The world experiences 12 cybercrimes per second and a total of 1 million people are victims to these crimes daily (Henschen, 2014). If this isn't alarming enough, the recent security breaches in giant companies such as Sony, highlight the dangerous situation cybersecurity is in. We use the internet every day to watch movies, read news, listen to music, socialize and research. The internet is definitely making our lives easy and enjoyable. Nonetheless, the network is so big that it cannot be controlled or limited since it is a common privilege to everyone who uses it. With an ever growing virtual network, society faces one of its biggest challenges yet: How to manage information and tame the internet. As an attempt to secure the Internet and deny any virtual crimes, cybersecurity was defined. Many big IT companies, computer companies and even the government research on how to improve cybersecurity. However, even with all these prevention efforts, hackers always seem to have the upper hand. That is why criminal hacking must be solved as soon as possible by combining three solutions: changing cybersecurity legislation and specifically information sharing that helps coordinate defenses, cyber-supply-chain security since it is the main problem in cybersecurity, Cyber Self-Defense because targets must know how to do their part in hacking prevention, and finally, awareness, education, and training because if the whole population knows how to react against malware than cybercrimes shall become much less frequent.

The Internet holds our entire economy as well as our most private information. Consequently, hackers and pirates use the internet illegally to harvest information about certain people or companies so that they could use it for their personal interests. Each one of us today is exposed to those hackers via the internet; our personal information and sometimes our private lives can be stripped away instantly and easily. Sometimes hacker attacks are very big to an extent that they impose a huge threat to a nation's economy and security. This year, a giant US

company called J.P. Morgan was attacked by a group of hackers. As a result, the secure information for 76 million households and 7 million businesses got compromised. "The attacks, no matter that they were for the most part fended off, are still a major concern for U.S. law enforcement" (Weise, 2014). Another efficient way to illegally access private information is through the use of malware or so-called viruses. There are countless types of malware and the internet is filled with them. Sometimes, if one is not cautious enough and lets an intrusion inside his device, messages start to pop up and unknown files appear out of nowhere. The next thing is we start losing personal data and we can't access them anymore. "When the same device is used for both personal and business tasks, that risk increases still further" (Rapoza, 2012).

First, the aforementioned combination of solutions helps plan defenses wisely by information sharing. Usually, after companies are penetrated by security breaches, they hide all the technical information about holes in the system and overall system performance in fear that other hackers acquire this information. But in fact, this collection of reports can be very helpful when shared with the private and public sectors. This a very efficient to predict and counter future attacks and also enables other companies to improve their security. But, giving away this collection is not that easy is it can cause unintended damages and risks. "This information is helpful to all cybersecurity actors as it allows them to prepare for these threats and patch or disable offending software." (Bucci, 2013). This way, there will be a concentrated workforce targeting hacker attacks which is very efficient and makes crimes much less likely to happen or at least makes the job much harder for pirates. Also, it can prevent any future damages to all companies while working together and sharing resources to solve a common problem which makes this change cost efficient.

The next advantage of this solution combination is indexing products in terms of security by changing cyber-supply-chain legislation. Most people think that cybersecurity problems reside mostly on the software side. Let's say a company's software gets infected, they can just update it easy and fast to stop any damages occurring or to an extent delete the whole software. On the other hand, when that problem happens on the hardware side, fixing is nearly impossible. There is a big number of products that are already infected at production in which malware is embedded, which initially makes detection really hard. If discovered, the most common way to counter infection is disposing of the object which is very costly, slow and inefficient. This is also how cyberespionage works. Foreign companies makes products that our countries import. These products can be embedded with certain functions that threatens our security. The best way to solve this is to attribute security grades to the diverse companies around the world. This gives the consumers the choice to take the risk or go safe. This solution is very efficient since it requires low resources and organizes companies so that consumers can make a well informed decision.

A third effective advantage of the combination is fighting fire with fire also known as cyber self-defense. Most of the time, changes in legislation take a really long time. Companies cannot wait to be attacked and collect information…They should act and stand against these intrusions. Many governments and companies are using sophisticated tactics to trap and uncover the hidden attackers. For instance, the government of Georgia used a method called "Honeypot" (Flamini, 2013) to catch a hacker that was sent by a Russian intelligence agency. Although these tactics are themselves malware, they are not very dangerous and can be an efficient way to defend ourselves against hackers if they are used in cooperation with law enforcement or the concerned forces. A controversial solution nonetheless an effective one. It is cost efficient because it resides on the software side and can act as a backup plan if other solutions fail.

The last advantage of the combination is awareness and that is by education and training in cybersecurity. Although, some actions were taken to raise awareness, they were definitely not enough. People were not very affected by the awareness programs that the government didn't pay too much time on them. Washington is not the only one with a cybersecurity agency. Each state has one and it is the role of these agencies to cooperate with organizations and research institutions to raise awareness about cybersecurity. "If we're going to build a safer Web, we have to make it easier and more attractive for everyone in the ecosystem to step up and do their part" (Clemitt, 2011). In addition to that, there should be training available to non-IT workforce. Nearly every job today is managed by computers and networks and virtual systems. That is why each one must know how to handle them and not get easily fooled or deceived by security threats.

We notice that changing cybersecurity legislation largely affects cybersecurity in many different ways thus making it the optimal solution. Some might say that legislation change is very slow and may never happen. However, changes in cybersecurity laws are the only way to counter criminal hacking on the big scale. Also, changing the legislation of one of self-defense alone cannot be enough to resolve a widespread big scale problem around the world. Consequently, we desperately need a complete reform of many law so we can stand a chance against the arising problems in cybersecurity.

In conclusion, cybersecurity legislation change seems the most effective way to solve cybercrime especially if the laws concerned with information sharing, cyber-supply-chain security, Cyber Self-Defense and awareness, education, and training are changed to the better. The combination of these four solutions is the optimal way to solve cybersecurity problems once and for all and we should indeed go for it.

References

Weise, E. (2014). *Citi, E*Trade attacked by JPMorgan hackers, reports say*. Retrieved October 10, 2014, from http://www.usatoday.com/story/tech/2014/10/08/citigroup-etrade-jpmorgan-hackers/16923659/

Rapoza, K. (2012). *Top 10 Security Issues That Will Destroy Your Computer In 2013*. Retrieved October 10, 2014, from http://www.forbes.com/sites/kenrapoza/2012/12/05/top-10-security-issues-that-will-destroy-your-computer-in-2013/

Bucci, S. (2013). A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace. Retrieved November 12, 2014, from http://www.heritage.org/research/reports/2013/04/a-congressional-guide-seven-steps-to-us-security-prosperity-and-freedom-in-cyberspace

Henschen, D. (2014). 10 Ways to Fight Digital Theft & Fraud. Retrieved November 12, 2014, from http://www.informationweek.com/government/cybersecurity/hacker-weev-free-after-appeal/d/d-id/1204411

Flamini, R. (2013, February 15). Improving cybersecurity. *CQ Researcher*, *23*, 157-180. Retrieved October 24, 2014, from http://library.cqpress.com/cqresearcher/cqresrre2013021500

Clemmitt, M. (2011, September 16). Computer hacking. *CQ Researcher*, *21*, 757-780. Retrieved October 24, 2014, from http://library.cqpress.com/cqresearcher/cqresrre2011091600