zivver

# A new era of data loss prevention and email security:

## How smart technology can prevent the leading causes of data incidents

Whitepaper

# Foreword

## Stephen Khan MSc CISSP

Data is the lifeblood of all organizations; the way in which they secure that data underpins customer confidence and maintains economic functions for our society to operate. And the amount of data we handle is increasing, and will continue to grow through digital transformation, changes in working practices with more remote working, and flexible operating models.

Data will be shared with third parties and fourth parties in a complex ecosystem, making the act of securing this data much harder. This challenge applies to private, public, and government entities across all industry sectors; examples include financial services sharing data with partners to deliver products and services; healthcare providers sharing patient information with local and central government organizations. Of course, much of this data will be exchanged via third party services such as hosted email services like M365 and Gmail.

I have worked across multiple industry verticals, and implemented data loss, and data protection tools at scale. I am rarely surprised when data is accidentally sent out by a well-meaning person to either an accidental distribution list or inappropriate audience. In my view, the tools we use for vital communications are not integrated into daily working practices and require additional action and knowledge to be applied by our colleagues and partners.

Data will become more distributed across devices and third parties, and must be appropriately managed to maintain customer confidence in our businesses. In fact, in a recent survey, Experian stated that **"74% of consumers say security is the most important factor when choosing a business".** Even Interpol regards business email compromise fraud as a top risk and started a campaign to raise awareness.

Security communities also know not all communications are always secure due to insecure practices allowing for interoperability at the expense of security. This challenge falls on the doorstep of the Chief Information Security Officers and technology executives as data inappropriately managed attracts regulatory fines, and reputational damage.

To do their best work, both inside and outside of our organization, our colleagues and partners need information technology to be as frictionless as possible, and integrated into their existing workflows. They are not security professionals, despite being given security awareness training – it's not their core function during a busy day.

And so we need to find a better way to use frictionless technology and help our colleagues and partners to exchange and share data whilst protecting our customers and businesses. Only then can sensitive data shared digitally be truly secure.

## Stephen Khan MSc CISSP

Global Head of Tech & Cyber Security Risk (former security exec HSBC)

Stephen is an information and cyber security practitioner, and international speaker with 20+ years of experience working for global firms across financial services, healthcare, and defense.

Stephen has held senior group level positions at firms including HSBC, RBS, GSK, and Siemens with experience of global regulatory and cyber security frameworks to drive execution and implementation for the management of risks to support business strategies especially as technology and business models are changing at pace.

He contributes to the Cyber Security community as Chairman of Club-CISO advisory board by engaging with 500+ global CISO executives on important matters affecting cyber security and risk leaders and their organizations. He supports the wider industry and academia through his board membership of Research Institute for Sociotechnical Cyber Security (RISCS).

# Introduction

Hyper digitalization and hybrid working sees employees handling more data than ever. The compliance and digital security landscape continues to evolve and the average cost of a data breach is on the rise.

It is no secret that the majority of data incidents reported today result from non-cyber related errors – more than **70%** in 2022 according to the ICO. This includes sending sensitive data to the wrong recipient, failure to recall emails sent in error, using Cc in place of Bcc – the list goes on.

It's up to IT leaders to ensure the platforms they employ for the confidential handling of sensitive data are secure, compliant, and efficient.

While the likes of Gmail and M365 are fantastic productivity platforms for widespread teams, due to the decentralised nature of email, email clients fall short on vital security requirements, leaving your organization open to data leaks, reputational damage and considerable fines.

In this report, we investigate the security flaws hidden in plain sight in email and how progressive organizations are employing smart effortless technologies to support compliance and protect their data, whilst giving employees the freedom to focus.

# 01 Driven to distraction: How much is too much communication?

While cloud-based productivity platforms such as Microsoft 365 and Google Workspace do enable all-important flexibility for remote working teams, they lack the smart functionality required to secure sensitive data in transit and thereafter, leaving organizations wide open to large fines and reputational damage.

