

DATA PROTECTION: KEEPING YOUR INFORMATION SECURE, CONFIDENTIAL, AND INVALUABLE

Chris A. MacKinnon
Freelance Writer for Business Solutions magazine

INTRODUCTION

Data is the lifeline of any business. If that lifeline was cut, your business would literally lose its life. The push to protect the corporation these days must begin with data, because protecting that asset is the key to your company's continued success. When it comes to business continuity planning, securing information internally and externally is the central challenge that information-driven organizations face today. Business data is now everywhere, from USB devices, to laptops, servers, etc., so the risks of data leakage and the possibility of threats spreading across data media increase dramatically.

CHALLENGES

A recent study by Ponemon Institute (www.ponemon.org) reports that data breach incidents in 2009 cost U.S. companies \$204 per compromised customer record, compared to \$202 in 2008. The Ponemon Institute is considered the pre-eminent research center dedicated to privacy, data protection and information security policy. Their annual consumer studies on privacy trust are widely quoted in the media and

their research quantifying the cost of a data breach has become valuable to organizations seeking to understand the business impact of lost or stolen data.

Another key finding in the study found that malicious attacks and botnets were more costly and severe. On the upside, negligent insider breaches have decreased in number and cost due to staff training and awareness programs, and 58 percent of staff have expanded their use of encryption (up from 44 percent the previous year).

But it doesn't end there. Mobile employees, for example, are bringing business data from their local networks to the global markets that they compete in. So businesses need a well-oiled, centralized approach to protect their business data. But using traditional methods to protect specific devices or data is no longer sufficient to provide cross-enterprise data security. To protect your data, mitigate risk, and meet compliance requirements, businesses must implement a complete enterprise data protection strategy.

Another main challenge, when it comes to data protection, is unre-
lenting data and application

growth. Also, traditional backup windows are becoming obsolete because employees, partners, and customers alike are expecting to have their applications and data available around the clock.

For adequate data protection, your business needs a data backup system that archives business data regularly, creates data backups on reliable media, and keeps updated data backups in secure, off-site locations.

DATA ENCRYPTION

Any good data protection plan includes encryption. In fact, the main attraction in the pursuit of data protection is encryption. Data encryption is the process of scrambling plain text into cyphertext, which is nonreadable data to unauthorized eyes. The person intended to read the data is given a key that triggers an algorithm mechanism to decrypt the data. The use of keys is the foundation of encryption because users can encrypt data and also decrypt data that is intended for them. When the keys are the same, this is called symmetric key encryption.

On the other hand, when asym-

metric keys are used, a private key allows users to encrypt and decrypt data, but a public key (used by anyone) only encrypts the data. The newest industry standard for encryption, AES (Advanced Encryption Standard), permits a maximum of 256-bits.

ZENITH'S APPROACH TO DATA PROTECTION

Part of Zenith's job is to help keep your business data protected and available at all times. The company's BDR solution includes 256-bit AES Encryption. The BDR appliance is a disk-based NAS (network attached storage), which provides access to point-in-time snapshots that only take minutes to restore. This happens without any impact to your business environment. During the restore process, your data is decrypted, which offers peace of mind in knowing that your data is protected while it was being stored. And restoration is easy, simply mount your backup file as a drive on the NAS and copy your data locally or to the network.

If you choose the option of synchronizing your backups offsite to Zenith's secure co-location facilities (offsite storage), your data is copied over an industry standard 256-bit encrypted tunnel. For security purposes, your data is fully encrypted. Zenith employs the 256-bit AES algorithm because it has never been broken, is considered the gold standard of encryption techniques, and renders transmitted data immune to theft.

This process ensures that your backups have not been compromised during transfer. The good news is, if you're existing site is destroyed, Zenith has your back

and your data is protected. The data is shipped to you on a replacement BDR, by air the following day. Your servers are virtualized on the BDR until you have your replacement hardware. It's a simple and secure process to send your base images to Zenith managed collocation. You'll also save time with Zenith's automated daily incremental image synchronization.

The Zenith ARCA (Advanced Recovery and Continuity Appliance) is yet another way that your business can protect itself. The ARCA is a network-attached storage device that comes preloaded with all the backup, recovery, and virtualization software that it needs to protect your business. If you're looking to manage your own solution, the ARCA uses the same proven technology of Zenith's Backup & Disaster Recovery, but the ARCA is a complete stand alone product. The ARCA provides the speed and reliability of enterprise-class business continuity and recovery solutions — without the enterprise-class price.

DATA PROTECTION BEST PRACTICES

Use the following examples to implement (and stick to) a data protection policy:

- Implement a data classification program with designated owners of the information.
- Develop a business-wide data architecture to manage the flow of important information.
- Encrypt critical information throughout the business environment.
- Be careful when using new technology because security protection mechanisms are often immature.
- Understand what data is most sensitive to your business and know

where this sensitive data resides.

- Manage security centrally.
- Audit security to constantly improve your protection.
- Ensure that all endpoint devices are secure. These devices include PDAs (personal digital assistants), laptops, USB-based memory sticks, cell phones, and other handheld devices that are used to store critical information.

CONCLUSION

Protecting your data against theft and ensuring that it remains confidential — no matter where it is stored — is paramount for continued business success. Without security components like encryption, information transferred across the internet can be grabbed and viewed virtually by anyone. You wouldn't leave the front door of your business open after hours, but when your data is not protected, the front door is always open to thieves. When you consider that information-based crimes are on the rise, your business can't live without data protection.

Sponsored by:



Infotech Ltd

zenithinfotech.com