eFax Corporate®

White Paper

How eFax Corporate Lowers Costs and Strengthens Data Security

eFax Corporate®

White Paper

How eFax Corporate Lowers Costs and Strengthens Data Security

TABLE OF CONTENTS

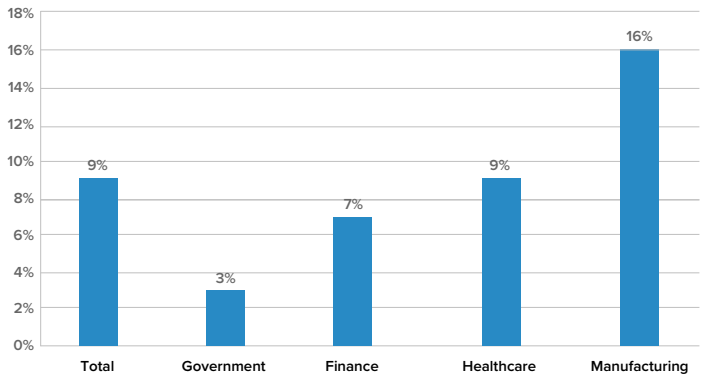
Myth Buster: Business Fax is Growing, Not Slowing

It's a common assumption: Fax is a waning technology supplanted by email and other cutting-edge business communication tools. It's going the way of the buggy whip so why invest in it further?

That may be true for the individual consumer, who rarely needs to fax except when applying for a loan or submitting a medical insurance expense claim, but if as an IT security professional you have ever been tempted to let your business fax infrastructure fade into cost-saving obsolescence, it's time to think again.

The latest research from the International Data Corporation (IDC) shows that fax usage in key industries is *going up*, not down. In a recently released paper titled "Fax Market Pulse: Trends, Growth, and Opportunities," IDC reported that 82% of survey respondents said that fax usage increased over the past year by an average of 9%, as shown in the chart below.

IDC - 2017 Net Fax Usage Growth



One reason for the surprising staying power of fax, long after the advent of email, is that even now most email is not as secure as it needs to be to transmit sensitive data such as personally identifiable information (PII). And the cost and hassle of making email more secure have thus far proved prohibitive (contributing to the explosion in recent years of email hacking incidents).

According to the FBI's "2017 Internet Crime Report," business email compromise (BEC) and email account compromise (EAC) are on the rise, outpacing even ransomware. With an estimated 85% of cybercrime victims failing to report fraud, the figure is likely even larger.

On the whole, the **Identity Theft Resource Center** (ITRC) identifies poor security, hacked IT systems, inside jobs, lost or stolen hardware and media, and employee negligence as data-breach sources capable of costing an organization millions or putting it out of business altogether.

Last year alone they estimated that over 179 million records were exposed because of data breaches, with the average cost per breach reaching $7.3 million, an all-time high.

Similarly, the *"Verizon 2018 Data Breach Report"* reveals such attacks having doubled from 2017 to 2018, resulting in a substantial rise in ransomware.

So fax, lo and behold, is still here, and still perceived as more secure than email for transmitting sensitive data, if only because it's a terribly inefficient means of transmitting malware for a ransomware attack. Certainly it's no coincidence that 75% of all medical information is currently being transmitted by fax.

Perhaps the principal reason for the enduring utility of fax, though, is that regulated industries such as healthcare, finance, government, and legal are required to meet increasingly tight security regulations to protect their confidential data, and fax offers the most efficient and regulatory friendly means to do so. Under HIPAA, for example, traditional fax machines are exempted from certain aspects of the Security Rule because it is assumed that the transmission will travel over the public telephone network and not the Internet.

The Consequences of Poor Fax Security

The objective of this paper is to explore the fax security benefits and vulnerabilities faced by businesses, the costly nature of addressing them, and how other companies have overcome these challenges while strengthening overall fax security.

The reality is that organizations have never been more vulnerable to data theft and the way it can quickly translate to loss of revenue and reputation, and even regulatory fines. With fax being relied upon more than ever, overlooking it as a potential security risk is to invite disaster.

Most security breaches result from poor email or password security, but poor fax protocols also leave an organization vulnerable. IT managers should realize they can't afford to transmit and store faxes without adequate security, including physical and role-based access controls.

