Digital Documents, Compliance and the Cloud

A Perspective on Navigating the Complexities Associated with Digital Document Transmission and Security for the Modern Enterprise.

- What are Digital (Electronic) Documents
- The Rise of the e-document Definition
- Security Concerns Associated with e-documents
- The Spector of Compliance
- e-document Transmission Management
- Minimizing the Transmission Costs of e-documents
- Using the Cloud as a e-document Transmission Platform

Abstract:

This white paper illistrates the challenges associated with managing critical documents in the digital age, especially focusing on the prevelent best practices that add security to document portability, while enhancing accountability and reducing the transmission management and retention costs associated with e-documents.

Executive Summary:

Business Case:
Electronic (or digital) documents have become a staple of today's businesses. Simply put, a modern business cannot expect to function, unless it has a way to transmit and receive documents electronically. Those documents, whether they are faxes, email attachments, digitally shared, or processed in some other digital form, have become a critical component of business communication, creating both benefits and burdens for the majority of businesses.

Digital documents have also evolved to become a primary method of communications, creating a situation where everything from contracts to memos to proposals can now be considered data that is bound by compliance and other regulations that are designed to protect personal and corporate data. That places the management of digital documents squarely into the hands of those responsible for communicating those types of documents with both internal and external sources, and is also bound by corporate policy. The consequence of those responsibilities makes it critical to educate end users on the appropriate dissemination of information via approved technologies.

That has turned electronic document dissemination into a costly management burden that businesses can no longer afford to ignore. Knowing the who, what, when and where of electronic document transmission is now a critical element of e-document control that should be used to prevent policy violations, compliance violations and most importantly, assign accountability to the information transmitted or received. Unfortunately, those control methodologies often come at the cost of productivity, where those controls, rules and policies prevent staffers from sharing the information needed to accomplish projects or meet their daily work objectives.

Digital Documents, Compliance and the Cloud

Addressing those issues takes technologies that can balance the burdens of protection against the need for productivity, all without exposing critical information to unauthorized entities, while still maintaining affordability. In other words, the challenges associated with digital documents can be costly and almost impossible to address, unless management is willing to consider new ideologies, technologies or techniques to deal with the sharing and transmission of electronic documents.

Adding to those concerns is legality, in the form of compliance, where federal legislation has defined what information can be transmitted and how that data is secured. Compliance regulations, such as HIPPA, SOX, and PCI are designed to protect privacy, as well as financial information, from interception or receipt by unauthorized individuals. Businesses are finding that including something as simple as a social security number on a faxed document may violate compliance laws are hard pressed to find solutions that will counter compliance violations, without impacting productivity.

Naturally, the use of digital documents is on the rise as businesses seek to reduce the costs associated with physical documents. Research firm Gartner estimates that in the US, $25 to 35 billion dollars are spent each year filing, storing and retrieving paper. K2 research claims that it costs $25,000 to fill and $2,000 a year to maintain the average four drawer file cabinet, which holds 15-20,000 pages. With the exponential growth in digital documents to replace physical documents, one can only assume that more digital documents will be transmitted and received than ever before.

Key Recommendations:

- Implement electronic document transmission technologies that incorporate reporting, logging and tracking of digital documents as they are transmitted, which will also provide an audit trail, as well as the methods for verifying transmission and receipt.

- Ensure Reliable Document Capture: Use technologies that can transform paper documents into digital files that can be transmitted, as well as tagged and stored in an electronic document repository for quick and easy retrieval, retransmission and archiving.

- Secure Access to Sensitive Documents: Compliance dictates that some documents containing personally identifiable information have restricted access and secure sharing. Adopt a document transmission methodology that can incorporate authentication and password protection, allowing electronic documents to be only transmitted (or received) by those with the proper authorizations.

- Optimize Workflows: Improved business efficiency is one of the core benefits associated with technologies that enable the transmission of electronic documents. Cloud-based repositories can be used to organize electronic documents and even enable self-service delivery, where a recipient can request documents via a website and have those electronic documents faxed, emailed or delivered electronically using automation technology. Automated tasks and email notifications can help keep employees informed of requests and on track to follow up with other electronic documents.

- Consider alternatives: Investigate cloud services that incorporate document capture and transmission, allowing for a distributed methodology to work with electronic documents that must be secured, tracked and meet compliance regulations.

- Accountability: Do not forget to use management techniques that combine digital document transmission controls with policy based accountability to ensure that compliance and legal requirements are met, while enabling to ability to audit workflow and document movements.

