Managed USB and Optical Media Encryption For Small Businesses

Roxio Secure Managed Helps Small Businesses to Prevent Unauthorized Access to Data on USB Flash Devices and Optical Media

Introduction

In the recent past, data security was not a high priority for small and medium businesses. This situation has changed dramatically, and Small and Medium Businesses (SMBs) are looking for cost effective ways to secure their data. Roxio Secure Managed provides an inexpensive solution for managed encryption of data on optical and USB flash media.

Increasing Awareness of Risk

In 2006, the Council of Better Business Bureaus announced an education initiative geared toward helping small business owners improve their security and privacy readiness in a climate of data exposure risks.[1]

Steve Cole, president and CEO of the Council of Better Business Bureaus, said, "Small businesses aren't quite in step with their larger industry counterparts in addressing data security. They often believe they're better protected than they really are, because they don't have in-house experts to advise them on what else they should be doing beyond locking up their storefronts. It's difficult for them to know where and how to access support. This makes us all vulnerable, as small businesses are a strong part of our economy. Business owners of all sizes need to be vigilant in protecting their customers, their employees and themselves."

A series of recent highly publicized data breaches such as the recent publication of diplomatic cables by Wikileaks has increased public awareness of the vulnerability of confidential data. Open Security Foundation publishes a report of data losses at http://datalossdb.org/ . A search on the terms 'CD', 'DVD' or 'USB' provides a frightening glimpse into the prevalence of data loss on these media types.

According to a survey published in 2010 [2], data loss and cyber attacks are now the top two risks that concern managers of SMBs. According to the survey, SMBs spend two thirds of IT's time and US $51,000 annually on protecting information. Furthermore, 42% of those surveyed have actually lost proprietary or confidential information.

The Cost of Data Breach

Threats can come from many sources, but breach can often be attributed to employees who carelessly store unsecured data on portable media. Such media is carried outside of the office, and can be stolen or misplaced, and accessed by unauthorized persons. The data may include confidential customer records (such as medical, legal or credit card data), company financial data, and other sensitive information.

Poneman Institute conducts independent research on privacy, data protection and information security policy. In 2010, Poneman Institute published a summary of the results of a Cost of

---

[1] "Think Data Security Isn't a Small Business Problem? Think Again." Better Business Bureau press release announcing education initiative geared toward helping small business owners improve their security and privacy readiness in a climate of data exposure risks. http://www.bbb.org/us/article/think-data-security-isnt-a-small-business-problem-think-again-614

[2] Symantec 2010 SMB Information Protection Survey: http://www.symantec.com/content/en/us/about/media/pdfs/SMB_ProtectionSurvey_2010.pdf?om_ext_cid=biz_socmed_twitter_2010Jun_worldwide_SMB

Data Breach study.[3] Included in the research were the costs of detection & escalation, notification, ex-post response and lost business. In 2009, the cost per lost record in the US was $204. Furthermore, 36% of losses were due to lost or stolen devices. Lost business and notification requirements constitute a large percentage of the costs of data breach.

According to the National Conference of State Legislatures, forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.[4]

National legislation such as The Gramm-Leach-Bliley Act ("GLBA") and the Health Insurance Portability and Accountability Act ("HIPAA") require that financial and health care providers take steps to ensure that personal information is secure. These laws may impact SMBs such as doctor's offices, insurance companies or other businesses. As with any legal issue, it is best to consult with an attorney to determine exactly how these laws affect any business.

Notification can be expensive and can damage a firm's reputation, resulting in lost business. However, if data is encrypted, notification may not be required.

As a specific example, California Senate Bill 1386 requires that affected individuals must be notified if ***unencrypted*** personal information is acquired by an unauthorized person.

