Final BCDR Plan

Adalberto Ruiz

Allan Wheelock

University of Advancing Technology

 BCDR & Incident Response Computer Forensics and Crisis Management -

Incident response, business continuity, disaster recovery, computer forensics, and crisis management all tie closely together and support one another throughout each malicious attack and there are many reasons why this is an industry-standard of today. To start off the first step before any of these is that you have to be ready for any type of attack. No matter the size of your company, there will always be cybercriminals looking out to attack even the smallest business’. The reason small businesses may be a target to these criminals is because these small businesses typically tend to be much less secure. This allows the criminal to access possible login credentials, customer data, sales data, and lots more much easier as opposed to larger targets.

 Incident response is typically defined as a term that describes the process of a group of trained individuals who handle cyber-attacks and data breaches. Business continuity is crucially as important as incident response. The reason business continuity is so important is because with services going down, your business may be at risk of losing money as well. If you’re an online-based site and somehow your website gets taken down, your potential customers will have nowhere to make purchases or get into contact with you outside of the site. Inevitably this leads to exponential money loss. While business continuity’s focus may be to keep business operations up and running, incident response ties in closely due to their job being to find a solution to the problem. These two rely on each other because one is actively trying to keep everything up, while the other is trying to stop what’s going wrong within the business.

 Disaster recovery is an attempt to recover as well as protect a business's IT infrastructure after an attack. Something a disaster recovery team member may do is attempt to regain access to data, hardware, software, networking equipment, as well as power connectivity. The basic three-step disaster recovery phases include assessment, restoration, and recovery. Business recovery ties into business continuity because depending on what damages were assessed during the evaluation, some customers may have to be contacted depending on if their personal information was leaked during an attack. Another reason disaster recovery ties into business continuity is if there was a ransomware attack. During the assessment phase, the question of whether or not you’ll have access to the data after the ransomware attack typically depends on if you want to pay the ransom, especially with sophisticated cybercriminals. The reason this ties into business continuity is because you have to ask yourself, what parts of the data do I still have access to that my customers need? Some customers may completely leave if you lost some of their valuable data which directly damages business continuity. You may also have to spend more “man-hours” on recovering data also directly hurting business continuity because there’s no proactive progress being made towards the business but instead, you’re trying to recover lost damages.

 Computer forensics examiners usually search through existing data, previously existing data, as well as deleted data. These examiners may also have the skillset to look at damaged hardware. Computer forensics may be able to help out disaster recovery because they may be able to bring back some of the encrypted data during a ransomware attack. In some cases, these computer forensics specialists have also been known to be able to decrypt locked data entirely. Inevitably recovering data after a ransomware attack directly helps disaster recovery significantly. This helps them recover much faster and they’ll be able to do other things while the incident response team is actively ready to deal with the next event.

 Crisis management plays an essential role in any devastating situation. The main reason for this is that people tend to make more mistakes under pressure. If you have a proper crisis management plan, you’re more likely to find the solution sooner as opposed to not having one. Crisis management plans also help everyone understand what to do if a situation such as a cyberattack were to occur. This also helps outline the do’s and don’t’s during a real crisis, meaning there’s less of a possibility that people panic causing another possible crisis or setback. This is how I perceive and understand how incident response, business continuity, disaster recovery, computer forensics, and crisis management all tie together closely definitely helping and benefiting one another.

Man-Made Threats:

Man-made threats vary from company to company. This all depends on whether or not your company is virtual, in an office space, or a warehouse. Another factor that plays into a threat is the type of company you are. If your company is virtual and dealing with a customer’s sensitive information, the biggest man-made threat is an employee releasing your customer’s information. This serves the biggest threat due to potential privacy issues and most importantly HIPPA regulations if you are dealing with a customer’s health information. It’s undeniably one of the biggest threats because it could lead to a million-dollar lawsuit which can potentially leave your company in debt. While it’s very unlikely for your company to face a lawsuit, it is very likely for your employees to potentially leak sensitive information carelessly as we are human and we all make mistakes. Other less threatening man-made threats include potential workplace disagreements. Workplace disagreements can be severe or minimal. The scope of this threat ranges from assault to a political disagreement. Workplace disagreements can be found between your business partner employees and employees of your own. This will inevitably slow your business down and make you lose a couple hundred to thousands of dollars depending on how big of an impact the employees make on the company, and depending on how big of a workaround you’ll have to make for this threat. This happens daily, especially with a large number of employees leading this to be a very likely event.

 IT/Technology-based Threats:

IT and technology-based threats can be very devastating. These undeniably have the biggest impact on your company due to the severity of the incident. The biggest threat is a ransomware attack. Depending on how much of your network ransomware attack imacted, it can completely put your organization on hold. Ransomware threats can be measured through training as someone unfamiliar with technology will have a more likelihood to fall for phishing scams. This will can potentially prevent your employees from logging in, customers from placing orders/using your website, and even completely encrypting all your data. While this threat isn’t very likely, it does have the most impact on your organization. Smaller less impacting technology-based threats can be basic IT issues. This can range anywhere from having trouble at a computer, having an employee or customer locked out of their account, or even needing to do maintenance on your systems or machines. While this may not have a massive impact or revenue cut on your company, it is very likely to happen. There is little to no organization that has never gone through IT issues making this an absolute expectation within any business. Basic IT issues can result in affecting your suppliers too. If an inbox isn’t properly set up, you may lose a potential order, a shipment, or even a supplier shipment update. This is also impacted by your employee’s tech skills, which can be preventative or detrimental depending on how much technology and volume of IT issues there are in your organization.

 Natural Threats:

Natural threats are very unlikely to happen; however, they can be extremely costly and devastating to your company. The most severe natural threat to a company is natural disasters. Natural disaster threats are something that is completely out of your control. Natural disasters threats include hurricanes, tsunamis, tornados, floods, and other threats caused by mother nature. Depending on the severity of the natural disaster, it can cost thousands to millions of dollars. A severity one tornado can completely destroy your physical employee building, while a false alarm will only affect one workday for employee safety until the warning is called off. These threats impact customers, suppliers, and employees due to the severity of the threat. Natural disasters have a very small chance or likelihood of impacting your organization; however, they do pose the biggest threat. Other examples of natural threats that are bound to potentially happen are power outages and plumbing issues. I categorize these man-made luxuries in life under natural threats because they’re something everyone has to face, and these have become a natural part of everyone’s lives in today's world. You’re unable to control power outages or potential water issues; however, there are potential workarounds when you do come across these. The likely hood of a power outage happening once, if you don’t have backup generators, is inevitably going to happen maybe once in a few years to a decade. This will put a hold on your business if they do occur impacting your customers and potential suppliers if communications are lost.

