

Bryley Tips and Information November 2009

1. Secure your electronic data with Encryption

Encryption scrambles the contents of an electronic file or device, making it unreadable to all except the intended recipient or user. It is a common technique used to protect confidential information that might transmit or travel outside the organization.

The primary items that organizations target for encryption include:

- Disk drives – USB memory sticks, USB-attached drives, and notebook disk drives
- Email, email-based attachments, and external file transfers
- Wireless transmissions
- Handheld devices
- Backup tapes

We address the first two items below.

2. Tools to encrypt disk drives and storage devices

Computers have fixed-disk drives, read/writable CD or DVD drives, and external ports (USB and eSATA) to accept memory sticks and attached drives. Any of these drives or devices that might contain confidential information and travel outside an organization should be encrypted.

Some disk and file-encryption options:

- Microsoft BitLocker – Disk-encryption software included free with Windows 7 and Vista
- TrueCrypt – A well-known, free, software utility to create a virtual, encrypted drive
- USB Encrypt – A highly-rated, free utility to encrypt USB-based drives
- PGP Whole Disk Encryption – Popular, cost-based encryption program
- McAfee Endpoint Encryption – Cost-based encryption software
- PKZip – Industry-standard file encryption

Visit <http://download.cnet.com/windows/encryption-software/> for free software-encryption tools.

Related tool: Use Tolvanen's Eraser (<http://www.tolvanen.com/eraser/>) to securely remove sensitive files from your computer drives.

3. Encrypting email and attachments

Emails are typically sent as free text, meaning that anyone who can intercept an email over the Internet can read its contents. (This type of interception, by “sniffing” packets of data exiting your email server, requires effort and dedication on the part of the eavesdropper.) Encrypting an email scrambles its message, keeping outsiders from reading its contents.

Unfortunately, once encrypted, the email-recipient is now forced to take steps to decrypt the message after it is received, a process that can be somewhat frustrating the first time through for the casual user. Also, some email encryption software cannot encrypt email attachments.

Visit http://ask-leo.com/how_do_i_send_encrypted_email.html for details on email encryption (via GPG) and <http://netsecurity.about.com/cs/emailsecurity/a/aa051004.htm> to find out why you should encrypt your email.

Email encryption can be purchased in one of three forms:

- Appliance or server-based software
- Workstation-based software
- Ongoing service

Appliances and server-based software permit policy-based encryption with central management. (Policy-based encryption forces automatic encryption when the contents of an email trigger the policy. For example, most financial organizations enable an encryption policy to encrypt any outgoing email with a 9-digit number on the presumption that this number could be a social security number.) They cost upwards from \$7,500 and usually have annual maintenance costs.

Email-encryption appliances and server-based software include:

- Cisco IronPort – Stand-alone appliance with centralized management
- PGP Universal Gateway Email – Linux-server-based software
- Tumbleweed – Windows-Server-based software
- WebSense – Windows-server based software

Workstation-based software encrypts all or selected email from the workstation. The sender must provide decryption information to the recipient, typically in the form of a key. Costs range from free to about \$150 per workstation.

Some workstation-based email-encryption options:

- GPG (Gnu Privacy Guard) – Free, command-line-based tool for general email encryption
- PGP Desktop Email – Key-based email encryption; must create key for each recipient
- Trend Micro Email Encryption Client – Encrypt all email to a selected recipient

Email-encryption services provide a *Software as a Service (SaaS)* method of delivery, typically charging a monthly fee per user to encrypt email. Some require a minimum number of users; some are free for the base package but offer upgrades for greater functionality.

Several email-encryption services:

- HushMail – Free web-based with upgrade to domain or Microsoft-Exchange-based email
- WebSense – Microsoft-exchange-based at about \$18/user per year; minimum 25 users
- Google Message Encryption – Inexpensive encryption powered by Google's Postini
- Zix – Policy-based service for regulatory (usually HIPPA) compliance

Rather than email attachments, these file-encryption services permit encrypted file transfer:

- LeapFile.com – Easily transfer encrypted files at \$20/user per month

- Box.net – File-sharing service to store encrypted files; free to \$15/user per month
- DropFile.net – A free service to store and encrypt your files; requires a Windows client

Please call Bryley Systems at 888.280.5799 for more information.

4. Free pickup and recycling from Willie's Computer Recycling during December

Willie Bergeron has extended his offer of free pickup and recycling to friends and clients of Bryley with a minimum of five items (PCs, monitors, or printers) through the month of December. Please call 978.562.6077 and select extension 218 for details.

5. Announcements, news, and events

Free webinars on Unified Communications – Join an enlightening discussion on *Unified Communications: What can it do for your business?* on December 9th or 16th at 2pm.

These sessions are sponsored by Avaya Inc., a world-leader in communications solutions. Bryley Systems, an Avaya Business Partner, is fully versed in these solutions.

Please email Sales@Bryley.com or call us at 888.280.5799 and select option 2 for sales.

Complying with 201 CMR 17.00 – Please join Bryley Systems for a free, how-to seminar on complying with Massachusetts 201 CMR 17.00, Standards for the Protection of Personal Information of Residents of the Commonwealth, to see how it will impact your business and what you will need to do to meet its physical and electronic (computer-based) requirements.

