Computers in the Law Office and the Dangers

Computers in the law office are vital for the law firm's success. Not only has computer usage reached its prime in society but in the law offices as well. The rise of computer use in legal organizations brings about increased power through advantages in court, lower costs, and greater efficiency in the use of computers.[1] Document management, word processing, legal research, time keeping and billing, are just a list of a few things computers are being used for. Computers are also being used to communicate and exchange documents with clients.[2] Although computers seem to be ideal to have in the law office they still have a downside and dangers.

One downside to computers in law offices is that not many people are proficient and do not know how to use computers and all the legal programs. For that reason, it is imperative for paralegals entering the job market to have a thorough understanding of computers.[3] Computer skills allow paralegals to be productive and efficient.[4] It gives attorneys and paralegals a competitive advantage in court, and allows the users to stay competitive in the job market.[5] It is essential for paralegals and lawyers to have understanding of computers and be efficient. Lawyers have to take classes like "Introduction to Technology" to improve their computer skills,[6] because technology changes faster than people can learn. A law firm that does not keep up with technology simply will not be able to match the ability of competitors to meet the needs of its clients, resulting in lower profits and loss of customers.[7] To get a job in the legal field it is

[1] Matthew S. Cornick, Using Computers in the Law Office,2 (6th ed. 2012)
[2] Id.
[3] Id. 1
[4] Id.
[5] Id.
[6] Lewis Elsen, REPORT ON THE OFFICE AND COMPUTERS Computer-literacy is becoming increasingly vital for law firms, Globe & Mail 1 (Nov. 7 1988) http://ic.galegroup.com/ic/ovic/NewsDetailsPageWindow
[7] Id. 2

important and even a pre-requisite to have computer knowledge and understand how to use computer programs.

Another problem with computers in the law office is that they hold personal and sensitive information on servers. This information can be hacked into if it is not protected by passwords or if the password is not strong enough. Security breaches occur if employees do not follow policy guidelines. Companies of all sizes are suffering consequences due to security network breaches.[8] A way to prevent this is to establish an electronic information, privacy and security policy. This policy should be shared with every employee. Security and privacy settings should be used when communicating electronically, making sure to use passwords.[9] Internet, Intranet, or Extranet should be solely used for business conduct only.[10] Security breaches occur when passwords are stolen because unprotected wireless networks are being used.[11] Passwords should be complex and changed on a regular basis.[12]

Many Internet Service Providers (ISP's) offer the convenience of accessing software and storing customer's information offsite on the Cloud.[13] This allows people to access information from anywhere at anytime, usually through a web browser.[14] Security on the Cloud is often as good or better than other traditional networking systems.[15] A benefit of storing data in the cloud is that you do not have to worry about backing it up anymore.[16] This is true but servers go down, there is always a risk that the internet connection will go down or that the web application server

[8] Edward A. Schirick, Risk Management, CAMPING magazine 16 (March/April 2012)
[9] Id.
[10] Id.
[11] Id. 18
[12] Id.
[13] Id.
[14] Id.
[15] Id.
[16] Gina Trapani, The Hidden Risks of Cloud Computing, 2 (Nov. 29, 2009) Lifehacker.com/5325169/the-hidden-risk-of cloudcomputing

will.[17] However do not expect ISP's to be responsible for security breaches. More and more people are moving their computer lives from their desktops to the Cloud, relying on hosted web applications to store e-mails, photos, documents and more.[18] Be aware of the privacy dangers that come with storing information on the Cloud. Police officers need a search warrant to seize documents stored on your computer, they only need a subpoena to get information stored on a third party server.[19] In fact, under the Patriot Act, the federal government has the right to demand some details of your online activity from service provides and do not have to inform you about it.[20] With that said understand the Cloud is a great idea for storing information, but by storing that information on the Cloud you lose privacy rights that you would normally have if it was stored on your own personal computer.

It is common to store clients information on other devices like flash drives, to work on a case at home. The problem with this is flash drives are easily lost, if lost any one can have access to that sensitive information. One way to avoid this from happening is to have the device encrypted, that way a password is needed to access the information. However, some employers may prohibit downloading personal information to notebook computers and flash drives.[21] To prohibit such devices is not a bad idea, and is most likely to be listed in the employer's policy.

The best way to prevent these dangers from happening is to have a well drafted, company-wide policy regarding computer and internet use. An adequate policy not only protects employers property and prevents liability from employee misuse of computers, but would also

[17]Gina Trapani, The Hidden Risks of Cloud Computing, 2 (Nov. 29, 2009) Lifehacker.com/5325169/the-hidden-risk-of cloudcomputing
[18] Id. 1
[19] Id.
[20] Id.
[21] Edward A. Schirick, Risk Management, CAMPING magazine 16 (March/April 2012)

explain reasons for enacting the policy and the goals the policy strives to achieve.[22] The policy should address whether a company e-mail communication system can be used for personal messages.[23] If communications can be addressed outside of the company, to what extent will the company monitor contents of e-mail communication?[24] What types of files and images are prohibited from being sent in company computer systems?[25] Employers should also develop and adopt policies regarding e-mail communication retention and deletion.[26]The policy should also outline procedures for disciplining employees in violation of the policy.[27] Require each employee to read the policies and acknowledge with a signature that the employee has received a copy of the policy, read it, and agrees to follow guidelines set forth in the document.[28] Employers have the legal right to monitor employee e-mail communication and internet use.[29] However, searches must comply with the constitutional standard of reasonableness.[30] For a workplace policy, employers should advise employees that defamation, harassment, or discrimination or creation of a hostile work environment on any basis will not be tolerated.[31] Furthermore, the policy should establish the process for investigation of such complaints,

[22] Gene D. Vorobyov, Computer and Internet Use in the Work Place: A Common Sense Approch, Psycologist-Manager Journal 8.2: 181 (2005) available at: http://web.ebscohost.com/ehost/delivery?sid=0048bb09-a8a9-403d-8b41-ef5299737d2c%
[23] Id.
[24] Id.
[25] Id. 182
[26] Id. 186
[27] Id. 182
[28] Edward A. Schirick, Risk Management, CAMPING magazine 16 (March/April 2012)
[29] Gene D. Vorobyov, Computer and Internet Use in the Work Place: A Common Sense Approch, Psycologist-Manager Journal 8.2: 178 (2005) available at: http://web.ebscohost.com/ehost/delivery?sid=0048bb09-a8a9-403d-8b41-ef5299737d2c%
[30] Id. 179
[31] Id. 184

resulting in disciplinary measures.[32] Encourage employees to come forth with complaints or concerns.

Computers are extremely important for a law firms success. It is essential to have computer knowledge and an understanding about how to use legal programs. However, be aware of the dangers, and understand the importance of following a company's guidelines; they are in place to keep employees and the company out of trouble. When using other devices like third-party servers and flash drives know the problems that come with them. Clearly the most effective way to avoid these dangers is to have a well drafted workplace and computer use policy. Be sure to have each employee read the policies and have them agree in writing. Know the dangers of computers in the law office, look out for them and be careful of how information is used and stored.

[32]Gene D. Vorobyov, Computer and Internet Use in the Work Place: A Common Sense Approch, Psycologist-Manager Journal 8.2: 184 (2005) available at: http://web.ebscohost.com/ehost/delivery?sid=0048bb09-a8a9-403d-8b41-ef5299737d2c%