In addition, these platforms are increasing. Reflect on your own working day and it is likely that you are communicating via a range of applications – as many as three or four may be open in your browser or on your desktop at any one time.

In fact, in a recent survey of more than 6,000 employees globally, **we found that more than half (55%)* have seen the number of communications tools and channels increase in the last two years.**

So, what's the result?

Sure, we're able to communicate at any time, and from anywhere, with our colleagues, clients, suppliers, patients, residents etc. But this flexibility is having a very real negative impact on people:

- **39%** feel distracted from their day-to-day jobs due to increased training
- **34%** refer to frequent interruptions preventing them from getting the job done
- **29%** feel more stressed in wake of increased notifications and alerts
- **25%** state they struggle to 'switch off' because they feel the need to be always contactable

Solution fatigue is preventing employees from focusing on their core role. And, unfortunately, distractions inevitably increase the likelihood of security leaks.

It's time to question, is it up to your workforce to understand the complexities of data protection and digital security? Are your communications platforms doing your business a disservice? Does mandatory security training really fix the issue?

In the simplest terms, should technology be working harder for us?

*Zivver Freedom to Focus research 2022

## It's time for change

Progressive business leaders are seeking out technologies to empower their people to work efficiently and securely. We call it a new generation of secure digital communications – solutions designed to make sharing sensitive information nothing short of effortless by enhancing existing platforms with data loss prevention tools driven  by contextual machine learning, advanced encryption, and seamless integrations.

It's about instilling security beyond company culture to make it a lifestyle and an instinctive mindset for everyone, every day.

# 02 The state of digital communications security today

Remote working, digital fatigue, evolving regulatory pressures; these are security challenges confronting businesses across all industries today, and a traditional approach to digital security is no longer fit for purpose. After all, security breaches are on the rise, and so is the average cost of a GDPR fine.

As such, one thing is clear – you cannot train an employee to avoid making mistakes. But there are ways to navigate this challenge.

Rather than expecting employees to change their behavior,  IT leaders are realizing the benefits of innovative technology that embed into existing workflows. In this way, employees are armed with the tools they need to act securely with ease, without adapting their processes or utilizing additional platforms.

And if there's one workflow we're all familiar with today, it's email. Instant messaging and file transfer platforms come and go but email is king.

In fact, nearly **90%** of employees and IT leaders rely on email to get the job done, with over **80%** considering email to be the most secure way to send sensitive information.

This, however, is not always necessarily the case.

## Building on existing communications infrastructure

Since its invention several decades ago, email technology has stagnated. Afterall, it was never built to be secure.

Email isn't 'owned'; it is a completely independent distributed system which operates seamlessly via multiple providers. However, the standards email relies on to ensure interoperability aren't keeping up with digital transformation or today's changing threat landscape.

Email technology is underpinned by inherent trust. The vulnerabilities exposed by inherent trust don't catch the attention of the media like with other digital security incidents. The objective of email is to get a message from point a (the sender) to point b (the recipient) as quickly as possible – making security a second priority.

Although email has seen the addition of (often conflicting) functionalities to improve security, such as anti-SPAM, the fact is, the aging standards underlying email haven't adapted in nearly 20 years.

Adoption of new email standards is varied. Things like SPF and DMARC are relatively widespread, but the likes of DANE, DNSSEC and MTA-STS have far lower adoption.

Email is decentralized, meaning that the adoption of universal security protocols is difficult.

Take, for example, transport layer security (TLS) encryption. TLS encrypts messages sent between two compatible email servers – unless the recipient's server is not compatible, in which case the email is sent unencrypted, meaning it is at risk of being intercepted in transit. To make matters worse, the sender is unaware that their email has been sent unencrypted. With no way of knowing their data is even at risk, identifying a potential data breach and taking corrective action takes much longer and costs significantly more.

