Final Business Continuity/Disaster Recovery Plan Presentation

Hunter Autrey, Ethan Boren, Jonathan Luna, & Avery Worker

University of Advancing Technology

NTW440-Business Continuity/Disaster Recovery

Professor Galatas

April 18, 2021

Business Continuity/Disaster Recovery Phase I

Identify All Natural Threats

- *For each threat, identify threat sources.*

Floods, hurricanes, tsunamis are all-natural threats Japan faces every year. Approximately 5,000 minor earthquakes occur in Japan per year, with more than half measuring between a 3.0 and 3.9 magnitude. These mainly go unnoticed by people. However, around 160 earthquakes with a magnitude of 5 or higher can shake the Japanese archipelago each year.

- *For each threat source, identify the likelihood of occurrence and perform upstream and downstream loss analysis.*

The Japanese archipelago is located where several continental and oceanic plates meet, causing frequent earthquakes, volcanic eruptions, and hot springs. Japan implemented the world's first building code for seismic forces following the Great Kanto Earthquake of 1924. Amendments in 1981 implemented more rigorous standards so that buildings can withstand any damage from medium-sized quakes and won't collapse during large-scale ones. Therefore major cities like Tokyo, Osaka (Capcom's headquarters), and Kyoto only witness little or no damage.

- *Based on the likelihood of occurrence, assess the company's vulnerability to each threat source.*

Due to modern-day improvements and the amendments implemented in 1981, earthquakes in the Tokyo and Osaka regions no longer pose a great threat to the company or other businesses in the

area. Even with the small occurring earthquakes that occur every day, is not enough to disrupt the daily life of the residents.

- *Based on likelihood and vulnerability, prioritize a list of threats to the company.*

Small earthquakes under 4 will go unnoticed therefore remains the smallest threat to the company's functions. Categories of 5 or higher will prove as a medium factor to the companies operations.

- *Based on the prioritized list, assess the impact of each threat on business operations.*

Whenever there are occurrences of great earthquakes with a magnitude over 5, business activities are held for a pause, disrupting the company's time and efforts. This would cause downtimes for the duration of the event.

Identify All Man-Made Threats

- *For each threat, identify threat sources.*

Unintentional (employee mistakenly accessing the wrong information), adware companies, disgruntled employees. Such man-made threats also include crime from arson, civil disorder, terrorism, war, cyber-attacks.

- *For each threat source, identify the likelihood of occurrence and perform upstream and downstream loss analysis.*

Unintentional employee mistakes are going to happen, from a recent study about 60% of employee mistakes happen at work a year. Based on the OSAC (Overseas Security Advisory Council) the crime threats in Osaka, Japan has assessed the city as a low crime city. The Economist Intelligence Unit has even ranked Tokyo and Osaka as the world's number one and number three safest cities for 2019 and 2020.

- *Based on the likelihood of occurrence, assess the company's vulnerability to each threat source.*

The likelihood of these occurrences is very different. For one the likelihood of an employee making a mistake or intentionally doing this to the company is very high. Over 60% of employees make a mistake at work just because they are tired alone. The chances of Capcom being hit due to crime-related problems are slim to none as the city is known to be one of the safest cities in the world.

- *Based on likelihood and vulnerability, prioritize a list of threats to the company.*

A cyber-related attack on a company like this is going to be high but based on research Capcom is not always the target for these. Just last year in 2020 they were attacked but before that, they were attacked in 2010, so nearly a 10-year difference. For employee-related this is medium to low as most employee mistakes are usually easy to fix. The last threat being crime-related is low to none.

- *Based on the prioritized list, assess the impact of each threat on business operations.*

If there were a cyber-related attack it would greatly slow the operation of a business for this company. Employee or crime-related attacks would not have a big impact on the operations of the company.

Identify All IT and Technology-Based Threats

- *For each threat, identify threat sources.*

Spyware, malware, unpatched vulnerability, hidden backdoor programs, poorly configured user privileges, phishing.

- *For each threat source, identify the likelihood of occurrence and perform upstream and downstream loss analysis. (Think suppliers and customers)*

Spyware: Unlikely.

Malware: I think malware is something to be worried about at Capcom.

Ransomware: A ransomware attack happened at Capcom last year.

Unpatched Vulnerability: Unlikely. For a large company, Capcom is most likely on top of its security vulnerabilities.

Hidden Backdoor programs: With the most recent ransomware attack, I think this could be likely.

User Privileges: Capcom would have a properly configured user privileges system.

Phishing: I would say this is the most likely out of all the threats listed.

- *Based on the likelihood of occurrence, assess the company's vulnerability to each threat source.*

The company should be prepared for phishing or possible backdoor programs installed in their servers. With the most recent ransomware attack as well, Capcom should be prepared for a possible visit from another ransomware group. I believe that Capcom should focus on ensuring that employees are not clicking links in emails and not giving out user information to people. This will help prevent phishing and social engineering tactics. Capcom does not store customer payment information in their servers, so they won't have to necessarily worry about an issue in which a cybercriminal group steals user information.

- *Based on likelihood and vulnerability, prioritize a list of threats to the company.*

- Lost or Stolen Devices
- Sensitive Data Exposure
- Malicious Insiders
- Denial of Service

- *Based on the prioritized list, assess the impact of each threat on business operations.*

Lost or stolen devices- having a device stolen no matter what type of device it is could have some valuable information. If it's yours you use for personal stuff and or work at home, this could lead you to have your personal information stolen and sold. Also if you simply just lose the device, you could be holding back projects and or information the whole team needs.

Sensitive Data Exposure- If someone sees sensitive data they are not allowed to see, they could use that information against the company and or sell it to rival companies so they know what the plan is.

Malicious Insiders- These are the people that no one knows about within your company. These are people sent in by other companies that intend to get information and or destroy the system from the inside. They are up to no good and at any time you notice suspicious activity, they need to take action.

Denial of Service- this is an outside attack that can cause your system to go offline for a good amount of time. Without the system online, no one will be able to do their jobs right and or able to access the needed things to get the job done. Depending on how long the system is offline, the company could lose a large amount of money by not being able to tend to the customers.

Business Continuity/Disaster Recovery Phase II

Identify All Environmental/Infrastructure Threats

- *For each threat, identify threat sources.*

Some of the environmental issues Japan faces today are waste management, global warming, coral bleaching, nuclear power, fishing and whaling, urban planning, and electronic waste management.

- *For each threat source, identify the likelihood of occurrence and perform upstream and downstream loss analysis.*

Japan burns close to two-thirds of waste in municipal and industrial incinerators. An estimated seventy percent of the world's waste incinerators are located in Japan. Combined with the incinerator technologies, Japan has the highest level of dioxin in its air. Dioxins are highly toxic and take a long time to break down once they're in the environment. It can cause cancer, reproductive and developmental problems, damage to the immune system, and interfere with hormones. In cases when Dioxin levels become dangerously high, it can lead to the company shutting down for some time until it's safe to return. Additionally, Japan is the world's fifth-biggest emission emitter contributing to global warming.

- *Based on the likelihood of occurrence, assess the company's vulnerability to each threat source.*

In an event where toxic levels become at a dangerous state, all personnel will be needed to evacuate the area until further authorized approval. This will cause major downtimes in the company and much unproductive time. In the city of Osaka, Capcom's headquarters generates approximately 1.3 billion tonnes of municipal waste each year and is expected to increase to 2.2 billion by 2025 according to the world bank. With this, the company can face major threats if further actions are not taken to improve the country's waste management.

- *Based on likelihood and vulnerability, prioritize a list of threats to the company.*

The likelihood of threats that are to occur to the company is mostly going to happen through cyber attacks (i.e malware, hackers) to mistakes simply made by our employees as well as natural disasters.

