What’s the Worst That Could Happen? (50 points)

This is a question you should (and will be) asking yourself as you take on a security officer role. Quite honestly, this statement could become your undoing if you do not think it through or try to avoid answering such a question; however, the extreme “voice of doom” is not one you will be visiting very often. You should be evaluating the possible circumstances and ask yourself the above question as it pertains to something that could happen, such as a fire or user error.

For this exercise, you should think about a local company (one which you work or have worked) or a fake marketing firm in Kansas City Missouri. Ask yourself this question as you think through what they have and what could be lost. Think of a minimum of 7 threats to this network (one for each of the 7 IT Infrastructure Domains [pg.7]) and describe “What’s the Worst That Could Happen?” if these threats came true. For the threats, you should think of 5 within the realm of possibility and 2 on the fringe of possibilities.

Organize this response as an APA formatted paper. For each threat, you should write at least one paragraph responding to the question to each threat.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Not Met | Basic | Proficient | Distinguished |
| Identified and describes threats or risks (15 points) | Did not identify any threats (0) | Listed 1 to 6 threats (1-7) | Listed 7 threats (814) | Went above and beyond minimal requirements (15) |
| Demonstrates knowledge of vulnerabilities (15 points) | Did not demonstrate knowledge (0) | Demonstrated  basic level knowledge of vulnerabilities (17) | Showed a proficient grasp of vulnerabilities and how they affect their environment  (8-14) | Showed an advanced level of knowledge of how threats impact their environment (15) |
| APA formatting (10 points) | Did not utilize  APA formatting  (0-3) | A few APA formatting errors with multiple mistakes (4-7) | Little to no APA formatting errors (8-10) |  |
| Grammar and structure (10 points) | Student submission is below college level writing expectations (0-3) | Multiple grammar and structure issues (4-7) | Little to no  grammar and  structure issues (8-  10) |  |

Course Outcomes Assessed:

1. Identify and define risk and risk management techniques.

5. Identify and evaluate threats, vulnerabilities, countermeasures, and mitigation recommendations.

The first domain is User domain, and a possible threat would be users accessing non-work-related sites or checking their personal email leading to the user swinging the door open to allow in a lot of bugs and hackers. This can lead to the loss of a lot of information and would end up with the person being fired and potentially charged. To mitigate this risk would be to block a lot of sites and only allow access to the work sites and hold a class to go over the risks with the users.

The second domain is Workstation domain where there is the risk of the workstation not being secure and becoming a door for hackers to access. To mitigate the risks here it would be best to make sure that the firewalls are in place and that the workstation get regular virus screenings as the workstation could lead to a lot of information being taken.

The third domain is the LAN domain which has the possible threat of an unknown and unauthorized user which if not caught opens the network for attacks like DOS. To mitigate this would be to check the network access logs to make sure that there are no discrepancies of users on at strange times or that are not known.

The fourth domain is the LAN-to-WAN domain which has the possible threat such as man in the middle and can end up with not receiving data or sending out information that gets intercepted. To mitigate this, they could implement filtering to make sure that the IP packets are correct and can use multiple levels of encryption to protect anything outgoing.

The fifth domain is the Remote Access domain which has the possible threat of someone remote accessing a workstation and gathering data to sell. This can be avoided by turning off remote desktop in Windows and setting up authenticators for remote access.

The sixth domain is the WAN which has the threat of the internet and hackers going through there to send trojan horses or malware. If everything is connected to the internet the company could lose a lot of its secrets. A way to mitigate this would be to keep the main database storage disconnected from the internet if possible and set up multiple switches it has to go through to even get close.

The seventh domain is System and Application domain where there is the threat to the database such as an insider threat where a person working for the company steals data and information that could crush the company. A way to mitigate this would be to properly screen workers and set up levels of authority so that an intern can not access all of the database.

Abdullah Alshehri, C. P. P. (2021, December 12). *What are the seven domains of a typical IT infrastructure?* LinkedIn. Retrieved September 18, 2022, from https://www.linkedin.com/pulse/what-seven-domains-typical-infrastructure-alshehri-cpp-pci-psp-/?trk=public\_profile\_article\_view

Alexandra, J. (2018, January 15). *The seven domain of a typical IT infrastructure*. School of Information Systems. Retrieved September 18, 2022, from https://sis.binus.ac.id/2018/01/15/the-seven-domain-of-a-typical-it-infrastructure/#:~:text=Seven%20Domains%20of%20IT%20Infrastructure,%2C%20and%20System%2FApplication%20Domain.

Gibson, D. (2015). *Managing Risk in Information Systems* (2nd ed., Ser. Information Systems Security & Assurance).

Securing the 7 domains of an IT infrastructure: A multilayered approach. (2019, September 21). Retrieved September 18, 2022, from https://neilhartsfield.com/defenseindepth/

Slandail, & Author Slandail. (2018, July 1). *Systems and applications security - SSCP domain 7*. IT Security Career. Retrieved September 18, 2022, from https://itsecuritycareer.com/sscp-domain-7-systems-and-applications-security/