opentext™

Security in fax: Minimizing breaches and compliance risks

opentext™

Contents

opentext™

Introduction

Government regulations requiring organizations to conform to certain policies, specifications, standards, or laws are raising the stakes on fax security. As a result, 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

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, Healthcare, Legal, and Government.

Compliance requirements are constantly changing. 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 and adjust their security and privacy protocols, understanding they could potentially be exposed to compliance risk.

Because the fax communication protocol is inherently secure, requiring peer-to-peer direct connectivity prior to transmission of data, faxing remains the most trusted form of secure information exchange. Since faxing is easier to use than other secure exchange technologies that require encryption keys, passwords, portals, or other clunky methods of access, faxing is widely adopted. It remains the communications standard for a variety of industries to protect privacy, maintain compliance, and decrease breach risks.

As businesses strive to go paperless, it's imperative that their commonly used technology, including fax, also transforms. Eliminating the risks through digital fax technology is an important step to achieving security, compliance, and digital transformation.

Healthcare

Fax remains the standard method of communicating protected health information (PHI) for healthcare organizations to maintain compliance with HIPAA. However, paper-based faxing with standalone fax machines or MFPs can be a breach risk if the device is not secured in a location accessed only by authorized individuals.

Digital fax solutions exchange content electronically and deliver it directly to its intended recipient. Recipients most commonly access the content at their computer, within an application or secured network folder. This helps keep content private to only authorized users.

Digital fax solutions also typically integrate with electronic medical records (EMRs), making it easy to upload or deliver PHI from within 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 business processes requiring 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.

Through digital fax technology, financial organizations provide secure information exchange with increased communication speed, improved cycle times, reduced costs, and improved customer satisfaction.

Government

Government agencies tend to be highly risk averse and rely on faxing to decrease the risk of interception and hacking. However, 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 to implement digital fax solutions that are Joint Interoperability Test Command (JITC) certified.

Legal

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

A complete audit trail is perhaps the most important communications feature in the legal industry and has proven most effective when proof of delivery and receipt of content can be established and proven. With digital fax, law firms have full visibility of fax content, as well as who sent it and when, who received it and when—and even who viewed it and when. Through integrations, organizations can easily build fax into document management strategies for the timely retrieval needed in e-discovery and auditing.

Addressing fax security

Enterprises heavily reliant upon fax must take initiative and remain steadfast when investigating the privacy and security of their transmitted and archived fax data. Management needs to promote programs for ongoing risk assessment to make sure that security procedures and product standards 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 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?

opentext™

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, civil or criminal penalties can be attached.

Some regulations hold not only the corporation but individuals within the corporation—such as the CEO or CFO—personally responsible for compliance violations. Other regulations 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 10 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.

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

An organization must be able to provide documented proof that it is addressing security and privacy in a way that complies with the standards that govern its business. To minimize risk, an organization must look at how to:

- Automate document delivery processes
- Centralize information delivery and receipt
- Safeguard document confidentiality
- Protect information from tampering/alteration/unauthorized access—both at rest and in-transit
- Limit information access
- Track and monitor access—who and when
- Provide secure storage and historical data as well as manage document destruction

Given the impact that these measures can have on compliance violations, it's no surprise that securing fax transmissions remains 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:

1. **Process control**
   Examine controls in place to make sure the document information is verifiably received by the right people.

2. **Information integrity**
   Business documents that are uncontrolled are potential security threats.
3. **Privacy**
   A cornerstone of many regulatory requirements is protecting confidentiality, so it is vital that information is kept private. Controlling who has access and when is essential.
4. **Tracking, reporting, and audit trails**
   Regulations dictate that businesses physically protect information and provide a history of what has happened to it.
5. **Document archiving**
   Because of its impact on long-term retention and legal discovery, secure archiving is an issue most organizations face.

Using fax to ensure data privacy

Digital fax allows for eliminating non-secure standalone fax machines in favor of direct, digital delivery, allowing you to take advantage of your network's established security system. Some solutions offer an extra layer of protection with integrated encryption.

Here are the ways the right enterprise digital fax solution can promote data privacy improvements:

Centralized delivery
Fax solutions can act as a centralized document delivery hub. Each step 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, EMR, 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.

Backups, 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 in the event of retention or legal discovery events. Encryption should be used to secure repositories.

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

Electronic fax repository
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 when and where users need it.

opentext™

- OpenText Cloud Fax Services
- OpenText Digital Fax Solutions
- Blog: Why now is the time to a modern fax solution

Fax solutions for supporting compliance

OpenText is the global leader in enterprise fax, replacing fax machines and their associated expenses with a secure, compliant software or cloud-based digital fax solution. Our digital and cloud fax solutions provide simple, cost-effective, tailored, and secure alternatives that power modern business and integrate seamlessly into existing workflows and processes.

With digital fax solutions you can:

- **Accelerate operations**
  Automate processes and integrate with key enterprise applications to increase productivity and shorten business cycles.
- **Access crucial information**
  Gain access to business-critical information and deliver it in a structured format to and from any location.
- **Increase security and compliance**
  Leverage cloud or hybrid IT environments for secure, auditable information exchange and compliance with HIPAA and PCI DSS configurations.
- **Improve satisfaction and experience**
  Create custom, cloud-enabled workflows to increase transaction speed with consistent, reliable, and secure digital fax communications.
- **Unlock analytics and insights**
  View historical fax data, including volumes, deliveries, and exceptions, to gain full visibility and discover actionable insights.
- **Unify fax data and information**
  Automatically extract text and metadata from fax-delivered documents to support organization-wide information capture and intelligent document processing.

Conclusion

Maintaining regulatory compliance will remain a business issue for the global enterprise. 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.

Organizations must develop well-crafted strategies that focus on securing and tracking the exchange of information. OpenText enterprise fax software and cloud services drive data security and reduce compliance risks.

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
- X (formerly Twitter) | LinkedIn

opentext.com/contact