Jan. 01, 2008

From the 2008 Tax Season Survival Guide

Every day, we transmit private information across public networks or store it in secure databases. Business communication that was previously done in person or in written form with signatures for identification is now conducted using the Internet and e-mail to transmit confidential information from one party to the next.

The difficulty encountered is the inability to trust the secure transmission or storage of the information. How do we know that something we send will only be read by the person whom we intended to read it? How do we know that our message
has not been intercepted and changed? How do I know that information I receive is unaltered during its transmission from the sender to me?

Encryption is a methodology to provide confidentiality and authentication. Also known as Cryptography, these technologies use cipher-coded text to transform information into code that cannot be decoded without a special key. Encryption uses an algorithm and a key to alter the plain text into coded or encrypted text. Subsequently, a key is used to decode or decrypt the coded message. In some cases, the data is encrypted and decrypted multiple times using different keys, such as Triple Data Encryption Standard (TDES) keys used in ATM machines.

Much like a password, the longer the key, the more difficult it is for someone to "guess" the key. Key lengths are described by their bit length, typically 56, 64 or 128 bits. Access and control over those keys is critical to maintaining the confidentiality of the information. If the key is not well

protected, the encryption methodology is weakened. Key generation, distribution,

not be reused between two different people because its security would be compromised
(someone else would know the key). Instead, the key would have to be provided from the sender to the recipient in some manner that would not subject it to interception. Hence, you couldn't transmit the key to the recipient via the Internet because someone else might intercept the key; the encryption would then be useless because of the possibility that someone other than the intended recipient would have the key and be able to access the information.

The key would have to be given to the recipient in a way you could authenticate that only that person was receiving the key, such as personally giving them the key. If you have to personally give them the key, you could just as easily personally give them the information, and the need for the encryption would be eliminated. However, symmetric keys are sometimes used when the exchange of the key is going to be very quick and temporary in nature. Data Encryption Standard (DES) keys are a common form of symmetric keys.

On the other hand, public key encryption uses two different or asymmetric keys. One key encrypts the information, and the other (asymmetric) key is used to decrypt the information. The two keys are mathematically created together. One of the keys — the public key — may be disclosed to anyone because it cannot be used to decrypt the information. Only the private key can be used to decrypt the information. The private key must be kept secure by the sender. For example, I want to receive information that is private from my colleague, Ben. I send Ben my public key. Ben encrypts the information using my public key and sends it to me. I then use my private key, that no one knows except me, and I decrypt the private information.

Encryption is used in many different ways in business. The chart below shows

the use of encryption methodologies.

Numerous products and resources are available to provide encryption technology. Certificate Authorities (CA) such as Verisign, are trusted entities that provide public key management for users. Popular products are available for key management,
such as Pretty Good Privacy (PGP). Before choosing a product or vendor, be sure to assess their key management process and reputation. The key is only as strong as the management and security of the key itself.
Understanding the basic concepts of encryption will enable you to appreciate the value of encryption and give you the tools to evaluate the need for encryption and the use of encryption by your clients.

———————————————-

Catherine Bruder is a Director with Doeren Mayhew in Troy, Mich. She is a former member of the AICPA's Information Technology Executive Committee. Contact Catherine at bruder@doeren.com.

Digital Currency • Technology