opentext™

WHITE PAPER

Security in fax: Minimizing breaches and compliance risks

Maintaining regulatory compliance is a major business issue facing organizations around the world. The need to secure, track, and store information for compliance purposes is critical because the risks of noncompliance are real. Now more than ever, there is pressure to closely manage fax communications and document processes. It's not surprising that organizations are turning to enterprise digital fax technology to support compliance requirements. This white paper addresses fax communications and the steps you can take to help keep your organization compliant.

opentext™

Contents

Introduction

Constantly evolving government regulations and standards are impacting how businesses around the world secure and manage information. Information is ubiquitous—whether paper-based or digital—and the requirements for effectively securing, maintaining, exchanging, and auditing information for compliance can be complex.

Simply stated, government regulations requiring organizations to conform to certain policies, specifications, standards, or laws are raising the stakes on fax security. Therefore, many organizations are turning to enterprise-grade, digital fax solutions to help address information exchange policies and procedures and to meet compliance requirements.

Fax security and corporate compliance

Compliance regulations abound

Regulatory compliance is a business fact of life, with new government regulations and standards introduced all the time. The impact of regulatory change is a global phenomenon as organizations are required to conform to new mandates taking effect in every region. Industries most affected include financial services (banks, non-bank mortgage lenders, loan brokers, financial or investment advisers, debt collectors, tax return preparers, insurance, and real estate settlement service providers), healthcare, legal, and government.

The landscape is one of constantly changing compliance requirements. Corporate ethics violations and scandals have resulted in tighter legislative regulations in the United States, such as Sarbanes-Oxley. Privacy concerns are addressed by the Health Insurance Portability and Accountability Act (HIPAA), as well as the Gramm-Leach-Bliley Act. European legislation has resulted in considerable regulations, including the Data Protection Act 1998 and the Freedom of Information Act 2000 enacted in the UK. Even private entities are instituting their own modes of compliance, such as the Payment Card Industry Security Council's Data Security Standard (PCI-DSS). These various regulations require businesses to constantly evaluate their security and privacy protocols and understand how those protocols could potentially expose them to compliance risk.

Fax, as a method of secure information exchange, continues to persist around the globe and across all industries. Faxing remains the most trusted form of securely exchanging information because the communication protocol itself is inherently secure, requiring peer-to-peer direct connectivity prior to transmission of data. Therefore, a document doesn't get transmitted unless the outbound fax transmission has a secure and direct connection with the receiving fax device. Since faxing is easier to use than other secure exchange technologies which require encryption keys, passwords, portal or other clunky methods of access, faxing is widely adopted.

As businesses strive to go paperless and drive toward digital transformation, it's imperative that their commonly used technology, including fax, transforms also. Eliminating the risk of paper-based faxing is an important step in security, compliance, and digital transformation. Digital fax technology enables paperless, secure information exchange.

Fax is widely used in a number of industries to protect content privacy, maintain compliance, and decrease the risk of a breach.

Healthcare

Fax remains the standard method of communicating protected health information (PHI) for healthcare organizations to maintain compliance with HIPAA. Patient information must be exchanged securely. Paper-based faxing with standalone fax machines puts a healthcare organization at risk if the device is not secured in a location accessed only by authorized individuals.

Digital faxing eliminates the risk of paper-based faxing with standalone fax machines and the unintentional exposure of PHI. Digital fax solutions exchange content electronically and deliver the content directly to its intended recipient. Recipients most commonly access the content at their computer, within an application or secured network folder. This helps eliminate the risk of unintentional exposure and keeps content private to only those with access.

Digital fax solutions also typically integrate with electronic medical records (EMRs), making it easy to upload or deliver PHI from the application. This eases the burden of manually shuffling paper documents, scanning, and processing paperwork. Digital fax also helps minimize the risk of lost or misplaced fax content.

Finance

Financial services organizations depend on fax to support several business processes, which are highly regulated and require secure and trusted forms of communication. Financial institutions use fax to comply with regulations such as Sarbanes-Oxley and Gramm-Leach-Bliley. With transaction transparency, irrefutable audit trails, and the ability to transmit original signatures, banks, lenders, and creditors use fax to process credit applications, trade confirmations, claim forms, and collection notices.

Communications are often time-sensitive for both the financial institution and the customer. Financial agencies leverage digital fax technology to provide secure information exchange, along with the means to increase communication speed, improve cycle times, reduce costs, and improve customer satisfaction.

Government

Government agencies tend to be highly risk-averse, and faxing remains the communication method that keeps content secure and decreases the risk of interception and hacking. However, with the known inefficiencies of paper-based faxing with standalone fax machines, there is an opportunity for these agencies to implement a digital fax solution that meets strict security requirements while improving information exchange. Government agencies should seek digital fax solutions that are Joint Interoperability Test Command (JITC) certified to implement within their organization.

