Extending Cybersecurity to Faxing

TABLE OF CONTENTS

The security landscape

When it comes to the security conversation, much is made of how existing systems and approaches are ill-suited to tackle modern threats. With many organisations wrestling with ongoing digital transformation journeys, most are caught in a dangerous no-man's land. As they digitise their operations, they also increase their risk, but their security processes have yet to evolve at the same rate.

And this problem is likely to increase as enterprises accelerate digital transformation initiatives. In fact, 60% of IT decision-makers are now accelerating the speed of their transformation projects as a direct result of the disruption caused by COVID-19.[1]

The message is simple: Sophisticated threats require appropriate countermeasures.

Yet in the rush to deploy the latest defences, opportunities may be missed. Having the appropriate response is not always a case of acquiring new security solutions – in fact, many experts believe that the proliferation of solutions offers attackers a way in.[2] This is because the increased complexity of having multiple defences, each protecting against a different threat, can overwhelm enterprises, particularly when it comes to keeping them all up to date

Security has to be a priority; that is a given. It also needs to be implemented in such a way that does not add onerous work to already time-poor, overstretched teams. If it does, workarounds might be deployed. This in turn creates new security risks, as unofficial ways of working go undocumented and out of sight of the IT department, and therefore out of scope of security policies and protocols. It might also lead to the deployment of shadow IT, which can drain company resources while sitting outside of corporate governance.

Sometimes, the focus should be on how existing solutions can be deployed to provide modern cover. They should be up to date, certainly; but they should also be appropriate for the broader needs of the business. For example, the fax is a critical communications device, even as its origins can be traced back to the 19th century.[3] Nearly 17 billion faxes are sent around the world every year, while in the UK, more than 125,000 were sent and received by the public sector in 2019. In the US, it accounts for 75% of medical communication.[4]

That said, in 2018 the technology was dismissed as "archaic" by health secretary Matt Hancock,[5] with the Minister for Health and Social Care mistakenly declaring that "everyone else got rid of them years ago." He went on to name-check email as being more secure and effective, and set a deadline for the removal of all fax machines from the NHS.

However, there are flaws to this approach. Simply banning it is not an option without an appropriate solution, while the suggestion that email is a like-for-like replacement is undermined by the fact that if that were the case, the sectors that rely on fax for certain communications would have migrated over a long time ago. Ultimately, there are too many businesses and vital services that rely on it daily to dismiss it as a relic that needs replacing, without considering how.

It's important to remember it still poses risks. For organisations wanting to improve security, the question is how they deliver that protection while enabling operations to continue as normal.

Combating the digital threat by going analogue

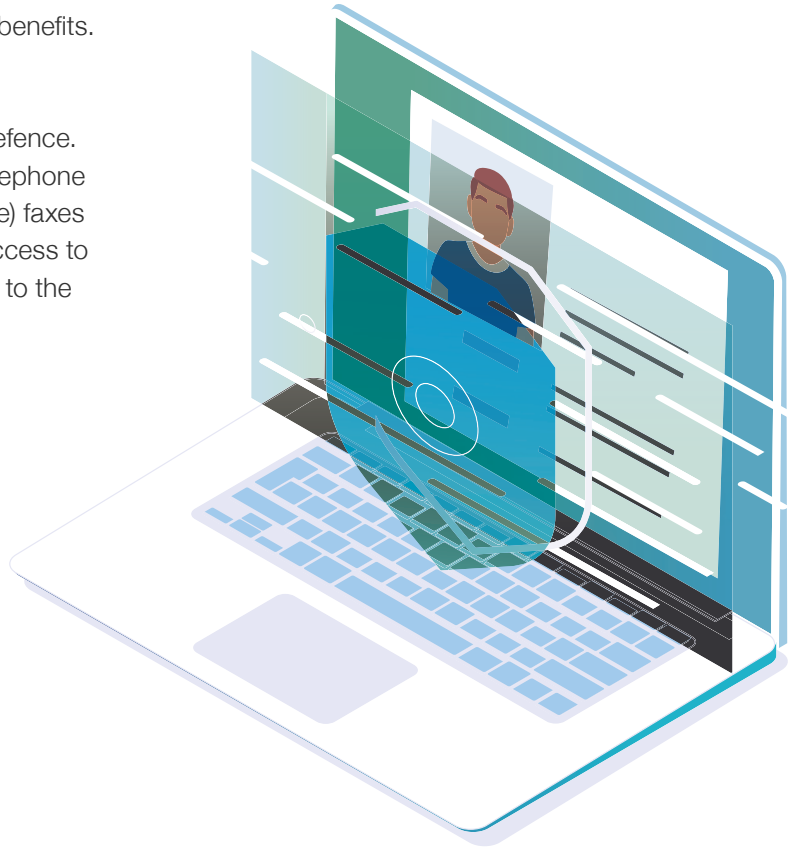
There is a tendency to think that if sophisticated threats are going to use modern technology to access sensitive information and cause massive disruption for rapidly digitising businesses, the solution could be to become more analogue.