Another security drawback of TLS is that it protects an email in transit, but not at rest. In other words, once an email is received and sitting in the recipient's inbox, the email contents are no longer encrypted and can be accessed by anyone who has access to that inbox. A lack of multi-factor authentication and expiration control functionality means employees cannot take control of their sensitive communications after pressing 'send'.

We also see many vendors retaining access to decryption keys, meaning your data isn't necessarily as protected as you believe it to be (this is a question for your security suppliers – who holds your decryption keys?).

In simple terms, while email providers such as Gmail and M365 offer many benefits for businesses today, they do not meet the compliance and security requirements of organizations today.

# 03 Why email isn't as secure as you think

You'd be right to assume that email remains the lynch pin of office communications due to its user-experience. It's universal and reliable, regardless of your stakeholder.

However, from a business perspective, email presents a number of hurdles for your people.

We've all felt the stomach-drop moment of sending an email to the wrong person. Yet today, most solutions lack an adequate email recall function. For example, in Gmail, emails must be recalled in under 30 seconds after sending to be effective.

As already mentioned, once sent, employees are unable to control access to or track email performance. Users cannot set expiration periods on emails or their attachments; they cannot manage access to emails once sent with standard multi-factor authentication controls.

These are simple pieces of functionality that are absolutely integral for businesses today yet they are lacking from email clients.

> "Relying only on employee awareness training is clearly not enough. Because we're seeing the problem getting worse, not better. (...) We live in an era of smart cars, smart houses, smart power that is helping people to overcome a problem with technology that's not obtrusive. On the contrary, it's modern and usable."
> Barry Moult, Director at BJM IG Privacy Ltd

We also see employees switching between multiple platforms to complete different tasks. For example, Outlook limits attachment sizes to just 20 megabytes. For sharing a video, large files, or high resolution images, employees are forced to use third party file transfer sites. This is problematic for a few reasons:

- Third party platforms are not integrated with existing platforms and workflows, forcing employees and their recipients outside of their familiar email environment.
- They are restrictive; often, free versions of file sharing platforms limit file sizes to 2GB.
- Some do not deliver on compliance requirements.
- Finally, while third party platforms may provide some security measures to protect files in transit, they do not prevent the leading cause of data leaks today – human error – meaning a major data incident is only ever a click away.

This is just one example of a common task which, in today's digital age, should be nothing short of effortless.

> "Sending large file sizes is a fundamental part of healthcare email traffic. Whilst some clinical systems and solutions tackle common files, for example sharing of CT scans between hospitals, there is demand for a secure way of transferring large files. We are using large file transfers to receive patient videos for remote consultations or updates as an example, which is essential to encrypt end to end."
> Sarah Judge, Digital operational lead and CCIO at West Suffolk NHS Foundation Trust

Put simply, traditional email clients and productivity platforms cause friction: disruptive alerts or delayed notifications, lacking functionality... Instead of adopting security best-practice, employees are learning how to avoid clunky processes in order to work efficiently and to meet the needs of their stakeholders – effectively increasing the chances of a data incident.

## Compliance made complicated

Every industry has their own data protection standards to adhere to in addition to the GDPR.

When sharing sensitive data online, organizations are often required to have access to data logging, including proof of delivery, which many traditional email clients fail to provide.

Data regarding how emails are sent, encryption levels, delivery and open rates should all be available for export. The ability to analyze this data on a granular level, down to a user and team basis, ensures data protection and IT leaders can protect their organizations when it comes to third party audits and compliance reporting, as well as identifying potential gaps in data loss prevention strategies.

We operate on data today, it is the lifeblood of every business. Employees must be empowered to manage it securely, and business leaders must have access to it in order to navigate complex compliance legislation.

Instead, we see security leaders accepting the technical limitations of email clients and the impact these have on workflows. It is time to expect more from our solutions to ensure digital security and power productivity.

# 04 The flaws in digital security training

Traditionally, malicious and inbound attacks dominate the conversation around cyber security, with little to no focus on outgoing communications. This is the equivalent of locking your front door but leaving the windows wide open.

