

# [Legal and regulatory environment research paper example](https://assignbuster.com/legal-and-regulatory-environment-research-paper-example/)

[Law](https://assignbuster.com/essay-subjects/law/), [Security](https://assignbuster.com/essay-subjects/law/security/)

## Research on Legal and Regulatory Environment

Abstract

The modern world had greatly improved the way of living in all aspects of daily life. Technology and Information Technology in particular had evolved to the point that it became a crucial element in building a business empire. Many business organizations rely on IT in order to deliver goods and services at the fastest possible rate. But in recent years the fast phased environment of information technology also paved way for a bigger threat to economic and national security. Cyber crimes elevated to a greater level of competence that seeks to take advantage of the available technological resources to commit theft and other crimes. The common types of crime done in the virtual environment are fraud, identity theft and robbery. Because of these acts, many organizations are vulnerable to cyber attacks which in return will cause loss of revenue. The question here is how strong are the existing laws to prevent cyber crimes from rising in numbers in terms occurrences. This paper will discuss the importance of security measures and will give an insight of the applicable laws that will prevent cyber crimes.

## Keywords: Cyber Crime, Security, Information Technology and Policies

Legal and Regulatory Environment
Committing cyber crime is the same as acting against a prevailing law for which the act of offense also comes with a judicial punishment as mandated. But because of the nature of the crime, law enforcements are having a hard time apprehending the culprits. That is because the crimes are being done without physical intervention involving a face to face act during the crime. With the use of available technological resources, criminals are able to steal a lot of information and other revenue generating crimes though the internet. Being said that tracking them down would take a lot of work in terms of investigation in order to point out the source of the crime.
Once the risk of virtual attacks are done and the criminals were apprehended the problem does not end there, because even if the offenders are caught, there is still not enough law to convict them. If there is one existing it is still not enough to provide a full extent of punishment, as a result offenders still can get away with the crime. The lack of security in policies and prevailing laws forced private and government organizations to take preventive measures by implementing their own information security system. By considering data security in the face of modern IT compliance to regulations were set to prevent any damages that cyber crime may inflict to the organization as a whole (Sjouwerman, Stu. January 5, 2012).
Cyber crimes have limited legal responses at a national level as far as protection is concern because existing laws are applied to very limited jurisdiction (Deflem, Mathieu, and J. Eagle Shutt. 2006). Like for example, Digital Millennium Copyright Act and Electronic Theft Act only focuses of electronic information, while The Economic Espionage Act only apprehends offenders that threatens national economy. Given that fact there the legal framework is indeed not adequate.
The problem law makers are facing to successfully prevent cyber crimes is the amount of understanding how the entire system of the cyber crime works as far as crime operations are concern (Neiassociates. org October 2011). It is quite difficult for them to determine the starting point of legislation structure to draft a strong policy. In order to draft a strong policy law enforcers must be updated with the prevention process for the following; data interception, modification, data theft, network interference, sabotage, virus dissemination, aiding and abetting, computer forgery and fraud (Gordon, Ron N. D).
Cyber crimes impact not only government and private organizations, but the greater public as well. That is because the public are the frequent computer users who rely on the internet to do faster transactions regarding their personal finances. Consumers can do almost everything with the touch of their fingers even shopping for goods ad services. Cyber criminals’ takes advantage of the situation to steal pertinent personal information which is the key to the victim’s financial information (Fas. org. January 29, 2008). Because of the personal data stolen from an individual, cyber criminals can now perform money related transactions for their personal gain also referred to as Identity fraud and theft (Justice. gov N. D).
The rising number of occurrences of cyber crimes would definitely call for the public’s demand for a strong policy in preventing virtual criminal activities. During the last five years the umber of cyber crime cases already reach from 100 in 1997 to 60, 000 as of 2002 (Crime-research. org June 9, 2003). At this point where cyber crimes are able to adapt to the changes in preventive security systems, law makers should look into the issue with utmost priority, because in the long run it may greatly impact not only in economic terms but as well as national security.

## References

Deflem, Mathieu, and J. Eagle Shutt. 2006 “ Law Enforcement and Computer Security Threats and Measures.” Pp. 200-209 in The Handbook of Information Security, Volume 2: Information Warfare; Social, Legal, and International Issues; and Security Foundations, edited by Hossein Bidgoli. Hoboken, NJ: John Wiley & Sons Web. Retrieved January 22, 2012 from http://www. cas. sc. edu/socy/faculty/deflem/zcompsec. html
Sjouwerman, Stu (January 5, 2012). P nd The #1 Security Risk for 2012 IsWeb. Retrieved January 22, 2012 from Retrieved from http://blog. knowbe4. com/category/cybercrime-2/
Gordon, Ron. (N. D.) Cyber Crime and Internet Terrorism: Issues, Regulatory Problems, and Legislation Web. Retrieved January 22, 2012 from http://jupapadoc. startlogic. com/compresearch/papers/JCR05-3. pdf
Neiassociates. org. Solving the Serious Issues of Today. (October 2011). Meeting Law Enforcement's Responsibilities Web. Retrieved January 22, 2012 from http://www. neiassociates. org/seriousissues. pdf
Justice. gov. (N. D.). hat Are Identity Theft and Identity Fraud? Web. Retrieved January 22, 2012 from http://www. justice. gov/criminal/fraud/websites/idtheft. html
Fas. org. CSR Report for Congress. (January 29, 2008). Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress Web. Retrieved January 22, 2012 from http://www. fas. org/sgp/crs/terror/RL32114. pdf
Crime-research. org. (June 9, 2003). Cyber Crime Rate Increases 500-fold in 5 Years Web. Retrieved January 22, 2012 from http://www. crime-research. org/news/2003/06/Mess0904. html