- *Based on the prioritized list, assess the impact of each threat on business operations.*

The impact of a cyberattack on our company would be the biggest threat we need to prepare for. The reason for this is that cybersecurity issues are becoming a day-to-day struggle for every company. In 2020 there were over 30 million cyberattacks a year. If we were too vulnerable we could lose thousands of dollars trying to get our data back, to being secured. The next impact from the list is human error. This also goes back to cybersecurity. 95% of successful breaches were caused by a human error, this could be someone opening the wrong link or email. This needs to be stopped if we can. The last is a natural disaster to our company which is located in Japan. The biggest natural threat to us are earthquakes to tsunamis. Lucky for this we could be prepared for at a moment's notice but the loss of physical data could cost us millions. All three threats are more on the higher end of things.

Prioritize Business Functions into Mission-Critical, Important, Minor

- *For each mission-critical business function, assess the impact of the loss of this function.*

Critical Functions:

-Servers

-Accounting & Finance

-Marketing

-Production.

The loss of these functions could be massive for a company like Capcom. Servers going down and parts of finance going down could mean hundreds of thousands of dollars of revenue lost for the company. Issues in these areas could also have a huge effect on the reputation of Capcom, causing worsened sales.

- *For each mission-critical business function, assess the impact of various threats to this function.*

For accounting, finance, servers, and production a power outage or natural disaster could devastate these critical business functions. Potential data breaches like those in Capcom's past could also hurt these functions.

Poor marketing could greatly inhibit product sales for the company.

- *Develop a prioritized list of mission-critical business functions with the highest business impact.*

Missions-critical business functions from most important to least important are accounting & finance, servers, production, then marketing.

- *For the highest priority functions, identify the recovery time requirements including maximum tolerable downtime (MTD).*

Accounting & Finance- The recovery time for accounting & finance issues can be recovered within a few hours depending on how serious the issue is, with the MTD being about 2 hours before there is an incredible amount of revenue loss. Although the revenue could be remade, it would be a substantial amount of loss of Capcom.

Servers- The average downtime per year on 7 y/o servers is almost 7 hours while the average downtime for 2 y/o servers per year is about 2.5 hours. The MTD would be possibly a day or two before it became a serious issue. Although a few hours of downtime would also be terrible for Capcom, but not detrimental to revenue.

Production- The average downtime for manufacturers is 15 hours/week. A production downtime could lose money for Capcom within the thousands if not hundreds of thousands of dollars per hour. The MTD for production would be 7 hours in a single day.

- *For business systems, business functions, and IT systems, identify the following: business process criticality, financial impact, operational impact, recovery objectives, dependencies, and workarounds.*

In an event where any of the following goes down, servers, accounting, finance, marketing, or production, further action will need to be taken. For servers, all operating systems running the server will need to be temporarily put under maintenance until further notice. All customers will not be allowed to use the product until the completion of the maintenance. This will change the production timings of the company, addressing more important issues in restoring the servers back online. Accounting and finance are also huge factors of the business and will require immediate attention if anything goes wrong. This will require some of the functions of the company to be addressed or changed.

For Each Mission-Critical Function (non-IT), Identify Risk Mitigation Strategies for Consideration Including Risk Acceptance, Avoidance, Transference, and Limitation

- *For each mission-critical function (non-IT), identify the recovery requirements and potential recovery options.*

- Servers- data backups, multiple servers, and second-floor access only.
- Accounting and finance- Making sure that all the finances are accounted for and also that nothing goes wrong to lose money
- Marketing- to make sure the marketing does not fail, you need to appeal to the audience and do certain things to get a response from the buyer.

- Production- Making sure everyone does their part in the production and such is a great way to mitigate risks. Also making sure if anyone needs help they as to get it done in time.
    - *For each recovery option considered, identify the time, cost/capability, feasibility, service level requirements, and existing controls in place.*
- Servers- Servers can cost a lot of money especially if you need more slots than usual, this can cost up to $175,000 a year. Keeping this safe and such is very feasible, requirements for service are very high cause if it shuts down you can lose a lot of money.
- Accounting and Finance- for pricing, this is the main thing that comes up with the money for the company, so making sure that everything is right is very important, if it's not the company can lose a lot of money. Keeping it stable is very feasible and should be so that nothing goes wrong.
- Production- This can cost a lot of money and if anything goes wrong in the process, more and more money could be lost, as restarting and fixing mistakes could push back the release date and paying the employees more. The time working on this should be maximized as nothing can go wrong.

    - *For each mission-critical option, select the optimal risk mitigation strategy.*

Servers- Keeping them updated on security and making sure they don't overheat and little things like that.

Accounting and finance- making sure everyone is on the same page when budgeting and making good purchases.

Marketing- Making sure things that relate to the production is correct and that it accounts to the purchasers

Production- not wasting any time and making sure that everyone gets their part of the project done and asking questions to others to make sure everything goes smooth.

Business Continuity/Disaster Recovery Phase III

- *Create a checklist for contacting an insurance provider.*

  Be sure to include:

  - insurance carrier contact information
    - Asurion global headquarters 648 Grassmere Park Nashville, Tennessee 37211. The phone number is (615) 837-3000.
  - Estimate
    - An estimated cost for an average company headquarters electronics would be around 500,000 a month for all the technological appliances.
  - assessment of damage
    - $2,000 coverage per claim and up to $5,000 per 12-month period. With a flat fee of either 0, 49, or 99 dollars.
  - potential insurance coverage
    - Asurion covers any make or model of the following devices, televisions, streaming devices, VR headsets, handheld gaming, gaming consoles, theater systems, Bluetooth speakers, desktop pcs, laptops, headphones, tablets, printers, external monitors, mouses, keyboards, external hard drives, modems/routers, and even security cameras.
  - identify potential insurance gaps
    - Any breakdowns not caused by manufacturer defects, power surge, normal wear-and-tear, or dust, heat, and humidity may not be covered by the insurance.

        - legal counsel (insurance, other liability, regulatory issues, etc.).
            - Asurion insurance does not cover family leave, sick leave, etc. It's mainly for technological appliances and tech. Therefore it neither covers worker classifications, retirement, joint employment, health care reform, or workplace safety.
- *Perform research over the internet to discover possible risks to the company as reported by FEMA*

The strategic goals for FEMA can be broken down into 3 parts. They are to build a culture of preparedness, ready the nation for catastrophic disasters, and reduce the complexity of FEMA. In order to be proactive, the company of CAPCOM must incentivize investments that reduce risks such as protecting life and property and pull back the increasing costs of disasters. Also, we must bring resilient mitigation investments forward either by lowering the cost of the disaster or eliminating the need for Government need in Japan. The company can start by looking into the building codes secretive manner when not actively engaged in disaster operations.t in place so this can enhance the public safety and also the property damage as well. FEMA's next goal is to prepare the nation for catastrophic disasters and for this we can utilize what FEMA calls BEST (Build, Empower, Sustain, and Train). If we follow the BEST concept we can achieve the 2nd goal. Building the capabilities and capacities to fulfill our responsibility to effectively respond to a catastrophic event, empowering organizations and individuals to act decisively through leadership intent, sustaining proficiency as emergency management professionals, and Training, educating, and exercising in an open-minded creative manner when not actively engaged in disaster operations. FEMA's last goal is reducing the complexity of FEMA which is providing some AID on behalf of our company if a disaster is to occur. And if something were to happen to

our company we can look at FEMA for This starts with a review of the available forms of assistance and how we can access the various programs.

- *Include a detailed analysis of the services that FEMA provides.*

FEMA has services for individuals such as Unemployment assistance, which gives unemployment benefits and re-employment assistance to survivors affected by a disaster. These benefits usually last for 26 weeks (182 days) after a post-disaster declaration. FEMA also provides mass care and emergency assistance which includes food, shelters, and distribution of emergency supplies. There is also assistance for those whose homes have been affected by a disaster. This kind of assistance helps with childcare, medical expenses, or clean-up items. There is also a disaster case management program that involves partnerships with a case manager. The case manager will help assess an individual and meet their needs. There are also counseling programs as well as legal services. The legal services go toward those who qualify as low-income and are limited to cases that would not incur legal fees (help with insurance claims).

