

Tech Talk: Encryption technology becoming a must for business use

By **MJ Shoer**

February 12, 2010 2:00 AM

Confidential information is a fact of life for most businesses. Whether it's personal or financial data about your customers, trade secrets or other types of information, it is critically important this information be properly secured.

It's a common practice for businesses to secure this type of information in its hard copy form, either in locked file cabinets or perhaps even a safe. When it comes to their electronic counterparts, that same data security is not quite as standardized. In part, this is because data can be in numerous systems, files, databases, etc. How these are secured often varies by the system.

It's also not uncommon to see confidential data being sent between parties via e-mail. This may be the message itself that contains confidential information or it may be attachments sent with the message. Both are bad business practices and expose your business to unnecessary risk and possible liability for breach of confidentiality agreements, privacy or regulations like the Health Insurance Portability and Accountability Act, which governs the privacy of health-related information. With increasing regulation of these types of issues, failing to properly secure this information will cost your company large amounts of money in fines and potentially massive amounts of money in the form of bad public relations, or worse.

When it comes to e-mail, encryption is becoming a common practice when dealing with confidential information that must be sent between parties. Whether it's information you may be exchanging with doctors offices or financial information flowing between companies, e-mail encryption is the way to secure the data so it is safe and only readable by the intended recipient.

Historically, encrypted e-mail has not been the simplest of technologies to work with. It has required both the sender and receiver are using the same software and having gone through a process of exchanging unique "keys" between them that allow the sender and receiver to securely communicate back and forth. With the need to make encryption more accessible to everyday business users, the technology has improved dramatically the last several years. It's no longer necessary for both parties to use the same software, though it does make the process simpler. When it's not, senders can still send secure e-mail and the recipient is able to retrieve it from a secure portal, much like you are able to log in to your bank Web site and securely manage your accounts. Some technologies allow this to be even more seamless, so you can read encrypted messages from others, even if you don't use their software. The bottom line is it's no longer acceptable to send confidential information via unsecured e-mail. Technology exists to do this safely and the costs and complexities are reasonable for even the smallest businesses.

Encryption technology also plays a large role in securing data on portable devices like notebook computers and USB keys. If it's not encrypted, the data on these devices is accessible to anyone who gains physical access to the drives. Imagine you lose your notebook computer containing sensitive financial data on your company, or documents with information about your products or services. A malicious person who finds the notebook can remove the hard drive and access your data. If the hard drive is encrypted, it is useless to whoever finds it, in or out of the original computer.

The same is true for USB keys. These incredibly convenient devices allow you to save massive amounts of data for easy transport between computers. They are very small and easy to misplace. Even if you password protect the USB key with the built in utilities that many come with, that can be defeated and the data retrieved. If your USB keys are encrypted, they are useless to anyone but you, as you set and know the secure passphrase that grants you access.

Like SSL certificates that secure Web sites like Amazon.com or your bank and make it safe for you to do business online, encryption technologies make it safe to save confidential data on portable computers and USB keys. Encryption technology makes it safe to transmit confidential data via e-mail. If you are not using encryption technology, I urge you to make a plan to do so as soon as possible. It will be one of the best things you can do for your business this year.

MJ Shoer is president and virtual chief technology officer of Jenaly Technology Group, a Portsmouth-based outsourced IT services firm. E-mail him at mshoer@jenaly.com.