IT leaders realize that data security cannot be the responsibility of employees. Yet despite this, only 18% of security professionals have their approach to risk and email security under constant review.

And while training certainly does play an important role in preventing incoming attacks (think malware, phishing, general security best practice), people cannot be trained to avoid making simple mistakes.

Often treated as a tick-box approach to compliance, studies show that training is effective for just four to six months before it must be repeated. In fact, we found that only **67%** of employees have received security training in the past two years. Of these, **31%** state they have not used their learnings in their core role, yet **76%** of IT leaders think data security training alone will reduce email security risk.

Add to the mix intrusive protocols, processes, and platforms, and it's no wonder employees are feeling burdened by IT security:

- **50%** say current security methods slow them down
- **47%** say they felt more frustrated by network security measures when working from home
- **39%** say IT teams are so paranoid about threats that it hampers them from doing their job

Evidently, our approach to training isn't fitting the bill. Employees don't have time to complete compulsory sessions and when they do, they aren't truly benefiting from their learnings.

**23%** of all reported incidents last year were the result of human error; **13%** of all incidents were due to emails being sent to the wrong person. It is clear that training alone cannot protect organizations from data leaks. However, through a combination of real-time awareness training and smart technology, employees can be empowered to avoid these most common mistakes.

"Every colleague comes into work to perform their job to the best of their abilities, with knowledge and experience. For many people, the burden of security is regarded as an IT problem, and they simply want to follow existing processes without having to perform additional steps or access multiple technology tools. Their core skill set is not security but will follow company policies and procedures if it does not impact them doing their job.
It is the responsibility of technology leaders to find frictionless tools which allow people to perform their work without impacting productivity."
Stephen Khan, Global Head of Tech & Cyber Security Risk (former security exec HSBC)

# 05 Welcoming the next Generation: Smart technology to empower smart businesses

By now it should be clear that digital communications security is not a people problem – it is a technological one. Because only with access to the right tools can people protect the sensitive data they handle every day.

Our days have never been busier. Employees need to be free to focus without fear of causing a major data incident.

**“(…) forcing users to change their behavior or to remember to encrypt important data is not going to work. However, the intelligent application of machine learning can automatically apply additional controls and simultaneously educate users about the information they are sharing and the risks that involves.”**
OMDIA Market Radar – Outbound Email Security

Super smart email security solutions, designed with people in mind, integrate seamlessly with email clients to enable frictionless workflows. This is what we call the next generation of email security.

Innovative solutions empower employees to invoke security with a single click – or no click at all, depending on your preference – by alerting them to potential errors in the moment emails are being drafted so they can manage sensitive data effortlessly.

By operating silently in the background of your email client (Outlook, Gmail, or M365), employees can share sensitive data and large files effortlessly, securing sensitive communications:

- **Before sending**, with prompts to encrypt emails and act on potential errors
- **During transit**, with advanced encryption and zero knowledge, zero access methodology (because we don’t hold your encryption keys)
- And **after sending**, with recall functionality users can rely on, MFA, the ability to manage access controls, and data logging

## Best practice, in practice

**This email contains sensitive information**
Zivver Smart Classification automates classification methods and triples the accuracy of security alerts by leveraging millions of data points to identify patterns in the body and attachments of emails.