Mission-critical business function:

There are mission-critical business functions within a company. These mission-critical business functions allow your company to proceed smoothly; however, in a case where there is an impact on these functions, your business is at great risk. An example of this is your email system. If your email systems are to ever fall, you’ll lose a great portion of communication throughout your company, business partners, and clients. Since email is the main source of business communication today, you’ll begin falling behind with your business plans. This has a major impact on your company with the loss of this function. The maximum recovery time could be one to two days depending on if the domain’s hosting servers were impacted with either data loss, power loss, or system upgrades. The recovery time for this is typically a couple of hours; however, it could last days depending on what the issue was with the host. If your business or organization is a call center or a support center, a major mission-critical business function loss is the phone systems. If you lose your phone system, the entire point of your organization is completely shut down. This will end in communication loss with your entire customer base, and if you’re contracted as a business partner with another company, you’ll most likely be replaced. This is a major threat to your business as it has a major impact on your business clients and customers. Typically, this issue takes a few hours to resolve as there are workarounds. This isn’t necessarily one of the biggest threats to a company if you have a business continuity recovery plan. One easy workaround is to use phone systems through your company computers. This is a solid backup as you don’t have to rely on landlines if your phone systems ever fail. There won’t be too much of a financial impact to fix as it’s typically an easy fix; however, there will be a much greater financial impact to the business area as you’re losing business partners and potentially missed calls from clients.

 Environmental/Infrastructure Threats:

Environmental threats are very unlikely to happen; however, they can be extremely costly and devastating to your company. The most severe environmental threat to a company is environmental natural disasters. Environmental natural disaster threats are something that is completely out of your control. Natural disasters threats include hurricanes, tsunamis, tornados, floods, and other threats caused by mother nature. Depending on the severity of the environmental natural disaster, it can cost thousands to millions of dollars. A severity one tornado can completely destroy your physical employee building, while a false alarm will only affect one workday for employee safety until the warning is called off. These threats impact customers, suppliers, and employees due to the severity of the threat. Natural disasters have a very small chance or likelihood of impacting your organization; however, they do pose the biggest threat. Infrastructure threats will also have a major impact on your organization. These include man-made luxuries in life under natural threats because they’re something everyone has to face, and these have become a natural part of everyone’s lives in today's world. You’re unable to control power outages or potential water issues; however, there are potential workarounds when you do come across these. The likely hood of a power outage happening once, if you don’t have backup generators, is inevitably going to happen maybe once in a few years to a decade. This will put a hold on your business if they do occur impacting your customers and potential suppliers if communications are lost. The cost of each infrastructural threat typically are cheap fixes. These fixes usually don’t go higher than $1,000 since it’s been around for years, and anyone in the industry is able to troubleshoot the issues found. This, however, is not always the case where an entire system needs to be replaced. If the entire sewage, water, electrical, or air conditioning system must be replaced, it will be in the thousands of dollars category.

Mission-critical function (non-IT):

While most organizations and businesses are run online, there are some cases in which non-IT mission-critical functions will impact your business. A good example of this is if an electrical power grid system fails. This will completely put a stop to your business for a few hours until backup systems are put into place. This will cause a big financial cut as it ceases all operations within your business. Not only will it cease operations within your business, but you’re also more than likely going to have to shut down the business for the day. This is due to many factors that an electrical power grid upholds when it’s running. The most important one is you won't have any air conditioning within your business to operate. This is unsafe and can lead to a massive lawsuit if conditions are poor. It’s unsafe because employees can have a heatstroke, or begin getting sick if the conditions are very poor. Another example is the loss of emergency services communication. This poses a big threat in case of an emergency situation. If an employee were to ever die due to this, your entire business risks the possibility of being shut down forever alongside a million-dollar lawsuit. It’s essential to have emergency services communication 24/7 since employees are not required to use cellular devices in case of an emergency due to business legal reasons. The employer must have a standardized way to always have contact with emergency services. While this isn’t likely at all to happen, there is always the possibility it may. There is no financial way to recover from this situation if an employee passes while on the clock for your organization.

Insurance Provider Checklist:

* Progressive Commercial - 1-888-806-9598
* $272 Median Cost of small to large-sized businesses
* Assessment of damage: 1 million/1million aggregate. This covers the business up to $1 million for a single incident, but no more than 1 million for the policy term.
* Potential insurance coverage:
	+ General liability - is the most common business insurance coverage. This also protects against third-party bodily injuries, property damage, and personal/advertising injury.
	+ Commercial Auto - This covers making deliveries, or traveling between job sites. These overall covers any vehicles used within your business.
	+ Workers’ Compensation - Most businesses throughout the United States, require a business to have worker’s comp insurance. This helps cover expenses related to employee-related injuries while working for your organization.
	+ Business Owners Policy (BOP) - BOP is typically used when small to medium-sized businesses rent or own commercial property. This is typically done when your organization uses warehouses, office buildings, or storefronts.
	+ Professional Liability - This liability insurance type protects professional negligence claims.
	+ Cyber Insurance - This will protect against incidents such as data breaches and cyber attacks. It covers instances where you’ll need services such as investigative services, data recovery, and potential legal incident costs. Legal protection is great for managing customer data such as credit card information and social security information being lost in a data breach.
	+ Overall, this insurance provider will cover all the necessary bases for BC/DR plans, emergency contact lists, inventory lists pulled from the bank and financial records, and cover the loss of communication links.
* Some potential insurance gaps are theft. With individuals stealing from your business, it may be difficult to prove with smaller items as they’re typically distributed in bulk for various employees. This can include “lost” laptops, tablets, or even USB stored data containing crucial business information. The smaller
* Legal Counsel - CorporateFinancialInsitute (CFI) - The benefit of legal counsel is lawyers typically specialize in a single area of practice such as intellectual property, immigration, bankruptcy, and negotiation. On the other hand, legal counsels handle all legal matters within a company, allowing you to pay less, and avoid the need for multiple lawyers.

 FEMA is the US. Federal Emergency Management Agency. FEMA conducts the Threat and Hazard Identification and Risk Assessment, THIRA. THIRA is a three-step risk assessment process that helps the community understand the potential risks, and what those risks are. The three questions asked are, “What threats and hazards can affect our community?,” “If they occurred, what impacts would those threats and hazards have on our community?,” and, “Based on those impacts, what capabilities should our community have?” Fema provides National THIRA. This prepares the entire nation t to understand what risks to prepare for and how we’re able to prepare for them. FEMA provides us with Stakeholder Preparedness Review (SPR). SPR is a self-assessment of a jurisdiction’s capability against the targets and potential risks which were found in THIRA.

Notification procedure:

To start with location, I think that a backup location should be near the primary office but not too close. You want it to be away from the main office so it’s not very likely that it’ll be affected by the same disaster that brought down the primary building. But you want to make sure that it isn’t too far away so that employees are still able to get to that building without too much extra struggle. Something that would be the next town over would be more ideal. As far as personnel that would need to be there, I think it’s important to keep the essentials as the parties that get moved to the backup site. The technology we have in place for normal operation days should be portable enough that in an emergency most, if not all employees have the capability to work from home. If a secondary location is needed, only the necessary employees will be re-located to the new location. Those that can work remote should be able to work remote. To keep communication, open I think there should be an emergency phone system setup that has emergency numbers for each department. That way whoever is in a leadership role for a certain team would get calls to that number. There would also be another emergency number to a few teams. One team would be IT as there are certain to be technology issues while going through an incident. Another hotline that would need to be in place is a hotline for the incident response team. That way employees can get updates on the situation at hand and get accurate information on what’s happening, and what the plan is moving forward.

