Secure Transmission of Sensitive Documents

By Jeffrey Streif, CPA, CFE, CISA, QSA

Are your sensitive documents that you send to your business partners secured in a way that they cannot be intercepted or viewed by unauthorized individuals? Years ago, businesses sent their sensitive documents by mail, fax or some third party courier. In today’s business environment, a high percentage of sensitive documents are sent electronically. Has your business looked at how these documents are exchanged and performed a risk analysis on your process of communication with your business partners?

There are numerous ways to send your sensitive documents and while some are secure there are others that are not so safe. Regular email and the old File Transfer Protocol (FTP) are not secure methods to transfer sensitive documents. There are numerous email programs that can be protected, but you need to understand the security methods they employ before you utilize them. Some of the most popular email programs provide some kind of security options, but they are not usually configured as a default.

There are many variations today of FTP such as: separate encryption, Secure Shell File Transfer Program (SFTP), FTP over Secure Shell (SSH), Internet Protocol Security (IPSEC), virtual private networks, and FTP over Transport Layer Security that can provide good security, but they also come with some issues. These issues can include clear text passwords, manual encryption, data integrity issues, platform compatibility issues and other conversion issues.

Risk of Transmitting or Exchanging Unsecured Sensitive Documents

The risk of sending unsecured sensitive documents includes, but is not limited to, the following:

- Document being intercepted during transmission;
- Unauthorized access to sensitive information;
- Failure to comply with laws and regulations, such as:
  - Payment Card Industry (PCI) compliance requirements — credit card data
  - HIPAA — personal health information
  - Gramm-Leach-Bliley Act — financial information protection
  - European Union Directive on Privacy and Electronic Communications — data protection and privacy
  - State privacy laws
  - Reputation risk due to breach of customer sensitive data; and
  - Financial risks — fines and penalties for noncompliance or breach.

While this list is not all inclusive, it highlights a significant number of reasons to review your process whereby you exchange sensitive documentation with your business partners.

Document Control and Digital Signatures

When you discuss the protection of sensitive documents, the following criteria come into play: confidentiality, authorization, accountability, integrity, authenticity and non-repudiation. The first three criteria deal with document control while the last four deal with digital signatures. Document control provides for making sure that the sensitive document is confidential with only authorized individuals having access to that document. It also provides for accountability with regard to the use of the sensitive document. This is done through some sort of tracking mechanism that communicates back with the original sender. Digital signatures verify that the document has not been altered and that it came from the person who actually sent it. It also provides for non-repudiation in that the sender cannot deny sending the document. Because this article is about providing for the secure transmission or exchange of sensitive documents, it will focus on document control and the related three criteria for achieving that security. Authentication will be discussed briefly as it pertains to confirming the identity of the business partner.

Confidentiality

The most common way to protect the confidentiality of sensitive documents during transmission is to use an encryption system. The most popular are symmetric keys, asymmetric keys and hybrid keys. Symmetric key cryptography uses the same key for both encryption and decryption. The security of that key is critical for this type of encryption to remain secure. Examples of this type of symmetric key system are AES, DES and 3DES.
Asymmetrical key cryptography, also known as public key cryptography, uses pairs of keys for encryption. The first key will encrypt the document, and the second key will decrypt the document. This is also true if the second key encrypts the document then the first key will be used to decrypt the document. The one key is referred to as the public key, which is distributed to business partners, and the private key is kept secure. Because you have the private key, only you can read the encrypted document. This solves the security problem that symmetric keys face. The problem with asymmetric keys is that they tend to be slower at equivalent strengths. Some common examples of asymmetric key systems are RSA and DSA.

Hybrid key cryptography utilizes both symmetric and asymmetric keys to secure the document. The asymmetric key is used to encrypt the symmetric key, which is used to encrypt the document. This method solves the issue of securing the symmetric key, and also solves the performance issue with using just asymmetric keys.

Authorization

Document control authorization protects the document by restricting what the user can do with or to the document. This is achieved by managing the document’s permissions and dynamic document controls. These permissions can restrict access rights, editing, printing and copying capabilities. Dynamic document control also can set expiration and revocation rights whereby the documents revoke those rights after being accessed a set number of times or when a specific date or time frame has passed. Adobe Acrobat is an example that allows you to configure these permissions and dynamic document controls relatively easily.

Accountability

Document accountability tracks document usage and communicates back with the original sender. It can verify that the recipient received and opened the document. Notifications can be sent back to the original sender that certain permissions have been used. This gives the sender critical information when time sensitive documents are involved.

Authentication

Authentication is critical as it confirms the identity of the business partner accessing the sensitive document. This is usually achieved by entering a username and password to open the document. This identity that was set up by the user is assigned certain permissions. It is important to know that password security is critical to keeping the sensitive document secure. Password configuration requirements should mirror what level of security is needed. There are also certain compliance requirements for password complexity that need to be met.

Client Portals

In addition to discussing ways to keep sensitive documents secure during transmission, you also need to consider the use of client portals as a means for exchanging information with your business partners. These portals are a common means to obtain documentation from your clients, and they provide for security of those documents. There are a lot of vendors who offer these services, so what should you look for when determining which vendor to choose? Think of the portal as being your new direct contact with your business partners. When you do this, you will realize that a cheap portal is not as attractive anymore. You want a portal that will reduce costs, increase employee productivity, allow your business partners 24/7 access and overall improve customer service.

When comparing portals, look for the differences in the following areas:

- Ease of use — minimal training necessary, pleasant and user-friendly interface, uploading and downloading features;
- Easy to configure and set up users;
- Access provides for security and is easy to manage; and
- Audit trail and notification capabilities.

These are just a few of the capabilities that client portals have today. Besides providing a secure method to exchange documents, more advanced portals now integrate with other software systems to increase efficiency and productivity. Certain tax software systems can now interface with portals to easily upload and download tax information from 1099s, K-1s and W-2s.

Conclusion

In conclusion, there are various ways and methods to provide security for documents when exchanging them with business partners. The key is to be aware of the methods that are used and the associated risks with those methods. Sensitive documents need to be protected, and the procedures used should take into account that need. Business procedures need to be reviewed and revised periodically to provide security for sensitive documents and to ensure that the security is aligned with compliance requirements. New technology used to exchange sensitive documents should be included in the risk assessment process before it is implemented.

Jeff Streif, CPA, is a principal with UHY Advisors in St. Louis. He chairs the MSCPA Information Management and Technology Assurance Committee and serves on the board of the St. Louis Chapter of ISACA. Jeff can be reached at jstreif@uhy-us.com.