In our ever-changing society, cybercrime continues to evolve, leaving us with the decision of how to effectively punish offenders in the most ethical way. Overall, it makes the most sense that cybercrime punishments should be focused primarily on rehabilitation rather than retribution. This approach is a far more constructive approach that helps determine the root cause of the crime and how to stop it and encourages societal reintegration rather than being locked away for extended periods (in cases that are less serious or violent) It is notable that “the typical cybercriminal looks very different from the criminals of serious organized crime, she said. The average age of a cybercriminal is 19, as opposed to a drug trafficker’s 40 to 50 years of age. Their recidivism levels are also very low, and it doesn’t take much to deter them away from cyber offenses” (Chan, https://now.fordham.edu). Many cybercriminals are very young and new to the world of crime, so getting them to not re-offend is much less a tall task than older criminals who have more developed brains and have reoffended before.

Rehabilitation focuses on the underlying issues many of these cybercriminals face, such as financial desperation or lack of a moral compass. These individuals are often extremely intelligent and therefore can have their skills redirected toward practical applications such as jobs or projects. Police will take part in what are called knock-and-talks, where they will arrive at a soon-to-be criminal’s door to give them a warning and educate them on the moral implications and boundaries of the act they’re on track to commit. Chan notes that “Francis said, “Every single one we’ve delivered over the four years—up to 500 cease-and-desists have been signed—not one has pushed back. I think we’ve got only got one case where we can say that individual has gone back and committed a crime” (Chan, <https://now.fordham.edu>). This quote shows the effectiveness of police exercising their right to service and not just to punish people for crimes. The question is what is a more productive response to a potential crime?” Francis asked. “To wait for it to happen, because that’s where the blood and thunder is, or to make sure that the ones that we’re investigating are there because they’ve made an informed choice?” (Chan, https://now.fordham.edu). Police should not just wait for the offensive to take place, but rather do what they can to prevent it. There are also a variety of programs that convicted cybercriminals can enroll in to rehabilitate. These are not intense correctional programs, but rather educational programs that help offenders develop a moral compass online.

Many argue that retribution is the way to go because rehabilitation undermines justice and causes offenders to avoid proportional punishments for their actions. It seems as though justice in a jail cell is essential to uphold societal norms and deliver justice. However, while in certain more violent/detrimental cases, this is probably the way to go, there is no way to guarantee that this will prevent offenders from doing what they did all over again because they may not fully understand the implications of their actions.

In conclusion, focusing on rehabilitation rather than retribution opens the door for a second chance for many young offenders, which has a high success rate and low rate of recidivism. Their skills can be redirected toward beneficial applications and their morals realigned.

ARTICLE

“Hack Right: How to Deter First Offenders Away from Cybercrime.” *Fordham Now*, 25 July 2019, https://news.fordham.edu/university-news/hack-right-how-to-deter-first-offenders-away-from-cybercrime/.