the crisis management team members needs to be contacted.

What to do during an earthquake
If you are indoors during an earthquake you should stay indoors. Get under a desk, table or stand in a corner as soon as you can. Do not under any circumstances use an elevator during an earthquake. Corners with windows need to be avoided. If you are outside during an earthquake get to an open area away from large objects such as trees, buildings, walls and power lines. After you are in a safer location like the ones described above crouch and cover your head and neck with your hands and arms if possible.

After an earthquake
After the tremors have subsided do not use the phone unless needed for a life threatening situation. Using telephones after a natural disaster ties up lines for those needing medical services. Walky-talkies are inside local equipment storage areas to ensure everyone is accounted for throughout DigiKnights. There are portable radios in the emergency supply storage areas after the tremors have stopped they will be turned on and any advice or instructions given to the public from public safety officials need to be followed. It is important for everyone to be prepared for aftershocks as well.

The damage assessment team has responsibilities to ensure the continuing safety of all employees and persons at DigiKnights. The tram includes damage assessment team members are Mark Saunders, Alicia McKellips and Carlton Smith. If the members of the damage assessment team are unable to fulfill their duties due to injury or any other reason Rod Hatherly, Lorna Hastings, Jessica Talen, Kurt Goassard, Lance Addams, Allison Bell and Kevin Albright can step in to perform the duties outlined below. The damage assessment team will check for downed power lines or exposed live wires, tape off these areas with caution tape and inform others to
steer clear of these areas. The damage assessment team will next check the building for cracks and damage, which will include the roof and foundation.

Certain procedures will have to be followed if there will be any animals in the building such as service dogs. In the event that there are any service animals within the building food and water will have to be kept for them in the emergency storage areas. Additionally a working can opener has to be kept in the closets. It is important that they stay away from contaminated waters and spilled chemicals such as anti-freeze. First aid kit items may be used to treat any injuries on these animals.

**Wildfires**

**What to know and do beforehand**
This section covers information and procedures relating to wildfires. Flammable items such as newspapers and other trash items need to be disposed of regularly to avoid unnecessary hazards. If any hazards exist that could cause a fire are spotted in proximity to the DigiKnight offices they need to be reported to officials as soon as possible. Proper officials may be able to eliminate or reduce the associated risks. If propane tanks need to be used for business purposes they will need to be stored at least thirty feet away from the building. Any vines that grow along the DigiKnight building exterior will need to be cleared regularly. If there are any branches on power lines they power company will need to be notified to clear the hazard.

Parents and legal guardians please note that you should **not** leave to pick up children while school is in session. The school districts will evacuate them safely to shelters and evacuation sites. Going to pick them up will only lead to confusion, traffic congestion and will reduce the safety for everyone. For added safety before a wildfire breaks arrangements should be made with other family members and neighbors to evacuate children and persons with special needs while you are at work and school is not in session.

Evacuation routes should be mapped out before a wildfire occurs for safety reasons by the evacuation and shelter team. Several routes should be chosen, the more the better to ensure the safety of everyone. The conditions during the wildfire such as wind and public safety broadcasts will determine which route should be taken to safe sites.

**What to do if a wildfire is threatening the surrounding areas**
One of the crisis management team members will need to turn on the exterior lights. If it is feasible to do so members of the crisis management team that are skilled in doing so will need to turn off propane gas services in the building. Radios will need to be turned on and any notice given by safety officials to evacuate the area will be followed. Everyone will need to be prepared to evacuate immediately if necessary. Michael Winters and Michael Churchill are responsible for leading all persons at DigiKnight through evacuation procedures after it is deemed necessary to do so. Michael Winters and Michael Churchill will also be responsible for finding adequate transportation methods to shelters and evacuation sites.

If evacuation is necessary the evacuation and shelter leaders will escort everyone out of the building into proper transportation. It is important that employees have medications and medical supplies that are necessary for them on hand. Safety officials may advise to tie a white towel or
white cloth to the front doorknob so that rescuers know that the area has been evacuated, if such
directions are given then the evacuation and shelter team leaders will do so. After everyone is
safely into the selected mode of transportation a route away from fire hazards will have to be
chosen. Watch for changes in the speed and direction of the fire and smoke.