- *Then using this information, write a memo to the Task Coordinator detailing your findings.*

FEMA offers assistance for individuals and small businesses. Because CAPCOM is not considered a small business, the company itself would not qualify for any assistance. Employees can receive assistance for post-disaster recovery if it has been presidentially claimed as a disaster. Common assistance services that employees can qualify for would be Mass Care and Emergency Assistance, Individuals and Households Program Assistance, Crisis Counseling, Disaster Legal Services, and possible Unemployment Assistance.

- *Identify resources required including:*
    - computer equipment- computers are a big resource in what they do as they need to get supplies and order them.
    - communication links (Internet, dial-up, etc.)- they need good communication to interact all over the united states and they need to make sure it's not a weak one.
    - communications equipment (walkie-talkies, cell phones, landlines, etc.)- Computers, Phones, and radios are some of the biggest ones, as they can be a closer range rather than have to be used from far away and are fast.
    - office equipment- Office equipment is very important so that they can do all their work fast and easily.
    - office supplies- computers, paperwork, servers, things to make sure the job is done.
    - BC/DR plans- make sure to have backups for everything make sure all the equipment they sell works and also have backup software.
    - contact lists- managers, workers, CEOs, and big tech guys of the company.
    - inventory lists.- inventory lists could include stuff lost to natural disasters, and or what could be saved by big hits.
    - Be sure to consider the need for vendors, and/or contractors.- some vendors could include the tech company that provides the

computer and or software to Capcom. Who provides the internet service and also who provides the backup servers.

Business Continuity/Disaster Recovery Phase IV

- *Develop a procedure to notify and activate an alternate worksite.*

  Create contact information including:

  - Location
    - Just like what's happening currently, an alternate worksite can be in each employee's homes. Capable of working full-time remotely with the impression of getting more work done. Though the levels of team engagement and meetings won't be as interactive as live meets. The company initially will have each and every member's location marked and kept from public view. Additionally, each member will need to keep in contact with their designated Production Studios.
  - Personnel
    - Executive Management Kenzo Tsujimoto Chairman and CEO, Capcom, Co. Ltd. The external directors are composed of Hiroshi Yasuda, Makoto Matsuo, and Takayuki Morinaga. External Auditors with Yoshihiko Iwasaki and Akihiko Matsuzaki. The management representative is President and Chief Operating Officer Haruhiro Tsujimoto.
  - phone numbers to key personnel including management, BC/DR team, crisis management team, and HR as appropriate.

- Customer Service (650) 350-6500 (USA). Compliance structure that consists of the Headquarters and Subsidiaries first. Then the Internal Reporting System, followed by the Compliance Committee, and lastly the Board of Directors. Head Office located in 3-1-3 Uchihirano-machi, Chuo-ku Osaka 540-0037, Japan.
- *Create a plan to run a cold site backup location, detail what equipment and other resources are needed.*

  Also create an executive summary of the site explaining its pros and cons (is it fast to set up, but very expensive? etc)

Because the cold site is a backup, it would need to be away from the general office to ensure that the disaster does not spread to the cold site. If we had a cold site directly next to the general office and a power outage occurred in the entire block, the cold site would be affected as well.

The headquarters of Capcom is located in Osaka, Japan. Osaka is a city that is along the coast. Earthquakes and tsunamis are common in Japan. Because of this, it would be ideal to have a cold site in a location that is further inland.

The cold site will have computers for employees to work and be in a large enough building to add whatever else hardware is needed. The warm site will have backup servers. With the backup servers being in the warm site, the cold site will not need an extra set of servers to maintain unless it is absolutely necessary. Because the cold site is mainly just hardware that has a one-time fee, it should not have any exponential cost. There would need to be scheduled backups of the equipment at the location to ensure it is up-to-date and ready for a potential disaster.

Outside of that, the cold site will need to transfer over and set up the rest of the equipment necessary to complete the job. This site will have little maintenance to keep it relatively up to date and quick to transition to.

- *Create a plan to run a warm site backup location, detail what equipment and other resources are needed Also create an executive summary of the site explaining its pros and cons*

When it comes to the types of speed of recovery you might need, you have three different types of disaster recovery which are hot, cold, and warm. A warm site recovery simply means that your hardware and network connections from your site to the secondary site are not equal. The recovery will be delayed white you retrieve your data from the remote backup site. The equipment you will need to establish a warm site backup location is office space/datacenter space with some pre-installed server hardware. Some differences between a hot site and this warm site are that a hot site provides a mirror of the production data center while the warm site will contain only servers ready for the installation of production environments. A pro to having a warm site is that it makes sense for aspects of the business that are not critical.

Business Continuity/Disaster Recovery Phase V

- *Create a plan to run a hot site backup location, detail what equipment and other resources are needed.*
    - Also create an executive summary of the site explaining its pros and cons (is it fast to set up, but very expensive? etc).

A hot site is a backup facility that represents a mirrored copy of the primary production center. The location for this company will still be located in an urban area, just unlike the main company's location, it will be in a less dense area. The setup will take time and much effort to try to get as close as replication to the original site as possible. All the equipment will consist of servers, computers, routers, printers, mouses, keyboards, monitors, etc. The hot site must be an exact copy of the production site, including personnel, network systems, power grids, and instant backups of the data. Therefore lots of time and money need to be dedicated for this to happen.

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

One thing they could do for a mobile site backup is to go through a cloud. The cloud has many things it can hold and do for a business and individual. The good thing about the cloud is that it's fast and can store information in a safe environment. Some pros of this are that it cuts infrastructure costs by not having a dedicated room for the information. With cloud storage, data is distributed amongst bi-coastal data centers. Syncing technology makes it possible to link up and update data quickly, but storing data in the cloud makes syncing unnecessary. Some cons are that because the infrastructure of the cloud is owned and managed by the service provider, businesses may worry about not having enough control over the service. This is where the provider's end-user license agreement can help you out. It's also pretty expensive depending on the provider and how much info you are storing.

- *Create a plan to run a mirrored site backup location, detail what equipment and other resources are needed.*
    - Also create an executive summary of the site explaining its pros and cons (is it fast to set up, but very expensive? etc).

To run a mirrored site backup location, we must have a warm site. We need a warm site as this provides office space and will have pre-installed hardware. The warm sire then will mirror the servers ready for the installation of production environments. Mirroring could be described as using a RAID 1. This is the most common disk mirroring configuration from hard disks on two different servers to improve the availability of the database. The RAID controller will provide fault tolerance by copying data from one disk to another which is what mirroring is. Whilst mirroring it is highly recommended for applications that require high availability and high performance. incorporating mirroring means you need to buy RAID controllers and dedicated hard drives, both of which can drive up your operating costs quite a bit. In summary, it is more of a luxury to have this, as it takes a while to set up and very expensive.

- ***Develop a procedure to notify the crisis communication command center.***

  Create contact information including:
    - location

      Because we are wanting a crisis communication command center (CCC), it would be a good idea to place it in a position that is the least likely to be impeded by a disaster itself. It would be ironic if the CCC underwent its crisis. With this in mind, we recommend that the CCC is placed in Nagano, Japan. Nagano is toward the middle of Japan and is a perfect location for a communication center. This is a central location and far enough inland to prevent damage due to natural disasters. Nagano is also known as an industrial center, which makes the location suited for our needs.

    - personnel

Doing a bunch of research, Capcom doesn't seem to have a CCC currently. Because of this, we aren't able to add currently employed workers who are in this field. We can instead list a few job titles that are commonly seen in this field.

- Director- Crisis & Public Affairs Communications
- Crisis Aftercare Specialist
- Director of Communications
- Corporate Communications
- Strategic Marketing and Communications
    - phone numbers to key personnel including management, BC/DR team, crisis management team, and HR as appropriate.

Because there are no currently employed people at Capcom, we are unable to name or give out any information about this question.

Business Continuity/Disaster Recovery Phase VI

It would be best to have a backup plan on the cloud. The cloud is inexpensive, constantly updated, and adaptable. An even bigger advantage of having backups on the cloud is the data is on another company's servers. This ensures that any disaster that could affect work in the immediate area does not affect the backups. We could work with a cloud provider that has their own BC/DR plan that is good for us.

