Data Security and Privacy Findings Final

Name: Dalton Jeske

Purpose: Summarize what I have learned in this course.

Date: 5/15/2024

**10 Data Security and Privacy Themes**

1. General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and California Consumer Privacy Act (CCPA) help regulate security and privacy standards to ensure a base level of protection.
2. Personal Identifiable Information (PII) of all levels deserves a certain level of protection, not just private, sensitive information.
3. Security permissions for employees can go a long way for overall data security. Not everyone needs access to everything.
4. Encryption is a relatively simple yet effective method to add a layer of protection to digital information. Just don’t lose track of the decryption key!
5. ALWAYS approach suspicious emails with caution. Don’t click something that seems fishy. Hover over images and links to see where they will take you. If it is too good to be true, it probably is a scam.
6. Social Engineering attackers want to take advantage of strong emotions like sadness, anger, and fear. Take a step back and think, “does this make sense?” before you do something you will regret.
7. Network Vulnerabilities can be physical OR digital. It is important to have the physical devices in the correct hands AND to make sure that all software is up to date.
8. Password management can be a fun and easy way to bolster password strength which also leads to an overall increase in security strength.
9. Transparency is important when a security breach happens. Do not try to sweep it under the rug or make light of it. Own it and learn from it so that you can make sure it doesn’t happen again in the future!
10. Technology develops at a rapid pace, and it is important to stay on top of best practices for security and privacy. The recent developments of AI can be both a blessing and a curse when it comes to security so continually educating yourself is a great first step to be safe.

**Security/Data Breaches**

I have chosen security/data breaches as my topic to expand upon. I chose this topic because I think that the reaction to a breach is as important, if not more important than the actual breach. I also believe that every individual that sets off for a career in the IT field will encounter some form of security breach so being prepared is vital to long-term career success. You do not want to be known as the person who buckled under pressure or continued to let a problem persist. Developing solid response plans is a great way to have some sort of foundation in place for when the inevitable breach happens.

So, what are these response plans? What plans, systems, and tasks need to be in place and assigned to combat a breach when it occurs as well as in the aftermath. A data breach response plan typically has six steps which are as follows: Preparation, Identification, Containment, Eradication/Recovery, Communication/Notification, and Lessons Learned/Documentation.1



Figure 1https://www.cymune.com/incident-response2

When making a data breach response plan, following these steps is the best way to ensure that the breach is ready to be addressed. Every step is important so what exactly does each step entail?

Step one being preparation is kind of self-explanatory but is the foundation for the rest of the response plan. In this step, the plan is documented, members of the response team are designated, and communication protocols are established. During this time, it is also important to identify critical data assets, conduct risk assessments, and implement security measures. Employee training also plays an important role in preventing data breaches from occurring. The preparation step basically has you do everything in your power to prevent a breach from occurring but assigns and defines the roles and responsibilities of individuals if a breach does occur.

Step two is identification specifically pertaining to recognizing when a breach occurs. This step is not as much about identifying the source of the breach but more about knowing that a breach occurred. Having systems in place to detect unusual traffic, access, or data extraction is important to notice when potential breaches have or are occurring. These systems should immediately trigger and activate the response plan when these oddities are present. It is also important to note that these systems should frequently be tested and updated (in the preparation stage) to ensure that there are not missed breaches or false triggers.

Step three is containment and just like it sounds, it is to make sure that the breach does not worsen or spread. The damage has already been done and now what can be done to stop it. This can include isolating affected systems, temporarily (maybe permanently) disabling compromised accounts, or blocking restricted or unauthorized access points. These containment strategies should be methodical and well documented so that it is known exactly what has happened, what has been done, and what can still be tried to contain the breach. This step is vital to avoid a complete data breach which could ultimately lead to a complete system shutdown and halt of all activity/production.

Step four is Eradication/Recovery. These are sometimes separated into two separate steps, but they are intertwined so keeping them together makes sense. This step is simple in concept. Eradicate the root cause of the breach and recover/restore the affected systems afterwards. Once the breach has been handled, implementing improved security measures or patches can further aid in preventing further breaches from happening. It is also important to make sure that the breach source is completely removed when restoring systems.

Step five is communication and notification. This is another step that can be broken up, but they go hand in hand. Maintaining transparency and communicating/notifying the breach to all parties involved is crucial to maintain trust within and outside of the organization. Users will want to know what happened, if they are safe, and what they can personally do to protect themselves. There will be anger and frustration, but it is better than hiding what happened. This is also a great time to say sorry and educate those affected on what measures have been taken to prevent a future breach from occurring.

The final step is lessons learned and documentation. Documenting everything that occurred through this entire process is important not only for the breach, but also for how the breach was handled. Reflecting on the entire process can help find areas of improvement so that future breaches are handled even better. They also can be a guide for if a similar breach happens in the future. Lastly, the documentation of all events is great for the potential legal aftermath that may occur within courts or regulatory agencies.

Data breaches can be a scary and daunting event. Everyone makes mistakes and everyone will face a breach of some magnitude at a point in their career. Having the proper response plan in place is vital to handling a breach when it inevitably occurs. Following the 6 steps of Preparation, Identification, Containment, Eradication/Recovery, Communication/Notification, and Lessons Learned/Documentation is a great way to formulate a response plan. Having this base will hopefully make handling any security/data breaches less stressful and lead to great execution and success!

References

1. Jarmul, Katharine. Practical Data Privacy. 1st ed., O’Reilly Media, 2023, pp. 109–112. Accessed 15 May 2024.
2. potenzaglobalsolutions.com. “Incident Response: 6 Step Plan, Process and Benefits | Cymune.” Cymune, 2024, www.cymune.com/incident-response. Accessed 15 May 2024.