**Tornado**

**What to know and do beforehand**
Tornados occur have occurred in every state and may occur at any time. However tornados
usually occur during the summer between the hours of 3:00pm and 9:00pm. It is important to
note that tornados may be nearly transparent until dust and debris are picked up, so it is
important to be cautious around high wind conditions. The nation weather service will announce
tornado warnings. Much of damage and injuries occur when wind gets inside a building through
a broken window, door or damaged roof. If a threat occurs it will be important to board windows
and doors.

It is important for the crisis management team to find the lowest point in the building away from
windows and glass so that all in the building during a tornado situation may get to that
designated area. A small area like a closet is usually the best however not everyone within the
building will be able to safely fit in these areas. The center of the building is also a safer place.

**What to do during a tornado**
Safety is always the first concern. The radios will need to be listened to for warnings when there
are very high winds, large hail, cloud of debris, funnel cloud, roaring noise, severe thunderstorm
and or a wall of clouds. It has been said that an approaching tornado sounds like a freight train at
times. It is important to stay away from windows and glass during tornado warning times. If no
evacuation is advised or necessary then everyone is to move to the lowest part of the building
away from windows and glass. Staying under sturdy piece of furniture such as a desk or table is
also a safer option. If you are under furniture use one arm to hold the furnit
ure down and the
other arm to cover you head and neck from flying objects and debris. If there is no furniture for
you to hide under use your arms to cover your head and neck.

After the tornado has passed continue listening to the radios for updates on conditions and road
blocks. All those with proper experience or training should help those who have been injured or
trapped under debris. However do not move serious injured persons because this may only
further injury. If there are severe injuries call for help.

The damage assessment team will step in to perform various tasks after the tornado has passed. It
is important to use extreme caution when entering damaged areas. Sturdy shoes are needed for
moving around after a tornado because cut feet are the most common injury after a tornado. Use
battery powered flashlights because a fire hazard may occur using interior lighting. Be on the
lookout for loose plaster, drywall and ceiling that could fall and injure. Look for fire hazards in
the immediate area. Broken and leaking gas lines and damage to electrical systems are the
common causes of fires after tornados. Additionally fire is the most common hazard following
natural disasters. Make sure to clean up any spilled chemicals such as bleach and detergents.
Looking for electrical system damage is important, common signs of such damage are broken or
frayed wires, the smell of burning insulation. If any of the above warning signs are present turn
off the electricity at the main fuse box, however if water has to be crossed to get to it call a professional first.

Flash Flood

What to do and know before a flash flood
Floods may occur at any time in the bay area. Summer and fall are peak flooding times for California. Flash floods generally occur with six hours of rain fall or if a dam or levy fails. The intensity of rain and the duration of rain are factors in flash floods. Downspouts and rain gutters need be regularly cleaned and cleared because this will prevent misdirected flooding. Floods have several dangers associated with them including that they can roll boulders, destroy buildings, tear out trees, damage or destroy bridges and more. If severe rains are present and persistent use the radios to listen for alerts of flooding in the area. Before the flood becomes critical it is advisable to fill sinks and water bottles with clean water for additional supplies. Water may become contaminated and undrinkable after flooding.

What to do during a flash flood
Before water becomes an evident issue, plug water faucet with corks. If there is a threat of a flash flood then everyone needs to move to high ground immediately. Even if the water rises slowly, the pressure and force of the water can be dangerous and overwhelming. The most dangerous thing that can be done once water is present is to try walking, swimming or diving though the water. Remember only two feet of water will carry away a vehicle. Listen closely to the radios or additional information and updates.

If local authorities deem that evacuation is necessary then the evacuation and shelter team will step in and take action. It is important that employees have medications and medical supplies that are necessary for them on hand. After everyone is safely into the selected mode of transportation a route away from flooding and debris needs to be chosen. Roads and areas with dips, low spots, washes and canyons should be avoided. Do not under any circumstances attempt to cross flowing streams on foot or by car, this is how the majority of fatalities relating to floods occur.