It would be best to have a cloud service that is Platform as a Service (PaaS). Platform as a service has us build our apps on top of a platform with a well-defined software development kit. The app is deployed on the cloud provider's data center. We would still have to monitor this data though.

The systems that should be backed up are the data where the data is transmitted to the remote storage system. The remote storage system should be the one that is backed up in case of any disaster is to occur. The remote storage systems should include about three things. Those are block storage, file storage, and the last one being object storage. The block storage has the larger volumes of data into small units called blocks. This is to have each block having a unique identifier and placed in the system's storage device. File storage is the system that helps organize that data in a hierarchy for the files and folders. A file storage-based cloud can make data access and retrieval easier. The last system being the object storage consists of three components. Those three components are the data stored in a file, metadata associated with the data file, and the unique identifier. Also, note that most cloud-based storages use a vast number of hard drive storage systems as well that are mounted in the system which they become linked by a mesh into the network's architecture.

One of the examples of software utilized to back up data is Arcserve. Trusted by over 10,000 customers including those from Microsoft, Comcast, T-Mobile, and Virgin Mobile. It comes with a complete one hundred percent cloud-based storage system attached with zero limits on user numbers or storage space. A full Office 365 integration significantly enhancing email searching and storage functionality. Furthermore, a

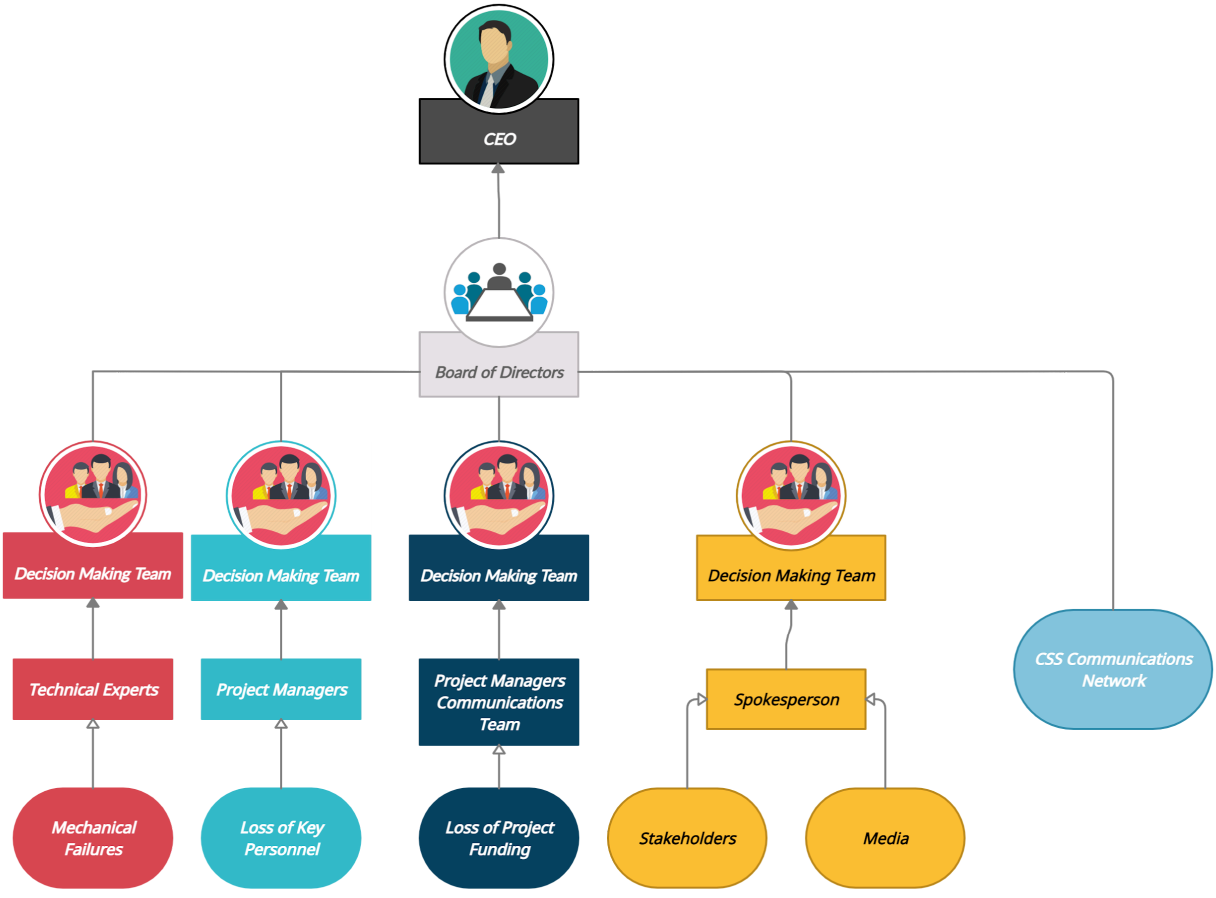
powerful search tool is included to archive and retrieve instantly cutting costs and time. Additionally, ArcTitan provides a huge saving in email storage costs, saves seventy-five percent of email storage space which reduces a load of mail in the server from one thousand gigabytes to just two hundred gigabytes. With that ArcTitan has a secure right to be forgotten functionality to help ensure compliance with all regulations, GDPR, Legal, and eDiscovery compliance. Therefore the product as a whole gives its customer enhanced compliance, encrypted software, one hundred percent cloud-based, improved productivity, Office 365 integration, and a powerful search tool.

Regarding our company's layout and design, the transition of backup should be incremental. Though full backup progress copies the entire data set and allows fast recoveries, incremental steps should be taken to save storage space. Being a video game company, each set of data will be blocked together and backups will be made from the previous one. This will cause the backup time to be fast without losing precious time. Unfortunately though, if an error was to occur the recovery time wouldn't be as fast as a full backup. Lastly, incremental backups require less bandwidth to complete the process.

The first time uploading to the cloud always takes the longest. As you keep uploading to the cloud, the time it takes less and less time, also depending on how much data you upload. In most cases, big backups could take up to 3 weeks if you upload about a terabyte of data. But as for 100GB and smaller, it could take less than 48 hours.

Business Continuity/Disaster Recovery VII

- *Develop a communication template to assist in crisis communication situations.*
    - Develop message content (see next)
    - Identify message and distribution authorization or escalation channels.
    - Identify and establish distribution channels.
    - Identify the frequency of communication.
    - Develop a template for the communication log.



Each case of incidents is divided into different teams. If the person or group of people above from the start isn't able to solve the issue it continues up the diagram until it gets

resolved. This is divided into parts so that not all fields of the company have to address the issue only the ones who are involved and have specialties in it. CEOs of a company have the final say if needed.

- *Create a disaster declaration statement to be communicated to BC/DR team, employees, investors, shareholders, customers, vendors, contractors, as well as community and media contacts.*
  The disaster declaration statement should include the general disaster information:
    - Notification and clarification of the event
    - Impact of event
    - Current status and condition of people, facilities, and equipment
    - Frequency of updates, estimated time of next update

    - The disaster declaration statement should include specific information and instructions for various stakeholders and groups including:
        - Employees
        - Vendors, suppliers, contractors
        - Customers
        - Business partners
        - Community and media
        - Legal and regulatory notification requirements

Employee Statement:

We regret to inform you that there has been an incident that has affected the performance of the company's workflow. The (insert disaster) has affected (insert what has been affected). Because of this, we ask that the employees in the (insert name of department) follow the steps outlined in the BC/DR plan.