Cold Site:

A few more of the bare necessities for the organization’s budget-friendly cold site would include necessities such as air conditioning, water for employees to drink, electricity for employees to see within the building, and on-site portable restrooms to save money. These are bare necessities as they are required for basic everyday human rights. Air conditioning is required as it is used to moderate the temperature within the building. At the worst-case scenario, your employees would have to move to the cold site on a hot day as the main building is out of power. Without air conditioning you would have to send employees home as that muggy day in a hot building serves as a safety hazard. Water is required as we all need to drink water to stay alive, and there is no guarantee that every employee has brought enough water for them to drink at work to survive that day. Electricity is required for electrical devices which are used within every organization today, as well to illuminate the dark building. Since the cold site backup location is designed to be budget-friendly, direct restrooms to the drainage system are not required. Instead, portable restrooms are a suitable alternative as they are easy to dispose of and clean up after when needed, and overall save the organization thousands of dollars. This cold site was designed to be budget friendly.

Warm site:

Since warm sites are typically referred to as the in-between for hot and cold sites, this will combine budget-friendly with efficiency. Throughout this warm site, we must compensate for on-site readiness. This means all employees that have been transferred there will be fully functional within an hour or two upon arriving. Complete desks with laptop to desktop docks will be spread throughout the warm site. This allows employees to arrive, plug in their dock, and begin working as needed. The completed desk setups will include three monitors, a chair, the compatibility dock, and a two-drawer dock. These office spaces will also have a water fountain and a refrigerator to maintain the office readiness. These will avoid the need for out of the way tasks and prepare for on-site readiness such as providing the employees with water bottles or ice to refrigerate their lunches. Some bare necessities for the organization’s warm site would include necessities such as air conditioning, water for employees to drink, electricity for employees to see within the building, and on-site restrooms. Every workplace is required for you to have these; however, unlike the cold site, these are not budget-friendly options. These will have fully functional and consistently paid for utilities. There will be a full building multiple area air conditioning unit, a consistent purifying water source, full office style lighting above every desk, and actual built-in restrooms that require plumbing to the drainage system. Some of the pros to this warm backup location is it will be ready on the go whenever required, you will not need to go out to buy additional supplies, and it will be an easy an easy transition for all employees moving from the main building to the warm site. The only con there really is, is the cost of conditioning the warm location. If you want it to be ready with only needing to move employees' personal belongings into the building, maintenance fee will cost hundreds of dollars monthly. Another con to this is failures could occur at any moment. At any time, there will not be a backup phone system if the phones are down, there will not be a backup network connection if the internet goes down, and there may not even be a guarantee that all facility items will work if left to idle for extended periods of time. This is due to the environment not being the main functioning environment for your employees as a hot site alternative would be.

Create a plan to run a hot site backup location, detail what equipment and other resources are needed.

A hot site is a mirrored site of your datacenter infrastructure. In the situation that one is needed, it should be populated with servers, cooling, power, office space, as well as common facilities for the employees. This includes bathrooms, a kitchen or kitchenette for meals, and a place for them to go during breaks. The advantage to a hot site is that it has relatively no setup time. The idea of a hot site is that it will run concurrently with your main location so that you can just pickup where you left off once you arrive at the hot site. One major caveat to this is the cost. It will cost the company a lot of money to keep this site up and running alongside the primary location. I still think this is worth the cost of keeping the site running. What money you spend in keeping both sites up and running, you save in downtime and recovery from an outage.

Create a plan to run a mobile site backup location, detail what equipment and other resources are needed.

 A mobile site would be a bit more difficult than a hot site to setup. This could be interpreted in a few diverse ways. You could have a mobile site be something like a bus that you work off, or it could also be like a shipping container office space like they have at construction sites. Personally, I think the most convenient would be to have something on wheels like a bus or a trailer so that if the disaster were bad enough you would be able to continue moving the location wherever you needed to. One big problem with this is that the workspace would be exceedingly small so most employees would have to switch to remote, and only the most essential would have the space they need to work on the mobile unit. Setup would be cheap as well. If you have the bus and the equipment inside of it that you would need for those essential employees.

 Alternatively, the mobile workspace could also be a smaller off-site building like what they have at construction sites. This would not be as mobile as a bus or trailer workspace would be, but it would most likely have a bit more space on the inside for more employees. The advantage to this is that you can have more people working out of the mobile location while the incident is managed. The disadvantage of this situation is that it is not as mobile. Both mobile options will cost less than a hot site, however setup time will take longer as the sites will not be actively running in conjunction with the primary site.

Create a plan to run a mirrored site backup location, detail what equipment and other resources are needed.

To run a successful mirrored site, you must have a decent number of servers. The standards of a mirror site consist of large backup space, high-quality servers, and very high upload and download speed in case of a disaster recovery situation. A large amount of backup space is required due to many reasons. In a case where the business needs to conduct the process of disaster recovery, they would need every file and document accessible in order to do their jobs. In a case where a job is only able to recover important essential documents and templates, they may be in the case where they’d need to reach out to customers and consumers. This would burn lots of the company's time, which is the equivalent to losing money in nearly every case scenario. Very high upload and download speed on demand is an essential aspect as well. Without high upload and download speed, your organization may be suffering from waiting a long period of time to recover documents in case of a ransomware attack or a similar attack. This will recover and decrease the amount of time business operational services are down. The reason you would need high-quality name-brand servers with strong security and consistent monitoring is due to the fact that weak servers will have many downfalls. Weak outdated servers can be exploited through various vulnerabilities. This means that the ransomware your organization faced would also have impacted your mirrored site. This would eliminate the entire purpose of a mirrored site. These modern servers typically have extra layers of security; however, it doesn’t ever hurt to have extra added layers of security such as end-to-end encryption between both servers. I would finally recommend a cloud server that is uploaded weekly through physical transportation instead of a direct cloud upload. Since security will never be perfect, this will ensure ransomware will not completely affect cloud storage in the worst-case scenario.

Develop a procedure to notify the crisis communication command center.

A crisis communication command center would be great to be hosted in Arizona. Arizona is the best place to do it as we do not suffer many natural hazards such as hurricanes, tsunamis, tornadoes, or mass flooding. Many organizations are known to host their command centers out of Arizona. Personnel that would be located in this location are security experts. Once these security and response experts are notified of the disaster situation, they would react through their well-documented standardized operating procedure. Their standardized operating procedure would include directions for every case scenario that could potentially occur. It would include questions regarding what they have done to reduce loss in the situation, whom to contact and reach out to, and support they can give the site. Knowledge of contact points is essential for these operators to know since they are the first point of contact for onsite leadership. Once these analysts have obtained the information, they will begin reaching out to various stakeholders. These stakeholders could include a legal team, a human resources team, a disaster recovery team, and potentially even insurance companies. This will trigger all the other organization’s standardized operating procedure, which will be the start of a clockwork function in order to recover the loss the organization has faced. Once the notification that a loss has occurred is mentioned, the start of a conference call will occur during the day as soon as possible.