Hurricane

What to do and know before a hurricane
Hurricanes or tropical cyclones are rare in the bay area of California but do occur and can be very dangerous. Regularly removing debris from the exterior is essential to prevent injuries during high winds. Downspouts and rain gutters need be regularly cleaned and cleared because this will prevent misdirected flooding. Supplies to board up windows and other glass should be kept on the property, many injuries occur during hurricanes due to broken glass. Before the hurricane becomes critical it is advisable to fill sinks and water bottles with clean water for additional supplies. Water may become contaminated and undrinkable after flooding.

What to do during a hurricane
During a hurricane the portable radios need to be turned on. The conditions may and very often do change very quickly in direction, intensity and speed. Any advisement needs to be taken from local safety officials. If no evacuation warning is issued it is important to stay indoors, ideally on
the first floor away from windows, skylights, doors and other glass. The crisis management team needs to make sure everyone is away from the above mentioned areas for safety reasons.

If evacuation is necessary the evacuation and shelter leaders will escort everyone out of the building and into proper transportation. It is important that employees have medications and medical supplies that are necessary for them on hand. If it is safe to do so the water and electricity should be shut off by properly experienced personal.

**Basic and Quick Emergency Supply Checklist**

- Portable, battery powered radios and or televisions
- Flashlights
- Extra Batteries
- Supply of medications
- Matches in a waterproof container
- Signal Flares
- Maps of the area
- First aid kits

**Man-Made-Based Threats**

**Generic Man-Made-Base Threat Memo**

Dear,

In the event of a man-made-based threat the testing team has created a disaster recovery plain. This plan is going to address why these are threats, what types of threats, the likely hood of this threat, and how would we recover.

The reasons man-made-based is considered a threat is because of the nature of our records. Our records contain many different aspects of our companies, and other companies as well. We currently have games that are in production, but not released to the public. All of this information is secured in a safe location, but people have access, and the possibility of another corporation’s action might affect us as well.

The types of threats range from the extreme to the less extreme. Keep in mind that anything can happen. The types of man-made-based threats are as followed:

- Bomb Threat
- Power Outage
- Evacuation
- Biological Threat
- Sabotage

- Riot
- Chemical Spill
- Computer/Data/Network Outage
- Employee strike
- Etc…

After assessing the list of potential types of man-made-based threats I see many possible types of threats. These threats have the possibility of majorly disrupting the operation and productivity of our products. These test that will be conducted will assets our systems, plans, and policies in place to prevent these types of threats.
Sincerely,

**Bomb Threat**  
*Situation Background and Exercise Scenario*
During the previous week, DigiKnight has received several bomb threats. The administration office (Building 1) has received the calls, and the employee answering the phones has attempted to ask the caller about the time and location the bomb will go off. The caller has not relayed any specific information, other than the saying it will happen soon. The caller seems more agitated with each call. Following each threat, the authorities were contacted, the building was evacuated, and the facility and surroundings were searched but no explosives were detected. Each call has been made from a different payphone and police have not identified any suspects.
In the afternoon of day 12, the employee in the administration office notices a suspicious package underneath one of the chairs. The employee notifies his/her supervisor, who then notifies security. Security calls the police officer who has been assigned this case following the previous threats. Security instructs all employees and personnel to evacuate the building. During the evacuation process, and prior to the arrival of the bomb squad, an explosive detonates in the administration office.

Prior to the explosion, some of the employees were able to exit from the lobby. Most of the people towards the back of the building, including both staff and personnel were able to make it out. In the administration office, the explosion destroyed the west side of the building. The explosion and resulting debris injured and trapped many people still inside the building. Debris from the explosion also hit some personnel and staff as they were walking out through the main entrance. The electrical panel in the west storage room was damaged as well, so the power has gone out.

Those who are able to, make their way outside and gather together to meet at the designated assembly/safe haven site. The other two buildings are evacuated as well. The police are delayed in responding, partly due to a major accident on the freeway nearby, but also due to a decreased sense of urgency because of the previous false alarms. The fire department has not yet been called. The managers must launch Incident Response commands and begin emergency response activities, including communicating with the Incident Response team members, calling authorities to alert them of the developing situation, helping victims who are trapped inside the building, and treating the wounded.

Police and fire officials do not arrive until after the response activities are well underway. They must link up with the Incident Response Team to be briefed of the current situational status.