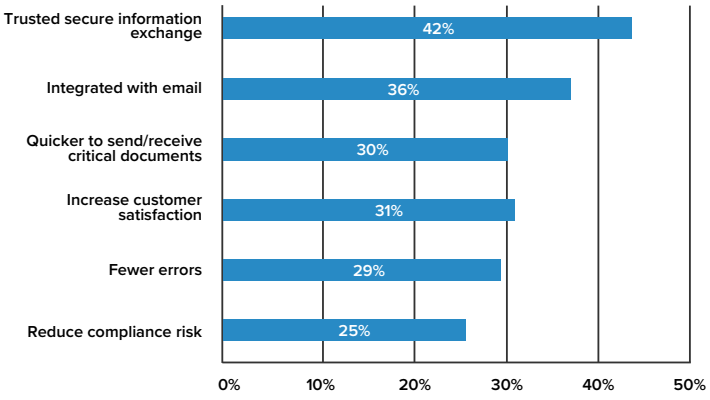
Of course, not all breaches are avoidable. But weaknesses related to lax security and compliance are addressable and cannot be tolerated. The question then becomes which vulnerability is more critical, security or compliance?

Security and Compliance Go Hand in Hand

Security and compliance are so interrelated that a deficiency in one often leaves a business weaker in the other, and vulnerable to any of the threats specified by the ITRC.

Research shows that fax continues to be accepted as a trusted and secure means of exchanging information, and, if done correctly, can reduce the risk of noncompliance. In fact, the right cloud fax security protection will not only leave customer data better protected, but also ensure that relevant compliance obligations are met.

IDC - Top Fax Benefits · Security & Email Integration



However, if your business still supports aging in-house hardware such as fax machines, fax-enabled multifunction printers (MFPs), or even on-site fax servers, the inherent insecurity of these devices could mean that your business may already be in violation of relevant data-privacy laws, including HIPAA, GLBA, SOX, FERPA, as well as payment-card industry standards such as PCI-DSS.

Following are multiple snapshots of what a fax security and/or compliance disaster-in-the-making might look like:

- **Paper faxes containing personal customer data are left out in a public area.** No matter how secure your transmissions are, faxes containing PII, or personal healthcare information (PHI), that are left unattended on a fax machine violate privacy and chain-of-custody requirements mandated by federal privacy laws.
- **Your retention process for fax records falls short of compliance.** Privacy laws for records containing PII typically require that records be maintained for a certain number of years, be stored securely at all times, and be accessible to regulators on demand.
- **Hard drives and nonvolatile memory for fax machines and MFPs contain fax transmission data.** This could be meta-data or actual document images – either way, this represents a commonly overlooked security weakness made riskier because securing all of these devices and bringing them into compliance is laborious, time-consuming, and expensive.
- **When an enterprise fax server's hard drive or storage module reaches capacity,** standard operating procedure is for an administrator to purge the contents. This often means printing out the fax records for filing, which can create security gaps similar to those of a desktop fax machine, where documents run the risk of being misplaced or viewed by unauthorized personnel.
- **Many fax servers do not encrypt their hard drive's data** effectively, using old, nearly out of date algorithms, creating another security risk for the company. This can be particularly concerning if the fax server is connected to the organization's network and the network is hacked.
- **These vulnerabilities can be further trouble** for any company that handles the sort of PII/PHI falling under the protection of data-privacy laws, such as healthcare organizations regulated by HIPAA, or financial institutions overseen by GLBA.

It's in light of vulnerabilities and challenges like these that the promise of cloud-based faxing comes more sharply into focus.

Cloud Fax Fills the Gap

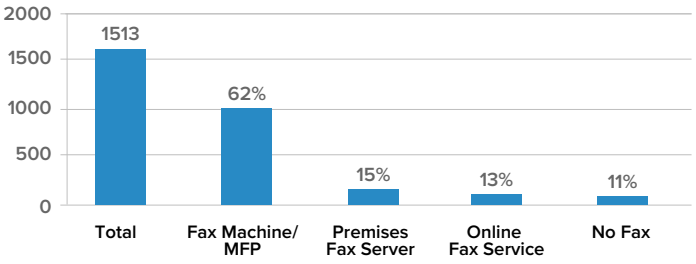
As we have seen, stand-alone machines and in-house fax servers can leave conspicuous security and compliance gaps if not properly managed. The cost and effort required to bridge these gaps begs the question: is there a less expensive, more secure way to maintain the integrity of corporate fax?