Communication template -

In a communication template, there are various crucial steps you must follow for every crisis situation. To start, you must identify who is in charge. This template will notify and demand all hourly employees to notify their manager/higher-ups on the shift of the situation. This will escalate the problem to leadership in order to resolve the situation as soon as possible.

 Disaster Declaration Statement -

The on-shift leadership on site of the crisis will then notify their higherups as they’re sure to be in a salaried role. Typically, most employees on salary must be on call for disaster situations. Once notified, the salaried leadership that was contacted will then begin to push a notification out to responders via email. These responders will be managed through certain groups and stakeholders throughout the company. This can include, depending on the severity, the CEO, emergency services (911), supporting vendors, other shifts managers, etc. A meeting chat room will then be created where stakeholders will then discuss what actions must be taken in order to de-escalate the situation. The meeting must be within 15 minutes of the email being sent out. This is a place where there will be questions asked to the incident commander. The incident commander is typically someone who witnessed the incident first hand and will be able to provide as much information to support teams as possible. An assessment of employee status, physical building security, possible injuries, emergency services contacted, and potential operational impact will be taken during this time.

 Organizational chart -

The organization chart will go by a “Level” system. The lowest level an employee can begin is at level 1. Level 1 employees are technically not employees as they are contractors. This will strictly give them access to areas where needed and only needed. Contractors can include construction workers working on your site, routine janitorial staff, food vendors, and security. Level 2 employees will be given the bare minimum access as well. These are your bottom-level hourly employees which typically only get access to the office space and their personal cubical area. Level three employees are your assistant managers. These employees will have some extra permissions as they will handle time/punch corrections for level 2 employees and have the ability to access meeting rooms when needed. Level four employees are managers or technical staff. These employees will have access to data rooms, storage areas, spare supply closets, and emergency disaster recovery supplies. Level five employees are typically hired by the CEO. These are corporate employees that make executive decisions and will have access to all rooms as they will escort government employees throughout inspections such as OSHA.

 Vendor List -

Vendor lists are important as they handle all your external business work. This can be your supplier, construction organization, and potentially transportation. For my wholesaling company such as plastics and products, I would use wholesalecentral as my backup organization. If I were to neet any construction done to my work areas, I would hire McCarthy US. They’re a global US construction company that follows rules and safety regulations with various awards. If I needed a semitruck to move loads with a supplier, I would use the contractor a1transport. They’re a global trucking company moving products all over north and south America giving lots of flexibility and area to cover.

For the backups that will be done for DigiKnights, the best form of long-term backup is a tape library. This is an older form of backup and is not the most efficient to recover data, but it is significantly cheaper than some other options. For that reason, this is the best choice when choosing a method to backup data for the business.

When comparing the cost of backing up to tape and data disk, we can see a massive difference in price. According to backupworks.com, if you use tapes instead of disks, in five years you will save approximately $1,581,016.00. This is broken down in a table included in the like below. For long-term storage utilizing a tape library is the most effective form of backup. It is not too often that you need to access data that has been backed up, and you could always do a rotation to keep certain items still attached to the network and easier to access. For example, at the company I currently work at we use a tape library to manage all our backups. We rotate the tapes around every week. Once tapes have been written to a certain number of tapes, they get retired and are put into storage until we need them again. But the data that is backed up a few weeks before is still accessible on the network. So, anything that is recent is still available, while the older tapes get archived for long-term storage.

The data that would be backed up is everything that is on the data and storage servers. You do not want to back up every single workstation and machine in the environment because that would simply be just too much data to have to back up and it would take up way too much space. Alternatively, you could give each user a certain amount of storage on a data server for them to put important documents and files on so that they could decide what would be backed up and what they do not need to be backed up. This will keep the footprint for backups down while still keeping the vital information on the tape. How the backups would work is the tapes will run twice a day, every 12 hours, and backup everything on the network at the time. Overwriting everything that is already there with the newest versions. Then every week when tapes are full, we can go in and swap them out for other tapes. My company uses the service provided by Iron Mountain Data Center to manage these backups. That way the tapes are secured with their security and the tape chassis is housed in an off-site location so that it is protected. I would like to replicate this ideology with DigiKnights. I feel confident in tape libraries and think this is the best way to manage backups for any company.

The way we oversee the timeline at my current job is that we use tapes for a little while, swapping them out as needed every week. Once these tapes have been active for a long time, we move them from a weekly rotation to a monthly rotation. They stay in this monthly rotation for a little while. Once they have been used in the monthly rotation for a while, they get migrated to long-term storage and archived. This is where Iron Mountain holds them until they are needed again if they are needed again. This is the most cost-effective way to control backups for a company.

There are other options that are more convenient to use for backups than tape libraries, but I do not think any of them are worth the additional cost.

Communication template -

In a communication template, there are various crucial steps you must follow for every crisis situation. To start, you must identify who is in charge. This template will notify and demand all hourly employees to notify their manager/higher-ups on the shift of the situation. This will escalate the problem to leadership in order to resolve the situation as soon as possible.

 Disaster Declaration Statement -

The on-shift leadership on site of the crisis will then notify their higherups as they’re sure to be in a salaried role. Typically, most employees on salary must be on call for disaster situations. Once notified, the salaried leadership that was contacted will then begin to push a notification out to responders via email. These responders will be managed through certain groups and stakeholders throughout the company. This can include, depending on the severity, the CEO, emergency services (911), supporting vendors, other shifts managers, etc. A meeting chat room will then be created where stakeholders will then discuss what actions must be taken in order to de-escalate the situation. The meeting must be within 15 minutes of the email being sent out. This is a place where there will be questions asked to the incident commander. The incident commander is typically someone who witnessed the incident first hand and will be able to provide as much information to support teams as possible. An assessment of employee status, physical building security, possible injuries, emergency services contacted, and potential operational impact will be taken during this time.

 Organizational chart -

The organization chart will go by a “Level” system. The lowest level an employee can begin is at level 1. Level 1 employees are technically not employees as they are contractors. This will strictly give them access to areas where needed and only needed. Contractors can include construction workers working on your site, routine janitorial staff, food vendors, and security. Level 2 employees will be given the bare minimum access as well. These are your bottom-level hourly employees which typically only get access to the office space and their personal cubical area. Level three employees are your assistant managers. These employees will have some extra permissions as they will handle time/punch corrections for level 2 employees and have the ability to access meeting rooms when needed. Level four employees are managers or technical staff. These employees will have access to data rooms, storage areas, spare supply closets, and emergency disaster recovery supplies. Level five employees are typically hired by the CEO. These are corporate employees that make executive decisions and will have access to all rooms as they will escort government employees throughout inspections such as OSHA.