In the wake of the Snowden leaks, for instance, there were reports that some foreign intelligence services and diplomats were considering using typewriters for secure communication.[6] The thinking was that if a document were not digital, it could not be hacked. A leading security specialist suggested that inserting analogue technology into predominantly digitised systems could work as a back-stop against cyber threats,[7] an idea that has been mooted in the US to protect the power grids from digital attacks.[8]

Elsewhere, Sony Pictures CEO Michael Lynton revealed that, in the wake of the infamous 2014 hack, he had taken to sharing sensitive information via fax. The theory is sound – if something is not connected, then the connection can't be a way-in for attackers.

Yet for the majority of organisations, this simply is not practical. Digitalisation is driving ever greater levels of efficiency, cost savings, operational optimisation, and innovation – inserting any sort of analogue technology could diminish those benefits.

There is also another reason why so-called analogue technologies are not a suitable defence. In the case of faxes, while the traditional telephone line is not digital (and therefore not hackable) faxes are not encrypted in transit. Anyone with access to the line can, theoretically, also have access to the information sent via fax machine.



The human factor

Is that a real threat? It is debatable whether the majority of organisations using fax will ever have to deal with an attack that targets phone lines. However, the fact that it is unencrypted runs counter to many governance, compliance, and industry-specific regulatory concerns.

There's also the issue of fax machine location and output. Often in the centre of open-plan offices, or certainly not in a secure office, and left unmonitored for the majority of the time, a sensitive fax could sit out in the open for some time until the recipient collects it. That is before one considers how often physical documents have been misplaced, stolen, or exposed.

These all link back to the human factor in data breaches – where mistakes by people are the cause. Back in 2014, IBM suggested that employees were in some way responsible for around 90% of breaches[9] – while that figure has now dropped, Verizon still put it at around a third in 2019.[10] It's no different for faxes. While all forms of communication are prone to human error, faxing has to contend with the clumsy finger problem, and the sheer number of mistakes that can easily be made when dialling a phone number - there was once the issue of patient prescription information being inadvertently faxed to a hotel group.[11]

Then there's the challenge of connecting a decades-old technology with newer solutions. With more and more offerings involving multi-functional devices, fax machines are now often integrated with wider business systems. It becomes a bit like leaving a small window open downstairs – it might seem like too small an opportunity, but any opening can be exploited. The problem here is that when connected to digital systems, the lack of modern security in fax machines becomes that small window, in much the same way that connected CCTV systems can, ironically, be an easy way into otherwise secure networks.

Put simply, there are too many risks in relying on the analogue nature of the fax to consider it an effective cybersecurity weapon, whether as a means of securing communication or by just not seeing it as a risk. Yet few organisations are going to be doing away with it any time soon.

The new, secure fax

What then, are the options available to those sectors that rely on the fax as a means of effective communication?

The answer lies in one of the technologies driving digital transformation – cloud computing. Gartner says that total cloud revenues will grow from US$ 242.7 billion in 2019 to a predicted US$ 364 billion in 2022, fuelled by demand for what the analyst called "customer preference of elastic, pay-as-you-go consumption models."[12]

No more upfront costs, no more worrying about physical hardware – the cloud provides easy access to the technology a business needs. Cloud faxing does exactly that, but for faxes. It allows the entire fax process to be handled digitally via the web; either through a company's email application, an MFD, workflow application, mobile app or secure web-portal.

Users no longer have to rely on a physical fax machine, at either end. If party A requires an order via fax, party B can now simply use a cloud faxing app to upload and share the required information.

This does more than improve flexibility – it dramatically increases security. Cloud faxing provides high-level encryption, both in transit and when faxes are stored, in addition to audit trails of everything sent and received, improving governance and compliance where required.

CASE STUDY - Delivering a secure fax solution

Moorfields Private is the private division of the Moorfields Eye Hospital NHS Foundation Trust, the leading provider of eye health services in the UK and a world-class centre of excellence for ophthalmic research and education.

Faxing is an important means of communication for Moorfields Private, with patient referrals, medical records and scans all being received via fax. When the company made a strategic decision to move their telephony system from analogue to VoIP, it had an impact on its ability to fax. Without telephone lines, it would not have a reliable way of sending and receiving faxes, so it needed to find an alternative solution.

Security was at the top of its lists of priorities, with a requirement for fax transmission encryption, fax data retention and archiving, centralised control of the faxing function, and the ability to provide secure fax access to select hospital and administrative staff.

Since moving to eFax (Corporate solution), Moorfields Private has eliminated paper from its faxing process and today all faxes are sent and received digitally, so medical referrals, reports and scans can be easily shared, saved and securely stored online, removing the need to print, scan or manually file.

Sensitive documents no longer sit openly on a fax machine and staff can be more productive as they no longer need to wait by a fax machine. And because faxes are now in digital format, administrative staff can retrieve and access patient records much quicker and respond to queries in a shorter timeframe, improving patient services.

