Of the many things Kevin Mitnick is famous for, the part that stands out is his journey from being on the wrong side of the law, to his current-day role as a protector of it. Unfortunately for him, the transition involved spending 5 years in jail, with 8 months of that time in solitary confinement.

Mitnick, talking at the CeBIT 2015 conference that was held in Sydney, Australia this week, made it clear that he saw his type of hacking as something very different from cybercrime. Mitnick hacked out of curiosity and the sport of pitting his wits against machines and the administrators trying to protect them. The punishment however, as is so often the case in hacking trials, was set to serve as a deterrent to others. The added twist in Mitnick's case was the solitary confinement which resulted from the prosecution's claim that Mitnick allegedly possessed the ability to "start a nuclear war by whistling into a pay phone". Astoundingly, the judge agreed, and special restrictions were placed on Mitnick's custody to avoid the possibility of him gaining access to a phone and whistling the codes that would launch nuclear missiles.

Given that the prosecution and judge were prepared to believe that launching missiles by whistling was possible, it is hard to see how they could possibly have been able to assess the true extent of damage that Mitnick was claimed to have done.

It would be tempting to think that things had changed since the 1990's when Mitnick was arrested and prosecuted. Sadly that is not the case. Prosecution lawyers are still vociferous in their demands to punish to the full extent of the law and to set examples for others, despite there being no evidence that this actually works.

In the case of Aaron Swartz's prosecution, the matter unfortunately never made it to trial. He faced a possible sentence of up to 35 years for using MIT's network to download research publications from the repository JSTOR without permission. The pressure of the investigation coupled with the unwillingness of the prosecution to tone down their pursuit of exercising the full extent of the law proved too much for him and he committed suicide on the 11th January 2013.

The 5 year sentence of some time journalist and activist Barrett Brown has also been regarded as

excessive. Brown was sentenced for his role in making available emails stolen from intelligence company
Stratfor
in a hack by Anonymous on the 24th December 2011. Brown was not a hacker, but was a public face for the activities of Anonymous and his equally public attempt to bring the activities of Stratfor to the world's attention.

Also convicted for the Stratfor hack was Jeremy Hammond who was the actual hacker responsible for accessing the Strator machines. As a result of the hack, he
stole
200 GB of data and Stratfor's client list, including their credit card details. He faced a life sentence for this crime but eventually was sentenced to 10 years in jail. He was also asked to pay Stratfor $800,000 in compensation for their "damage" he had caused.

What made Hammond's punishment even more questionable, was that he gained access to the Stratfor machines based on information supplied to him by his co-hacker Hector Monsegur aka "Sabu" who at the time was acting as an FBI informant.

Today, Kevin Mitnick runs a successful security company Mitnick Security . His Global Ghost Team test for weaknesses in companies' security by trying to hack them, ironically using all of the skills he would have learned as a Black Hat hacker. Clearly, extremely intelligent and skilled at his job, Mitnick has written 3
books
and has largely defined what we know today about "social engineering". Social engineering, the practice of obtaining information such as passwords from people by deception and other means, is still the predominant means by which hackers gain access to systems.

When prosecutors and judges seek to punish hackers, the extent of the damage they are alleged to have caused is calculated in a way to make concrete, abstract concepts such as "damage to computers" as instantiated in the US Computer Fraud and Abuse Act . Mitnick, and others hackers such as
Kevin Poulsen
have shown that they have been able to put their Black Hat days completely behind them and use their talents for the public good. Instead of putting hackers of Mitnick's kind behind bars for years, there are clearly more constructive ways of getting them to repay their debts and make amends.

Asked if whether if had been offered the option of becoming a White Hat hacker and turn his skills to good rather than serve 5 years in jail, Mitnick replied with an emphatic “Yes”.

**Read more** http://theconversation.com/kevin-mitnicks-story-shows-why-we-shouldnt-use-jail-to-make-examples-of-hackers-41038