 Vendor List -

Vendor lists are important as they handle all your external business work. This can be your supplier, construction organization, and potentially transportation. For my wholesaling company such as plastics and products, I would use wholesalecentral as my backup organization. If I were to neet any construction done to my work areas, I would hire McCarthy US. They’re a global US construction company that follows rules and safety regulations with various awards. If I needed a semi truck to move loads with a supplier, I would use the contractor a1transport. They’re a global trucking company moving products all over north and south America giving lots of flexibility and area to cover.

The nearest fire station to DigiKnight Technologies is only 7 minutes down the street, or about 3 miles. The address is, Fire Station 2, 37299 Niles Blvd, Fremont, CA 94536. Next on the list for first responders is police. The nearest police station is only 4 minutes away, or about 1 miles. Located at Fremont Police Department, 2000 Stevenson Blvd, Fremont, CA 94538. The next emergency response we may need is search and rescue. The nearest search and rescue is a bit further away coming in at 22 minutes, or 16 and a half miles. The address is, Santa Clara County Search and Rescue, 55 W Younger Ave, San Jose, CA 95110. Next on the list is a hazardous materials team. This emergency responder is also located a bit further away at 29 minutes or about 20 miles. The address for this emergency responder is, Sunnyvale Hazardous Materials, 700 All America Way, Sunnyvale, CA 94086. Luckily the nearest hospital to DigiKnight technologies is only 6 minutes away walking, at only about a quarter miles away. The address to this hospital is, Washington Hospital Healthcare System, 2000 Mowry Ave, Fremont, CA 94538.

In the event of an incident that happens on the digital side of things DigiKnight’s infrastructure will be designed in such a way that it will auto-generate the logs required to track the incident from where it began. As a form of redundancy to this they will also have analysts on the security side keeping track of the logs and monitoring what is happening on the network so that they can find an incident as it happens. For an incident that happens to be a physical incident such as a fire, everyone in the company will have to undergo annual training so that everyone knows how to respond to an incident like that. One of the most important parts of something like this is to ensure that drills are being run as well. Whoever is in charge of the building for DigiKnight should be preparing (at least) quarterly drills so that everyone can get the proper practice required to make sure that they respond to certain incidents in the proper fashion. In the event that they don’t, training will be updated to highlight those areas.

With every good assessment for determining structural damage, health, safety, and risks template, you must fully consider every potential occurrence even if it has a below one (1) percent chance of occurring. To begin, the structural map layout will be distributed to everyone in the building in an emergency scenario. This map will have every room, watersource, door, emergency door, emergency bumper and every electrical control panel labeled. This will highlight the emergency safety room in case an active threat emerges within the building. This will also come with a template that will have a list to label the affected areas and their impact to operations. The list can be as little as a personal computer being impacted by a roof leak or as big as an entire room being destroyed by a hurricane along with the inventory of the smaller property and item damages. In the case there will be operational impact, an estimate ranging from hours to days will be required to be filled out. In the case the operational impact is less than one hour, it will not be recorded as it can be made up. An estimate of the damages, before and after professional assessment, will also be recorded by the manager and inventory assessor.

 Every workplace must practice emergency drills. This is due to the fact that if nobody ever practices a drill, and there’s an emergency situation such as a fire, it can lead to a potential employee loss which is never good. This can completely ruin your business reputation and potentially end up with legal issues. During the bi-monthly emergency drills, employees must undergo a fire simulation evacuation. This is where the fire alarm will go off, and all employees will evacuate the building and meet at the designated rally point. After the drill, all associates will be guided, inside and outside, to be shown the emergency exits. Once they’ve completed the emergency exit guide, they will then be guided to be shown every available fire extinguisher in the area’s they typically work and reside on a day to day work basis. After both the guides are done, they will be shown all emergency first aid locations as well as be walked through on how to use an AED and other forms of emergency medical equipment.

 Emergency evacuations can occur for many reasons. A few of the consistent evacuation purposes are fire alarm triggers, evacuation drills, power outages, etc. During an evacuation, everyone will meet at the designated rally point. This will either be in the parking lot or the back yard area depending on where the employees are working. Maps for the evacuation procedure will be placed throughout various places within the building. Maps will also be dispersed through every entry of the room, right next to the door’s entrance. This will have red arrows guiding people where to go during an emergency. These will be the designated emergency escape routes. This will also outline all emergency exits. Near the rally points, the employees will have access to bins that contain living supplies that will help them survive any weather conditions. These supplies will consist of water, blankets, tents, emergency heating supplies, towels, flares, and rafts in case of flooding. Two emergency telephones will also be outside of the site in case emergency services need to be contacted.

 There are also many reasons employees may need to conduct a shelter-in-place procedure. A few examples of when employees need to conduct a shelter-in-place are tornado warnings, hurricane warnings, and tsunami warnings. Shelter-in-place notifications are typically received via local news guidance reports. During a shelter-in-place, employees must meet within the middle of the building or a room below ground level. This will ensure associates within the organization’s building have the greatest survivability rate while experiencing natural disasters. These shelter-in-place maps will not be dispersed throughout the facility; however, it will be up to the managers and leadership to properly provide the resources to the employees. Water, purification tablets, shelf-stable food supplies, clothing, blankets, emergency phones, and heat producers will all have a designated room within 100 feet of the shelter-in-place rally point within the building. At the shelter-in-place rally point, there will also be designated maps that will be handed out to everyone that have the location of utility closets, circuit breaker panels, gas lines, electric lines, water lines, and power lines. On the back of the map, there will be designated instructions on how to operate said utilities and resources for living.

 The checklist for interviewing a disaster recovery specialist should include list of the following, names and titles of employees who are authorized to contact the disaster recovery service providers, contact information of these specialists, how the facilities and locations of should be identified to these service providers, information on the negotiated contracts with these service providers, information on paying these service providers, information on paying these service providers if there are no negotiated contracts, and finally how to access emergency funds to pay disaster recovery service providers. This information is vital in order to properly contract the correct disaster recovery specialist. This is an incredibly important position in any company and it is even more important to ensure that the proper specialist is chosen for this position to keep the company going. Second on this list is how to contact and inform the company’s stakeholders. For this you’ll need the following items, the names and titles of employees who are authorized to talk with stockholders and investors, a list of executives assigned to stockholder and investor relations, contact information and locations of large stockholders and investors, how to establish a stockholder and investor relations area at the emergency operations center, a process to update stockholders and investors on the status of disaster recovery efforts, and finally a process to provide stakeholders and investors with a final report when recovery is complete. All of these steps are important to consider for a disaster recovery plan in order to ensure that all parties with connections to that company are aware of what is going on. Keeping everyone informed is incredibly important.

