William Lentini

Management of Information Security

Professor Geoffrey Dick

12/12/21

Assignment #3

For this assignment, I have been appointed as a member of the security team for an organization of my likening. This organization seems to have no disaster recovery plan for recovery from loss of information resources, which is pivotal to the ongoing operations of the organization. For the disaster recovery outline I am going to first briefly describe the organization that we are working for, and the key elements of what is going to be included in the disaster recovery plan. The organization that I am working for is an organization that works on making and editing softwares that will prevent things such as malware, viruses, adware, etc for the general public. The eight main points that are going to be in the disaster recovery plan according to kmicro.com are “Set your recovery time objective (RTO) and recovery point objective (RPO)”, “Take inventory of hardware and software”, “Identify personnel roles”, “Choose disaster recovery sites”, “Outline response procedures”, “Identify sensitive documents and data”, “Create a crisis communication plan”, and “Run continuous practice tests to ensure your plan is effective.”

The first main point of the disaster recovery plan is to figure out how long it will take you to recover all applications and the age of the files that must be recovered for normal operations to continue to take place. This can help the organization figure out which solutions are needed and which are not needed to survive a data breach and suffer the least amount of losses by determining which hardware and software configurations are needed to recover the lost data.

This is important because this essentially provides a template for how and where you need to go to possibly recover your data in the event that a data breach actually happens. Being able to know whether it's a hardware configuration, a software configuration, or both can help you recover your files in a very timely manner and get you and the rest of your organization back to working normally and making money for the organization. The second main point of the disaster recovery is to take inventory of hardware and software, the easiest way to do this would be to split it into three sections depending on necessity. The first section would be critical applications you need to operate with, the second section would be applications that you would need to use within the next couple of days, and the third section would be applications that you wont need for the next couple of days. This list of critical applications should be reviewed a couple of times a year as you are always upgrading and downloading new applications. This is important because being able to identify the applications that you need to be able to work and using them will help in getting the organization back to working normally in a quicker fashion than if you were to try to recover all applications, even the ones you don't particularly need for work in the circumstance that a breach would occur. The third main point of the disaster recovery plan is to assign roles to the personnel of your organization. These roles will help with figuring out the responsibilities between each person in the event of a disaster. This should include a list of disaster recovery personnel with each person's position, responsibilities, and emergency contact information. It is also important to have lists of back up employees in case any of the disaster recovery personnel are not around in that given time. This is important because it helps organize and lead the organization into the correct direction when going into a disaster. Having certain people who can focus on certain parts and have certain responsibilities is much more efficient and time saving because it allows someone to have their full attention on one part of the disaster. The fourth main

point of the disaster recovery plan is to assign sites where disaster recovery will occur. This means having a spot where all of the company's essential data, assets, and applications can be temporarily moved during a disaster to prevent mass data loss. There are typically three types of data recovery sites: hot sites; these are used as data centers for hardware, software, and personnel and customer data, warm sites; these are used to allow access to all critical applications, and cold sites; these are used for storage of IT systems and data. All of these data recovery sites should perform backups and replicate workload speeds to the best of its ability to help recovery speeds. This is important because being able to transport all important and even non important data to a separate space where you know that all the information is safe is a big stress reliever for the company. They know that most, if not all of their critical information is safe and they are able to keep working at relatively close to workload speeds while the rest of the recovery is taking place. The fifth main point of the disaster recovery plan is to document your recovery strategy so that you and your team understand what to do in the event that a disaster happens. Writing down guidelines such as communication procedures, data backup procedures, instructions for initiating a response strategy, and post disaster activities that take place after operations are up and running again can help give the team a starting point and template for what they need to do and how they are going to do it. This is important because having all employees on the same page and knowing what to do and how to bring the company back to normal operation will bring forth a smooth transition from disaster to normal operation, and in a relatively shorter time than if they were disorganized and did not know what to do or where to start. The sixth main point of the disaster recovery plan is to identify which documents and data you think are sensitive, documents such as Personally Identifiable Information are very important documents that you would hope not to lose in a big data breach. All sensitive documents are also limited to who can access them during

the breach. This is important because being able to identify sensitive documents that the organization can not afford to lose can help in separating the documents that the organization does not really care about, and puts the focus in the sensitive documents, which has the organization put more effort into protecting those documents by doing things such as limiting who has access to those sensitive documents until operations are up and running again. The seventh main point of the disaster recovery plan is to create a clear strategy for communicating with people such as employees, vendors, suppliers, and customers in the event that a disaster does occur. Letting the public know the situation of the disaster will bring them more confidence in your ability to handle the situation. Being able to let them know the estimated time that everything will be up and running is great information to know as a customer instead of keeping the customers on a cliffhanger and leaving them wondering when the services will be back up. This is important because it allows for the organization and the people to coordinate when they can be using their service, it also helps the public understand the severity of the attack and lets the public have more peace of mind knowing that the service will be down temporarily and will be back up sooner than later. The eighth and final main point of the disaster recovery plan is to test your disaster recovery plan at least once a year to make sure that it works, things that you should be looking out for when doing these tests are failed backup hardware, slow internet connection, or other red flags that can pose a risk to your plan. You should also be reviewing your personnel list and inventory list to ensure that everything is running smoothly and is kept up to date. This is important because doing recovery plan tests once a year can help you figure out what needs to be worked on and can help you fix the potential problems that can hurt you in an actual disaster situation given you do not do the annual test. It also allows you to go over personnel roles to make sure that everyone has the correct roles and responsibilities and that

everyone knows what to do in any given disaster situation, and it also allows you to go over inventory to see if anything needs to be updated, added, or moved between the three sections of criticality.

To summarize my disaster recovery plan, I am working at a organization that creates software for the general public and there are 8 points to my disaster recovery plan that help the organization minimize risk, continue normal operations as soon as possible, maintaining industry compliances and the penalties that can come with not reaching the obligations, and addressing the concerns of the disaster with your fellow customers, employees, investors, and owners to help them feel at ease and have a clear mind from the disaster.

Works cited

- “8 Things to Include on Your Disaster Recovery Plan Checklist.” *KMicro Tech, Inc.*, 12 July 2020, https://kmicro.com/things-to-include-on-your-disaster-recovery-plan-checklist/.