The impacts of cyber crime

This essay investigates the impact of cyber crime on businesses relative to the traditional forms of crime. It looks at the relative magnitude of punitive measures that should be imposed on the two forms of criminalities. According to the literature, cyber crime, like any other crime, should be reported to the law enforcing agencies to investigate and bring the culprits to book. In addition, the essay establishes the idea behind cyber terrorism and the people behind it (Turkle, 1995).

The impacts of cyber crime go beyond affecting financial integrity of businesses. These are criminal activities that specifically target computers or the computer networks. They usually involve outside parties hacking into computer systems with the main intention of divulging the systems' sensitive information. These criminal acts have left big businesses reeling from loss of revenues, damaged reputation, reduced overall productivity and a waste of precious time (Jackson, 2010).

It certainly becomes a burden to employees especially when they have to enter more passwords before they can eventually start their jobs thereby reducing their general productivity. Besides making the work cumbersome, these threats lead to serious waste of time when computer systems have to shut for the IT personnel to mitigate the effects of the crimes. Therefore, cyber crime should be treated just like the traditional crime as the impacts are equally damaging. For instance, criminals who hacka bank computer system should be investigated thoroughly by the FBI and subjected to the same punitive measures that traditional criminals have always faced (Friedman, 2005).

Cyber Terrorism

Cyber terrorism as an attack targeting computer systems has always sought to disrupt personal computers that have internet connections through computer viruses. The main intent of these activities is to cause a massive disruption of communications systems as a nation’s infrastructure. However, communication is such a critical aspect of human life that should not be exposed to such threats (Mueller, 2004). As such, the government agencies including the Federal Bureau of Investigations must act swiftly to curtail the crime. Although individuals have a responsibility to guard their computers against cyber terrorism by avoiding accessing information from unknown sources, the law enforcement agencies at the state level must put in place stiffer penalties against the cyber terrorists (Moustaira, 2004).

In most cases, the cyber criminals interfere with customer records or compromise their security concerns leaving the image of the whole company dented. For instance, customers who accidentally have their credit cards intercepted may completely lose confidence in the organization and opt to conduct business elsewhere. These challenges often keep the company on its toes trying to implement policies that would counteract cyber crime (Kellner, 2000).

Adagia Telecom and Compliance

There is little doubt that there are adequate laws to curtail cyber crimes. However, compliance remains a great challenge considering that locating the physical location of the culprits is a serious problem. For instance, the attack of Adagia Telecom could have been avoided if the laws were more

enforceable. Nonetheless, reports should be made to the relevant authorities to investigate these crimes although it may take time to conclude them (Machlis, 1997).

The major impact that cyber crime has had in the business world is loss of revenue. This usually occurs as a result of an outside party getting access to sensitive financial information of a business. Consequently, they use this information to withdraw funds from other organizations. This has become a cause of concern with the rapid development of e-commerce. Hackers often make the system inoperable implying that consumers cannot access the site. That is why the law must strictly apply to them as that is the only way to root them out (McCullough, 2004).

In conclusion, cyber crime has made online business a very unsecure affair that could easily bring down big organizations. Besides, cyber terrorisms could paralyze all computer systems if not properly checked. As such, the FBI must be more tactical in finding and prosecuting these criminals. That would be the only way to ensure a safe and secure environment in the places of business (Jackson, 2010).