The answer of course is yes. Unfortunately, too many companies continue to rely on fax technology that dates to the previous century.

Spiceworks, which claims a membership of over 500,000 information technology professionals, polled their users on the subject of fax. According to the 2017 Spiceworks poll, approximately 89% of small to medium-size organizations still use fax in some form, and 62% of IT pros still support physical fax machines or MFPs with fax capability.

The same survey revealed that only around 26% are using some form of modern electronic faxing, including on-premises fax servers or the more advanced, cloud-based on-line fax services.

2017 Spiceworks Survey · Fax Usage By Type



One of the greatest benefits of cloud faxing, beyond the known advantages of increased cost savings, productivity, and reliability, is that the right provider can also significantly improve security by plugging the gaps left by legacy systems to protect your data and keep you on the right side of the regulations.

For these reasons, now is a good time to retire those antiquated and and insecure fax systems and move to the next generation of secure, streamlined and cost-effective faxing.

Cloud Fax Explained

Cloud faxing is simply the latest term for a more advanced method of faxing once known as “online faxing,” “Internet faxing,” or “virtual faxing.” It gained traction in the early 2010s following the explosive use of the term “cloud” as a metaphor for hosted virtual servers accessed via the Internet that store, manage, and process data in place of local devices, servers, and software that are purchased, installed, managed, and maintained by IT staff on the customer premises.

The enduring advantage of fax over rival means of business communication has always been the secure nature of a dedicated point-to-point connection – one sender, one receiver, no middleman gaining access to data in transit. The unporous nature of fax explains its durability, particularly in an age of malware and rampant data breaches.

The advent of cloud-based systems to manage the transmission and storage of faxes has brought to faxing all the great security advantages of traditional fax but with none of the disadvantages. There is no longer any need for sender or receiver to each possess a fax machine, for instance, or for businesses to spend money on fax printing supplies and upkeep.

All that’s required is a web-enabled device with Internet access to send or receive faxes, and a fax-capable device or service on the other end to receive the fax transmission.

Along with the increased speed and convenience come the meat-and-potatoes advantages inherent to cloud faxing: tighter security, built-in redundancy, and improved compliance in the form of powerful data encryption and access controls that frustrate hackers and satisfy regulators.

What to Look for in a Cloud Fax Provider

Companies overcome security vulnerabilities, and the high cost of addressing them, primarily by doing their homework. It’s here they discover that not all cloud fax solutions are created alike.

Most online fax services do not, for example, provide the privacy, security, redundancy, and administrative capabilities, or forensic analysis tools to support the strictest regulatory mandates. Likewise, some may claim to be HIPAA-compliant but are not willing to sign a business associate agreement (BAA) to back up that claim as required by HIPAA.

Nor do all solutions offer the high level of security necessary to overcome the compliance requirements regarding data encryption. This is where it may be said that compliance does not necessarily equal security.

HIPAA rules, for example, do not mandate that all data be encrypted either in transit or at rest. Be assured, however, that if your customer data should be hacked, and your security solution has not encrypted that data, you can expect to be explaining to regulators why not.

Finally, what type of company, and what sort of infrastructure, is backing up the fax service? If a vendor is not a public corporation, how transparent is their financial situation? Can you trust critical communications to a provider that might not be in business next year?

This consideration leads to a related question: How reliable and stable is the underlying network? Does the service operate from a single server rack in a garage, or from multiple, geographically diverse, high-security data centers and colocations, with inherent disaster recovery built in to the network architecture?

eFax Corporate,® as an enterprise-grade, cloud-based solution used by small, medium, and global corporations worldwide, and backed by a billion-dollar public corporation (j2 Global®), keeps your valued data simultaneously secure, compliant, protected, and easy to manage.

In fact, eFax Corporate has been regarded for over two decades as the world leader of cloud fax, trusted by nearly half of the Fortune 500.

It's easy to see why.

eFax Corporate Security: Drilling Down

1. Compliance

As noted, not just any cloud fax service can help your organization achieve and maintain compliance. Federal and state financial disclosure and privacy laws place tough privacy, security, and accountability rules on public and private corporations and the financial industry, while in healthcare HIPAA has become even stricter, with enforcement actions more common and costly.

eFax Corporate's fax technology is designed to comply with financial security and privacy regulations such as the Sarbanes-Oxley Act (SOX) that regulates the financial disclosures of public corporations, the Gramm-Leach-Bliley Act (GLBA), also known as the Financial Modernization Act of 1999, as well as the Family Educational Rights and Privacy Act (FERPA) that protects the privacy of student education records, and similar federal, state, and industry regulations.

eFax Corporate has also been tested to meet the most important security and quality assurance protocols for data protection, including ISO-27001, FIPS 140-2, and the PCI-DSS v3.2 encryption requirements for 2018.

