Cyber Security Laws and Policy Implications of these Laws

In an age where so many businesses and systems are reliant on computer systems, there is a large incentive for maintaining the security of their information systems, especially because most systems require security for profit, and/or trust of their clients. Also with the progression of technological capabilities, there is a pattern of increased cyber attacks against a multitude of computer systems. Computer crime is now seen as both traditional crime being committed by new methods, as well as crime unique in character and requiring its own legal framework. Thus, although computer security has remained largely private, many laws regarding cyber-security have been dramatically written and revised as a result of the events of 9/11 and the creation of the Department of Homeland Security. However, even with these current laws, there are obvious flaws with the enforcement of these laws, and/or lack thereof. Through the examination of current laws on cyber-security as well as security strategies and research initiatives on behalf of the government, one can begin to articulate the need for change in this area. By focusing on the major discrepancies between the government and private cyber-security firms, it is evident that a compromise between the two could have the capability to be the best policy option for the current and future state of cyber-security.

Prior to 9/11 there were laws regarding cyber-security which, since then have been revised, still laid the grounds of dealing with cyber-crime. In 1979 the Department of Justice put computer crime into three categories which included: computer abuse, "the broad range of acts involving a computer where one or more perpetrators made or could have made gain and one or more victims could have suffered a loss;" computer crime, "illegal computer abuse that implies direct involvement of computers in committing a

crime," and computer-related crime, "any illegal act for which a knowledge of computer technology is essential for successful prosecution." (Dept. of Justice) From this point, laws have been aimed to treat each in already established laws by making certain to apply words such as computer, cyber, or computer crime to the text, or to create another law altogether. In 1996, the National Information Protection Act of 1996 was passed and enacted as a part of Public Law and also amended the Computer Fraud and Abuse Act. The law was written as one of the first laws prohibiting unlawful access to information by means of computers and or computer networks. The law specifically targets computer fraud, stating that "whoever intentionally accesses a computer without authorization or exceeds authorized access," and limits any violation to "a fine or imprisonment for not more than twenty years, or both." (18 U.S.C.) Although the law was refined post 9/11, it set up conditions for punishing criminals via cyber-crime strictly involving unauthorized information. Also in 2001, the Computer Hacking and Intellectual Property Units (CHIP) that were proving to be successful had nine additional units added to them. "That project demonstrated the benefits of a unit of prosecutors working closely with the FBI and other agencies to establish a relationship with the local high tech community and encourage them to refer cases to law enforcement." (Dept. of Justice) Not only did the CHIP program work to enable relationships with private security companies, it also trained more government officials to recognize cyber-crime, in order to prosecute them. Often criticism of government laws regarding cyber-crime is that there are not properly trained prosecutors or enforcers of the laws, so in expanding the CHIP program, the government began to combat these criticisms.

With the passage of the PATRIOT Act, following the events of 9/11, there were many adjustments made to the laws regarding cyber-crime and cyber-security. Obviously, the laws were revised to try to prohibit more of the former and make a better attempt at making the latter more preventative and thorough. The Electronic Communications Privacy Act was revised which aims at information gathered through any form of communication that may have been obtained through illegal means. It also treats stored communications in the same manner, making unauthorized information in these stored communications punishable by law. Also with this law, it is amended such that it grants the government the ability to access stored emails as well as other electronic communications. (Patriot Act) However, unlike prior to 9/11, the act states that "Although the use of such devices requires a court order, it does not require probable cause: there is no judicial discretion, and the court *must* authorize the surveillance upon government certification. A government attorney need only certify to the court that the "information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation." (Patriot Act) The Computer Fraud and Abuse Act was revised and made to include more accurately terms for which computer fraud was punishable and exactly through what measures. In expanding the scope in which the government could either punish or intercept knowledge of fraud seemed to direct more towards information that had been obtained to disclose information of national defense, and "could be used to the injury of the United States, or to the advantage of any foreign nation." (18 U.S.C.) Like many of the other laws that were amended through the Patriot Act and Department of Homeland Security, the law directly aimed to deter cyber-terrorism, but it also allotted the government much power over hackers trying to acquire information for personal gain.

