

# Example of research paper on research on crime vs cyber crime

[Technology](#), [Internet](#)



## **Analysis on the Difference between Crimes versus Cyber Crime**

### Abstract

In most parts of the world crime has always been a major concern on every state. The same reason why legislators and law makers exists because their primary role is to create laws that will suppress if not totally diminish crimes in their respective countries. In common terms crime is identified if a person committed an act in violation of a prevailing law. This act of crime is categorized in different levels and gravity of offense in which a specific punishment applies. But in recent years, crimes have crossed the continental boundaries. Before, crimes do occur but only isolated in particular location and that is because the crimes are committed in physical interaction. With the overwhelming development is development particularly in continuous advancement in Information Technology, major crimes are now being initiated with just a few clicks with a touch of finger. That is because crimes are now present not only in physical encounters but also over the internet. This is what we call ‘ Cyber Crimes”, there are a lot of activities happening over the internet that leads to profit loss and even moral damages to the victim. The question is what are the laws that will condemn cyber criminals are and what are the security measures that each country is implementing to reduce if not totally to put a halt on the hiking number of cyber crimes. This paper will discuss the differences of the two types of crimes and their impacts to the global economic environment.

## **Keywords: Cyber Crime, Crime Laws, Fraud, Statistical Data, Comparison and Contrast**

### Crimes vs. Cyber Crimes

In all countries crimes are the major concerns of the government, ratifying laws and state policies that seeks to control the number of criminal incidences. In the past few years these crimes evolved from a simple theft and robbery activity to a more advanced form of offense which involves the use of technology. The availability of the internet and sophisticated electronic makes it easy to hack other internet users, and steal their personal information to use for fraudulent activities. The number of such occurrences becomes a trend for most criminals because it involves limited physical intervention to execute crime. There are even companies who are experiencing at least 50 attacks in a week and some gets successful attacks on every company in the United States per month (Riskandinsurancechalkboard. com, 2010).

In terms of impact to the business it is a fact that cases of bank robbery for example will cost as much as \$4, 000 per robbery in the United States. That amount is equivalent to 60% of losses in the financial industry per incident. The amount might seem not alarming, but the frequency of robbery incidents range from 6, 000 to 8, 600 every year and still rising. With regards to recovered money, only 20% of the stolen cash is possible to be recovered, that is why banks limit the amount and access to their cash on hand in every branch (Weisel, Deborah Lamm, March 2007). The only advantage in this crime is that there is huge possibility for the perpetrators to get caught especially if the robbers are amateurs and careless about unconsciously

leaving tracking evidence.

On the other hand, Cybercrime works differently, they are like night burglar that works behind the seen attracting lesser attention as they commit the crime. The thing about Cybercrimes is that they do not steal the money from the bank directly by sticking their hands straight to the bank vaults. Instead, they attack the bank systems, copying and stealing bank information and creating fraud transactions, then eventually taking money by means of electronic transfers. What hackers do is they infect systems with malicious software that will act as their gateway to the DNS server. In some cases they also steal customer's information to use for fraudulent transactions with the bank, it happens when the customer's computer was also infected with malwares which interfere with their internet browsing (Fbi. gov. November 2011). These acts lead to an annual loss of revenue of about \$5. 9 million dollars annually, using the benchmark from \$1. 5 million to \$36. 5 million every year per company as measured by Hewlett Packard (Nusca, Andrew August 2, 2011).

When it comes to judicial punishment, bank robbery for an instance is a felony offense in the United States, it includes life imprisonment without parole and worst is death penalty if there is another crime committed during robbery (LaMance Ken N. D). On the other hand Cybercrimes or otherwise known as Computer Crime is defined by the United States Department of Justice as follows; for trespassers an act causing international damages will fall under felony, reckless damage will be the same and negligent damage. For authorized computer users, an act causing international damages will also fall for felony, but no-crime classified for reckless and negligent

damages (Justice. gov N. D).

Given the fact that the two crimes are committed in an entirely different approach, the impact to the economic statute of every nation is severe in the long run. There should be a definite and more structured law that must be imposed for cybercrimes. It is evident that all industries even private citizens are vulnerable to computer crime attacks; the punishment for cyber criminals must be more severe than of the conventional crimes.

## **Discussion**

In the age of technological advancement, it is not a surprise if the virtual world is being bombarded with rampant cyber crimes. The prevalence of the existing local and international laws are not enough to put a stopper into this kind of activity over the internet. The consideration for a well structured law and policy must be implemented because of the rising trend in this kind of cyber crimes. The existing laws on conventional crimes are already well established to the point of effectively prosecuting the offenders. What the international community and the trade sectors must accomplish is to persuade all leaders to make a stand against cyber crimes and to somehow create a safer virtual environment for the computer based society.

## **References**

Riskandinsurancechalkboard. com. Benchmark Study of U. S. Companies (July 2010) First Annual Cost of Cyber Crime Study Web. Retrieved January 19, 2012 from <http://www.riskandinsurancechalkboard.com/uploads/file/Ponemon%20Study%281%29.pdf>

Weisel, Deborah Lamm. Bank Robbery. (March 2007). Problem-Oriented

<https://assignbuster.com/example-of-research-paper-on-research-on-crime-vs-cyber-crime/>

Guides for Police Problem-Specific Guides Series Guide No. 48 Web.

Retrieved January 19, 2012 from [http://www.cops.usdoj.](http://www.cops.usdoj.gov/files/ric/publications/e03071267.pdf)

[gov/files/ric/publications/e03071267.pdf](http://www.cops.usdoj.gov/files/ric/publications/e03071267.pdf)

Fbi.gov Stories. (November 2011). International Cyber Ring That Infected

Millions of Computers Dismantled Web. Retrieved January 19, 2012 from

[http://www.fbi.](http://www.fbi.gov/news/stories/2011/november/malware_110911/malware_110911)

[gov/news/stories/2011/november/malware\\_110911/malware\\_110911](http://www.fbi.gov/news/stories/2011/november/malware_110911/malware_110911)

Nusca, Andrew. Between the Lines. (August 2, 2011). Cost of cybercrime up

56%, HP says Web. Retrieved January 19, 2012 from [http://www.zdnet.](http://www.zdnet.com/blog/btl/cost-of-cybercrime-up-56-hp-says/53737)

[com/blog/btl/cost-of-cybercrime-up-56-hp-says/53737](http://www.zdnet.com/blog/btl/cost-of-cybercrime-up-56-hp-says/53737)

LaMance, Ken. (N. D.). Bank Robbery Lawyers Web. Retrieved January 19,

2012 from [http://www.legalmatch.com/law-library/article/bank-robbery-](http://www.legalmatch.com/law-library/article/bank-robbery-lawyers.html)

[lawyers.html](http://www.legalmatch.com/law-library/article/bank-robbery-lawyers.html)

Justice.gov. Computer Crime. (N. D.). THE NATIONAL INFORMATION

INFRASTRUCTURE PROTECTION ACT OF 1996 Web. Retrieved January 19,

2012 from <http://www.justice.gov/criminal/cybercrime/1030analysis.html>