Customer Statement:

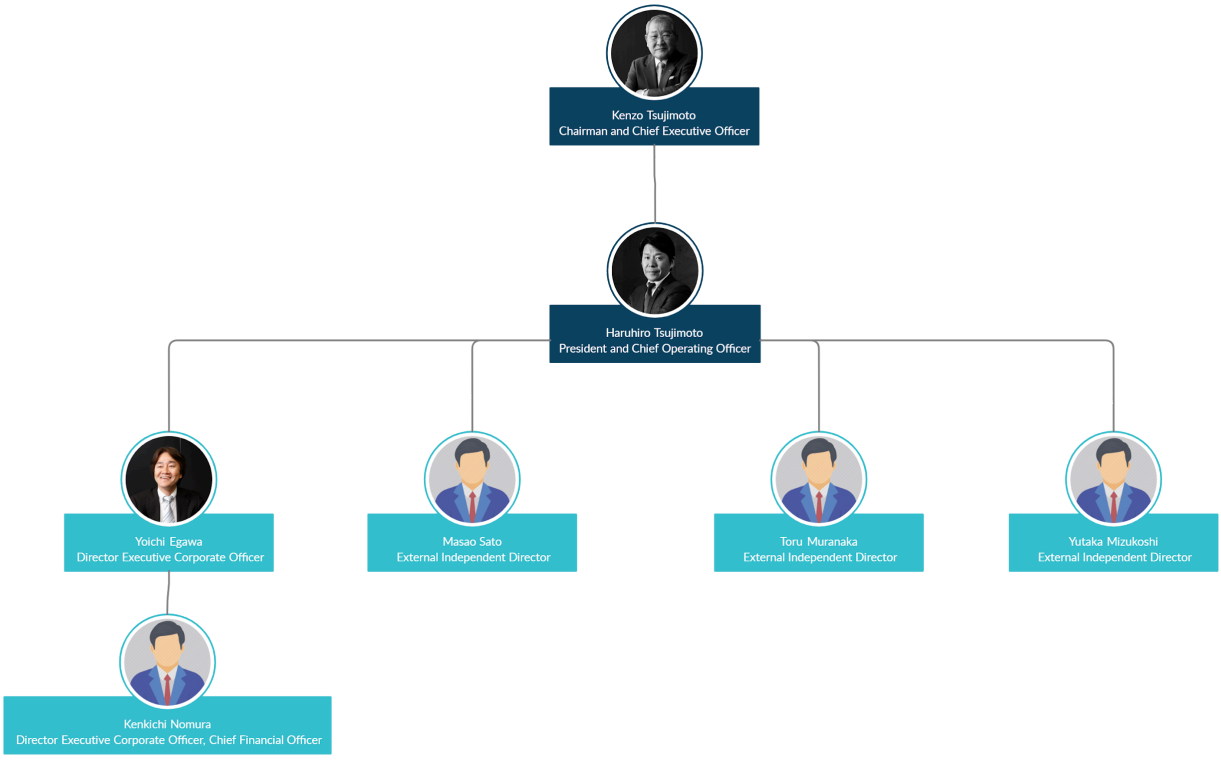
We regret to inform you that the company has been affected by (insert disaster). We respectfully ask that you be patient with our (insert service) while we work on fixing

the issue. Our estimated recovery time is (insert estimated recovery time). Thank you for your understanding.

Create an organizational chart of key employees in the company.

For this task, the key employee for each department is the head of that department, underneath him should be one additional employee from that department.

- What organizational authority and facility/key access. In an emergency, it is important to know who has keys to the necessary facilities.
- It is very important to know which and who has key access in different emergencies. For example, if there is a crisis happening with personnel it wouldn't be sensible to go to a spokesperson to resolve the issue. Instead, it should go to the dedicated person/people who are associated with it.



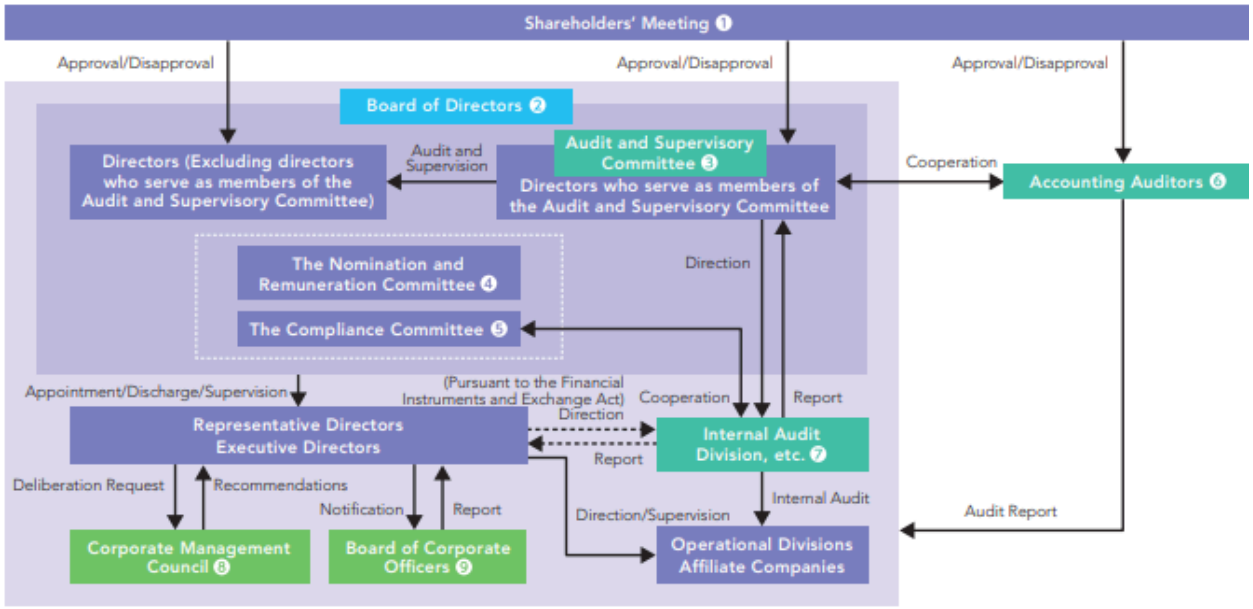
- Create an assessment template for HR regarding the status of all employees.

■ Board of Directors/Board of Corporate Auditors Rate of Attendance (Year ended March 2014)

	Name	Independent director	Reasons for selection	Board of Directors/Board of Corporate Auditors Rate of Attendance (Year Ended March 2014)
External Directors	Hiroshi Yasuda	○	Appointed with overall consideration for character, business acumen and successive appointments to important posts	Board of Directors Attended 14 of 15 meetings (93.3%)
	Makoto Matsuo		A legal professional able to provide precise guidance and advice and ensure the effectiveness of corporate governance	Board of Directors Attended 14 of 15 meetings (93.3%)
	Takayuki Morinaga	○	Appointed with overall consideration for management experience at other companies, professional career, track record, and personal connections in the business world	Board of Directors Attended 15 of 15 meetings (100%)
External Auditors	Yoshihiko Iwasaki		It was determined that his professional experience in tax administration would be of benefit to the company	Board of Directors Attended 15 of 15 meetings (100%) Board of Corporate Auditors Attended 15 of 15 meetings (100%)
	Akihiko Matsuzaki		Appointed to leverage the wealth of experience and knowledge accumulated during many years in law enforcement administration to help the company further enhance its corporate governance	Board of Directors Attended 15 of 15 meetings (100%) Board of Corporate Auditors Attended 15 of 15 meetings (100%)

(Image Credited to Capcom)

Additionally, HR will need to know the employee's information, knowledge of the job skills, experience/qualifications, education, communication skills, and confidence skills.



Create a Vendor List of companies where additional supplies can be purchased to keep the company running.

During a business disruption, we must focus on many different aspects of administrative tasks that must be handled. So I believe we should have an administrative support team that can be deployed during or after a disaster is to occur. This support team will focus on tasks such as getting in contact with the vendors we rely on to keep us successful. The list of vendors I am thinking of are companies who can supply us with emergency supplies, work with vendors arranging deliveries, helping with phone calls from the media and our investors, tracking shipments, and organizing papers or documents. This admin team will also focus on contracts such as contractual terms which are agreements and terms that are appropriate for our company. Also, keep in mind for specialty vendors which can help us with our BC/DR plan. This list includes chemical oxidation, CO2 blasting, deodorizing, sanitation, steam blasting. The list is already filled with many vendors that we may need but it’s not impossible. With this list already made, our company can come back faster and run which in return will save us time and money in the long run.

