

MT MORTGAGE TECHNOLOGY

Data Security in Today's Doc Delivery Landscape

By Art Tyszka, Senior Product Manager, Wolters Kluwer Financial Services



The advent of the Internet and e-mail have created new opportunities for financial institutions in recent decades. The process of moving information

and documents that once took days by printing paper documents can now occur in seconds, and it can be as simple as clicking "send" on an e-mail.

Because of the pervasive nature of e-mail and the Internet in today's world, it's almost becoming second nature to rely on this technology for the most efficient way to transfer information, but along with the convenience factor comes a new set of considerations financial institutions need to think about related to data security.

While Internet document transport services have helped lenders make great strides in terms of time and cost savings, financial institutions and technology providers need to take a second look at the issue of security. Between ever-increasing reports of data violations and identity theft, gaps in security measures have become the weakest link in many organizations. Not only could a data breach create severe financial and legal

implications for a financial institution, it also has the potential to cause irreparable damage to a company's reputation, particularly when the issue is played out in the media.

Numerous Internet delivery offerings have emerged across the landscape of the financial services industry. Promoted with similar promises of efficiency and profitability, these competing products have created a serious challenge for financial institutions attempting to determine the best tool for their business. Large companies, which spend vast amounts of resources on shipping documents overnight, have been quick to implement Internet delivery solutions to realize time and cost savings.

However, many financial institutions continue to rely on other methods. Nearly half of the financial institutions in a recent Wolters Kluwer Financial Services online poll responded that they continue to pay for overnight shipping of hard copies. Meanwhile, others, attracted by easy accessibility, utilize the unpredictable practice of e-mailing documents. The disadvantages of these methods are clear, both ultimately pose significant financial inefficiencies and even greater security risks.

That's why it's so important for financial institutions to carefully reevaluate their needs, assess available solutions and choose the best technology to avoid the costly damages of insufficient security, negative publicity, and a damaged reputa-

tion among customers and stakeholders. Clearly, the optimal Internet document transport system needs to deliver the absolute maximum in security measures, as well as time and cost saving benefits.

There are several key factors an institution should consider when choosing an Internet document delivery provider that meets their data security needs:

Usability

The common practice of using unprotected e-mail programs for exchanging critical documents demonstrates how immediacy and perceived simplicity is important when selecting an Internet document delivery system. Of course, standard e-mail is not a good option for sending documents containing confidential information. But there are secure Internet document delivery platforms available that mimic an e-mail program, making them particularly user-friendly and intuitive.

Locking Down Channels

As the industry with the highest risk of data security breaches, financial services must protect data from outside and inside threats equally. Such measures require implementing the strongest security methodologies available and performing ongoing surveillance and system updates as needed. In the scope of a financial institution's security strategy, redundancy is the key to realizing complete data lock-down. Secured channels present the first

layer of redundancy by preventing outside intruders from gaining access to sensitive data.

The security of a system's channels is the main line of defense against attack by a number of external threats. Securing all paths by which information can travel provides sensitive data with the greatest amount of protection and significantly minimizes the opportunity for breaches to occur by accident, design or malicious intent. Such channels include any portal designed into the system like routes to servers and pathways to heartbeat services, which provide mechanisms for monitoring the health and status of processes. Securing these gateways and monitoring access to them is a fundamental piece of a financial institution's defense system.

Limiting Access

Before establishing a single test account or exchanging even one file with an Internet document delivery system, companies must consider the overwhelming evidence of internally generated security breaches. By severely limiting access to non-public information across the organization, financial institutions stand to

reduce the risk of data leaks and the damage they deliver. Optimal access administration takes a variety of routes, from restricting organizational roles from the system to authenticating user identity and encrypting content. And your Internet document delivery system should be flexible enough to allow that.

Location

While securing packages with encryption technology is essential to preventing security breaches, it is equally important to know the whereabouts of document packages before, during and after transmission. Tracking features, reporting functionality and audit trails are not only excellent workflow management tools, they are also essential components of an overall security strategy. Given the likelihood of internally originated data breaches, it is crucial to put controls in place to deter potential leaks as well as detect and detail any suspicious activity.

Lasting Value

Business growth requires constant attention, as do ongoing procedural and technology refinements, as well as regulatory

and legal issues. These factors require great time and talent while necessitating tools that can adapt to changing times, and it's important to select a data security vendor that will be able to continue to adjust with you along with the times.

The return on investment a company can see by using an Internet document delivery service can be priceless. Not only do they save \$3 to \$5 per closed loan package in the cost of shipping hard copies of documents, but even more valuable is preserving the good relationship developed with customers and mitigating corporate reputational risk.

As data leaks continue to make headlines, Internet document transport services need to deliver the highest data security and performance capabilities possible. Added measures will increase the value of this offering, such as providing the intrinsic flexibility to cross technology platforms and bend with the needs of unique business models without breaking.

Art Tyszka is Senior Product Manager at Wolters Kluwer Financial Services. The Minneapolis-based company can be found on the Web at <http://www.wolterskluwerfs.com>.