Protecting YOUR FIRM'S DATA

By: Blazer Catzen

Today's headlines are scattered with stories of identity theft and lost information that compromise individuals' information. Whether they are network penetrations that result in the loss of national security secrets, compromised banking information, HIPPA data that leaked out on stolen laptops or lost hard drives, the impact to society is staggering. This article is intended to identify some of the avenues for these leaks and equip the legal administrator with the knowledge to steer policy and make informed decisions with respect to protecting the law firms, and subsequently their clients', information.

The first task in protecting the information is to understand where the information resides and how it moves. For purposes of this article, we are going to assume that all the information possessed by the law firm is sensitive and should be protected. When mapping your information, you should be focusing on the ingress, egress, and location of data. How do we get the data into the firm and how can it leave the firm? Where does it go when it leaves? Recent events have highlighted the loss of backups containing PHI (Personal Health Information) however the loss of backup media, while devastating, is a rare event. Other more common forms of data loss include stolen laptops, compromised passwords that result in unauthorized network access and unauthorized email access, and perhaps the largest causes are lost thumb drives and lost stolen smart phones.

Thumb drive or USB data sticks have become a very common way to transport data. Rather than taking a laptop home, it is very easy for the employee to copy files to the thumb drive, throw the thumb drive in their pocket or purse and work the files from a home PC. By virtue of this, our data map should now include the homes of our employees if they are taking work home. The discussion of home pc security and the implications of this action are beyond the scope of this article but as an administrator, you should be aware that a compromised home pc can result in a compromised firm network. More commonly, thumb drives are lost, stolen, or even inadvertently left behind when used to copy data at a client site.

Smart phones include our emails, phone books and in some cases password lists. I have encountered people who keep passwords, social security numbers and PHI on smart phones for easy reference. Rarely do they anticipate the consequences of the lost or stolen phone. The rapid acceptance of tablets and growing "app" pool that allows connectivity to firm networks can also result in data loss. Initially the exposure is firm email but as the tablets become stronger, the amount of firm data on or accessible to these devices will increase.

Invariably, when I discuss these topics with clients, they are quick to point out that their laptops and phones are password protected. At that point I pull the hard drive from their laptop and show them their data. New, and in some cases freely available, tools will bypass the security you are counting on to protect your data.

What can be done? All media containing firm or client data should be encrypted. Windows 7 Professional and Ultimate includes a utility called "Bitlocker" that will encrypt entire drives, thumb drives, and folders. There are also free utilities such as Truecrypt (http://www.truecrypt.org/) that create encrypted containers for your data. There are also software packages such as PGP that provide disk encryption, email encryption and container encryption. The encryption pass-phrase should be random and not include words found in a dictionary as the attacks to break the encryption will be dictionary based.

Smart phones that are managed from a central server (such as Blackberry Enterprise Server) include a remote wipe feature that will enable the firm IT staff to remotely wipe a phone. IPhones have a setting that will wipe the phone if 10 failed password attempts are encountered. Anyone carrying an iPhone or Blackberry with the firm's email and information should have the phone password protected and preferably use the more complex passwords and not simple 4 digit passwords to access the phone. Lost phones should be reported immediately.

In closing, information travels by disk drive, thumb drive, email, laptop, phone, tablet and backup media. Each of these media should be encrypted to protect the data in the event it is lost or stolen. The extra time required to access the data will bring complaints from partners and staff; however, the consequences of losing the data will outweigh the inconvenience.

Blazer Catzen has worked in Information Technology since 1986. Catzen Computer Consulting Corp. provides general consulting services. His clients include many law firms and small businesses as well as Johns Hopkins and University of Maryland Health Systems. He founded Cape Computing in 1991 and served as its president until 2008 when he sold the company. He has had hands on experience in all aspects of IT including network design and administration (local and wide area), database design, software development, software architecture, network security, and computer forensics. After the sale of Cape Computing he founded Catzen Forensic and Catzen Computer Consulting Corp. Catzen Forensic provides computer forensic and data recovery services in support of litigation discovery.