Losing someone’s data, it’s a resume generating event

By Ken Foster 9/4/2008

Every month there is some company or Government agency in the news trying to explain why they lost client data and how they are going to protect their customers in the future. What you don’t see is the human toll of the loss. That loss cost the organization more than the cost of a device. It cost them integrity, agility lost mitigating the event and someone most likely got walked out the door. Don’t be the person who lost their job as the result of someone else’s apathy or ignorance. Follow these five steps to protect your data and your job {more…}

Step 1: Users shouldn’t be Local Administrators:

There are several schools of thought on this. If you allow a user to have administrative rights on their laptop, then they can self-resolve any issues they may encounter while on the road. However there is a down side, they can also install file sharing and other unapproved applications that can cause the breach. The only way you can control what gets installed is for IT to be the sole owner of the administrative rights on the information systems. After all, the computer and its data belong to the company, not the user. If you are not currently doing this, prepare for significant user pushback. You will also need to do lab testing to determine if you must adjust directory or file permissions so non-administrative users can run their applications. Filemon and Regmon (free from Microsoft) are excellent tools to troubleshoot these issues.

Step 2: Control what Software you allow:

Every company should have an approved software list. Every device should only have items installed and used that appear on that approved list. There are always going to be exceptions, but those should be documented and approved by your Information Security Officer or Chief Information Officer as applicable. Many companies use Instant Messengers and other collaborative tools to increase worker productivity. These are also vectors to hemorrhage information. If you allow these applications, consider a content monitoring tool such as Vontu Network Data Loss Prevention from Symantec or McAfee Host Data Loss Prevention. Both have their own strengths and weaknesses. Whatever tool you consider, you will have to take into account vender experience, cost, and ease of use based on your unique environment. There never is a one size fits all solution, regardless of what the vender tells you. Require an onsite demo and pilot program prior to procurement.

Step 3: Encrypt your computer drives:

Three Years ago, whole drive encryption would cost you a lot of money and would have sucked the life from your system. It was the refuge of the NSA and the most sensitive of corporate data. Today, with most computers running dual core processors and 2 Gb of Ram, you can’t afford to be without this protection. It should be as second nature as anti-virus and cable locks. Don’t trust your users to remember to encrypt files themselves using some utility. Make the encryption process seamless and guaranteed. What whole drive encryption provides you is a method to deny a thief the ability to slave the drive and access your sensitive corporate data. Because only a small part of the drive isn’t encrypted (just the minimal parts for initial boot and checksum validation), the boot delay is quite minimal. If you attempt to slave the drive and use a Linux boot environment or Bart PE like tools to access the drive, the space shows as uncooked and inaccessible. Initial set-up can range from complex to simple. This space has several mature products with options that run the gambit of remote drive wiping, panic states that prevent a computer from booting off its home network, to a fairly transparent user experience. You adjust your paranoia to suit your needs. Any encryption product you consider, regardless of purpose, should meet the Federal Information Processing Standards (FIPS) 140-2. Why is this important? Only devices that have gone through rigorous testing can meet this standard. That means our friends at the NSA have hacked on the tool and even they can't break in. Lots of venders claim this coveted rating so ask to see their certificate for the product. Visit the NIST site for more information on this standard and to find venders who have successfully met the requirements.

Step 4: Encrypt your Flash Drives:

Flash drives are a great way to transport information from one location to another. Within the space of a few inches, you can store more information that you can fit on multiple DVD-R's. It's also a great way to lose a huge amount of sensitive corporate data in an instant. Because of their size and convenience, Flash drives have been integrated into the main stream of corporate life. Think back over the past year. How many times have you heard someone talking about losing a flash drive, washing it then pitching it in the garbage, or showing up to the workplace with a new Flash drive and no accountability of the old one? Ever wonder what data was on the drive? If you think it's no big deal, ask the President of Arapahoe Community College, who lost 15,000 social security numbers and various student data as a result of the loss of one Flash drive in August 2008. Flash drives represent a larger risk factor for corporate data loss than unencrypted laptops because of their size, storage capacity and lack of accountability. There are several venders in the marketplace that offer standalone encrypted drives. One drawback of a standalone drive is the loss of all data should the user forget their password. Corporate managed Secure Flash Drives offer companies the ability to provision, manage, and secure data in an integrated environment. Corporate managed drives provide you the ability to execute password recoveries, provision devices, and disable devices should one be lost, stolen or kept by a recently terminated employee. Some devices even offer a remote wipe capability. These secure devices will automatically wipe or destroy the recovery key should they be tampered with or exceed a set number of login attempts. There are several excellent venders in the space that include Kanguru, Ironkey, and MSI to name a few. Always check for a FIPS 140-2 certification prior to considering any venders product. That is unless the few dollars you saved buying a less secure drive doesn't hinder your sleep once it is lost or stolen.

Step 5: Logon Tokens and Smartcards:

Today it is estimated that there are over 1,000 keyloggers in the wild. A Keylogger is a piece of software that listens to your keystrokes and records everything you type, including user names and passwords and then send that data to someone else. Password complexity requirements can be increased but that doesn't defeat password cracking tools or the user who decides to write it down and keep it under their mouse pad. Stopping attackers from brute forcing a password can be difficult. One option is to eliminate passwords all together. Logon tokens and smartcards increase the complexity of breaking into a system by raising the standard from single factor authentication (e.g. something you know), to two factor authentication (e.g. something you know and something you physically have). Only with the combination of these two items can a user successfully logon. These are defiantly an added expense but increase the complexity for external attacks to a level beyond all but the most dedicated state sponsored attackers. RSA, VeriSign, and Entrust are some of the heavy hitters in this space. As always I recommend an onsite demonstration and assisted pilot prior to any procurement.

I hope this article was helpful. Data loss is a serious incident that can harm your customers, corporate integrity, and your long-term employment potential. A phased approach to implementing these five steps will increase your security. After all, it's a much different conversation to tell a client you lost an encrypted Flash drive or Laptop than one that isn't.