**Andrew Dykman - Web Security and Ethics - Lab 1 7/3/2012**

**Task 1.)**

1.) Done with Virtual Library

2q.) Example where improper use of the Internet / e-mail had a negative effect on a company:

2a.) Roger Duronio was sentenced to [97 months](http://www.informationweek.com/news/security/showArticle.jhtml?articleID=196603888) for planting a "logic bomb" using the company network (including e-mail and internet as part of his hacker's toolset) that took down as many as 2,000 servers around the country in UBS PaineWebber offices. This meant that the company was unable to make trades for up to several weeks in some offices and the company reported a cost of $3.1 million to recover from the attacks. It's unknown how much the company lost in business during the time its networks were disabled.

3q.) Example where it was good to have the company policy when improper use of the internet or e-mail was discovered:

3a.) Nosal was employed by recruiting firm Korn/Ferry.  He left the firm to start his own, competing firm.  After he left, he persuaded some of his Korn/Ferry colleagues to e-mail confidential information owned by K/F and provide it to him.  The K/F employees had access to the information as part of their work for the company, but were violating company policy in providing confidential information to a third party.  When Korn/Ferry discovered the theft of information, they initiated legal proceedings against Nosal. In addition to suing him for civil damages, they filed a criminal complaint stating that he had “aided and abetted” the Korn/Ferry employees in violating the Computer Fraud and Abuse Act of 1984 by encouraging them to “exceed their authorized access to information and e-mail” on Korn/Ferry computers.

In this case the Acceptable Use Policy provided and additional layer of legal protection on the criminal lawsuit level for preventing the e-mailing of confidential information from the company to unauthorized 3rd parties which was a serious violation of another code of company conduct that had already been violated.

**Task 2.)**

*Company Memorandum: "Company Policy Regarding Proper Use of the Internet (or E-mail*

Sir,

I would like to emphasize to you the need our company has to develop an acceptable use policy for our internet and e-mail system, and am writing you this memorandum to demonstrate to you exactly how critical this is for our company. Allow me to cite for you a reference where a former employee of UBS PaineWebber violated the Acceptable Use Policy and caused severe detriment to a company he worked for: Roger Duronio was sentenced to [97 months](http://www.informationweek.com/news/security/showArticle.jhtml?articleID=196603888) for planting a "logic bomb" using the company network (including e-mail and internet as part of his hacker's toolset) that took down as many as 2,000 servers around the country in UBS PaineWebber offices. This meant that the company was unable to make trades for up to several weeks in some offices and the company reported a cost of $3.1 million to recover from the attacks. It's unknown how much the company lost in business during the time its networks were disabled.

As you can see a company computer and internet Acceptable Use Policy would create an additional level of protection, as well as letting our users know that things of this nature (including things of a much less severe, but still questionable nature such as playing games on company time) will simply not be tolerated by our policy we plan to draft.

To further cite historical scenarios of this nature let me cite a situation where an Acceptable Use Policy allowed a former employee and other violators to be held even more accountable for their actions. I cite this for you to show how an Acceptable User Policy can be an additional "shield" to our company, because even though the former employee was brought up on other primary legal charges for this incident, he was also held liable for the misuse of the Acceptable Use Policy by bringing him up on criminal charges for encouraging others to violate the company Acceptable Use Policy: Nosal was employed by recruiting firm Korn/Ferry. He left the firm to start his own, competing firm. After he left, he persuaded some of his Korn/Ferry colleagues to e-mail confidential information owned by K/F and provide it to him. The K/F employees had access to the information as part of their work for the company, but were violating company policy in providing confidential information to a third party.  When Korn/Ferry discovered the theft of information, they initiated legal proceedings against Nosal. In addition to suing him for civil damages, they filed a criminal complaint stating that he had “aided and abetted” the Korn/Ferry employees in violating the Computer Fraud and Abuse Act of 1984 by encouraging them to “exceed their authorized access to information and e-mail” on Korn/Ferry computers. In doing so Nosal was held additionally accountable for violated the company Acceptable Use Policy for computers and internet.

Sir, I hope you will consider these examples (as extreme as they are) as reasons our company really does need an Acceptable Use Policy for our computers, internet and e-mail systems. Hopefully our company will never deal with anything this major, but I must stress that we as a company could also benefit from an extra "shield" from the accidental or intentional misuse of our company resources, meaning our internet, e-mail and computer systems here at work by creating our own Acceptable Use Policy. Thank you for your time.

Sincerely,

Andrew Dykman, IT Department @ Somebigcompany