The Cyber Security Enhancement Act of 2002 addressed the growing incidences of the offenses, and addressed "the need for an effective deterrent and appropriate punishment to prevent such offenses." (Sec. 225) Thus, the laws regarding cyber-crime were able to expand as a result of the events of 9/11, and continued revision continues to occur today. Aside from the discontent from the infringement of personal privacy, the content of these laws is not at the base of the legal issues with cyber-crime, but rather, the implementation of them by the government.

Although the cyber-security laws have been set up to prohibit cyber-crime, it would appear that the biggest policy question to be answered is whether or not cyber-security should be managed by the federal government that is making laws for it, the private sector who has more skills in the area, or by both, since they each have their own obvious stakes in providing cyber-security. However, in order to assess which policy would be the best policy implemented; the goals of cyber-security have to be established. Although not limited to, of the criteria needed for a successful cyber-security policy, are the following: Who can better detect cyber offenses? Who can better maintain confidentiality when necessary?, and Who can properly assess punishment relevant to the offense?

"Computer crimes are more difficult to detect than other forms of crime," which makes the ability to detect even more valuable in assessing the best policy to implement. (pg. 707, Mitchell) There continues to be a disproportionate number in favor of crimes that go undetected to those that do not. As detection tools continue to develop, one can determine that it is obviously one of the necessities in fighting cyber-crime. Private companies that focus on cyber-security tend to have better operation for detection

because they are solely trained in the field, and often times have the proper skills to detect cyber-crime. However, just because a private company has the means to detect offenses does not mean that they will report an incident they have detected to the federal government. "Businesses have a primary need to repair damage and restore service to the customers, a process often complicated by an ongoing criminal investigation." (pg. 709, Mitchell) Because trying to prosecute a criminal can be costly as well as timely, to report an incident may not be in its or its client's interest. Also, a private company itself must be careful when conducting detection cases because they too can be held accountable for intruding into information systems that are now illegal as a result of current laws. The federal government on the other hand does not have as much skill in being able to detect cyber offenses. "The expense of training, equipment, and conducting computer investigation often price computer crime expertise out of the range of state and local police resources." (pg. 710, Mitchell) Therefore, these skills required to maintain successful detection requires training that the government may not be able to afford.

Confidentiality, for companies who do most of their marketing via the internet or for companies that do their business on large computer systems, is vital in maintaining trust from their clients, and a belief that everything with the system is fine. Thus, if detection of an offense is made, a private security company may want to keep the detection confidential so that they do not lose clients. "News of data leaks can be public relations nightmares for a company especially when that company is trusted with confidential information." (Bowmen) However, because companies want to keep intrusions confidential, it makes it harder for the government to publicly make examples of punished computer criminals, since more would be reported, even if trust between the

client and company would falter. Because confidentiality is necessary for the company who doesn't want to publicly ruin their reputation, it is necessary for a successful policy to be able to grant time for confidentiality in a given case. Although the federal government does not have any direct ties to a business to maintain confidentiality, there are times when it too must be confidential. For example, when working on some lower computer crime to lead to a large scheme, it maintains confidentiality to detect that higher crime, and punish larger actors. However, in order to maintain legitimacy, the federal government has to report to the public, to demonstrate that they are providing protection and using money for protection properly. Both private security companies and the federal government can gain by having some aspect of confidentiality in a policy.