Legal

Legal firms throughout the world use fax daily to send and receive confidential documents with clients, attorneys, and the courts. The legal industry—both law firms and in-house counsel—need a cost-effective and secure way to deploy fax communications and increase the efficiency and productivity of their staff.

Document retention and retrieval for effective e-discovery is also a challenge with traditional faxing methods. With digital fax, law firms have full visibility of fax content, as well as who sent it and when, and who received it and when—and even who viewed it and when. A complete audit trail is perhaps most important and has proven most effective in legal scenarios when proof of delivery and receipt of content can be established and proven. In addition to proper authentication, firms can easily build fax into document management strategies for the timely retrieval of information needed in e-discovery and auditing

Actively addressing fax security

Because of compliance risks, enterprises heavily reliant upon fax must take initiative and remain steadfast when investigating the privacy and security of their transmitted and archived fax data. Faxes typically contain highly sensitive information about business transactions and decisions. Management therefore needs to actively promote programs for ongoing risk assessment to make sure that procedures and product standards to keep their fax data secure are being addressed.

To determine if your organization is on the right track, start by answering these questions:

- Do you have control over the security of your incoming faxes?
- Do you know exactly where your fax documents are being delivered—and to whom?
- Are there safeguards in place to prevent unauthorized people from accessing your fax data?
- Are faxes actually being received by the right people?
- Are you sure that confidential faxes are kept private?
- Do you have an audit trail for your fax documents?
- Do you have secure storage for your fax documents?
- Do you know the rules regarding when fax document destruction is authorized?
- Do you know the rules regarding how employees exchange confidential fax documents?

With these answers, you can start building a security strategy to effectively address compliance risks.

Risks of non-compliance

Requirements to protect and control the flow of information throughout an organization— including sensitive information transmitted by a company's vendors—are built into most regulations. In the US, there are laws and regulations that can have civil or criminal penalties attached. Some regulations hold not only the corporation but individuals within the corporation—such as the CEO or CFO—personally responsible for compliance violations. There are other regulations that impose serious ramifications even if a security breach is only suspected.

Consequences range from fines levied to forensic investigations, criminal prosecution, or even jail time depending on the severity of the violations. For example, Sarbanes Oxley violations can result in a fine of up to $1 million and a jail term of up to ten years for any corporate officer who doesn't adhere to the rules, even if inadvertently. For PCI-DSS compliance, card issuers, merchants, and service providers transmitting credit card data are also eligible for fines as high as $1 million. Needless to say, the fallout of compliance violations can affect the health of an organization in a variety of ways, including loss of the company's good reputation and market leadership.

Security and compliance challenges

To comply with regulations, you must be able to provide documented proof that your organization is addressing its security and privacy in a way that complies with the standards that govern your business. The implementation process can be challenging to say the least. To minimize risk, your organization must look at how to implement the following:

- Automating the document delivery processes
- Centralizing information delivery and receipt
- Safeguarding document confidentiality
- Protecting information from tampering/alteration/unauthorized access—both at rest and in-transit
- Limiting information access
- Tracking and monitoring access—who and when
- Providing secure storage, historical data, and managing document destruction

Given the impact that these measures can have on compliance violations, it’s no surprise that concerns around securing fax transmissions remain a strong point of emphasis for enterprises.

Developing a strategy

Developing a strategy to support compliance initiatives is a logical first step, and it starts with engaging your IT team to establish security and privacy guidelines for the top five IT compliance issues:

Process control: Examine the controls you need in place to make sure the document information is verifiably received by the right people. Controls around both the information itself and those in the process who are accessing it the most are part of a solid security plan for supporting compliance.

Information integrity: Business documents that are uncontrolled are potential security threats and can put your business at risk. A few examples include accounting documents, contracts, nondisclosure agreements, stock trade confirmations, and documents with payment card information.

Privacy: A cornerstone of many regulatory requirements is protecting the confidentiality of information, so it is vital that information is kept private; controlling who has access and when they have it is also essential in this case.

Tracking, reporting, and audit trail: Regulations dictate that businesses physically protect information, and provide a history of what has happened to the information and who has had access to it.

Document archiving: Because of its impact on long-term retention and legal discovery, archiving is an issue most organizations face. Thus, providing secure and long-term document storage is a priority for any strategy.

Using fax to ensure data privacy

Security

Fax software and services provide the most widely used form of secure information exchange. This is due to the inherent, enhanced security of eliminating existing nonsecure standalone fax machines and providing a centralized document delivery and storage hub. Some fax solutions offer an extra layer of protection with encrypted delivery options. These features help diminish the risk of confidential information falling into the wrong hands. Documents are delivered to intended recipients in tamper-resistant formats, protected from corruption, allowing you to take advantage of your network's established security system.