 Contacting and working with the company’s suppliers is incredibly important during an incident as well. In order to ensure that this part of the response is handled properly here is a checklist to contacting these suppliers. You need the names and titles of employees who are authorized to work with suppliers and service providers, contact information of these contractors and service providers, how the production lines or services should be identified when contacting service providers and suppliers, what to tell suppliers and service providers about the disaster, what to tell them about recovery of operations, and what suppliers and service providers should do if the need to contact the organization during the disaster. Making sure that your suppliers and service providers are aware of what’s going on and how they need to interact with your company and work with your company is incredibly important. This goes along with making sure that every party that is involved with the company knows what is going on and is informed. Finally, we need to ensure that the company has an open line of communication with its customers. A good list to follow to ensure proper communication with customers is, knowing the names and employees who are authorized to work with customers, contact information and locations of key customers, how product lines or services should be identified when contacting customers, what customers should be told about the disaster happening, what they should be told about the recovery of operations, and finally what customers should do if they need to contact the organization during the disaster. The customers need to know what is happening to the company during an incident just as much as everyone else. It’s important for the customers to know what’s going on because they are the people directly interacting with the company to exchange currency for a good or service. If the customers are out of the loop, your business is likely to lose a lot of customers. Communication is key when working through any incident and recovering your business from that incident.

Inventory or list of critical resources at damaged site:

In the case that a site is damaged we will need to know the damage to all of the resources. This includes needing to know if some of the resources are going to be fixed and how much it costs to fix them. If certain resources are unable to be repaired we need to know if they are able to be salvaged so that we can get some money back from salvaging them. With some of the equipment being down this will likely disrupt business for the period of time it takes to either repair or replace that equipment. After an incident we need to have an estimate on the impact that this outage will cause. Finally, the last piece of information we need to gather for an incident like this is how much it will cost.

 Policies and procedures for employees to follow explaining proper safety guidelines:

In order to ensure that everyone is going to get the proper training that they require to work here we will implement an online training program. In the times of Covid-19 a lot of people are working from home, and this will ensure that all of the on site employees get the same training as those that are remote. A simple online tool will allow for this training to be constantly updated with the workplace changes as well.

 Assessment for determining inventory or building, utilities (gas, electric, water)

In order to determine the inventory for the building we will conduct quarterly counts, as well as keep a running spreadsheet of everything that comes in and out of the facilities. This will ensure that we have up to date numbers with the running list, and that we are verifying the accuracy of these numbers with the quarterly counts. For utilities we will want to keep track of the usage from each month when we receive our bills and compare them to bills prior. This will help us develop an average for our spending on utilities each month, as well as plan ahead for fluctuations in production.

 Inspect for hazardous materials, chemicals, or hazardous conditions

In order to ensure the safety of the employees we will conduct random worksite checks for any hazardous conditions. Worker safety is the number one priority here. Any employee that will be working directly with, or around hazardous chemicals or materials will have to complete a special training around these chemicals and materials. This will ensure that everyone has the proper knowledge required to safely handle these materials and chemicals. In addition to handling them, it is important for these employees to know how to handle a scenario where the chemicals get spilled or something goes wrong with the handling of them. If everyone has the same training then we can be confident that they all know how to be safe around these chemicals and materials. This training will need to be repeated annually to keep it all fresh in their minds.

 Resources and vital records for damage including water, fire, water, dust, ice, or physical damage (crushed, tipped over, etc.)

In the event that any type of incident happens there will be a series of forms that will need to be filled out documenting what happened, and what will happen to remedy this incident. This will help the company keep a record of anything that could be broken or a potential hazard in the future. It’s also important to keep a record of these types of events in order to sort out worker’s compensation if there is an injury or a reason where they have to take some time off work. In the same way that the company can benefit from having this documentation with the employees, we can use it to ensure that equipment is repaired or replaced as it should be.

 Nature-based test scenario:

In the case of a tornado, first the management and upper leadership of the organization will verify if it’s a credible tornado. They will first check the local weather report, then proceed to check a credible local weather channel’s social media where they announce potential threats. If the threat is credible, leadership and management will refer to a local weather channel's guidance for updates. In the case the weather reports initiate a tornado watch, the management and leadership will then initiate a shelter in place for the employees within the building. They will follow the protocol as posted until the tornado watch ends. Once the shelter in place is fully set, leadership will reference updates to the weather channel until the tornado watch is concluded in the local area. Once the tornado watch is concluded, associates will then return to their regular scheduled shift or go home if their shift ends. An operational impact report will then be conducted to determine how much impact there was to the business.

 Bomb threat test scenario:

In the case of a potential bomb threat ideation, determining credebility must be the number one priority of leadership and management. It’s very important to determine the credibility of a bomb threat as it will potentially cease operations of hours on end. There are many examples of when a bomb threat is incredible. One example of an incredible bomb threat is someone writing the words “boom,” “bomb building,” or, “place will blow,” on a bathroom stall without a given date or time. These incidents however do need to be internally documented. In the case the threat is deemed to be credible, leadership will then evacuate the building and call law enforcement to investigate the potential bomb in the area. Until there is a credible or incredible determination made by the local bomb squad, operations will not resume as safety of employees is the number one priority. In the case it is determined to be credible or a bomb is found, all employees will be sent home until further notice and investigation.

 Mudslide list:

1. Managers must attend and assess the threat.
2. A determination of the potentially and currently impacted areas must be assessed.
3. Severity and life risk to associates on site will be assessed.
4. If there is a risk to associates, a determination of a potential shelter in place or evacuation will be made and executed per the routing procedure.
5. Local emergency services will be contacted if further assistance or guidance is needed.

 Memo to CEO:

In order to ensure the safety of our on-site associates, we must first execute consistent drills in the case an emergency arises. A few of the potential threats that we may come across are natural disasters, bomb threats, hazardous substance release, on-site fires, and even facilities incidents such as power outages. All these scenarios all have practice routines in case the building does face a potential risk. The pros to executing practice evacuations or internal drills is all associates will be properly trained on how to handle a real emergency situation. This can save the organization from potential lawsuits and at worst case scenario, an employee fatality. The downsides to executing these drills and practice scenarios are that there will be an operational impact, inevitably slowing down company numbers and financial earnings. The training objective to these test scenarios are to keep all employees safe and avoid any work-related potential fatalities that may occur from uncontrollable aspects around us. Each example drill will take no longer than 30 minutes from start to end. Depending on how many associates there are working that day, the maximum estimated revenue loss would be $5,000 in the worst case scenario; however, this cost comes nowhere near to the cost of a work related employee injury or employee death. The average work related injury costs $39,000 while a work related employee fatality can be upwards of 1.15 million dollars. Overall, these drills are essential to keep employees safe within the workplace and potentially save hundreds of thousands of dollars avoiding a fatality with appropriate training.

It is important to make sure we can maintain the business continuity and disaster recovery plan that we have been creating this whole time. To make sure that everyone is aware of what to do, there are a few ways the employees will be able to reference this information. The first main point of reference will be the online training that everyone must complete annually. They can reference back to this documentation if they have an internet connection or are able to download a PDF of the documentation locally to their machines. Alternatively, there will be hard copies posted throughout each facility in case there is a need for a hard copy instead of a digital copy. This information will be updated annually with each new wave of training that goes out.