**Exercise Directions and Approximate Timeline – FOR EMPLOYEES**
- Pre-exercise briefing
  - Introduction of facilitators and observers
  - Orientation (*example*: use of note cards to denote damaged areas, tags to be pinned on injured staff, and paper people to represent patients)
  - Instructions:
The uninjured staff must evacuate the building, regroup, call Security and/or 911 for police and fire response, and launch the appropriate Incident Response Team and emergency response activities. Make use of skills learned in previous emergency preparedness trainings and mini-drills.

- Expected time to complete: 30 minutes

- Exercise role play will begin, with the employee noticing the package under the chair.
  - Staff will resume their routine work locations.
  - Expected time to complete: 1 hour

- Following the completion of the exercise, the staff will return to the conference room for a round table discussion.
  - Expected time to complete: 1 hour

Additional Details of Scenario – FOR FACILITATORS

- Employees in the building were helping facilitate the evacuation and were caught still inside at the time of the explosion.
- Staff were injured and trapped in the administration office on the west side.
- The remainder of the employees and personnel were in areas further from the detonation area where the damage was less severe. Some are trapped by rubble and debris, but others are able to either get themselves out or help one another to the emergency exit at the front of the building.

Number of People in Bomb Threat Scenario – FOR FACILITATORS

<table>
<thead>
<tr>
<th>Department</th>
<th>Number of People in Initial set up</th>
<th>Remaining Inside After Explosion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sales</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manufacturing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Research &amp; Development</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintenance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Marketing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shipping</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personnel</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Checklist and Approximate Timeline of Events – FOR FACILITATORS

<table>
<thead>
<tr>
<th>TIME (Expected)</th>
<th>DRILL TIME</th>
<th>Action Completed</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Assumptions

- The timeline will be accelerated to fit into the allotted drill time period. Times in the timeline will be adjusted to fit accelerated timeline and exercise times during the drill.
- The plan may call for movement of resources and equipment. These actions may be simulated with no actual movement during the exercise.
- Exercises will incorporate conversations with and arrival of police, HazMat, and fire, but these departments will not actually take part in the role playing.
- Phone calls will be part of the exercise, but some will only be simulated:
  - Calls to the police and fire departments will not go through (act out the call only)
  - Calls to notify the manager and security will go through
- The power will not actually be turned off, but participants should be expected to use flash lights and other equipment in order to simulate a power outage in the building.

Stress Memo

Dear,

When looking at the human factor of security, efficiency, limits, and human’s adaptive nature. We can come to a conclusion that we make mistakes. This is a problem. It is extremely important to protect and plan for anything. While creating the disaster recovery plan we discovered that many people in the company did not know what was going on. This in turn caused fear. This fear affected their working causing mistakes, and resulted in undue stress.

We as a disaster team could not overlook this, and we decided to look into this matter. In turn we created a survey. This survey asked various questions pertaining towards work, home, and other matters. The result from this survey was stress. The test showed home matters are 40%, other matters are 50%, and work was 10%. These undue locations of stress are not good in a working environment. Digiknights should implement a counselor.

This counselor will be on site twice a week to discuss issues either group format or individually. This is just another service that will allow employees the ability to vent out the stress. In turn this will allow a happier environment and more productivity. Keep in mind if a major disaster happens we will consider having the counselor onsite more often, and when it dies down we will return to regular schedule.

Due to these finding I hope you will carefully consider these points made in this memo and authorize having a counselor twice a week onsite to help employees. Remember our employees are like family.

Sincerely,
Recovery Team Memo

Dear,

Over the last fifteen weeks the disaster recovery team composed of three people has researched many different aspects of the company. This was then compiled into a functional disaster recovery plan in which it has been implemented. Keep in mind this document requires to be updated.

As the disaster recovery plan progresses forward towards completion. I suggest that the team not being broken up. In the past 15 weeks these three people have learn about the whole company, geographical issues, natural issues, etc… The experiences and knowledge gained from creating this document is invaluable in keeping this document up-to-date, and this knowledge will allow these updates to be preformed at a quicker rate.

While looking at this in another perspective Digiknights is taking individual from various departments. In turn this is taking there expertise away from there department. This might be causing slower production and loss of money. So it might be smarter to higher a less experience employee to perform these ongoing changes.