Business Continuity/Disaster Recovery Phase VIII

- *Identify and locate the address of the appropriate emergency response organizations and determine the best method of initial notification of possible, impending, or in-progress disruption or disaster.*
    - Identify and locate the address of the damage assessment team and determine the best method of initial notification of possible, impending, or in-progress disruption or disaster.
    - Identify and locate the address of the crisis management team and determine the best method of initial notification of possible, impending, or in-progress disruption or disaster.
    - Identify and locate the address of the evacuation/shelter leaders and determine the best method of initial notification of possible, impending, or in-progress disruption or disaster

Nearest Police Station: *1 Chome-3-18 Honmachi, Chuo Ward, Osaka, 541-0053, Japan*

Phone: +81662681234

Nearest Fire Department: *2 Chome-1-6 Uchihonmachi, Chuo Ward, Osaka, 540-0026, Japan*

Phone: +81669470119

Nearest Hospital: *7 Chome-5-15 Tenjinbashi, Kita Ward, Osaka, 531-0041, Japan*

Phone: +81663515381

Evacuation Centers: *Here is a link to all the listed evacuation centers in the Chuo Ward, Osaka, Japan. Along with each evacuation center, there are listed phone numbers and the maximum number of persons each center can hold.*

https://www.city.osaka.lg.jp/chuo/page/0000001715.html

Notifying Disaster Services:

It would be best to call these locations in the event of a disaster. Listed here are the nearest locations to the Capcom headquarters. These will be the best chance of having an immediate disaster handled quickly by officials that are trained in that field. If you are unable to call these services, the locations are within a few blocks of headquarters.

- *Create and determine appropriate BC/DR activation steps.*
    - Prepare a preliminary event report and log template.

The first step would be to determine the risk assessment and business impact analysis. From there develop a business continuity plan documenting critical and time-sensitive processes. Next, develop a disaster recovery design and implementation with the associating deployments. Document an IT recovery plan including team definitions, communications, and runbooks. Later execute the BCP and train the IT personnel to recover critical applications and systems. Finally, establish processes and criteria to validate plans.

<u>More in-depth plan:</u>

The incident is detected at hour 0. Hour 1, activate the initial response team. Hour 2, establish an incident command center. Hour 3, notify a re4covery team and make recommendations. 4 hours since the past incident declared whether the incident was a disaster. If no, terminate, if yes continue taking actions to maintain it. Request/obtain offsite tapes and mobilize/prepare a recovery team. Next, restore the networks/telecoms and SAN. Once that is complete, the restoration of VMs and AS 400 is very beneficial. Once all the restorations are completed, validation of data integrity leads to validation of user connectivity. The total process is estimated to be around 35 hours in total since the start of the incident.

- *Create an assessment for determining structural damage, health and safety impact, and risks template.*

This is the layout of the building and the street names for the head office and building. On the bottom is what I found on this building. For Japan, the hazard for all these buildings is high from a river flood, earthquakes, to wildfire and cyclones. The cost for this to be fixed or if we were to go through a disaster will cost upwards of 500 thousand dollars.

- Once you do this you MUST distribute it to all other team members so that everyone uses the same map.

SECOND FLOOR PLAN

FIRST FLOOR PLAN

LEGEND:

Atlassian II
Offices

- *Identify and create the policy for location and testing of alarms, emergency signals, first aid supplies, CPR equipment, fire suppression equipment, and hazardous materials safety equipment.*

In the case of any emergency, there need to be the right resources to save as many lives and or important equipment as possible. Location of Fire extinguishers and AEDs are very important as you never know where the emergency could occur. Fire extinguishers should be placed in main areas with high populations of people and also things that are fire hazards. Just in case of a fire, you should always be prepared to at least make a bit of a difference in the fire spread. Alarms should be placed all over the facility and in all offices and bathrooms to ensure that everyone will know there is a fire. There should be first aid kits everywhere where a cut and or bloody mess could happen to clean up the cut and clean the blood too to make sure it does not cause a hazard to the other employees. All these are important as you never know when an emergency is going to happen, and are essential for all businesses.

Business Continuity/Disaster Recovery Phase IX

- *Identify and create the policy for evacuation procedures including evacuation, securing, shutting down the facility, and internal assembly points (safe areas). Be sure to consider the need for local transportation and lodging as well.*
    - Identify and create the policy and method for ascertaining if anyone is missing or unaccounted for and emergency communications equipment, water (hot climates), blankets (cold climates), and emergency communications equipment (walkie-talkies, batteries, etc.).
    - The policy should include if applicable:
        - Maps and floor plans should include:
        - Evacuation routes and assembly areas
    - Escape routes from the site—primary and secondary (may need several options depending on disaster scenario)
    - Location of water and/or blankets
    - Emergency communications equipment

  In the event of an evacuation occurring all employees are to remain calm and exit the building using the nearest safest exits and proceed to the designated refuge area. Do not whatsoever use the elevators and proceed safely down the stairs using the handrails. Department heads and security liaisons need to ensure all of their staff is accounted for and has left the office. Once the headcount is taken close the office doors as you leave. For disabled individuals, the stairwell landing is a safe zone to seek refuge until emergency personnel can safely bring you down. Every department is required to follow its departmental-specific duties. For example, securing the cash and files, securing all-important documents and guest information, or bringing the employee emergency telephone list.

Additionally, high-class personnel must have flashlights, batteries, and walkie-talkies in hand to effectively communicate with other management. All other equipment and resources will be in the care of the department heads in the designated refuge areas.

- *Identify and create the policy for shelter-in-place procedures including internal assembly points (safe areas), water, water purification tablets, shelf-stable food supplies, clothing, blankets, and other long-term stay materials.*
    - The policy should include if applicable:
        - Maps and floor plans should include:
        - Shelter-in-place assembly areas
    - Location of water, water purification tablets, shelf-stable food supplies, clothing, blankets, and other materials
    - Location of utility closets, circuit breaker panels, power lines
    - Location of gas, electric, water lines

Capcom doesn't seem to have any floor plans available to the public. Although it can be seen that the Capcom headquarters is roughly 8 or 9 stories tall. Shown below is an overhead view of the buildings.


松屋町筋
ドミノ・ピザ
Capcom Co. Ltd.
Capcom Co., Ltd. Head Office Building
内平野町
Capcom Co. Ltd.
Capcom Co., Ltd. Research & Development Office
内平野町食堂

Power lines are surrounding the immediate perimeter of the building. Due to resources provided by Capcom, we are unable to find other utility sources such as gas and water lines. 

Because of these power lines in the front of the building, it would be ideal to have safe locations in the back corner. At the back of the building is a parking lot. This should provide a quick route to evacuation if necessary and keep employees away from power lines in the case of a tsunami or other natural disasters. There are also a few shops nearby that supply food in case of a lengthened shelter in place.

- *Create a checklist for contacting and interviewing a disaster recovery specialist.*
    - Create a checklist for contacting and informing stakeholders (See Table 6-13 on page 176 of the “Guide to Disaster Recovery” textbook. A scanned pdf version is available in Files).

The checklist to contacting and working with business partners will include for the stakeholders are:

Names and titles of employees who are authorized to work with public utilities

Contact information and locations of public utilities and public works departments

How facilities and locations should be i.d for public utilities and public works departments

A list of all services provided by public utilities along with the capacity and consumption patterns

How to describe problems to public utility workers

Blueprints and diagrams that show all public utility hookups and shutoffs for the facility

A list of people who know the layout of a facility

The priorities set by the disaster recovery planning team dictate which communications systems are most important to the key’s business processes. This is all individual recovery procedures are required for each telecommunications service that our organization uses.

- *Create a checklist for contacting and working with suppliers*

Names and titles of employees that can talk to customers would be tech support lines and any of the higher-up managers that need to talk to them. Locations and

Numbers that belong to the customers should only be kept for a little, and then deleted or kept in a safe server where others cannot access. Customers should be told of what disasters can do to them and their product and that if something ever does happen to the main services, that there are backups of sorts, but not all services could be available. The customer should be told when services are expected to come back online and what is going to take some time to come back. If the customer needs to contact the company during a disaster, they should email us and we will try to get back to them as soon as we can. If other locations are available, email or call them to get answers.