Digital Documents, Compliance and the Cloud

The Cloud as a Document Platform:

One of the biggest challenges associated with managing electronic documents is offering equal access to the intended recipients while still incorporating security controls. For example, many businesses have turned to canned services that focus on file sharing for the delivery of electronic documents. However, those services often lack the ability to fax, email or otherwise transmit electronic documents in a secure and auditable fashion. What's more, file sharing services tend to be designed for long term relationships and are often ill-equipped to deal with isolated, or singular transmission events that are not part of long term business relationships. What's more, many of those file sharing services lack the ability to save electronic documents for the long-term and offer no transmission controls or management capabilities.

The limitations of file sharing services have forced enterprises to consider other options, including deploying their own internal fax servers, document servers or other transmission platforms. Nevertheless, those internally deployed document transmission systems often prove to be closed systems, and are ill equipped to deliver documents with external parties, especially those that may only have infrequent requests for electronic documents, such as forms, instructions, guides, or generic statements. What's more, internally deployed systems prove to be difficult to extend to external users, often introducing incompatibilities and creating user administration management overhead that can stress already burdened IT departments with frequent requests and security changes.

C level executives have come to realize that the burdens associated with internally deployed closed systems and file sharing services often outweigh the benefits realized. Those executives are now seeking affordable alternatives that offer cross platform compatibility, without compromising security or hindering productivity. Fortunately, the cloud offers a new platform ideology that levels the playing field and creates SaaS (software as a Service) offerings, which operate independently of internal systems, yet still offer the security and auditing capabilities needed by organizations that looking to securely transmit documents, yet still incorporates effective control of the information contained within those documents.

Cloud based solutions are able to accomplish those lofty goals by abstracting the management of digital documents from closed, internal systems and unifying access across a multitude of browsers, infrastructures and operation systems. That makes a cloud based service immune to the incompatibilities often encountered by extending closed internal systems across multiple domains to external users.

In other words, a cloud based service becomes the great equalizer between different platforms, users and applications. Furthermore, a properly executed cloud service incorporates security, encryption and auditing controls that can become the foundation of a digital document transmission system, allowing businesses to retire internal fax-servers.

Digital Documents and the Implications of Management and Storage

The best place to start with storage and management concerns is with the definition of what a digital (or electronic) document is. Unfortunately, the term "digital documents" encompasses a vast array of technologies and formats, ranging from PDFs to digital faxes to scanned paper documents. In other words, defining what a digital document exactly is depends upon the context of the business. For example, some businesses deliver catalogs, flyers and other marketing information either via a fax service, as email attachments, or as downloads – in essence, those are digital documents, however there is little need to secure those documents or track those documents, save for marketing purposes.

On the other hand, many businesses use digital (or electronic) documents to purvey information that falls either into the intellectual property realm, collaboration and project management ideologies, or even as contracts, agreements or other legally binding documents. Simply put, determining the level of management and storage needs comes down to what an organization considers to be an physical document that can be stored digitally – creating a situation where most anything can be considered a digital document, yet vast collections of printed materials may never become digital in nature.

It all comes down to intended use and how that use is impacted by compliance requirements or company policy. For most businesses, taking an all or nothing approach proves to be the simplest way to manage electronic documents, basically considering that any content that can be transmitted is indeed a digital document and must be managed. Or the converse, where nothing is managed and all documents (digital or otherwise) are considered fair game and are solely the responsibility of the document creators (or maintainers).

However, there are some distinctions that prove to complicate definitions – take for example spreadsheets or databases – in essence, those items are data files, which store information that can be manipulated for analytical purposes. Yet, those files can also be used to generate reports, embed data into documents or a whole other host of purposes that transform the information contained within into something resembling a digital document.

For businesses looking to protect proprietary information, those data files must be considered and the output available from those data files must become part of a secure system, that can offer encrypted transmission of electronic documents, while still providing an audit trail. Simply put, when it comes to digital documents, managing the transmission of those documents proves to be the key for controlling the information and keeping that information out of the hands of un-intended recipients.

In other words, if digital documents can only be transmitted via authorized services, such as managed email, fax services or other systems that prevent data leakage, then the origins of the data contained within become less of a concern and traditional security policies can be used to control access to the files, while the transmission of information can focus on the digital documents themselves. With the lines blurred between digital document definitions and what constitutes transmittable document content as well as what constitutes intellectual property, a new moniker has arisen for digital documents that are used for collaboration and transmission, e-documents.

Security of e-Documents

Security concerns have evolved with the introduction of e-documents as a subset of data files. One of the first concerns that come to mind is maintaining the portability of e-documents, while still securing those documents during transmission. With multiple e-document transmission capabilities available, the security policies and ideologies surrounding e-documents begins to fragment, with different security controls needed for e-Documents that are sent via a fax service from those sent via email attachments or via file sharing services.