This route might be effective, but at the same time it might cause issues within the documents that may cause conflicts with the company. The lack of knowledge and experience might be the issue. This individual may disrupt other department for information or disrupt the creators of the document for information. In turn may cause issues within the company.

Keep in consideration that the workers of our departments have shown the ability to function without the constant overseeing of the managers. This just shows that the time to update would not take a large amount of time, and Digiknights would be able to function just fine.

In conclusion I would see no change in our productivity or quality of our product by keeping the original disaster recovery team. These individual also have established themselves within the company for a long term period with the company. I would strong suggest keeping these individual for updating the disaster recovery plan.

Sincerely,

Mudslide Test
The test is a simulated scenario. To insure correct predictions and response the test will be performed as followed:

1) Schedule a date/time to meet with CEO of Digiknights Inc. This meeting will address taking manages away from daily responsibilities to conduct test, and all material needed for test. Even though this is a test it must be conducted as if this would happen to get best results. Get confirmation to begin.
2) Contact all managers involved through e-mail including date, time, place for meeting. In this meeting we will discuss the test. Confirm all information on times, dates, and responsibilities. If a manager does not show then contact through phone, and discuss.

3) Within one week time manages must show research all information found on topics assigned, and present information to group. This will be open for discussion and all information chosen to keep will be for reference for test.
4) Prepare all supplies for test. This test will be preformed in controlled environment to simulate mudslide.
5) Setup test.
6) The test will be preformed. This test will be recorded for archive and reference purposes. There will be discussion afterwards that will address all pros and cons of the test. The disaster recovery documenter will be present to review, and add/change anything to the emergency procedure.
7) There will be a debriefing. The final report will be given to the CEO. If this is approved it will be implemented.

Plan Distribution Analysis
Disaster recovery plans can be distributed in many ways; some examples include Intranet, web server, CD-ROM, USB Drives, network storage and paper copies. After the plan is created it is important to have a way to keep each person with an updated copy. More than one copy can cause problems as an outdated plan could be used when a newer plan exists. This section will go over the advantages and disadvantages for each of the ways to distribute disaster recovery plan and then propose a method that will work for DigiKnight.

Hosting the disaster recovery plan on the web server would be one of the least secure ways to store the plan. It would also be more accessible in the event of an emergency unless the disaster was wide spread and affected the web server. Team leaders would need a laptop, hand held device or such to make it possible to connect to the web server and get the updated plan. In addition to needing a computer it should be realized that it would take much more time to connect to the web server than using another storage device.

Distributing the disaster recovery plan by means of the DigiKnight Company Intranet would make the document accessible from inside the internal network. The company Intranet would be great for central accessibility of the documentation, also access controls are built into IIS (supposing that is what DigiKnight uses for their Intranet), and makes updating the document very easy. Notifications of changes made to the document can be configured so all users of the document will be notified for each update to the document. Disadvantages of the Intranet include limited to no access when the servers go down. Security still isn't up to par especially if there are users who have access to the Intranet from home.

Distribution by the use of CD's would be cheap considering the cost of CD's to be $0.25 each. Keeping them updated would be difficult, old copies on non-rewritable CD's will need to be destroyed to avoid multiple copies from floating around. CD's could be easily accessible especially during network outages as long as there is a computer that can read them. Portability
of the document is lost unless a laptop is used or if a paper copy is printed. Depending upon the
disaster a computer and printer may be hard to come by in an emergency.

USB drives would be more portable than a CD; the whole stick could be encrypted to avoid
leaking out important company information. USB drives can also be much faster than writing to
a CD. The disadvantages of using a USB drive include higher costs, and similar to a CD a
computer would be needed to read the documentation. Portability is lost unless a laptop will be
carried around in the disaster.

Network storage is another option which would give central access with tighter controls on who
can see and edit the disaster recovery document. Track changes can be done with a word
document, thus enabling people to scan the document and see recent changes. Unlike the Intranet
network storage wouldn't give users notifications when the document was modified. Portability
would be non-existent until copied to a disk or printed. Track changes would be generic and
would not identify which user made the change.