Business Continuity/Disaster Recovery Phase X

- *Create an assessment for determining inventory or a list of critical resources at the damaged site.*

For determining inventory and critical resources at the site of the damage, it is important to know which resources are valuable and the number of people on site. In case of extreme weather conditions, it is important to properly ration and distribute supplies to employees in worsened conditions.

Main Examples of Critical Resources:

Food

Water

Electricity

These are critical resources in the event of an emergency because they can keep business going if necessary. With proper supplies, Capcom can work through any situation.

- *Develop a set of policies and procedures for employees to follow explaining proper safety guidelines.*

You are responsible for your safety and the safety of everyone around you. Do not take shortcuts and always follow all expectations. If you are not trained for a certain task, do not continue without further notice. Access the risks before approaching work and always keep an organized workplace. All employees must adhere to the rules and guidelines given by each of their associate department heads. All national laws and local authorities must be obeyed without question. Failure to comply with any of the rules or guidelines given will result in consequences depending on the act.

- *Create an assessment for determining inventory or building utilities.*

Making sure all the pipes and electrical wire are in good condition and or not placed in bad locations is ideal so that you don't have bursts and or shortages in the building. Gas leaks are a major problem that could cause explosions and or cause death by inhalation. Electric wires that are exposed can cause electrocution and if they come in contact with water could cause major damage. Water pipes can cause you to flood out the building which would destroy most of your building. So making sure all these things are maintained is vital to your company and the employees to make sure everyone is safe.

- *Inspect for hazardous materials, chemicals, or hazardous conditions.*

In the case there are hazardous materials on-site, it is important to evacuate the building immediately to prevent inhalation of toxic fumes or exposure to dangerous materials. Capcom asks that after evacuating the building that employees call emergency services to help remove the materials as soon as possible. While hazardous materials are being removed from the site, employees should work in the backup sites set up by Capcom.

- *Inspect resources and vital records for damage including water, fire, water, dust, ice, or physical damage.*

Stuff like water and dust can cause some major damage and we don't even realize it. The build-up of dust and or other air pollutants can get into fans and servers causing it to slow down and overheat which can cause a fire. Water spills and or flooding can cause a massive amount of damage as water and technology do not go well together. Depending on how much damage is done by the water, some can be usable by replacing only certain parts of the computer, but most of the time the whole thing would need to be replaced, and depending on what it is, it can be expensive. Making sure that all of the equipment is in good shape is ideal for the company to keep moving smoothly and efficiently.

- *Write a nature-based test scenario.*

In the event, a nature-based incident occurs all rules and guidelines will be followed by local authorities. Based on the scenario authorities will give out different procedures to follow and must be followed strictly. Anyone who disobeys the guidelines will be noted and dealt with properly. Everyone will need to know where all the equipment for the different scenarios is and must be prepared for any occurrences.

- *Write a man-made-based test scenario.*

In the event something occurs to prevent work from being done, all laws set by local authorities and law enforcement must be followed. Everyone is to remain calm and locate the nearest exits in an organized and calm manner. Anyone who fails or behaves out of order will be dealt with once the incident has finished. Due to current incidents, evacuations will be practiced once every month towards the end of every month.

- *Develop a plan to do a tabletop test of what would happen in the event of a mudslide.*

We as people have the right to be trained in case of this disaster happening at our place of work. With this training, we are able to mitigate the cause of the mudslide also to make sure all of our employees know their part if this was to occur. In the training, we can start by keeping the people who work in the building up to date with how we are preparing them. One of these ways is to show how we are eliminating potential hazards as we can conduct a thorough survey of the workplace. This would help identify harmful objects and eliminate them. For example, placing heavy objects on top of the shelves is not a good idea if an event was to happen to us we could put them down also placing items that might fall into aisles or the walkway that are part of the evacuation routes. Next is to conduct training with the employees. This we will have an all-hands so people can know the safety procedures which in return will avoid panic among the employees. This we can identify the routes to take, medical kits, and where to get them when they need them.

- *Write a memo to the CEO of the company explaining how testing of the plan is going to be performed.*

To whom it may concern, we will be conducting testing in order to be well trained and equipped if a natural disaster were to happen. This will contain all hands on deck training for one day to better prepare our team for this disaster. We would only need one day to do this but overall inspection of the building should happen at least once a week. The objective of this is to make sure our team is overall compliant in all avenues for any disaster so we can make sure we have slim to no risks of injuries or deaths.

Business Continuity/Disaster Recovery Phase XI

- *Prepare a memo discussing the organizational options for maintaining the plan.*
    - Including the destruction or archive of old copies of the plan including hard and soft copies, on- and off-site copies, and copies that may be stored with trusted vendors, partners, or at alternate work sites or facilities.

To whom it may concern, to become the top company that we strive to be. We must be able to properly discard old copies of plans whether that being hard or soft copies. This will reflect our companies values and promises that we made to have our vendors and facilities trust us. The first option that we shall implement is shredding paper copies that are deemed irrelevant as this is the quickest, easiest, and cost-effective way to discard our paper data. For our data that are stored in hard drives we shall back them up but the data that are no longer in use for us will be wiped clean using the program DBAN as it is free and can erase all files on our hard drives.

- *Prepare a memo discussing the advantages and disadvantages of retaining members of the original planning team.*

To whom it may concern, as we have seen from events there are advantages just as there are disadvantages of retaining members of the original planning team. One advantage of having new members is simply having new minds to work and new ideas that will better help with our growth of security and planning. Keeping the same members is great as we can decide what to delegate ourselves in when it comes to trials, such as we become more familiarized with the team members. The disadvantages of keeping our original members are it becomes a potential for conflict, as personality can come in place when we tend to work with the same team over a while.

- *Write a recommendation of how the plan should be kept up to date; make sure to explain your reasoning.*

To whomever it may concern, I have composed this recommendation regarding our plans. I believe they should be updated every six months. This will allow plenty of time to try new things or make some changes to areas needed. Keeping an updated plan should always be one of the top priorities so we can determine what worked best for our company and what are some things we should avoid. Making changes to the plan once a year is too long and can cause problems to drag on instead of being dealt with early. Additionally, making changes every month would be too excessive and wouldn't give time to properly try out new situations.

- *Write about the different approaches that can be used for reviewing the plan, and make a recommendation for the company.*

    Different approaches that the company can take to review the plan could be, that at meetings every month or something or during natural disaster seasons, go over the protocols of what to do during the disaster to save as much info (and also the most important asset, employees) as possible. Maybe have a potluck of such and just have a good time while talking about disasters if they were going to happen.

- *Write a paper discussing the different ways plan updates can be distributed.*
    - Then make your recommendation of how the company should do so.

The company has implemented a script that will automatically update and replace the old copy of the plan when an employee logs onto the computer. Logging in and out of your account will take the latest version of the plan and automatically update it for the employee. This ensures that the employee has the latest version and it hasn't been lost in transit or somewhere in the communication line.

The plan can be uploaded onto the cloud and that version can be changed by an employee with admin privileges and be distributed throughout the company. This can also be a way to send the plan to certain accounts if needed using user ID's.

- *Create a checklist form for managing updates to intranet documents.*
    - Rank the documents in order of importance (this is your opinion) and include details of why it is important (e.g. make sure the server is running: Important because if the server is malfunctioning then the plan is unavailable.)
    - Create a checklist for managing updated paper and digital documents. Rank the documents in order of importance (this is your opinion) and include details of why it is important (e.g. Make sure that the file is being distributed: Important because if the wrong plan is distributed then the procedures to respond to emergencies could be listed wrong.)

  For the company's plan, it is important to split it into segments that are relevant for each department. The company has put the plan onto the cloud and has set permissions and access privileges for each department. This ensures that only employees in the department view the part they need.

  If you do not have access to the plan you should have access to, please reach out to our system administrator. You must read and understand the BC/DR plan that has been allocated to you.

