Security Lab 14 & Lab 15 - DR & Risk Essay

Fundamentals of Information Security: Cybersecurity (88252)

Ana Herrera Flores

Exercise 1 – Personal Disaster Recovery Plan (Case Project 14-4)

Companies today should have some type of Disaster Recovery Plan to ensure their business continuity. However, it is just as important that everyone using a computer has some type of disaster recovery procedure in order to ensure that valuable data is not lost; For example, Family Photos, Tax Records or Receipts, Personals Databases, and more. In addition, how long will it take for you to get back online with important software that you purchased or own?

For this exercise, Create a one-page document of a personal disaster recovery procedure for your home computer. Be sure to include what needs to be protected and why.

Does your DRP show that what you are doing to protect your assets is sufficient? Should any changes be made? How will you gain access or purchase a new computer?

In my house, I count with 2 computers where I have all my data, information, software, resources, and memories. One is a desktop (Windows OS), and the other one is a laptop (MacOS). My Windows computer contains all the software and tools for schoolwork and independent projects that I realized to develop tech skills. However, the desktop does not have any of my personal information like pictures or bank accounts. For this computer I just want to protect recent projects that I'm working on, I have 500GB on the cloud where I back up files, in case something happens to the hard drive. I don't have a big cloud subscription on my desktop because I usually delete the data when the

task is completed. I perform backups every time I create a new project or update an old one. This can be a day or a week, always depending on the last time I made changes. For software, I have accounts in all the software that I use, especially the ones where licenses purchased were made. Also, I update all of them when a new version is out to avoid vulnerabilities. Against malware, the antivirus installation on the computer is McAfee premium. I used to have a UPS in the past; in case of a power outage my progress would not get lost, and I think it is something that should be back in my Disaster Recovery Plan again. My Mac computer contains all my personal data, such as photos, videos, bank accounts, books, insurance information, and important documents. For this computer I have 2Tb on the cloud, and every file on the hard drive is also on the cloud, also an external hard drive that I update every two weeks. I don't really have a lot or important software on this computer. Intego is the antivirus software that I use on the Mac, and it also offers Internet security. I count with 2 portable chargers power banks that are always fully charged, in case I run out of battery and don't have access to outlets. Like on my Windows, I update all systems and software as soon as a new update is available. Three steps that I consider necessary to add to my recovery plan are: create a fund in case I need to make repairs to my hardware or buy a new computer; create a document with all the necessary recovery steps, licenses and backup locations.

Exercise 2 – Personal Backup Procedures (Case Project 14-6)

What are your personal data backup procedures? If you have none, create one, and answer the following questions:

Write a one-paragraph description of how you back up your data, what data you back up, how often you perform a backup, where your backup is stored, etc. Use the information in this module to compare it with your current backup procedures.

Write a second paragraph that identifies the strengths and weaknesses of your current procedures.

Finally, write a third paragraph that outlines how you could change your current procedures to make your backups more secure.

Backing up data is an important step to preserve information in case this information gets lost or contaminated, you have a copy of the original data. I have two computers which I use for different purposes and for different kinds of information. My Windows computer, which I use for learning projects and schoolwork, backs up its information on the cloud. I just backup the files of projects that I'm working on or that I just started. This happens every time I start a new project or when I modify an existing one. It could be every day or week; it depends on when the last time that I modified something. On the other hand, I use my Mac computer for my personal data like bank and insurance information, photos, and books. The data backups automatically every day, and I also possess an external hard drive that I update once every two weeks.

On my Mac computer, which is the computer that contains my personal data, I use 3 copies, in three different places of the data for backups. Which is a recommended method by professionals. However, the backups that I do using the external hard drive should be more frequent. Two weeks is a long period and the data gets modified a few times. In case of a disaster, and no access to the cloud, I might need data that I don't have because of the long time between backups on the hard drive. For the Windows computer, I should also use 3 different kinds of storage. I usually don't keep the files once I am done with a project, but what if I need to have access to some of them and I

am offline? Getting another external hard drive for this purpose must be one of my immediate to do.

As mentioned before, I already use 3 different backups on my Mac, which is well recommended in this chapter. Although, I should implement the same method on my Windows computer and get an extra one that does not contain the original copy. I should implement automatic backup on my Windows computer too, even though I always make changes to the cloud copy. This is done manually, and I can forget. Also, the use of a continuous data protection (CDP) product that allows me to restore my documents to a previous state seems like a smart idea. Another step that I would like to add to my backup plan is cloud security. Features like Impossible Travel by Microsoft, Risky IP address, and others can help against attackers trying to have access to my data.

Exercise 3 – Intellectual Property (IP) Theft (Case Project 15-2)

Use the Internet to find details on four recent incidents of intellectual property (IP) theft from an organization. What was stolen? What vulnerability did the threat actors exploit? How valuable was the IP? What did the threat actors do with it? What loss did it create for the organization? How could it have been prevented? Write a one-page paper on your findings.

In 2022, almost 23 million Pegasus Airlines files containing passengers and flights information were leaked. The error happened because of a cloud misconfiguration by a system administrator, exposing AWS S3 bucket linked to their flight system software. There was no malicious activity in this case, but a human error and insider threat left sensitive cloud data without

password protection. This IP was valuable in a way that contained identifiable information about customers and staff. The loss in this case was 6.5 terabytes of data accessible to the public and a fine of $183,000. Luckily, no affiliates were affected. This could have prevented monitoring user's interactions with sensitive systems and data and making sure that the person that was configuring the cloud had the proper training to do so.