201 CMR (Code of Massachusetts Regulation) 17.00 requires all organizations that have personal information on even one Massachusetts resident to protect this data. It implements the provisions of Massachusetts General Law c.93H and sets the standards for compliance and takes effect on January 1, 2010. (Below is a reprint on this topic from our October 2009 newsletter.)

These seminars will be held on Wednesdays at 9:00am at Bryley's second-floor conference room in Hudson, MA. Refreshments will be served.

Remaining seminar date: December 9th, 2009

To reserve a seat:

- Call 888.280.5799, extension 218, and register with Garin.
- Visit www.Bryley.com/news_and_events-Events.html.
- Email Events@Bryley.com.

Follow Bryley Systems on Twitter – Visit <http://Twitter.com/BryleySystems>.

6. Don't wait until March 1st to comply with new Massachusetts privacy law – reprint from *Bryley Tips and Techniques*, October 2009

In September 2008, Massachusetts issued 201 CMR 17.00, a new statute that requires any organization with personal information on even one Massachusetts resident to secure this data by March 1, 2010. Given the previous delays in finalizing this statute, most organizations are probably behind the curve in its compliance.

We started our compliance efforts late 2008 with a dedicated project manager and a budget of well over 250 hours, but were surprised at the actual amount of time and effort involved, which required physical, administrative, and technical changes to our operations.

Some of the administrative steps we took:

- Created our Written Comprehensive Information Security Plan (WISP)
- Updated our Employee Manual to include a section on 201 CMR 17.00
- Hired an HR consultant to assist with employee training

We made these physical changes to our office:

- Built locking cabinets to store our old paper files
- Physically locked-up several exposed computers with cable locks
- Locked-down all filing cabinets and moved the HR cabinet to a more-secure area
- Installed a security camera in our data-center (which is secured by locked fencing)

We addressed technology compliance in these three areas:

- Secured the gateway (Internet)
- Security-hardened the endpoints (PCs and servers)
- Performed a multi-point process to technically lock-down equipment and its access

For details on our technology actions, call me at 978.562.6077 x215 or email GHL@Bryley.com.

Even though we were better prepared than most organizations, we have exceeded our time-budget on this project and still have some finishing touches to complete.

Our suggestions:

- Start today and be prepared to devote significant time and effort.
- Consider hiring an HR consultant or project leader to assist in the implementation of the physical and administrative changes; call Bryley to assist with the technical areas.
- Attend a 201 CMR 17.00 seminar. (See below for our seminar dates and times.)

Client service

If you have questions about, or issues with, our client service or response, please contact Beverley Denio, Client-Service Manager, at 978.562.6077 x201, or Gavin Livingstone, President, at 978.562.6077 x215. (Respective email addresses are BDenio@Bryley.com and GLivingstone@Bryley.com.)

Bryley's Client-Service Portal

Over the past years, Bryley has made significant investments in our business systems and infrastructure to enable real-time communications regarding the timeliness and quality of services we deliver. A result is that client-service requests (with resulting service tickets) may now be added, viewed, or updated through our Client-Service Portal.

This real-time environment is available 24 x 7 at www.Bryley.com by selecting "Client Login" from the upper-right corner of the home-page. Registered users may perform these functions:

- View the current status and details of their service tickets
- Enter new service requests
- Review invoices
- View reports

To use this capability, please contact Beverley at 978.562.6077 x201 to setup a username and password. Training is also available at no charge.

Contact Bryley Systems Inc.

Bryley Systems is a full-service, end-to-end provider of business-technology solutions, fulfilling the information-technology needs of organizations throughout New England since 1987. Areas of expertise include:

- Managed Technology
- Computer-network performance and reliability
- Network security
- Unified Communications

Email: Info@Bryley.com

Phone: 978.562.6077

Fax: 978.562.5680

www.Bryley.com

Bryley Systems Inc.
12 Main Street
Hudson, MA 01749-9990

Business Technology Solutions Since 1987

How to Subscribe or Unsubscribe

Bryley Tips and Information is a free e-newsletter sent each month (except July). It provides information and user-level tips on computer and telephone-system issues.

You are receiving this e-newsletter because:

- You are a Bryley client
- You have received a quote or proposal from Bryley sales, or
- You have had business contact with Bryley Systems.

Subscribe

If you or a colleague wishes to subscribe to this e-newsletter, please e-mail Newsletter@Bryley.com, visit www.Bryley.com/news_and_events-newsletter.html, or contact Michelle at 978.562.6077 x216 or via MDenio@Bryley.com.

UnSubscribe

Options to unsubscribe from this e-newsletter:

- Please reply to this newsletter with the word "unsubscribe" in the subject header.
- Visit www.Bryley.com/news_and_events-newsletter.html.

- Email Newsletter@Bryley.com.
- Call us at 888.280.5799.

Copyright 2009. Bryley Systems Inc. All Rights Reserved.

THIS DOCUMENT IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. The information contained in this document represents the current view of Bryley Systems Inc. on the issues discussed as of the date of publication. Bryley Systems Inc. cannot guarantee the accuracy of any information presented.

INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED 'AS IS' WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND FREEDOM FROM INFRINGEMENT. The user assumes the entire risk as to the accuracy and the use of this document.