- *Develop, document, and implement formal BC/DR plan change management processes.*
    - The purpose of a change management process is to monitoring changes that impact or are impacted by the BC/DR plan. This process should include:

- Evaluating change notifications and requests.
- Implementing appropriate changes to the BC/DR plan.
- Testing, training, and auditing revised plan.
- Notifying stakeholders of changes incorporated, delayed, or denied.
- Revising BC/DR plan appropriately.
- Distributing updated copies of the BC/DR plan to appropriate parties.

To make changes to the official BC/DR document, there must be an absolute heads-up notice and department heads' approval. Therefore does the change brought about define key assets and operations of the company. Each change must take downtime, availability, and recovery windows into consideration. Additionally, with every change, there need to be defined recovery solutions. A drafted out plan with established communication and assigned roles to everybody before it can be tested out refined and retested before being fully implemented. All changes to the BC/DR document must be written out in full detail. Failure to do so will result in dire consequences. All departments that will be affected by any changes must be given a heads notice before drafting any written out changes. Once the final copy of the revised BC/DR is done all the associated departments must be given a copy as well.

References

110 must-know cybersecurity statistics for 2020. (2020, July 21). Inside Out Security. https://www.varonis.com/blog/cybersecurity-statistics/

https://images.sampletemplates.com/wp-content/uploads/2015/08/Disaster-Recovery-Plan-Template-for-Small-Business.jpg

Asurion Home+ what's covered. (2021, February 11). Asurion. https://www.asurion.com/homeplus/whats-covered/

Can mirroring replace backups in your disaster recovery strategy? - StorageCraft. (2020, December 22). StorageCraft Technology Corporation. https://blog.storagecraft.com/can-mirroring-replace-backups-disaster-recovery-strategy/

Capcom ir. (n.d.). CAPCOM IR. https://www.capcom.co.jp/ir/english/

CAPCOM | Corporate overview. (n.d.). CAPCOM IR. https://www.capcom.co.jp/ir/english/company/info.html

CAPCOM | Directors. (n.d.). CAPCOM IR. https://www.capcom.co.jp/ir/english/company/officer01.html

Civil, E. (2020, October 6). *Why Japan is earthquake prone and how it's dealt*. Japan Yugen. https://japanyugen.com/why-japan-is-earthquake-prone/

Coble, S. (2021, January 13). *Capcom data breach may have impacted extra 40k customers*. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/capcom-data-breach-worse/#:~:text=Capcom%20Data%20Breach%20May%20Have%20Impacted%20Extra%2040%2C000%20Customers,-Sarah%20Coble%20News&text=The%20Osaka%2Dheadquartered%20company%20became,been%20compromised%20in%20this%20attack

Comparison of disaster recovery sites: Which one to choose? (2020, February 20). Nakivo. https://www.nakivo.com/blog/overview-disaster-recovery-sites/

Data | Attractive local regions in Japan - Investing in Japan - Japan external trade organization. (n.d.). ジェトロ. https://www.jetro.go.jp/en/invest/region/data/osaka-city.html

Differences between a cold, warm and hot disaster recovery site. (2020, June 10). OTAVA. https://www.otava.com/blog/what-is-the-difference-between-a-cold-warm-and-hot-disaster-recovery-site/

ETool : Evacuation plans and procedures. (n.d.). Occupational Safety and Health Administration. https://www.osha.gov/etools/evacuation-plans-procedures

Evacuation procedures. (n.d.). Accredited Online College Degrees | UMGC. https://www.umgc.edu/current-students/student-life-and-support/safety-and-security/emergency-preparedness/evacuation-procedures.cfm

FEMA small business disaster grants. (n.d.). Small Business - Chron.com. https://smallbusiness.chron.com/fema-small-business-disaster-grants-61715.html

The first 7 things to do during an emergency evacuation procedure. (2020, November 2). BMS CAT. https://www.bmscat.com/2019/01/the-first-7-things-to-do-during-an-emergency-evacuation-procedure/

Full vs incremental vs differential backup: A detailed comparison. (2020, September 4). Knowledge Base by phoenixNAP. https://phoenixnap.com/kb/full-vs-incremental-vs-differential-backup

Full vs incremental vs differential backup: Which is better? (2020, December 4). MiniTool.

https://www.minitool.com/backup-tips/incremental-vs-differential-backup.html

The global garbage crisis: No time to waste. (2017, October 24). UN Environment. https://www.unep.org/news-and-stories/press-release/global-garbage-crisis-no-time-waste

Learn about dioxin. (2020, September 8). US EPA. https://www.epa.gov/dioxin/learn-about-dioxin

Maximum tolerable downtime. (n.d.). ScienceDirect.com | Science, health and medical journals, full text articles and books. https://www.sciencedirect.com/topics/computer-science/maximum-tolerable-downtime

Programs to support disaster survivors. (n.d.). FEMA.gov. https://www.fema.gov/assistance/individual/disaster-survivors#:~:text=Through%20the%20Individual%20and%20Households,expenses%20or%20clean%2Dup%20items

Servers - annual downtime by server age 2015 | Statista. (n.d.). Statista. https://www.statista.com/statistics/430801/annual-downtime-servers/#:~:text=The%20statistic%20shows%20the%20number,hours%20of%20downtime%20per%20year

Stakeholder communication for informed decisions: Lessons from and for the displaced communities of Fukushima. (n.d.). Fukushima Global Communication Programme. https://fgc.unu.edu/en/events/stakeholder-communication-for-informed-decisions-lessons-from-and-for-the-displaced-communities-of-fukushima.html

Switch-arctitan-ma. (n.d.). https://trust.titanhq.com/acton/media/31047/switch-arctitan-ma?utm_campaign=AT-ENG-BSN-Competitors&utm_adgroup=Arcserve-Exact&acctid=THQ&utm_source=bing&utm_medium=PPC&keyword=arcserve&matchtype=e&campaignid=391024771&adgro

upid=1197368780685271&gclid=&mh_matchtype=e&mh_keyword=arcserve&mh_adgroupid=1197368780685271&mh_network=o&msclkid=e0ed0e298e8917fa66e66e6cfd8fb385

This is how often earthquakes occur in Japan – Japan info. (n.d.). Japan Info. https://jpninfo.com/179564

The three stages of disaster recovery sites. (2016, October 11). Segue Technologies. https://www.seguetech.com/three-stages-disaster-recovery-sites/

The top 4 biggest threats to businesses today. (2020, September 18). BusinessBlogs Hub. https://www.businessblogshub.com/2019/09/the-top-4-biggest-threats-to-businesses-today/

Understanding the financial cost of downtime in manufacturing. (2020, November 15). Due. https://due.com/blog/understanding-the-financial-cost-of-downtime-in-manufacturing/#:~:text=Research%20shows%20that%20the%20average,%2422%2C000%20per%20minute%20of%20downtime

What is BCDR? Business continuity and disaster recovery guide. (2020, February 18). SearchDisasterRecovery. https://searchdisasterrecovery.techtarget.com/definition/Business-Continuity-and-Disaster-Recovery-BCDR

What is business continuity and disaster recovery (BCDR)? - Definition from Techopedia. (2013, September 7). Techopedia.com. https://www.techopedia.com/definition/13767/business-continuity-and-disaster-recovery-bcdr

What is cloud storage and how does it work? (2020, January 27). SearchStorage.

https://searchstorage.techtarget.com/definition/cloud-storage

What is hot site and cold site? - Definition from WhatIs.com. (2010, November 17). SearchCIO. https://searchcio.techtarget.com/definition/hot-site-and-cold-site#:~:text=A%20hot%20site%20is%20a%20commercial%20disaster%20recovery,all%20data%20processing%20operations%20to%20a%20hot%20site

What you need to know about cold site disaster recovery. (n.d.). SearchDisasterRecovery. https://searchdisasterrecovery.techtarget.com/podcast/What-you-need-to-know-about-cold-site-disaster-recovery

(n.d.). 株式会社カプコン：CAPCOM WORLD JAPAN. https://www.capcom.co.jp/ir/english/data/oar/2020/pdf/gov_02.pdf