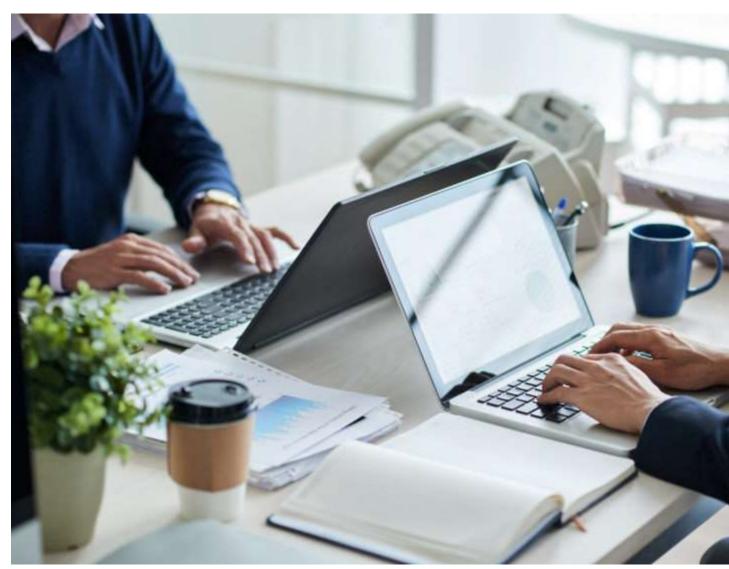# 3 Security risks of using analog Fax machines and how to avoid them

Traditional analog faxing has been around for decades and is used by millions of companies around the world. However, in this age of digital transformation, there are better and more secure ways of sending documents: **virtual faxing.** While keeping the idea of traditional faxing, virtual faxing offers advanced features and is much more secure. A necessity for doing business today.

Cloud technology is transforming traditional fax into innovative solutions for businesses of all sizes with many advanced features. Gartner predicts that the demand for new cloud fax technology will rise significantly in the next two years. Many companies have

or will have a "cloud first" strategy and are evaluating the most appropriate way to adopt a cloud fax service.

What are the security risks with traditional faxing?

1. Vulnerability to cybercriminals

There are many vulnerabilities found in traditional analog fax. If a cyber-criminal obtained an organization´s fax number (which can easily be found on the company website), they could send an image file by fax to the organization's fax machine. Using this vulnerability, they could enable malware or ransomware to be coded into the image file, which is then decoded by the organization's fax machine and uploaded to its memory. Once it's uploaded, it could potentially breach data or transfer to all the networks the fax machine is connected to.

2. Risk of non-compliance

By default, if you are sending documents by analog fax, you may not be complying with GDPR and MiFID II. There are a few reasons for this:

1. A standard, analog fax machine is rarely encrypted and may store electronic copies of the documents sent or received. Therefore, any sensitive data transmitted can remain on the unsecured hard drive. The only time they are removed is when they are overwritten by newer documents, which leads to the second problem.
2. The fax server. The majority of in house servers are not equipped with encryption software. These servers like fax machines can store unsecured electronic copies of the documents for a long period of time. To make matters worse, often when the server is reaching full capacity, companies print out hard copies to store them, making them even more vulnerable and further putting the company at risk for non-compliance.

3. Risk of third party viewings

There's a very high risk of someone else seeing sensitive documents, unless you wait at the machine for the fax to come in. Most companies have shared fax machines and anyone can access them, which of course violates regulations like GDPR, MIFID II, HIPAA and FERPA.

To summarize if you are still sending any confidential or regulated data via analog fax, you shouldn't be. The risks are too high.

How does virtual Cloud-Faxing combat these security risks?

1. Encryption

One major advantage of virtual faxing is encryption. Documents are encrypted before sending, during processing and transfer. Therefore, it is almost impossible for someone to get unauthorized access to private documents even if a cyber-criminal intercepted data, it would be encrypted and therefore completely unreadable.

2. Compliance

Virtual fax can improve compliance with data security and legislation such as GDPR and MiFId II. Under these laws, it is imperative that companies utilize technology that can keep data and communications safe; eComFax allows you to do this by having proof of delivery via SMS etc, and encrypting all documents.

3. Eliminate third party risk

Virtual fax solutions, such as eComFax, eliminate the risk of third party viewing documents. Sent and received documents are encrypted and secured and can only be viewed by those authorized to do so. Thus reducing said risk of others view sensitive data and adhering to compliance regulations.

How easy is it to migrate to virtual fax?

Moving from analog faxing to virtual faxing is actually quite easy. There is no hardware to install or maintenance fees, and it's a very flexible and scalable cloud solution.

July 30, 2020

Author: José Luis Pérez