Module 3 Journal Entry

Davis Plude
6/3/2025

Researchers will use information gathered from sites like privacyrights.org to quantify and identify trend analysis, find root causes of the breaches, determine policy impacts, and determine economic impact. Identifying trends in cybersecurity and social sciences is important to predicting important attributes later on. An example could be data breach up ticks after certain healthcare organizations decisions, this could allow cybersecurity professionals to prepare and protect themselves against these almost scheduled attacks. These information sites may also publish information about how these breaches started. This can be super beneficial to companies that may be going down the same road of poor cybersecurity and be a wakeup call to start fixing their internal systems and processes. Cybersecurity policies are becoming very important for any company small or large, but these policies are only as good as the weakest link. If a new technique comes out to obtain data maliciously that breaks the currently accepted policy it is important to notate and revise the policy before it happens again. The name of the game in cybersecurity is preventing attacks before they start and that's what these policies do. Another key factor to look at is the economic impact of these data breaches. This information is probably the biggest wake up call to unsecure companies. When researchers can show a direct financial loss due to a cyber attack it makes even non-technical companies rethink their systems. The main two social sciences that can use this information are psychology and economics. Psychologists may use this information to determine the connection between a data breach and the public perception of the company. Economists on the other hand will look at the financial problems with cyber attacks.

References

Privacy Rights Clearinghouse. (n.d.). *Data breaches*. PrivacyRights.org. https://privacyrights.org/data-breaches