In 2023, an attacker made use of social engineering techniques and gained access to 133 Mailchimp accounts. As we mentioned before, this attacker used social engineering techniques to get employee credentials and access the enterprise's systems. There were no serious repercussions for the organization in a financial way, but sensitive information such as email addresses and personal data. This can cause reputational damage and the loss of customer trust leading to financial repercussions over time. We can learn from this that training in recognizing and avoiding social engineering techniques is fundamental for employees.

In 2025 there have been various attacks from Chinese hacking groups to the US and European companies. Some of these attacks include the use of backdoors to gain access to the systems and the network. These attacks had a high value because the threat actors were able to steal trade secrets, patents and designs. There is not a clear record of what happened with this information, but speculations are that this information was sold for personal gain. For the companies harmed by these hacks, it is clear that they suffer financial losses, security breaches, and damage to their reputation. To avoid or minimize the consequences of these malicious actions, companies can implement advanced threat detection, robust security protocols, and collaborations between organizations to share threat intelligence.

In 2023, two former employees leaked Tesla confidential information to a German newspaper. The threat actors were insiders and had access to sensitive information. There is no statement why they did it; it could have

been revenge or financial gain. This was a high value IP, nearly 100GB with staff and customers' information, financial data, Tesla's production secrets, and customers' complaints. The consequences were exposure of data of 75,000 people, which resulted in a $3.3billion fine for the lack of protection and damage to the company's reputation. The company should have applied pseudonymization techniques and background checks during the onboarding sessions of these employees to have an idea of their intentions. Also monitoring their activities would have been helpful for detecting their malicious activity.

Exercise 4 –Unconscious Biases in Cybersecurity (Case Project 15-3)

How could unconscious biases impact cybersecurity? Review the information in Table 15-4 of Module 15 and select four of the biases. Then create a practical example of how each bias or effect could impact cybersecurity. Now return to the table and list in order what you consider your own biases from most prevalent to least. What can be done to minimize the impact of these biases? Write a one-page paper on your findings.

Unconscious biases can impact cybersecurity and have, in some cases, serious repercussions for an enterprise due to human patterns in their behaviors like trusting in your employees and not monitoring properly their use of the company's resources by them; it can also influence our decision-making about security measures, prioritizing some risks over others based on our own beliefs. In the hiring process, biases can also be prejudicial, and recruitment can be poor in diversity in the cybersecurity team. There is also the necessity for awareness, that might affect the design and delivery of training to the employees, and the failing to address specific well-known vulnerabilities such as social engineering techniques. Biases can also be responsible for the way that certain incidents are handled, believing that they

were caused by certain groups, closing the spectrum to analyze and address the threat.

The following four biases can impact the security of a company in the following ways:

- Fundamental attribution error: Companies might attribute security incidents or blame employees for phishing attacks, making it seem like a failure of that employee, rather than look at the bigger picture like lack of training, unclear policies and high-pressure work environments.
- Aggregate bias: Aggregate bias can lead to the assumption that all threats and vulnerabilities are the same, closing the window to look for other incidents. Companies focus on aggregated data and statistics, misjudging the likelihood of other risks to occur or impact the organization. The same way with the creation of security strategies based on general data, enterprises may create these strategies ignoring their own and custom vulnerabilities.

- Availability bias: Companies may focus on current and highly public known cybersecurity attacks like ransomware or viruses' attacks rather than look at equally critical risks from inside the company like insider threats or outdated systems. These can also affect the way the enterprise manages the security budget, investing in some vulnerabilities and leaving others unaddressed.

- Present bias: Organizations may prioritize cost savings or focus their budget on immediate needs rather than in long-term cybersecurity measures leading open door for future threats and risks. Not investing in quality training for employees can cause organizations to be victims of simple attacks such as phishing and social engineering. These two things together make an organization have a reactive approach and just

address cybersecurity issues after they occur when the ideal is to have a proactive approach and avoid these issues taking place.

The biases that I consider that represent a problem for myself and what can I do minimize the impacts of these biases are:

- Anchoring bias: The use of Risk Control Self-Assessment (RCSA) and involve multiple people on it to reduce the focus on a single perspective. When doing the decision-making process make sure to include cross-functional teams to have a broader spectrum of points of view. Use and analyze data to base decisions in facts rather than in the initial impression. Review cybersecurity strategies to make sure these strategies are not outdated or influenced.

- Framing effect: Use the RCSA to ensure decisions are based on the facts rather than on how information is presented. Exclude emotional language when communicating risk and solutions, focusing on clear descriptions. Train your team in how to think critically and look for all alternatives regardless of how data is presented. Include staff with different points of view in the discussions to provide diversity to the output.

- Availability bias: Use of the RCSA, and quantitative tools like Annualized Rate of Occurrence (ARO), and Mean Time Between Failure (MTBF) to ensure risks are identified systematically rather than relying on biases. Gather data from different resources to have a bigger picture of the problem. Give training to tech employees to evaluate risks based on evidence and not on memorable events.

- Fundamental attribution error: Train your team to raise awareness and consider external factors rather than just blame individuals. Implement simulations to make people understand how their actions can have consequences for the enterprise's security. Promote collaboration,

make teamwork where staff can work together to identify and understand cybersecurity problems rather than blaming each other.