In addition, it meets the security standards for the Criminal Justice Information Services (CJIS) division of the FBI for use by federal, state, and local law enforcement agencies, and is engaging in the rigorous certification process under the HITRUST Common Security Framework (CSF) for HIPAA compliance.

2a. Security – Data In Transit

How does eFax Corporate protect your organization's fax data security? It starts with meeting the most stringent requirements for secure document transmission, including 256-bit encryption, and certificate-based authentication via Transport Layer Security (TLS) 1.2, in compliance with the recommendations of the National Institute of Standards and Technology (NIST).

TLS (and its predecessor standard, SSL) works by authenticating that two parties trying to communicate are who they say they are through the use of digital certificates. An encrypted "tunnel" is established so that traffic flowing between the two parties is indecipherable to an intruder.

TLS has two modes of operation: opportunistic mode and forced mode. Opportunistic TLS is sometimes described as "best effort" mode, meaning that if the destination server supports TLS then the sending server will transmit the fax over a secure communication channel using the TLS protocol. If the destination server does not support the TLS protocol then the sending server will "decide" that it made its best effort to encrypt the fax and default to a nonencrypted communication channel.

Forced TLS allows for no such decision. The sending server must verify that the destination server is governed by the same TLS protocol or it will abort the transmission.

eFax Corporate uses only the forced mode of TLS 1.2 for documents in transit.

It should be noted that TLS 1.2 is strongly recommended by NIST for use by the federal government and for HIPAA compliance.

It is also strongly recommended in the Payment Card Industry Data Security Standard (PCI-DSS) 3.2. SSL and early versions of TLS have been officially deprecated by PCI-DSS, and are prohibited for use as a security control to protect credit-card-holder data.

2b. Security – Data at Rest

Faxes are in transit for only a moment. Beyond that they can live forever in storage, and how you protect your fax data there is equally important.

Data in storage is also known as data "at rest." If stored in plain text, data at rest is often a sitting duck for an eventual breach (think user passwords or credit card information), so it's both wise and required that this data be encrypted to make it readily accessible to you but no one else.

eFax Corporate protects data at rest according to the Advanced Data Encryption (AES) standard, which uses the NIST-approved Rijndael algorithm to create a 256-bit encryption key. This means a hacker would have to try 2^{256} combinations to break the coded text – virtually impossible by even the fastest computers.

Also, with eFax Corporate your fax data resides in our Tier III/IV-rated, highly secure colocations and private data centers, which are audited for compliance with SOC 2 and SSAE 16-type 2 standards to ensure customer data is protected 24/7/365. Faxes may be stored here for as long as you like, or not at all, depending on your document retention policies.

Further, eFax Corporate keeps your data stored redundantly, and (if you elect) encrypted across multiple data centers in different geographical regions to ensure that you always have access to your fax records, even if one data center experiences an issue.

Additional Security Frameworks & Features

As referenced above, eFax Corporate participates in the most rigorous compliance certification process under the Health Information Trust Alliance (HITRUST). This is an organization created to standardize a common, certifiable security and compliance framework to assure both vendors and covered entities within the healthcare industry that their information systems and exchanges are trustworthy.

Administrative user-management features enable administrators to easily set and manage corporate-account default settings for all users to control access to sensitive data. Settings include control over the complexity of user login passwords. This feature strengthens security by requiring up to 20 characters comprising a combination of digits, special characters, and capital letters.

Two-factor authentication (2FA) adds a second level of authentication to an account login, making privacy attacks harder and increasing overall data protection. Examples of two-factor authentication methods include PIN numbers sent to the user via SMS, or voice or fingerprint recognition.

Most web-based platforms now offer some kind of two-factor authentication process, although it is not always mandatory for the user to have it turned on. For those who value their privacy, using two-factor authentication should be a no-brainer, and is offered as a key feature of **Sfax**,® the cloud faxing product from eFax Corporate designed specifically for healthcare entities.