DigiKnight could also use a wiki for making changes to the disaster recovery document. The
advantages to using a wiki include all changes are tracked by each user, each page becomes a
link and the whole document can be linked together or the whole document can be on one page
and each heading is part of the outline or table of contents. The wiki can also be restricted to
certain users who can view and others who can view and edit. The disadvantages are each user
might need to be trained on how to use the wiki because formatting doesn’t come as easy as a
simple word document.

Paper copies could be located in easily accessible locations, and wouldn't require a computer or
network access. Paper copies could be printed on color paper and changed as the version
changes. The color of the paper would help clarify which version the paper is as well as help
confirm that the correct paper is being used. Between the version number of the document and
the color it should be fairly clear which version is in the person’s hand. In general it seems like
the best option. The disadvantages to a paper version are paper is easily destroyable, easier to
share with those who shouldn't have access, and might be just as hard to find. To overcome these
obstacles the paper copy could be stored in a weather tight safe. The safe could protect it from
damage unless the building can't be entered, and another copy would also need to be at the warm
site in a safe.

Overall look at the distribution options:

<table>
<thead>
<tr>
<th>Options</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web server hosting</td>
<td>Accessibility from any internet connection.</td>
<td>Not secured, more time than other options.</td>
</tr>
<tr>
<td>Intranet posting</td>
<td>Accessibility from inside the network easily modified and notifies all users.</td>
<td>Somewhat secure, no access if the company servers go down.</td>
</tr>
<tr>
<td>CD</td>
<td>Cheep, easily accessibility</td>
<td>Hard to keep updated, low portability of the documentation &amp; the need of a</td>
</tr>
<tr>
<td>Paper</td>
<td>No computer or network needed and would provide answers quickly. Also highly portable.</td>
<td>Easy to destroy or pass along to wandering eyes.</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>USB</td>
<td>Highly portable, Can encrypt the whole stick.</td>
<td>More expensive storage &amp; the need of a computer.</td>
</tr>
<tr>
<td>Network Storage</td>
<td>Centrally accessible, easily secured</td>
<td>Not portable, no automatic notification when changes are made.</td>
</tr>
<tr>
<td>Wiki</td>
<td>Track changes by user, headings automatically become links in a table of contents, and restrict users.</td>
<td>Training would need to be done.</td>
</tr>
</tbody>
</table>

Computers might or might not be available during a disaster. Even if they are it might be so difficult to look at the plan that a paper copy will be needed anyways. In lieu of this dilemma one or two paper copies could be distributed to each team, and backup copies could be located in the weatherproof safes. It may prove to the demise of DigiKnight if the only copies of the disaster recovery plan were on the wiki or USB drives and they couldn't be accessed for one reason or another. The DigiKnight disaster recovery team has considered storing the disaster recovery plan on the website for remote access during network outages but due to security risks of the plan leaking out the team has decided against storing it on the web server. CD’s were ruled out only because USB drives would be more portable and secure. Network storage is a great backup because a word document is easy to modify and the folder could be secure. Intranet posting is similar to the network storage and would be nice but not necessary. The Wiki seems to be the best digital way to store the documentation because it is easily edited, stored, secured and has a great feature of creating a table of contents. The ability to search is a great feature for editing the documentation. Training will need to be scheduled as necessary to make sure the document retains similar formatting as changes are made.

Proposal for Distribution of the DigiKnight Disaster Recovery Plan:
The DigiKnight disaster recovery team proposes to have a digital copy of the disaster recovery plan kept on the company wiki. The wiki will only be accessible by the Chief Executive Officer, members of the disaster recovery team, the recovery management team, the damage assessment team, and the evacuation and shelter leaders. Most disasters may consist of network outages, to facilitate the accessibility of the recovery plan an electronic version will be on an encrypted thumb drive. One USB drive will be given to each team leader. In addition a paper copy of the most current version will be printed on the current color of paper and given to each team. Two backup copies will be stored in the fireproof safe in the DigiKnight administration building, and in the fire proof safe at the warm site.

Summary of proposal
- Main copy kept in the company wiki which gives central access and control.
- Paper copy placed
With each team
Company headquarters weather proof safe
Warm site weather proof safe
- Encrypted copy on thumb drive for each team leader.

