Journal Entry #3

November 1, 2021

**How has cyber technology created opportunities for workplace deviance?**

According to a routine activity theory (RAT), a criminal act possesses three variables. (1) A suitable target, (2) a motivated offender, and (3) the absence of a capable guardian. Thinking within a workspace, its easy to see how an employee can cause some damage. Workplace deviance can be seen as the deliberate desire to harm an organization. An example of this can be employee sabotage. Because these individuals have the opportunity of accessing numerous amounts of data/physical equipment, this leaves a risk of theft or damage. Companies have to trust their employees and sometimes this backfires. One bad decision and things like hard drives and private information can be stolen. Another way an employee can harm organizations is by accessing unauthorized information. This can be easily done by accessing a computer in which the original user forgets to logout of. This leaves the company susceptible to any damage the user might want to do. Additionally, employees can be harmful by using unauthorized software on company computers. This can be hard to detect within a workplace and can create massive problems such as data breaches. As you can see sometimes the biggest threat to a companies security is within their walls. Its important to always improve security guidelines and safety measures to prevent these things from happening. Things like encrypting all devices can be helpful in preventing data theft. Ultimately it will always be a difficult thing to counteract as there will always just have to be a trusted bond between employee and organization.