 It’s important to have a team that controls the BCDR plan, that way there are people dedicated to making sure that it is updated and provided to all the parties that need it. It is important to make sure that some people remain on the committee for a long time to make sure that the plan stays consistent. The one caveat to this is that you want to make sure there are also some new people on the committee to bring in new ideas and helpful suggestions for changes to the plan in the future. Ideally, you’ll have a good mix of both older members and newer members to keep a balance. Too many of the old members will keep things stagnant, and too many new members will have the potential to make too many changes at one time.

 To make sure the plan is kept up to date I think the committee in charge of the plan should meet quarterly to propose changes to the plan and go over what the plan currently has in place. This will ensure that whenever there are big changes in the company the BCDR plan will be updated to reflect these changes. This is another good way to ensure that older policies and procedures are still relevant and effective.

 There are several different approaches that can be used for reviewing the plan. I think that the best practice would be to have a committee that reviews the plan quarterly and edits it as needed. To combat the idea that disaster planning is seen as not improving the bottom line, I think it’s important to include the rest of the company on the meetings by offering incentives or having a drop box for other ideas to be heard. Making sure that everyone in the company knows and understands that disaster planning is to keep the company running if something happens that is out of our control is the most important piece of keeping a good BCDR plan.

In a case where plan updates in an emergency situation need to be distributed to leadership and employees, there are many options of distribution depending on the scenario. In the case where the building needed to be evacuated with a false alarm, the associates and leadership can obtain updates from each other in person. This is typically the best method to distribute updates in a scenario where employees will not be evacuated for more than one hour. In a case where evacuation will be over an hour, associates will be sent home. Once they’re home and safe, updates will be pushed out through text, email, and the employee app if one is available. During a shelter in place scenario, there are also various other ways updates can be distributed. Within shelters in place, depending on the severity of the incident, associates may have access to cellular service. The main corporate office will then be sending updates on the situation; however, it is the leadership’s job to continue to refer to local weather updates when available. In a case where the associates no longer have access to the internet or cellular service due to the severity of the natural disaster or situation, leadership will then broadcast updates and guidance in person. In a case where employees are stuck in two different areas in a widespread facility, leadership will then radio each other the updates and information. Preferably and if available, these updates will be distributed through the building’s intercom system. In order to avoid any confusion or miscommunication, the intercoms will be announced a total of three times. If the intercom system fails, leadership will then resort to continuing the updates through radio. In a long on-going scenario where employees are safe and there needs to be building reconstruction, the updates will be pushed out via company email. This will continue to keep the employees and leadership updated with updates on what's going on. While there are many ways to distribute updates in a disaster recovery scenario, it is essential the associates understand what’s going on and how to stay safe.

Checklist for updates and intranet documents:

1. Note time drill started
2. Rally associates at the emergency rally point
3. Account for associates, is there anyone missing?
4. Have there been any injuries?
5. Will emergency services need to be contacted?
6. Is there a police report number associated with this incident?
7. Will there be any operational impact that cannot be made up by the end of the day
8. Is there an estimated end time to the incident?
9. What time did the incident end?
10. Internally document all the information above and submit it to the legal and corporate department.
11. Send out a notification to associates, and internally document the email
12. Follow up with the police report if needed
13. Document and organize property damage reconstruction if needed

BCDR Plan change management process

 In a case where a change will be implemented to the BCDR, shelter in place, or evacuation process, everyone must undergo training depending on the severity of the change. If it’s a major change such as moving the rally point spot for shelter in place situations and evacuations, every associate must undergo at least one drill. This is to ensure there is no confusion on where to exit the building properly and where to locate yourself and leadership. The drill is pretty much the exact same as the testing and training. If there is an error or an obvious flaw to the process, leadership will then make the proper changes and associates will once again have to undergo a drill at a later date. Once it’s confirmed by on site leadership, a revision must be done by the stakeholders to approve of the change. Once the change is approved the announcement will then go out to all associates via email as well as a physical hand out. Everyone must also sign a paper confirming they have undergone the emergency scenario process in order to confirm everyone is familiar with the changes. With the updates being approved by stakeholders and associates properly acknowledging the changes, there is no reason anyone throughout the organization would be unfamiliar with the changes.

Resources used:

Rouse, M. (2019, June 28). What is incident response? Definition from WhatIs.com. Retrieved September 20, 2020, from https://searchsecurity.techtarget.com/definition/incident-response

Maria, G. (2019, July 09). How to Create a Cybersecurity Crisis Management Plan. Retrieved September 20, 2020, from https://lab.getapp.com/cybersecurity-crisis-management-plan/

Rouse, M. (2019, June 28). What is incident response? Definition from WhatIs.com. Retrieved September 20, 2020, from https://searchsecurity.techtarget.com/definition/incident-response

Ashford, W. (2020, July 01). Time to rethink business continuity and cyber security. Retrieved September 20, 2020, from https://www.computerweekly.com/opinion/Time-to-rethink-business-continuity-and-cyber-security

Business, S. (n.d.). IT Disaster Recovery Management: Disaster Planning. Retrieved September 20, 2020, from https://www.stayinbusiness.com/resource/it-disaster-recovery-management/

About Richard Long Richard Long is one of MHA’s practice team leaders for Technology and Disaster Recovery related engagements. He has been responsible for the successful execution of MHA business continuity and disaster recovery engagements in indust, About, Long, R., & Richard Long is one of MHA’s practice team leaders for Technology and Disaster Recovery related engagements. He has been responsible for the successful execution of MHA business continuity and disaster recovery engagements in industries such as Energy & U. (2019, November 07). The Three Phases of Disaster Recovery. Retrieved September 20, 2020, from https://www.mha-it.com/2017/05/09/phases-of-disaster-recovery/

Data Recovery, Computer Forensics and E-Discovery Differ. (2016, August 17). Retrieved September 20, 2020, from https://burgessforensics.com/data-recovery-computer-forensics-and-e-discovery-differ/

*Man-made disaster*. Man-Made Disaster | Monroe County, FL - Official Website. (n.d.). Retrieved February 6, 2022, from https://www.monroecounty-fl.gov/904/Man-Made-Disaster

*How to prepare for man-made security threats in 2022*. OnSolve. (2022, February 2). Retrieved February 6, 2022, from https://www.onsolve.com/blog/rise-man-made-security-threats-prepare-attack/

*It threats and attacks*. Intellipaat Blog. (n.d.). Retrieved February 6, 2022, from https://intellipaat.com/blog/tutorial/ethical-hacking-cyber-security-tutorial/it-threats-and-attacks/#:~:text=Information%20Security%20Threats%20are%20possible,in%20sensitive%20data%20being%20exposed.&text=Security%20Threats%20come%20in%20all,%2C%20sabotage%2C%20and%20information%20extortion.