OAuth 2 is an authorization framework within an application programing interface (API) that lets applications obtain limited access to user accounts on an HTTP service. Once the application is authorized it may use its access token to enter the user's account via the service API (limited to the scope of the access) until the token expires or is revoked. API-based services are typically used for integration with a customer's high-volume fax applications.

What follows is the full portfolio of eFax Corporate products, and the complementary features and capabilities they provide.

eFax Secure and Sfax

The eFax Corporate portfolio includes two maximum-security products called **eFax Secure**™ and **Sfax**, services geared specifically for heavily regulated industries such as healthcare that automatically encrypt incoming faxes using AES 256-bit, while notifying the user's account via email that a new fax is available for access via a secure portal.

The email notification has a personal URL (PURL). When the user clicks on this link, a TLS connection is made to a secure HTTPS website where the user must log in with her user ID and a strong password to view or download faxes. Multi-factor authentication may even be optionally required.

In this system faxes are never sent as email attachments. However, the Sfax inbox can be polled for incoming faxes and automatically downloaded to the customer's local server. Additionally, the encrypted faxes can be stored as long as needed, reducing strain on any local storage devices.

eFax Developer

eFax Developer™ is an API-based product for high-volume fax environments such as national pharmacy chains, payment processors, and other businesses that need to integrate it with their production faxing workflow processes.

eFax Developer ensures maximum security by also implementing TLS 1.2 encryption for faxes in transit, and AES 256-bit for faxes at rest in storage.

Administrative Security

To meet security and compliance as well as customer needs, eFax Corporate has developed extremely robust and hierarchical administration capabilities.

For security purposes, user settings are highly flexible, offering the ability to set multiple access levels with granular permissions and privileges for your most sensitive data, controlling who can do what with faxes. For example, admins can control and/or restrict on a per-user basis:

- Downloading, forwarding, sending/receiving, deleting
- Custom storage duration
- Restricted domains

Due to the fact that compliance and security are such critical facets of faxing, eFax Corporate has flexible and comprehensive role-based administration tools. This makes it simple for a "Super Admin" to add other sub-admins for specific purposes, with differing levels of access to the Admin Portal, to meet specific business needs and compliance protocols.

For example, in large organizations, administrators can designate sub-administrators to manage user groups in branch offices, and role-based access can be extended across different departments to ensure that only authorized employees have access to ePHI, as required by HIPAA.

The Cloud Fax Service of Choice

The best fax security solution available today is a fully hosted cloud fax model from eFax Corporate. If you're not sure whether your organization falls under specific regulations, we'd be happy to show you how eFax Corporate can help bring your fax protocols into alignment with the relevant law.

Here is a short summary of the reasons eFax Corporate is the world's leading cloud fax service for small, medium, and large enterprises:

The eFax Corporate Checklist

- ✔ Our solutions are trusted by many of the world's leading businesses in the most heavily regulated industries.
- ✔ We provide service to nearly half of the Fortune 500 companies worldwide.
- ✔ We service nearly 40% of the ALM Top 200 law firms — all of which send highly sensitive information by fax.
- ✔ We sign HIPAA Business Associate Agreements (BAAs).
- ✔ Faxes in transit and at rest are secured with the strongest NIST-approved encryption standards – TLS 1.2 and AES 256-bit.
- ✔ j2 Global owns multiple patents on cloud and fax technology.
- ✔ j2 Global has invested millions of dollars to build a secure, compliant, and redundant global cloud fax network.
- ✔ j2 Global delivers faxes in 149 countries.
- ✔ eFax Corporate operates a geographically diverse global network comprising redundant data centers and Tier III/IV-rated colocations providing 99.9% server uptime.
- ✔ SLA for service availability and rapid fax delivery.
- ✔ 24/7/365 customer support.

eFax Corporate®

About eFax Corporate

eFax Corporate is the world's leading online fax solution, serving more than 11 million customers worldwide. eFax Corporate lets users receive, review, edit, sign, send, and store faxes by email or through a web interface. It offers plans for individual users as well as provides corporate solutions.

To learn more about outsourcing to a cloud fax model with eFax Corporate, visit us at
enterprise.efax.com.au

Australian Headquarters
j2 Global, Inc.
Level 2, 39 Chandos Street
St Leonards NSW, 2065

Worldwide Headquarters
j2 Global, Inc.
6922 Hollywood Blvd.
Hollywood, CA 90028

Contact Sales:
1800 243 308

Web:
enterprise.efax.com.au

Please Recycle