"SEC. 2. Section 1798.29 is added to the Civil Code, to read: 1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose ***unencrypted*** personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system."[5]

Preventing Data Breach on Portable Media

SMBs typically do not have in-house IT managers. The IT infrastructure is handled by Value Added Resellers (VARs) or by IT consultants. It is important for the SMB management and the VAR or consultant to develop a comprehensive plan for preventing data breach. Securing data on portable media needs to be included as part of this plan. When determining how to secure (i.e. encrypt) data, managers will need to consider:

1. Keeping an up to date inventory of devices and media
2. Educating employees
3. Implementing encryption software and/or other technology
4. Ensuring that this technology is used effectively by employees

---

[3] Five Countries: Cost of Data Breach, presented by Dr. Larry Poneman. http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2010%20Global%20CODB.pdf

[4] http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx

[5] http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

Unless management has a thorough inventory the devices used to carry data, it is virtually impossible to control data breaches. In the case of portable media, it is important to know which computers have CD or DVD burners, and also to know which USB flash devices are being used to carry data.

Employee education is an important step in effectively securing data on portable media. Employees need to be made aware of the need for ensuring that sensitive data carried outside of the office on optical media or USB media is encrypted. Furthermore, employees need to be aware that it is both a legal and ethical responsibility to report to management in case portable media is lost or stolen, and to confirm whether that media was encrypted or not.

Encryption software should follow approved standards such as FIPS 140-2 (a U.S. government computer security standard used to accredit cryptographic modules), and the encryption should be strong enough that it cannot practically be circumvented. The software should enable system administrators (or VARs acting as administrators) to control access to media in case it is lost or stolen, or in case an employee leaves the company.

The encryption software needs to be easy to deploy and to manage. It should be deployable across a network via a command line using standard and well documented tools. After installation, it should be possible for the system administrator or VAR to configure it so that different employees are assigned appropriate permissions to access the media. An additional plus is if the client software can be managed remotely in real time, and if data access can be logged in case an audit is necessary.

Last, but not least, the software needs to be so easy to use that the employee *does* use it, and does not simply ignore the use of encryption. One of the biggest challenges in protecting data on removable media is that it is so easy for workers to write files to disc or to a USB stick. Even if encryption is available, workers may simply choose not to use it because it requires extra time and effort.

Roxio Secure Managed

In the simplest terms, encryption of data on secure portable media can prevent unauthorized users from accessing it.

Roxio Secure Managed is a software product that helps SMBs to protect against data breach. The product enables users within an organization to quickly secure data on CD, DVD, Blu-ray Disc and flash devices using powerful data encryption that safeguards the contents from being accessed by unauthorized persons.

Roxio Secure Managed is specifically designed to make it extremely easy and transparent to encrypt data burned to optical media such as CD or DVD, or copied to USB flash memory devices. Furthermore, Roxio Secure Managed is designed to be scalable, depending on the needs of the organization.

With Roxio Secure Managed, decision makers as well as employees responsible for transporting data can be confident that data is secure.

Roxio Secure Managed includes:

- Burns data on CD, DVD and Blu-ray Disc using an easy drag & drop interface
- Copies discs and disc image files
- Encrypts data on disc using a FIPS 140-2 certified encryption module
- Spans files too big to fit across multiple discs
- Reads and writes disc image files
- Discs can be read on permitted PCs, while restricting access on PCs that are not permitted
- Group read permissions are set at installation via command line
- Read permissions can be changed after installation
- Discs can only be written by permitted users
- Discs can only be read by permitted users
- An authorization server controls permissions per organizational policies
- Permissions can be changed in real time by the system administrator via a web control panel
- Data on USB flash devices is encrypted, and can be destroyed if a device is lost or stolen
- Supports logging and reporting of files burned to disc, files sent to USB devices, and administrative changes to permissions

The product is provided as a subscription software service, and is ideal for offices and organizations of any size.

In Conclusion

Roxio Secure Managed enables encryption of data on removable media including optical discs and USB flash memory devices. Roxio Secure Managed makes it easy for employees to automatically encrypt data per organizational policies, and helps to protect SMBs from the expense of data breach and non-compliance with mandated regulations.

Roxio Secure solutions are an inexpensive and convenient way for SMBs to ensure that confidential records stored on optical and USB flash media are only viewable by authorized personnel, and can help to ensure compliance with mandated regulations.

Contact

To request a quote, contact the Volume Licensing Sales team at:

North America:

Tel: 866-825-7694 or 972-713-8110

Email: vlp@roxio.com

Europe:

Email: vlp.emea@roxio.com

© Rovi Corporation or its subsidiaries. All rights reserved.