Harm Discussion

A data collection company can face the vulnerabilities of; inability to access data or loss of data. When an attack is successful, and penetrates the system the data collection company uses. The system would face the harm of losing information it has gathered over a period of time, which will be expensive to replace an example is if the world bank data tool was hacked and lost information between the years of 1900-1920, it will be difficult to replace unless there is back up. Also if the is inability to access data due to log in security errors, constant attempts of log in can render accounts inactive which creates an issue for the user. A social media company shows the vulnerability of breach of confidentiality. A successful attack on a social media company will compromise user accounts, reduce user confidence and violate user privacy, thus the need to have control of the systems vulnerability. A file processing company can show vulnerability to integrity if the system demonstrates an inability to modify a file in the acceptable way. An example is a number of years ago a malicious macro in a Word document inserted the word “not” after some random instances of the word “is;” you can imagine the havoc that ensued. Because the document was generally syntactically correct, people did not immediately detect the change. In another case, a model of the Pentium computer chip produced an incorrect result in certain circumstances of floating-point arithmetic.