


Collection

Users can Collect posts into a printable, sortable format. Collections are a good way to organize posts for quick reading. A Collection must be created to tag posts. [More Help](#)


Thread: Discussion Post 4
Post: RE: Discussion Post 4
Author:  **LEAH DREW**

Posted Date: November 3, 2019 9:44 PM
Status: Published
Overall Rating:

Deloren,

I agree with your examples. Often the offenders are employees that are unsatisfied with their jobs, or trying to compete with other employees like you said. If an employee also has access to things that they could use to improve their situation, albeit illegally, then someone who is desperate or upset enough might use them. You bring up an important point that some employees might not even be looking to improve their situation; they just want to get back at the company for something. However, our reading mentioned that a lot of cybercrimes committed by employees go unnoticed by the company. Do you think that that might influence whether an employee might commit a crime out of anger, or the type of crime they might commit?

(Post is Read)

Thread: Cyber Technology and Workplace Deviance
Post: Cyber Technology and Workplace Deviance
Author:  **LEAH DREW**

Posted Date: November 3, 2019 9:09 PM
Status: Published
Overall Rating:

Cyber technology creates opportunities for workplace deviance in several ways. Criminals base their actions on three variables: whether they have a suitable target, whether they're motivated, and whether there is a lack of capable guardianship or barriers in the way. Technology makes it easier for an employee to commit a crime undetected; often, they are misusing information that they already have access to or can easily get access to. This means that there is virtually no barrier to committing this type of crime, which is a major factor in motivating criminals. Lack of capable guardianship also comes into play in international crimes, where it's much more difficult for law enforcement to catch and prosecute the perpetrator if the crime is committed through technology.

Because businesses are less likely to report when there's a breach, white collar criminals commit cybercrimes knowing that they'll face few, if any repercussions. Employees know that their employer likely won't publicize the incident for fear of a negative impact on their business. This reduces the chance that the offender will be prosecuted by law enforcement and contributes to the "dark figure" of this type of crime.

Even if the breach is detected and the offender is caught and prosecuted, it is usually long after the breach occurred, and the offender has already had the opportunity to profit off the information stolen or tampered with. Combined with the fact that it's unlikely that they'll be caught and

punished at all, a criminal would see that the reward is much greater than the risk. Cybercrime is typically very costly for a business, and a white-collar criminal is in an advantageous position to commit a very profitable crime with few barriers to discourage them.

(Post is Read)

← OK