Maintaining security means that the management of transmission services must be unified, so that the same policy rules and accountability requirements can be applied to e-documents, regardless of the transmission services used. Cloud services prove to be one of the better ways to achieve that management and bring order to the chaos of e-document transmission. However, adopting those methodologies usually results in a closed platform that makes it difficult to share e-documents and can impact productivity as well.

Success in securing e-Documents requires combining policies with open platform technologies, which leverage cloud services. Those services should provide:

- Encrypted transmission of e-documents
- Easily retrieved audit data and access logs
- Integrated faxing, email and e-document transmission capabilities
- Policy driven security controls to allow/deny transmission of e-documents
- Easy to use interface that works across multiple browsers and operating systems

Of course, security comes at a price – however that should not be at the expense of productivity, meaning that the end-user tools associated with a cloud based e-Document platform should be simple to use and work across multiple platforms and operating systems, enabling mobile users, on site users and even external partners to send and receive e-documents at will, without violating company policy or compliance requirements.

Compliance and other Legalities Impacting e-Documents

With e-documents quickly becoming a legitimate way for organizations to conduct business, the legalities of transactions associated with e-documents can no longer be ignored. In many cases, an e-document may be the only auditable element associated with a business communication. With that in mind, organizations have turned to platforms that support e-signatures and other legitimization technologies – all in a quest to lend credibility to e-documents and make them legal instruments. For many businesses, the legal viability of e-documents had become a credible concern and it only makes sense for those organizations to implement secure management of e-documents, which provide the tools to maintain the viability of what is now commonly becoming a legal instrument for conducting business.

The move to e-document ideologies actually offsets much of the burden of compliance by incorporating management and auditing into the document transmission process. Cloud based services can be configured to enforce compliance policy by detecting data that may violate compliance rules during transmission, preventing the subject e-documents from becoming a source of violation by terminating the transmission process before completion.

Call to Action: Solving the e-Document Problem

e-documents have introduced a plethora of concerns for today's businesses, where traditional transmission methodologies, such as manual faxing, basic email and free file sharing services have introduced security problems and have all but eliminated accountability. What's more, many businesses are dealing with e-documents using a mishmash of technologies that sap productivity and add unnecessary complexity to what should be a simple process, which in turn also limits the security of those e-Documents.

Cloud based e-document services can solve those problems and many others by centralizing e-document transmission controls and unifying the secure management of e-documents. Cloud based e-document transmission services provide:

- Security: e-documents can be encrypted and protected via policy based controls
- Accountability: Transmission and receipt of e-documents can be logged
- Auditing: Searchable history logs are available for auditing procedures
- Compliance: Policies can be created to implement compliance controls and detect violations
- Productivity: A user centric interface simplifies transmission and encourages collaboration
- Scale: Cloud based systems can scale from dozens of users to thousands with little effort
- Costs: Most cloud services use a flat rate methodology, where business only pay for the level of service needed
- ROI: Businesses no longer have to invest in hardware and software to enable e-document transmission
- TCO: Leveraging pay-as-you-go methodologies can reduce the Total Cost of Ownership (TCO)

With those benefits in mind, it becomes very clear that cloud based e-document delivery services have much to offer to businesses of any size and should become the default methodology for the majority of businesses looking to maximize the benefits of transmitting documents.

About the Author:

Frank J. Ohlhorst is an award winning technology analyst and author with over 25 years of experience in the technology arena. Frank has held senior editorial positions with several leading technology publications, including CRN, VarBusiness, eWeek and Channel Insider. As a freelance editor and analyst Frank authors reports, reviews, white papers and news articles for several publications, including GigaOM, eWeek, Enterprise Networking Planet, Tom's Hardware, Network Computing and TechRepublic.. Frank has also contributed to multiple technology books and has written several white papers, case studies, reviewers' guides and channel guides for leading technology vendors. Frank can be contacted via email at fohlhorst@gmail.com

About eFax Corporate®

eFax Corporate® provides industry leading Internet Fax Messaging solutions for global enterprises looking to streamline the exchange of business critical information and eliminate the costly infrastructure of in-house fax machines and servers. From single user implementations, to multiple users deployed across organizations and regions, to customized application faxing, our solutions help automate client business processes and workflow, delivering a strong return on investment. Benefits include enhanced employee productivity and improved relationships with customers and suppliers.

As the flagship brand of parent company j2 Global® (NASDAQ: JCOM), eFax Corporate spans over 49 countries, and six continents, offering document-intensive businesses a seamless and secure way to handle their most formidable communications traffic with ease. Visit us at efaxcorporate.com, or contact our enterprise sales team at 866-761-8111.