Banks, J. (2021, September 22). *5 cybersecurity threats for businesses in 2021-and 3 tips to combat them*. Security Magazine RSS. Retrieved February 6, 2022, from https://www.securitymagazine.com/articles/96146-5-cybersecurity-threats-for-businesses-in-2021and-3-tips-to-combat-them

*Top natural disasters that threaten businesses*. EKU Online. (2018, November 28). Retrieved February 6, 2022, from https://safetymanagement.eku.edu/blog/top-natural-disasters-that-threaten-businesses/

*Top four risks associated with natural disasters*. Resolver. (2021, September 20). Retrieved February 6, 2022, from https://www.resolver.com/blog/top-four-risks-associated-with-natural-disasters/

About Adam HarknessIn his role at NetMotion Software. (2021, January 18). *Mission Critical Systems vs. business critical*. NetMotion Software. Retrieved February 11, 2022, from https://www.netmotionsoftware.com/blog/mobility/mission-critical-systems

GB Tech. (2020, January 17). *Mission-Critical Systems, and why you need them managed*. GB Tech. Retrieved February 11, 2022, from https://www.gbtech.net/mission-critical-systems-and-why-you-need-them-managed/

*It Support Services Denver, Colorado: Mission Critical Systems*. IT Services Colorado. (2021, May 21). Retrieved February 11, 2022, from https://www.itservicescolorado.net/

Mission Critical Magazine. (2011, September 2). *Peter M. Curtis' maintaining mission critical systems in a 24/7 environment, 2nd edition published*. Mission Critical Magazine RSS. Retrieved February 11, 2022, from https://www.missioncriticalmagazine.com/articles/84082-peter-m-curtis-maintaining-mission-critical-systems-in-a-24-7-environment-2nd-edition-published-1

*Arizona Business Insurance*. Progressive Commercial. (n.d.). Retrieved February 20, 2022, from https://www.progressivecommercial.com/business-insurance/arizona/

 *How much does business insurance cost?* Progressive Commercial. (n.d.). Retrieved February 20, 2022, from

https://www.progressivecommercial.com/business-insurance/business-insurance-cost/

 *Legal counsel*. Corporate Finance Institute. (n.d.). Retrieved February 20, 2022, from https://corporatefinanceinstitute.com/resources/careers/jobs/legal-counsel/

 *National Risk and Capability Assessment*. FEMA.gov. (n.d.). Retrieved February 20, 2022, from

https://www.fema.gov/emergency-managers/risk-management/risk-capability-assessment

 *FEMA threat and Hazard Identification Risk Assessment (thira)*. FEMA Threat and Hazard Identification Risk Assessment (THIRA) | Adaptation Clearinghouse. (n.d.). Retrieved February 20, 2022, from

https://www.adaptationclearinghouse.org/resources/fema-threat-and-hazard-identification-risk-assessment-thira.html

*Comparison of Disaster Recovery Sites: Which One to choose?* Official NAKIVO Blog. (2020, November 27). Retrieved February 27, 2022, from <https://www.nakivo.com/blog/overview-disaster-recovery-sites/#:~:text=A%20cold%20site%20is%20a,the%20three%20disaster%20recovery%20sites>.

Sullivan, E. (2018, November 26). *What's the difference between a hot site and cold site for Dr?* SearchDisasterRecovery. Retrieved February 27, 2022, from <https://www.techtarget.com/searchdisasterrecovery/answer/Whats-the-difference-between-a-hot-site-and-cold-site-for-disaster-recovery>

The Three Stages of Disaster Recovery Sites. (2022). Retrieved 3 March 2022, from https://www.seguetech.com/three-stages-disaster-recovery-sites/

The 7-Minute Guide to Mirror Backup: What you need to ... - G2. (n.d.). Retrieved March 6, 2022, from https://www.g2.com/articles/mirror-backup

Mirroring your site. Electronic Frontier Foundation. (2017, September 29). Retrieved March 6, 2022, from https://www.eff.org/keeping-your-site-alive/mirroring-your-site

Establishing a business recovery center. Restore Your Economy. (n.d.). Retrieved March 6, 2022, from https://restoreyoureconomy.org/main/establishing-a-business-recovery-center/

Crocetti, P. (2015, December 30). What is disaster recovery site (dr site)? - definition from whatis.com. SearchDisasterRecovery. Retrieved March 6, 2022, from https://www.techtarget.com/searchdisasterrecovery/definition/disaster-recovery-site-DR-site

Miller, E. (2021, May 6). *Labor Department Drops Independent Contractor Rule*. Transport Topics. Retrieved March 20, 2022, from https://www.ttnews.com/articles/labor-department-drops-independent-contractor-rule-favoring-truckers

*5 steps for developing a disaster recovery communication plan*. Marco. (n.d.). Retrieved March 20, 2022, from https://www.marconet.com/blog/it-communication-plan

Brush, K., & Crocetti, P. (2020, January 23). *What is a disaster recovery plan (DRP) and how do you write one?* SearchDisasterRecovery. Retrieved March 20, 2022, from https://www.techtarget.com/searchdisasterrecovery/definition/disaster-recovery-plan#:~:text=A%20disaster%20recovery%20plan%20(DRP)%20is%20a%20documented%2C%20structured,on%20a%20functioning%20IT%20infrastructure.

Backupworks.com - Data Storage Solutions, Tape, Disk, NAS and SAN Solutions. (2022). Retrieved 21 March 2022, from https://www.backupworks.com/costofdiskvstape.aspx

Miller, E. (2021, May 6). *Labor Department Drops Independent Contractor Rule*. Transport Topics. Retrieved March 20, 2022, from https://www.ttnews.com/articles/labor-department-drops-independent-contractor-rule-favoring-truckers

*5 steps for developing a disaster recovery communication plan*. Marco. (n.d.). Retrieved March 20, 2022, from https://www.marconet.com/blog/it-communication-plan

Brush, K., & Crocetti, P. (2020, January 23). *What is a disaster recovery plan (DRP) and how do you write one?* SearchDisasterRecovery. Retrieved March 20, 2022, from <https://www.techtarget.com/searchdisasterrecovery/definition/disaster-recovery-plan#:~:text=A%20disaster%20recovery%20plan%20(DRP)%20is%20a%20documented%2C%20structured,on%20a%20functioning%20IT%20infrastructure>.

Before you continue to Google Maps. (2022). Retrieved 3 April 2022, from <https://www.google.com/maps>

Miller, E. (2021, May 6). *Labor Department Drops Independent Contractor Rule*. Transport Topics. Retrieved March 20, 2022, from https://www.ttnews.com/articles/labor-department-drops-independent-contractor-rule-favoring-truckers

*5 steps for developing a disaster recovery communication plan*. Marco. (n.d.). Retrieved March 20, 2022, from https://www.marconet.com/blog/it-communication-plan

Brush, K., & Crocetti, P. (2020, January 23). *What is a disaster recovery plan (DRP) and how do you write one?* SearchDisasterRecovery. Retrieved March 20, 2022, from https://www.techtarget.com/searchdisasterrecovery/definition/disaster-recovery-plan#:~:text=A%20disaster%20recovery%20plan%20(DRP)%20is%20a%20documented%2C%20structured,on%20a%20functioning%20IT%20infrastructure.

Business, S. in. (n.d.). *Emergency response and operations*. Stay In Business. Retrieved April 10, 2022, from <https://www.stayinbusiness.com/resource/emergency-response-and-operations/>