Assessing a crime committed by a computer is dependent on a number of factors such as what was inflicted by the crime, who were the victims of the crime, and the level of sophistication of planning and carrying out the crime. Even though a security company may be able to assess all of the factors committed by a crime, they may be influenced by what is more beneficial to their company, either having a civil suit brought against the perpetrator, or a criminal one. If the security company is protecting a business in which the crime was very costly, they may be driven strictly to punish on the basis of getting their money back. However, aside from the government being tied to the written law, they are not profit driven when punishing criminals. Not only can the federal government properly assess the punishment to the criminal but they are accountable to the public, so are driven by protecting the public from infiltrations. Also, in terms of national security, there may be jurisdictional issues because of perpetrators outside of the U.S. Thus, it would be easier if the government reigned in cyber-security,

since they are the ones who create international treaties and/or laws regarding international infiltrations. Although assessing punishment to cyber criminals is accomplishable by both the private security companies, and the federal government, it seems to be on the public's behalf that the federal government controlled cyber-security for punishment purposes.

In assessing each criterion for the best policy for cyber-security, it is evident that if the federal government and private security companies could compromise to work together to fight cyber-crime, there could be more potential for both sectors. Using the private sector's skills and ability for confidentiality would help the government in punishing more criminals. It has been argued that "The government should allow the private sector to develop and deploy security technology in partnership with it." (Jackson) There have been many options offered so that the government and the private companies could benefit from working together, such as creating an oversight mechanism. The oversight mechanism would be such that the federal government would create the agency and/or board which could issue licenses to private companies to be the detectors of cyber-crime. For example, there could be a federal license to engage in certain activities that would allow a private company to over-step current federal regulations in cyberspace, and then that company could report any intrusions they may come upon. There may be a rough compromise for both in terms of how confidential certain cases are, or for a given time, but each could work off of the positive characteristics that the other has to maintain a good balance. With the resources of the private company, and the flexibility the federal government could allow with a license, detection would increase. By issuing a license, "benefits include competitive advantages,

a more predictable legal and liability climate, more well-defined standards of practice, and enhanced trustworthiness of those engaged in the profession." (pg. 719, Mitchell)

Having a compromise between private security companies and the government, may have already started to shape. The "National Strategy to Secure Cyberspace," which outlines the next steps for the nation in regards to dealing with cyber-crimes , "was developed in close collaboration with key sectors of the economy that rely on cyberspace." (pg. 53) Also, amongst the strategies that will be determined, partnerships with private companies will continue to develop pieces for the strategy. Also, the Department of Homeland Security is "partnering with industry, universities, and other government agencies to help find, develop, and demonstrate innovative ideas." (Dept. of H&S) Not only will they work to facilitate research, but they will also work to address the "critical needs on the homeland defense scientific front." (Dept. of H&S) Therefore, although there are still many aspects of cyber-security that need to be dealt with, there is an obvious attempt by both the government as well as private companies to work together to achieve a safer place for the public.

Bibliography

18 U.S.C. 2703: Requirements for Governmental Access. Dept. of Justice. 21 Nov. 2005. <www.usdoj.gov/criminal/cybercrime>.

Briney, Andy. "The Legislative Landscape." (2003). 21 Nov. 2005. <infosecuritymag.techtarget.com>.

Bowmen, Lisa. "States failing at Cybersecurity." (2003). 21 Nov. 2005. <www.news.com>.

Computer Crime and Intellectual Property Section. Dept. of Homeland Security. 21 Nov. 2005. <www.cybercrime.gove/homeland>.

Jackson, William. "Cybersecurity laws coming." (2003). 21 Nov. 2005. <appserv.gcn.com>.

Mitchell, Steven, Elizabeth Banker. "Private Intrusion Response." Harvard Journal of Law & Technology 11 (1998): 700-732.

National Strategy to Secure Cyberspace. 21 Nov. 2005. <www.whitehouse.gov>

Research and Technology. Dept. of Homeland Security. 21 Nov. 2005. <www.dhs.gov/dhspublic>.

The No Electronic Theft: 17 U.S.C. and 18 U.S.C. Ammendments. Dept. of Justice. 21 Nov. 2005. <www.usdoj.gov/criminal/cybercrime>.

"Traditional Legal Responsibilities Translated to Cyberspace." (2002). 21 Nov. 2005. <www.infodev-security.net>.