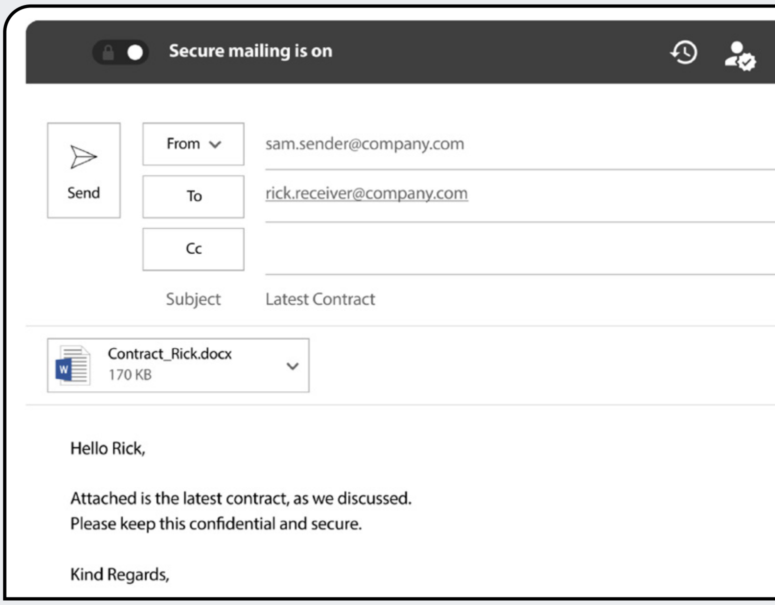
This is the next generation of data classification, using advanced machine learning to learn the intricate differences between sensitive and non-sensitive data.

Zivver then classifies the data according to the appropriate security levels and alerts employees to potential security hazards while emails are drafted. Employees can then apply advanced encryption to secure their data, as well as MFA, expiration controls and more, to prevent data leaks and ensure compliance.

**Simple for recipients**
We use email because it is universally simple. So if your security solution begins to compliance processes for recipients by requiring them to navigate to browsers or portals, or create accounts to access messages, it isn't working for your organization.

Zivver doesn't require recipients to create Zivver accounts to access secure emails. With MFA functionality, they can rest assured their data is being handled correctly – without having to jump through hoops to access it. Plus, you can even empower stakeholders outside of your organizations to send secure emails and files to employees, without creating Zivver accounts, meaning you can be sure incoming messages are protected without creating accounts.

**Simple for administrators**
Controlling access to data and functions within a growing and changing workforce is no easy feat. Zivver Synctool empowers truly effortless user provisioning by supporting complex identity workflows (including managing and delegating access to group or shared mailboxes), complex identity management scenarios (including employee email changes or managing users with guest accounts prior to the organization's onboarding), managing administrator access from external parties in parallel to managing access for employees, and creating alias email addresses for users and shared mailboxes.



From: sam.sender@company.com
To: rick.receiver@company.com
Subject: Latest Contract
Contract_Rick.docx 170 KB

Hello Rick,

Attached is the latest contract, as we discussed.
Please keep this confidential and secure.

Kind Regards,

Synchronization of changes can also be scheduled as an automated task to run at the frequency your organization desires, to ensure that users and rights to mailboxes are provisioned and deprovisioned as soon as changes are made in the underlying source system.

**Has my email been received?**
Say goodbye to inefficient couriers and fax machines and welcome in a new era of smart, secure proof of delivery for your most sensitive digital communications.

Zivver Prove empowers users to view, download, and print a Proof of Delivery or Proof of Receipt report for every message and file sent or received via Zivver. You can verify the status of your sensitive documents within your Zivver enabled email client (Outlook, Gmail) or via Zivver Web.