Those who will get a copy of the documentation:
Company Executive:
- CEO-Carlton Smith

Disaster Recovery team:
- James Tanner
- Sandy Smietanski
- Noel Richardson
- George Wallace

Damage Assessment Team:
- Manager of Administration-Mark Saunders
- Manager of IT-Alicia McKellips

Evacuation & Shelter Team:
- Evacuation & Shelter leader-Michael Winters
- Evacuation & Shelter leader-Michael Churchill

Crisis Management Team:
- Manager of administration-Mark Saunders
- Manager of Manufacturing-Linda Kraemer

Document Revision
The Disaster recovery document is a living document and as such must continually be modified as changes occur to the business. If DigiKnight expects to succeed in an emergency it is advised to update, test and revise the document on a continual basis.

The first question that comes to mind is how will revisions be maintained? A team of editors will gather the information and keep the plan up to date. It is proposed to have the team of editors be the same people who helped create the document. Familiarity with the document will greatly enhance the ability to make changes where appropriate, without consuming excessive amounts of time. The information will be gathered from a bunch of sources including the company directory, departmental changes, mergers and acquisitions, and other relevant information. This information will typically take a while to get to the editing team. Processes will be put into place to forward this information to the editing team. The forwarding will typically consist of a brief meeting where materials are exchanged and gone over to make sure that the disaster recovery plan will include the most relevant data and to ensure the information will be incorporated in a manner that would help the company in the unlikely event of an emergency. The next level of ensuring the plan is accurate is testing. The plan will be tested and gone over per the instructions in the simulation testing sections.
Revisions should be made not only after changes have occurred in the company and made it to the editing team but within 15 days of each testing of the plan. Information will be fresh in the minds of those who participated, and feedback will generally be addressed and built into the documentation. For more information please refer to the testing section.

Keeping the disaster recovery document current is a top priority. Each copy will be kept current by replacing them quarterly or as often as major changes have been made. The old paper copy will be destroyed, and replaced with the new document. The thumb drives will be rotated to keep the copy of the document current. To save time team leaders will be encouraged to update their copy from the network drive. If after a weeks notice the USB drive still isn't current then the editing team will replace the document on the USB drive. The document will have the version number on the main page as well as a part of the file name. The naming scheme will be BCDRDDMYYR#.pdf replacing the # sign with the current version number. Each time the revision is complete a PDF version will be saved thus preserving each revision while allowing the original document to be edited for the next revision. Saving to PDF will keep the USB drive copied from being changed, and losing important changes. All changes will be made to the disaster recovery plan on the company wiki. The editing team will update the information and then distribute the document to each safe, at both locations. The USB drives will be updated and the wiki will note the new color and version number on the front page.

**Summary of Revisions:**
- Continually being revised
- Revisions come from
  - Company directory
  - Departmental changes
  - Mergers and acquisitions
  - Other relevant information
- Problems incurred during testing
- Old copies destroyed
- New copies printed on current color
Conclusion
In summary the following are the breakdowns for the IT and technology-based threats analysis:

High risks include workstation failure, equipment reconfiguration, data loss, data corruption, and data security breaches, and wireless vulnerabilities. Medium risks include server failure or damage, switches, and printer problems. Low risks include T1, Production line equipment, cabling, and hand held device connectivity. Risks we will not discuss include bugs and glitches in system, and hand held device connectivity. As previously discussed the company would have adverse affects for many of these problems especially if they were to happen to the company.

The following is the prioritized list of important technology components at DigiKnights (with the number one being the highest priority):

1. Production line equipment
2. High speed printer
3. Servers
4. Workstation's
5. T1, switches, cabling, and other network infrastructure.
6. Data integrity
7. Software Bugs and Glitches, and Wireless Internet access.
8. Hand held device connectivity issues.

After reviewing that list it looks like the top four items are interchangeable because without one or the other they wouldn't work as easily. Production line equipment and high speed printers create the end product and get the product out the door. If the servers and or the workstation's go off line then it would be harder to print the owner’s manuals as well as send disk jobs to the production line equipment. This difficulty could easily be overcome with direct connections between the workstation and the printer and production line equipment although not optimal it would get the product out the door, and minimize the impact of the disaster.
References


http://www.calessar.org/index.html