MoorfieldsPrivate
Eye Hospital

On top of that, administrators can implement access restrictions, just as they would with any other data. With the use of cloud faxing, security professionals can implement the same cyber hygiene principles they apply across the organisation to faxing. That includes the aforementioned access management to implementing passwords (and appropriate password behaviour) and being able to update the software being used automatically, across the entire organisation.

By integrating fax into their digital transformation, enterprises can ensure that they have a consistent level of security across all their communications channels – whether brand new or with a heritage stretching back more than 150 years.

Your cloud fax provider security credentials

Whether an NHS trust, government department or private sector enterprise, you need to know that your cloud fax provider offers the highest levels of security and compliance for your communications.

As standard, they should offer:

- Highest Encryption Levels: 256-bit AES and TLS encryption protect your inbound faxes immediately.
- Tier-III Secure Servers: Servers in highly secure data centres keep your faxes protected 24/7/365.
- Transport Layer Security (TLS): Secure channel open and a PIN required when you access your fax online.

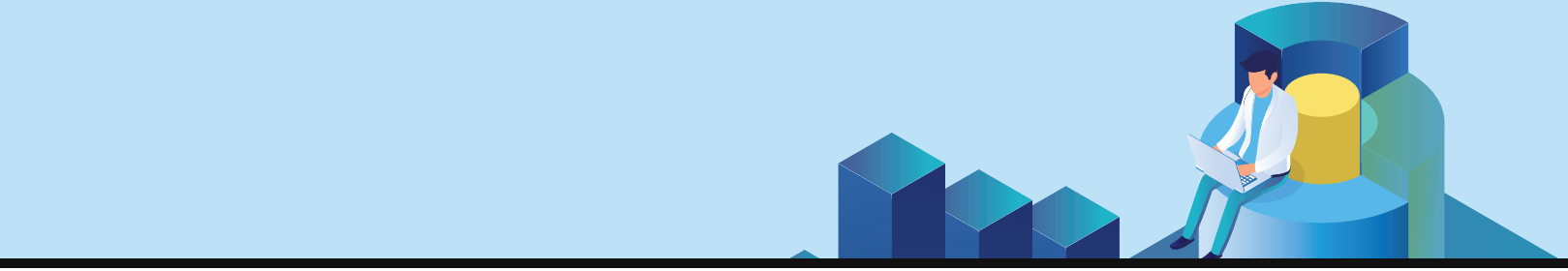
How eFax can help

Traditional fax equipment can place enterprises at risk of non-compliance with industry regulations, including GDPR. Processes have to meet industry standards for protecting data.

eFax has been a leader in fax compliant solutions for more than 25 years. It helps ensure that faxes are transmitted securely and accessible only by authorised personnel — helping organisations in a wide variety of sectors meet confidentiality requirements.

Its eFax Secure™ solution protects and secures sensitive and confidential faxes, offering an email-driven and convenient process for receiving faxes securely over the web, while remaining compliant with a variety of data regulations, from the Data Protection Act to GDPR.

[1] https://uktechnews.co.uk/2020/08/23/efax-research-reveals-it-decision-makers-accelerating-digital-transformation-due-to-disruption-caused-by-covid-19/
[2] https://blogs.cisco.com/security/when-it-comes-to-security-how-many-vendors-is-too-many
[3] https://www.bbc.com/future/article/20150224-why-the-fax-machine-wont-die
[4] https://www.vox.com/health-care/2017/10/30/16228054/american-medical-system-fax-machines-why
[5] https://www.gov.uk/government/news/health-and-social-care-secretary-bans-fax-machines-in-nhs
[6] https://www.bbc.co.uk/news/blogs-magazine-monitor-26081163
[7] https://securityledger.com/2014/03/is-analog-the-answer-to-our-digital-insecurity-dilemma/
[8] https://www.zdnet.com/article/us-wants-to-isolate-power-grids-with-retro-technology-to-limit-cyber-attacks/
[9] https://www.securitymagazine.com/articles/85601-of-successful-security-attacks-are-the-result-of-human-error
[10] https://enterprise.verizon.com/en-gb/resources/reports/dbir/
[11] https://psnc.org.uk/our-news/action-required-fax-messages-received-by-incorrect-recipient/
[12] https://www.gartner.com/en/newsroom/press-releases/2020-07-23-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-6point3-percent-in-2020



About eFax

eFax launched its digital cloud fax service with the goal of using the convenience of email and the speed of the internet to make it easier for people to send and receive faxes. eFax lets users and our 11 million customers receive, review, edit, sign, send and store faxes by email or through a web interface. Our appeal and success are built around three key features: the widest selection of phone numbers; an easy way to send and receive faxes and voicemail by email; and a fast, reliable and secure communications network.

To learn more about outsourcing to a digital cloud fax model with eFax, visit us at: efax.co.uk/corporate

European Headquarters

eFax
European Headquarters
Unit 3, Woodford Business Park
Santry, Dublin 17, Ireland

Contact Sales:
UK 0800 689 0588
Rest of Europe +353 (1) 656 4950

Web:
efax.co.uk/corporate

Follow Us

Please Recycle