The Effectiveness of Penalty Enhancements for Crimes Involving Computers

How Truly Effective are Penalty Enhancements?

Penalty enhancements for crimes involving computers are one of the key necessities in lowering the amount of cyber crimes currently occurring. The scope of most cyber crimes committed are classified as misdemeanors with small fines and little to no prison sentences. This is even if the perpetrators are even caught and prosecuted. Currently most cyber crimes are not found till well past the prosecution point, and coupled with lack of law enforcement resources and incident response, leads to most cyber crimes never being found and documented. Effectively making it impossible currently for the government to track the amount of cyber crimes truly happening across the country (Bossler, 2023). Because the true scope of cyber crimes being committed is currently unknown, I believe the first step is to first upgrade the country's incident response, reporting, and defense against most cyber crimes, along with better incident reporting for smaller scale cyber crimes like cyberbullying and forms of hate speech. When this is accomplished, increasing the fines for these misdemeanor charges with potential prison time for repeat offenders would scare off a lot of would-be cybercriminals. Furthering increasing fines towards larger scale cyber crimes would also be beneficial towards scaring off most cybercriminals. I believe this is the most effective way this policy can be adopted, however this method must be scrutinized with the concept of perception versus punishment.

Perception Versus Punishment

Perception versus punishment relates to making the punishment fit how the public views the crime. Take for example being charged twenty years in prison and a four million dollar fine

for jaywalking in a backwater neighborhood. Obviously, the punishment is far too outrageous for the crime being committed. With cyber crimes, the public view is heavily needed in understanding the correct punishments being given. The most well known case of a punishment far exceeding the accused crime is the case of Aaron Swartz. Swartz, was sentenced to 35 years in federal prison and over one million dollars in fines for releasing private university research documents to public forums. This caused Swartz to later commit suicide, causing extreme backlash from the public towards the controversial CFAA act, which almost never took into account the motivation of the accused or public opinion. The government prosecutor upon the indictment had stated, "stealing is stealing, whether you use a computer command or a crowbar" (Amsden, 2020). I want to note the university in question later released all research documents to the public.

Should This Policy Be Adopted?

For this policy to be adopted, I believe three factors must be heavily studied to create the best possible policy. These factors being the ethics of penalty enhancements, societal implications, and politics. To understand the ethics of the cyber crime being committed, the public must have a widely known perception of the crime. It is important to make all punishments fit how badly the crime is portrayed by the public. Society as a whole has become ingrained into the internet, and as such, have allowed cyber crimes to grow rapidly each and each year as more and more devices become connected around the globe. As a result, defensive strategies have been created in an effort to "stop the bleeding" of the multitude of cybercrimes being committed, along with potential aspects such as increased incident recognition, response, and reporting (IEEE, 2023). Most countries and governments have begun to make statements on their plans for cybersecurity and cyber crime deterrents. As an example, this year's National

Cybersecurity Strategy, published by Joe Biden and the White House states, “the Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors.” (White House, 2021). This policy if implemented with these three factors in mind would greatly benefit our country as a whole, and lead to a potential dampening of the cascading waterfall of cyber crimes currently being committed every single day.

References

The United States Government. (2021, May 12). *Executive order on improving the nation's cybersecurity*. The White House. Retrieved February 12, 2023, from https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Understanding cybercrime | IEEE conference publication - IEEE xplore. (n.d.). Retrieved April 3, 2023, from https://ieeexplore.ieee.org/abstract/document/5428417

Amsden, D. (2020, January 12). The brilliant life and tragic death of Aaron Swartz. Rolling Stone. Retrieved April 9, 2023, from https://www.rollingstone.com/culture/culture-news/the-brilliant-life-and-tragic-death-of-aaron-swartz-177191/

Dr. Adam M. Bossler. ReferencesFurnell. (n.d.). *Introduction: New directions in cybercrime research*. Taylor & Francis. Retrieved February 12, 2023, from https://www.tandfonline.com/doi/full/10.1080/0735648X.2019.1692426