TOP TEN THINGS TO KNOW ABOUT DATA PROTECTION

TOP TEN THINGS TO KNOW ABOUT DATA PROTECTION

According to the 2006 CSI/FBI Computer Crime and Security Survey, 46% of companies reported a laptop loss or theft. Furthermore the report stated that losses from laptop theft increased from $19,562 per respondent in 2005 to $30,057 per respondent in 2006. However, according to the report, “we are suspicious that implicit losses (such as the present value of future lost profits due to diminished reputation in the wake of negative media coverage following a breach) are largely not represented in the loss numbers reported here”. Other reports that attempt to include implicit losses rate the value in excess of $900,000.

This figure may sound incredible but it pertains to the inherent value of the information on the laptop. The damage to a corporation due to loss of data can result from:

1. Competitors using stolen data to reduce market share
2. Loss of customer confidence resulting in lower sales
3. Negative publicity lowering corporate value (or at worst bankruptcy)
4. Costs to injured parties, which can be legally required
5. Lost productivity to mitigate damage of stolen data.

Data protection is fast becoming part of the IT arsenal to combat data loss/theft. It can significantly reduce the amount of damage done by the above and their associated costs. Here are the top 10 things you should know about data protection:

#10: It’s the data that’s the cost:

Although a thief may be after the hardware and software, it is the loss of the data that ultimately causes the most financial damage. A recently published article by InfoWorld had the editor describing the value of her laptop as “$2 million”. This shows the type of damage a company can expect from data loss. By using data encryption techniques, the information is protected BEFORE and AFTER the data is stolen. Either a key or password is always needed to open the data.

How Dell’s solution is different: Dell’s Data Encryption service continuously encrypts data on a PC whether or not it is connected to the Internet and allows users to report laptop loss. This makes the data virtually useless and significantly minimizes the resulting financial loss.

#9: Keys, keys everywhere:

Ask anyone that has used an encryption solution what are the top three difficulties and chances are that key management will be in there. Managing keys, replacing lost keys, and explaining what keys do are the bane of the security professional when it comes to encryption solutions.

How Dell’s solution is different: Since Dell Data Encryption is a managed service, the headache of key management is handled by Dell. You don’t have to worry about it at all.

#8: Encryption is “key” to regulatory compliance:

Despite a bad pun, the heart of most regulations is protection of sensitive electronic data. In most cases the regulation explicitly requires that encryption is used to protect specific information.

How Dell’s solution is different: In many cases, responding to regulations requires a quick and inexpensive solution. Dell Data Encryption can meet most compliance budgets and timeframes and after implementation, robust compliance information is available.

#7: Server management – the bottom of the iceberg:

It's what you don't see that causes the damage. In addition to desktop software many solutions require additional servers to manage rights and keys. This not only adds to the capital expense but also to the maintenance cost.

How Dell's solution is different: As a "Software as a Service" solution, the entire infrastructure is hosted by Dell. There are no expensive servers to buy, deploy or manage and no VPN connection is needed for PCs to connect to.

#6: Encryption software needs protection:

Any security expert will tell you that there are no bullet-proof solutions even when talking about encryption software. There could be errors in the encryption algorithm or problems in the software implementation.

How Dell's solution is different: Data Encryption is only part of Dell's endpoint security solution. The complete solution manages and secures the PC and its software. Upgrades are automatically distributed as part of the service.

#5: Encryption is only part of the solution:
If you think that once you have encryption that you're protected, you'd be wrong. Encryption is only part of the solution. Data can be stolen while it is in use by employing viruses and malware. Making sure that hackers can't get the data when it is being accessed is also important.

How Dell's solution is different: Dell Anti-Malware & Virus Management protects desktops and laptops from Internet attacks and hackers helping to slow down any hacker attacks from Trojans or viruses.

#4: Don't forget about integration with the data backup system:
One of the challenges with encrypted data is integration with the back-up system. Storing encrypted data means having the key available when the back-up is done. This begs the question of where the keys get stored.

How Dell's solution is different: Dell Data Encryption is seamlessly integrated with Dell's Online Backup service. Encrypted data is backed up and can easily be restored, together with the user keys.

#3: Third party validation leads to greater security and reliability:

Having a trusted encryption solution is a must for any organization. A third party test must be provided by the vendor. All distribution of security credentials and software must be done securely.

How Dell's solution is different: Dell Data Encryption has been certified by the Federal Information Processing Standards (FIPS), a universally respected government certification agency. Transport Layer Security (TLS) is used for all connections to the PC.

#2: Federal data has its own standards:

The federal government requires that only the Advanced Encryption Standards (AES) or the Data Encryption Standard (DES) is used for encryption.

How Dell's solution is different: Dell Data Encryption uses both AES and DES. Plus it is FIPS validated per government regulations.

#1: All files should not be treated the same:

A common encryption challenge is ensuring that ALL sensitive data gets encrypted. A common solution is Full Disk Encryption. While this ensures that all data is encrypted, programs also get encrypted. This results in additional overhead to decrypt the program data and a drag on the PC's performance. Not to mention what happens if the encryption fails (answer- no PC).

How Dell's solution is different: Dell Data Encryption utilizes an algorithm that searches and encrypts data files automatically, removing any user decisions. Furthermore, if a user forgets the key, the PC still works and a new key can be delivered securely over the Internet. All of this with complete transparency to the end user so that they are as productive as they were before their data was encrypted.

Dell's Data Encryption and Online Backup services can be combined to deliver a proven, reliable and simple solution to a company's data protection needs. Key advantages include:

> Maximum security, whether PCs are online or offline
> Rapid deployment that's simple and silent
> Flexible options to fit your business needs
> Centralized management and reporting

ABOUT DELL

Dell Inc. (NASDAQ: DELL) listens to customers and delivers innovative technology and services they trust and value. Dell is a leading global systems and services company and No. 34 on the Fortune 500. With a focus on the needs of managed services providers (MSPs) and resellers, Dell Remote Monitoring is a distributed, multi-tenant platform for providing remote management across diverse, customer-controlled networks. This technology platform is combined with proven sales, marketing, and operations best practices to help the company's partners see successful results immediately. Dell Remote Monitoring supports systems, peripherals, security devices, network devices, and applications.

For information on the Dell Partner Program: www.dell.com/desktopmanager

Specifications are subject to change without notice.

6591 Dumbarton Circle, Fremont, CA 94555 ·888.307.7299/Fax 510.818.5510