

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 very real. For years businesses have relied on fax communications in day-to-day operations. Now there is more pressure to closely manage fax communications and document processes. It's not surprising that organizations are turning to enterprise fax technology to address compliance requirements. This white paper addresses the area of fax communications and the steps you can take to help keep your organization compliant.

Table of Contents

Introduction.....3

Fax Security and Corporate Compliance.....3

 Compliance Regulations Abound.....3

Actively Addressing Fax Security4

 Risks of non-compliance.....4

 Security and compliance challenges.....4

Developing a Strategy.....5

Using Fax to Ensure Data Privacy.....5

 Security issues5

 Legal issues.....5

 Solutions for supporting security issues.....5

Fax Solutions for Supporting Compliance.....6

 OpenText Fax2Mail Services.....6

 OpenText RightFax.....6

 OpenText RightFax Express.....6

Conclusion7

About OpenText7

Introduction

Constantly evolving government regulations and standards are impacting how businesses around the world secure and manage their information. Information is ubiquitous—whether paper-based or electronic—and the requirements for effectively securing, maintaining, 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 when it comes to fax security. Therefore many organizations are turning to enterprise fax solutions to help address the information exchange policies and procedures necessary for determining optimal means for protecting confidential data in order 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 being 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. In Europe legislation has resulted in considerable regulation 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 are requiring businesses to constantly evaluate their security and privacy protocols with an understanding of how those protocols could potentially expose them to compliance risk.

In most organizations, paper documents, faxes, email, and other office correspondence are typically stored in file cabinets, employee desk drawers, on desktop PCs, file servers, or archived in file boxes located offsite. As businesses strive to go paperless, it is challenging to assert and maintain control over this existing information. This means that whatever security and privacy processes you have in place may need regular modification.

Actively Addressing Fax Security

Because of compliance risks, enterprises heavily reliant upon fax must take the 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 actively needs to promote programs for on-going risk assessment to make sure that procedures and product standards needed to keep their fax data secure are being addressed.

In order to determine if your organization is on the right track, start by asking 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?

Once you've answered these questions, you have a baseline with which to start building a security strategy to effectively address compliance risks.

Risks of non-compliance

Built into most regulations are requirements to protect and control the flow of information throughout an organization, including sensitive information transmitted by a company's vendors. 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 where even if a security breach is only suspected, there are serious ramifications.

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 follow 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 today's 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 to have 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, 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 issues

Fax software and services enhance security by eliminating existing non-secure stand-alone fax machines while 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.

Legal issues

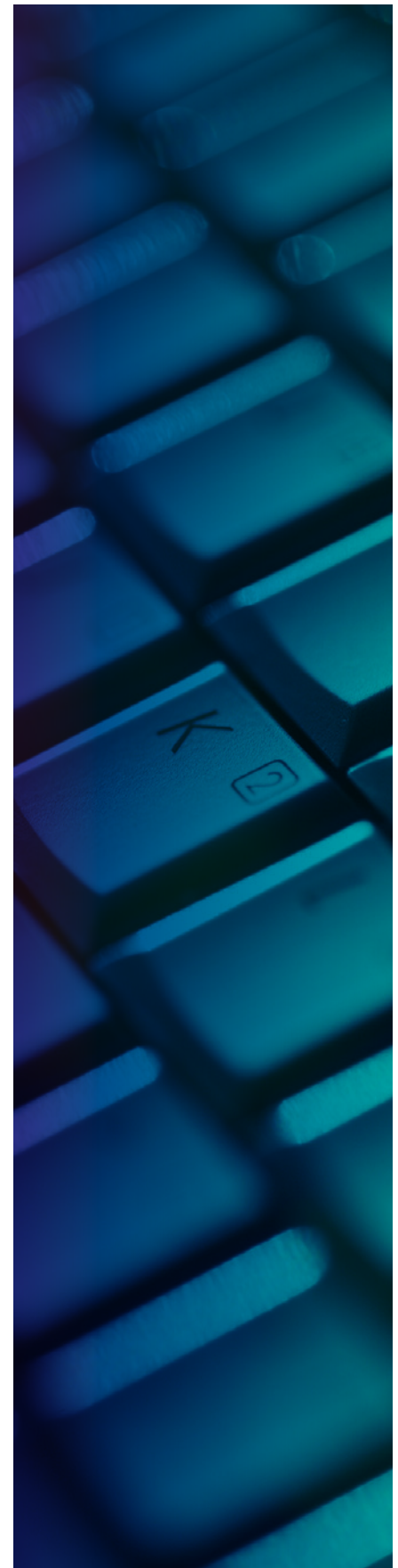
In most cases, signatures on documents received by fax are legally binding. Many countries including the US, the EU, and Australia have determined that faxed signatures (when recognized under the law of each jurisdiction) have the same legal consequences as the more traditional forms of executing documents.

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, 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 in your 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: 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.

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 it.

Fax Solutions for Supporting Compliance

A fax solution can not only accelerate 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 organizations' compliance goals.

OpenText is the global leader in enterprise fax, replacing fax machines and their associated expenses with a software-based solution; save money through increased employee productivity because of the ability of OpenText to empower fax users to send documents from desktop and email applications. OpenText fax solutions integrate 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 Services

OpenText Fax2Mail is a leading provider of fax Software-as-a-Service (SaaS) for large organizations that utilize fax as an essential part of their communications with customers, business partners and vendors. Fax2Mail offers a suite of outsourced fax solutions that eliminates the cost and support inefficiencies of fax server hardware and software management, while providing enhanced levels of scalability, security and redundancy.

OpenText RightFax

RightFax is a scalable networked fax solution that integrates with the industry applications which drive your business processes to maximizing productivity, reduce risk and decrease costs. OpenText RightFax provides comprehensive enterprise information exchange capabilities, shortening business cycles and increasing speed to revenue for companies of any size.

OpenText RightFax Express

RightFax Express provides a simple to deploy, all-in-one fax solution that is perfect for SMBs and departments to empower employees to easily fax from their desktop, email, back-end applications and MFP devices.

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 information exchange strategies that focus on securing and tracking the exchange of information. Enterprise fax software and solutions provides fax transmission capabilities featuring support for policies and procedures that drive data security and reduce compliance risks. As new regulations continue to arise, investigating information exchange policies and procedures that emphasize fax's ability to support security and compliance is a business-critical step that's can't be overlooked.

About OpenText

OpenText is the leader in Enterprise Information Management (EIM). EIM enables organizations to grow the business, lower costs of operations, and reduce information governance and security-related risks. OpenText focuses on the key drivers of business success to improve business insight, strengthen business impact, accelerate process velocity, address information governance and provide security.

OpenText Information Exchange solutions help organizations integrate and extend their information exchange systems and processes in order to improve their efficiency, decrease security risk and lower their transaction cost for internal and external information exchange.

faxsolutions.opentext.com

**NORTH AMERICA +1 800 304 2727 • EUROPE +31 (0)23 565 2333 • AFRICA, MIDDLE EAST +971 4 390 0281
JAPAN +81-3-5472-5273 • CHINA +86 21 28909063 • HONG KONG +852 2824 8223 • AUSTRALIA +61 2 9026 3480**