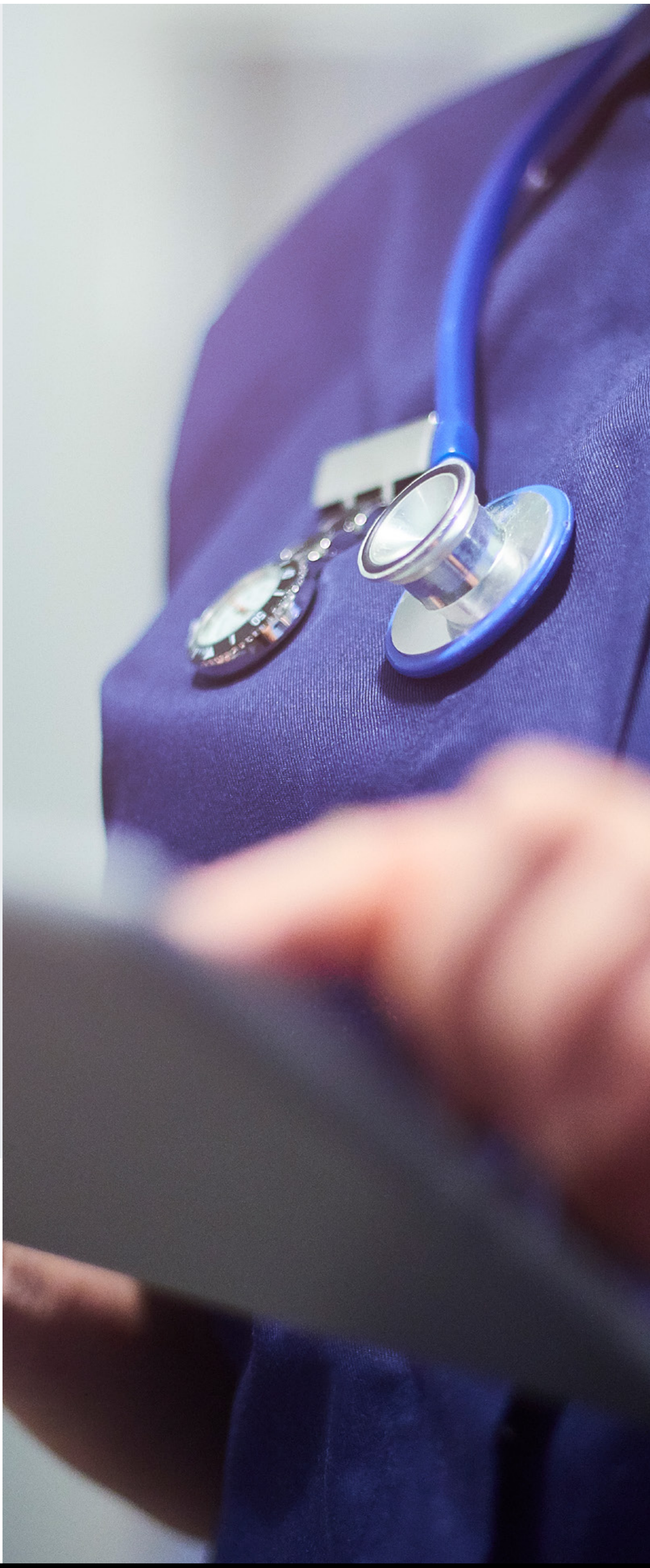
# The value of a new generation digital communications security

The magic of new generation digital communications security lies in its invisibility. Unlike traditional platforms, new solutions are disruptive only in the ways that matter, and work silently in the background of email clients to empower users with smart, right-sized security fit for businesses across every industry:

- **Effortless** – Capable of operating within existing email platforms intuitively, empowering your people to ensure security with a single (or no) click
- **Secure** – Not just 'good enough' but has a high level of end-to-end data protection, with zero keys, zero access, unparalleled encryption and user authentication
- **Smart** – semantic aware with tailored levels of data protection, along with machine-learning driven business rule-based error correction

Earlier generations of technology are not up to standard. They fail to keep pace in today's modern working world, causing friction in everyday workflows.

It's up to business leaders today to empower employees with innovative technologies designed to empower a security lifestyle. In this way, enterprises can ensure true security sustainability, today and in the future.



zivver

**Zivver**

5 New Street Square
EC4A 3TW London
United Kingdom

+44 (0) 203 285 6300
contact@zivver.com

zivver.com

Kon. Wilhelminaplein 30
1062 KR Amsterdam

085 016 0555
contact@zivver.com

zivver.nl

linkedin.com/company/zivver   facebook.com/zivver   @zivver_en / @zivver_nl