Legally binding

In most cases, signatures on documents received by fax are legally binding. Many countries, including the US, the EU, and Australia, have determined that faxed signatures (when recognized under the law of each jurisdiction) have the same legal consequences as the more traditional forms of executing documents.

Solutions for supporting security issues

Centralized delivery: Fax solutions can act as a centralized document delivery hub. Each step of the document delivery process is managed electronically, with routing rules that control how and where faxes are sent and received. Information can be exchanged electronically, in real time, directly from your applications without manual intervention.

Integration: For organizations that already use a document management system or database for long-term document storage, digital fax solutions can integrate with other systems to meet electronic document retention requirements. Solutions readily integrate with Customer Relationship Management (CRM), document management, email, and Enterprise Resource Planning (ERP) systems.

Tamper-resistant: With an enterprise fax solution, documents are received directly in end users' email inboxes, so they aren't sitting out in the open. When a fax arrives to the inbox, the document is tamper resistant—it cannot be edited without the event appearing in the audit trail.

Backup: Backup is intended to preserve data in the event of a disaster or other hardware or software problems; the idea is that data can be restored once the problem is resolved.

Security and management: Electronic fax solutions can create a trusted, digital archive where you can securely store any document type and then find it quickly. With fax, archiving is for retention and legal discovery. Encryption technology should be used to secure content stored in repositories.

Audit trail: With a variety of configurable, automatic tracking features to satisfy audit trail requirements, fax solutions guarantee that the details of every fax transaction will automatically be recorded, stored, organized, and available for auditing purposes.

Track history: An enterprise fax solution can track fax history, provide verification of fax delivery, assign access passwords, route incoming faxes to individuals' email inboxes, and be the on-ramp to automated workflows, providing a deeper audit trail for protected documents to help satisfy tracking and reporting requirements.

Electronic fax repository: Fax solutions allow organizations to manage business-critical documents from beginning to end. Fax solutions meet the challenge of controlling and managing information created from disparate sources by accepting and combining content, organizing it, distributing it via workflow, storing it, and providing secure access to it when and where users need.

Fax solutions for supporting compliance

A fax solution not only accelerates business processes in a cost-effective manner, but also allows you to gain control of document transmission in a way that supports your security and compliance objectives. The result is a secure, highly available, reliable solution that directly aligns with your organization's compliance goals.

OpenText is the global leader in enterprise fax, replacing fax machines and their associated expenses with a software or cloud-based digital fax solution. OpenText fax solutions empower fax users to send documents from desktop and email applications—increasing productivity, and thereby saving your organization money. Integrate OpenText fax solutions with your computing environment to establish fax implementations that securely track all faxes, both inbound and outbound, with an audit trail and archive copy of each faxed message.

OpenText™ Fax2Mail™

OpenText Fax2Mail is a leading provider of secure cloud fax services for large organizations that utilize fax as an essential part of their communications with customers, business partners, and vendors. Fax2Mail offers a turnkey cloud fax solution that eliminates the cost and inefficiencies of fax server hardware and software management, while providing enhanced levels of scalability, security, and redundancy. With built-in encryption technology, Fax2Mail protects your content in motion and at rest—at all times.

OpenText™ RightFax™

OpenText RightFax is a scalable fax server solution available in on-premises, hybrid, and managed services deployments. RightFax integrates with the industry applications that drive your business processes to maximize productivity, reduce risk, and decrease costs. RightFax provides comprehensive enterprise information exchange capabilities, shortening business cycles and increasing speed to revenue for companies of any size. RightFax is JITC certified, provides extra layers of protection with the RightFax Encryption Module, and has archiving tools for the secure, long-term storage of faxed documents.

OpenText™ XM Fax™

OpenText XM Fax is an enterprise-grade digital fax solution built to handle large fax volumes for small and medium business. Deployable on-premises, in the cloud or as a hybrid solution, XM Fax can be tailored to meet the needs of SMBs, departments and branch offices. The best-in-class fax solution for SMBs integrates with and streamlines workflows across the entire organization.

Digital fax blog

Fax2Mail demo

RightFax demo

XM Fax explainer video

Conclusion

Maintaining regulatory compliance will remain a business issue for the global enterprise. There are serious ramifications associated with non-compliance from both a financial and organizational reputation perspective. Therefore, organizations must develop well-crafted strategies that focus on securing and tracking the exchange of information. OpenText enterprise fax software and cloud-based provide fax transmission capabilities that drive data security and reduce compliance risks. As new regulations continue to arise, investigating information exchange policies and procedures is a business-critical step, and fax's ability to support security and compliance can't be overlooked.

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn