zivver

Report

How financial firms can mitigate risks with email data protection solutions

Report

Table of contents

01 Introduction

With so many communications being handled digitally and new channels coming online all the time, it's not surprising that data and information quantities have been exploding in recent years. But these days, safeguarding data goes beyond strong encryption and defending against cyber attacks. For a number of reasons, many companies have yet to adopt a more holistic approach to communication security, which in turn can put sensitive data at risk.

According to Statista, the global banking sector alone is projected to spend nearly $288 billion in 2021 on IT security (over $114 billion in the insurance sector). Much of this has been focused on anti-hacking and malware solutions, leaving other security areas such as email data protection potentially vulnerable.

In this eBook, we'll explore how financial firms can enhance their digital communication security with the use of integrated tools that are designed to improve data protection awareness across the organization while preventing costly leaks.

Most data leaks happen before sending

Despite not getting the massive headlines that breaches such as the SolarWinds or Microsoft Exchange Server hacks received, human error is routinely the top cause for data leaks worldwide, and the financial sector is no exception.

Security incident reports, including those from the ICO, routinely show that most data leaks happen before employees send information, specifically caused by:

Auto completion functionalities of email clients, accidentally adding the wrong recipient

Users not being aware that the information they are sharing is sensitive

Attaching a file that contains sensitive information the user is unaware of

Exposing recipients contact details by failing to use 'Bcc'

Most of us have made these mistakes before, sometimes the outcome is embarrassing and relatively harmless, other times it can be highly consequential and cause lasting damage.

The Ponemon Institute's annual data breach report for 2020 showed that financial sector organizations are currently spending an average of $5.85 million to manage the fallout from security breaches. On top of this, massive incidents such as the Capital One or Equifax breaches can end up costing firms many multiples of that, not only in the form of penalties, fines or the impact on share prices, but also due to investigative and mitigation effort costs which can be substantial.

Speaking to some of the challenges facing financial firms in properly securing their data, Wouter Klinkhamer, CEO of Zivver, said the following: ''Financial institutions will always remain a prime target for cybercriminals, in part because of the massive amounts of personal identifiable information stored in their databases. At the same time, threats evolve, that's why firms everywhere should review their data security protocols and, where necessary, invest in effective tools to ensure that sensitive information can be safeguarded at all times."

He went on to add: "This changing landscape is why Gartner's Market Guide to Email Security last year called on IT and Security leaders to urgently re-evaluate their communication security, with a focus on email data protection in particular."

A time for innovation

Mark Carney, former Governor of the Bank of England, said the following on the need for sectors to innovate: "The economy is reorganizing into a series of distributed peer-to-peer connections across powerful networks – revolutionizing how people consume, work and communicate. The nature of commerce is changing. Sales are increasingly taking place online and over platforms, rather than on the high street. Intangible capital is now more important than physical capital. Data is the new oil."

Carney went further: "In the financial sector, these innovations will allow people to manage their finances seamlessly, from tracking how much they spend, to managing their future savings and current loans. For the financial sector to be effective in this new economy, it needs to continue to be resilient, fair and dynamic, while acknowledging the responsibilities that come with employing this new data."

And financial firms are not alone in the need to innovate. During the onset of the pandemic, entire industries needed to swiftly adapt to new ways of working in order to ensure business continuity during these exceptional times.

A good example of this is the Dutch Judicial System. Once heavily reliant on the use of faxes and couriers, an emergency ordinance was issued last year in the Netherlands, granting Zivver, a secure email solution, the legal equivalency of fax and registered mail for certain types of correspondence. This helped to facilitate the timely exchange of information digitally when so many people were working remotely and communication processes were disrupted. Now the entire legal system has adopted a more convenient way of communicating that is both secure and compliant, opening the door to further digitalization.

02

Securing digital communications starts with email

Effective digital transformation that strikes an optimal balance between security and usability can seem overwhelming, leaving many companies unsure of how to achieve this. Often the best place to start is by properly securing outbound email.

By seeing email through the lens of people's habits, not simply as protocols, you can support a wide range of use cases from your 'email' whether it be transferring large files, questionnaires, documents to be signed or other types of more structured information sharing.

Every financial institution needs secure methods of sending emails and transferring files to customers or other contacts, even if they rely heavily on customer portals. Whether it's a bank sending out statements to clients, an insurance company offering online consultations, or a notary sharing documents with other parties for an estate transaction, companies everywhere are increasing their use of digital communication channels

In many cases, however, there's a lack of awareness on how best to protect sensitive data from within, let alone how to properly exchange information with others while complying with the GDPR, CCPA and other privacy regulations worldwide. This is on top of other requirements such as PCI compliance for credit card processing or SOX for securing electronic financial records.

Email is here to stay

Even with the increased use of other digital channels, on average people send and receive over 120 business emails every day. Statista research shows that more than 300 billion emails are sent daily, and this is expected to rise to over 375 billion per day by 2025.

Email remains popular for three reasons:

01 Standardization

Email is built on top of various official, public standards or so called RFCs, like SMTP, IMAP and many more. Standardizations enable vendors developing tools with unique features to be aligned to the needs of various users without impacting how the recipient receives the communication. This is similar to communicating by telephone; because of industry standards you can select the provider that best suits your needs without considering the underlying technology.

02 Simplicity

Most people in highly developed countries have an active email address. Today, the number of email users has already surpassed 4 billion and is projected by the Radicati research group to hit 4.6 billion by 2025. As the email ecosystem has matured, improving usability has become a bigger focus.

03 Habit

Until the emergence of WhatsApp, email was the only digital communication solution available to a mass audience. Due to its simplicity, it was widely adopted by users and businesses as their main form of digital communication. Although the limitations of email are well-known, the push to change the status quo is hindered by the fact that trying to get people to change habits is very difficult. With email, it's both the user and recipient who would need to adapt. When you must influence behavioral changes outside your own environment, it becomes much more challenging to implement.

Email and file transfer security, in a nutshell

According to Gartner's Market Guide for Email Security, "Email security refers collectively to the prediction, prevention, detection and response framework used to provide attack and access protection for email". Or, put more simply, anything to prevent data leaks related to the use of email.

IT-minded people tend to view email as the technology behind it, like SMTP. Preventing data leaks stemming from emails, however, means looking at email as a 'use case'; how do various people use it and for what purpose(s)?

When companies need 'secure email' they express the need to 'secure' (in their view) their way of working. This may include current communication tools for email, such as Outlook, O365 or Gmail, without any regard to the technology used. Sharing files, and therefore file transfer security, is fast becoming a vital component of the email use case.

Traditionally, most email vendors restricted attachment sizes to 10 MB per email. This meant that sharing large files necessitated the use of other platforms. With file size limits increasing, including up to 5TB with Zivver (essentially unlimited), users no longer need to switch platforms if they want to send a file that would normally exceed their email server limit. That's because with an integrated solution, people can send any type of file securely from their existing email client.

The reason why email security is a distinct topic is because email communication was not initially conceived with security concerns in mind. The first iterations of email came to life in the 60's, a time when security and privacy protection concerns were essentially nonexistent.

Since then, attempts have been made to improve the security of email, with transport encryption (STARTTLS), mail server authentication (DANE) and spoofing and spam protection (DMARC, SPF, and DKIM) becoming standards. Most of these features, however, are optional, they are not yet widely adopted and fail to address specific challenges such as phishing or user authentication. On top of this, these technical standards were not designed to mitigate the biggest cause of data leaks, which are mistakes made by people while emailing. These errors are bound to happen now and again, especially with people sending so many emails every day.

03

Mistakes in the financial sector happen

The financial sector will be at risk of breaches due to the vast amounts of sensitive information in their networks, but it's not always hackers causing the most damage. Instead it's often inadvertent mistakes by staff.

The New York Times reported in 2017 that 'Wells Fargo had turned over — by accident, according to the bank's lawyer — a vast trove of confidential information about tens of thousands of the bank's wealthiest clients.'

Instead of putting the sensitive information on a storage drive and then mishandling it, it could have instead been sent securely as a file transfer and with two-factor authentication in place to ensure only the intended recipient could access it. Plus, when sent securely with a file transfer solution, there would be the ability to revoke access if needed at any time.

Citigroup made a $900 million mistake by wiring funds to the wrong accounts

While an email data protection solution would not be used for this purpose, this costly error illustrates the severe consequences that can stem when there are no additional verifications on recipient identity, such as with the use of two-factor authentication.

Deutsche Bank made a similar mistake, to the tune of €26 billion in 2018 due to what the bank called an operational error. While they did manage to recover the funds, the share price of the banking giant took a hit of 25% during the year of the incident.

Data leaks and breaches also historically negatively impact share prices, although this can vary based on a number of factors, such as the scale and nature of the information that was breached. Email data protection solutions can help companies take a proactive approach to prevent incidents from occurring and share prices from tumbling.

Equifax forgot to update a server which led to the biggest financial sector breach to date

This massive breach was in 2017, when Equifax reported that hackers gained access to critical customer databases with sensitive information such as credit card numbers. The findings from the investigation? A single web server was running out-of-date software and this went undetected for 76 days, leading to the security breach. This was a costly mistake, while also putting hundreds of thousands of customers at risk with their personal information leaked. Their CEO, CIO and CSO resigned in the aftermath.

An American bank called Flagstar experienced a big breach in 2021 when hackers accessed their File Transfer Application software that was used to secure sensitive data.

In this case, the bank's sensitive data was put at risk with a vendor that maintained access to decryption keys within their infrastructure. When the vendor was compromised, so was the bank's data, which included customer social security numbers and many other types of personally identifiable information. A vendor that maintains these access keys can create additional risks by giving attackers another target to retrieve information. In this way, the bank would have benefitted with a different type of solution. Some email data protection solutions, such as Zivver, do not hold copies of decryption keys, which helps to minimize the risk of data falling into the wrong hands.

A system migration disaster forced this UK Bank's CEO to resign

TSB's online banking systems were disrupted for a week due to a botched system migration in 2018. Outcries from customers on social media went viral for people to close their account, and ultimately the incident cost the parent company in Spain, Sabadell, over €200 million.

04

The three core challenges of email security

To be able to improve email security, you first need to understand the range of challenges.

Email security can be grouped into three main categories:

- Threat protection; help to mitigate phishing, spam and malware attacks
- Email data protection; help to protect from unauthorized access to data sent or received by email
- Brand protection; help to ensure organization's email cannot be "spoofed"

Brand protection is mainly about implementing DMARC to avoid spoofing. As that is quite straightforward, this section focuses on explaining the difference between threat protection and email data protection.

The graphic below shows that email data protection involves various touchpoints at each stage of the communication's journey. This includes the process before, during and after sending an email, as well as upon receipt of an email (a reply for example).

Email threat protection, however, strictly entails the process of receiving email. That's why email data protection is so much more challenging than threat protection, as illustrated below.

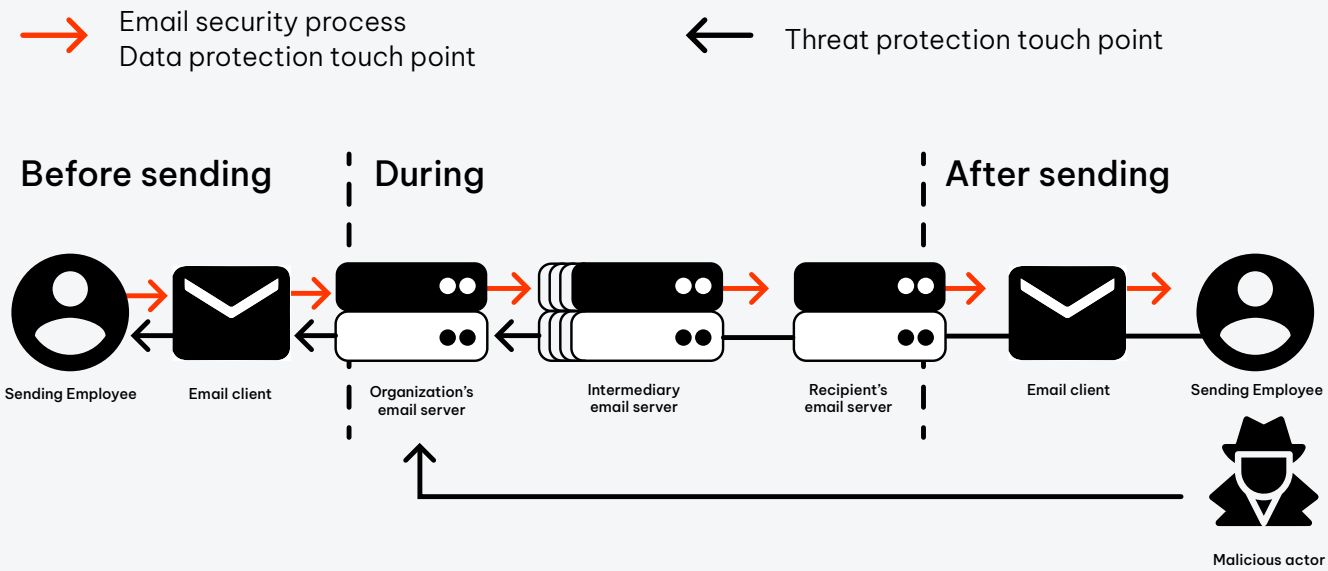
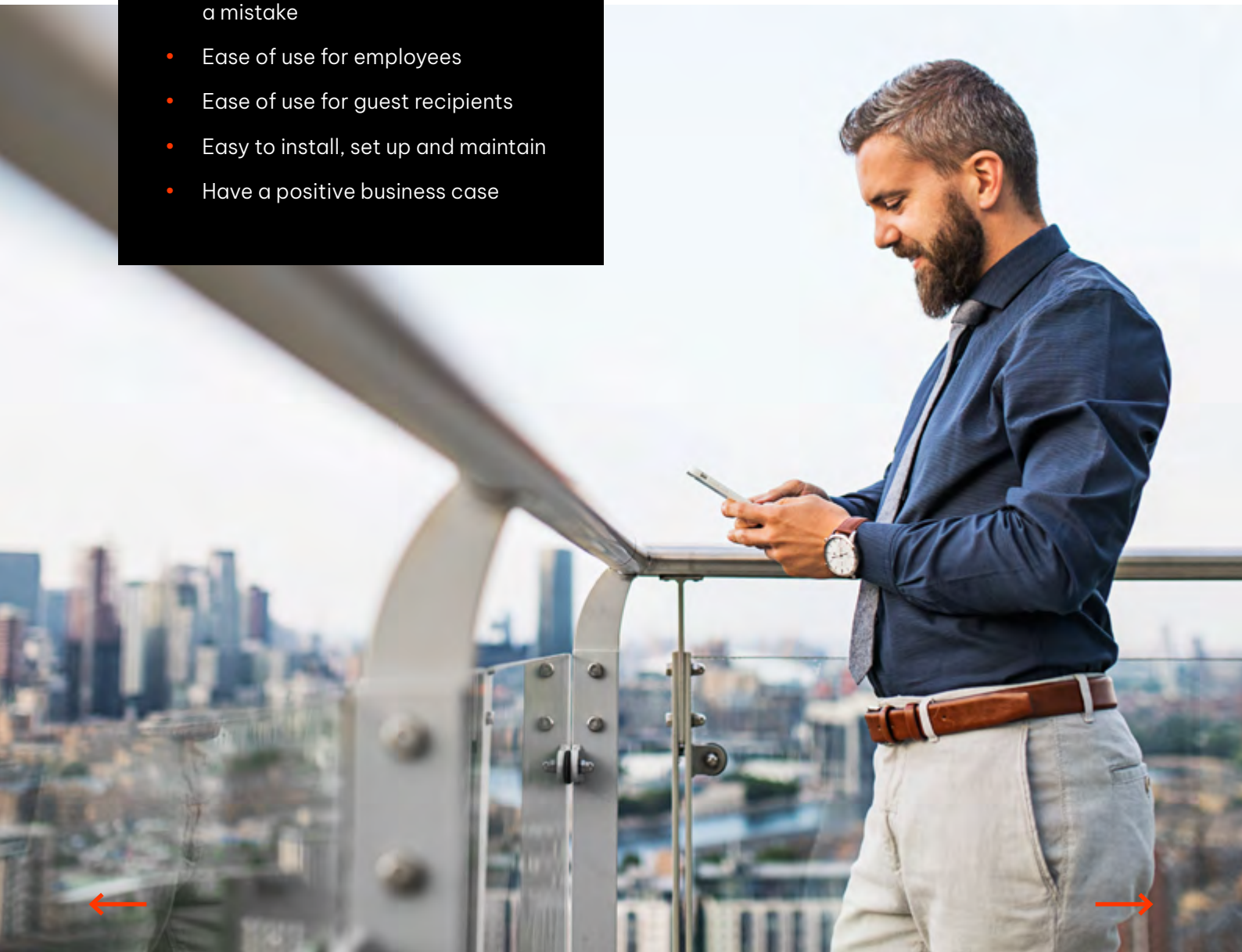


Figure 1: Schematic outline of the email process including security touchpoints

Below are the top challenges with email data protection that financial institutions are looking to solve by using supplementary tools or specialists that can enhance the security of Office 365, Gmail and other gateway based email systems.

- Prevent mistakes before emails and files have been sent
- Prevent interception of email data
- Prevent access by vendors and other third parties
- Prevent unauthorized access after delivery
- Limit and understand the impact of a mistake
- Ease of use for employees
- Ease of use for guest recipients
- Easy to install, set up and maintain
- Have a positive business case



05

How email data protection increases business value

Many people think of email security as protecting an organization from phishing, malware and hacking attempts, but as we've touched on already, this is no longer the biggest threat.

Preventing data leaks requires organizations to increase their focus on outbound email security, which includes preventing unauthorized access with two-factor authentication. If done in a way that is user-friendly, while also being simple to implement and maintain, financial organizations can unlock business value in areas including:

01

Increased productivity by using email instead of fax, snail mail or USB sticks

02

Cost savings generated by a reduction in the use of snail mail, USB sticks or couriers

03

Reduced need for costly and ineffective customer portals

04

Savings on the labour costs of manually copying information to a source system

05

Strengthening the brand (adding a company logo to each secure message that is sent, for example)

What this global financial institution did to minimize the risk of data leaks

Nationale-Nederlanden (NN) has been a leading name in financial services for over 175 years, operating in numerous countries with more than 25,000 employees. They were seeking to enhance their communication security and prevent data leaks with a solution that would enable them to email securely from Salesforce.

Alvin de Bock, Project and Implementation Manager at Nationale-Nederlanden said the following on the company's need to explore new solutions: ''The safe processing of personal data in 2021 must be in accordance with laws and regulations to guarantee the privacy of our customers and prospects. This includes provisions from the General Data Protection Regulation (GDPR) and the Code of Conduct for the Processing of Personal Data for Insurers. The complexity of our industry, combined with legislation and digitization, can make it challenging to take big leaps in digital transformation." The company opted to go with Zivver as their email data protection solution, in part because the solution could easily integrate with Salesforce. Mr. de Bock explained: "With Zivver, Nationale- Nederlanden can send prospects and customers information securely from Salesforce. In addition, an employee can choose whether or not to send the message securely (or as a "normal" email). After all, sending emails securely is not always necessary, but sometimes preferred or even mandatory."

This is a good example of a company looking in need of a solution to help them further digitize their communications, in this case it enabled them to do so from Salesforce in a secure and compliant way.

06

Why companies benefit from email data protection solutions

Although some solutions claim to offer email data protection, many companies find that they provide only a small piece of the puzzle and usually in a non-user and/or non-recipient friendly way.

For two consecutive years, Gartner has listed Zivver as a Representative Vendor for Email Data Protection (EDP) in 2021 Gartner Market Guide for Email Security. The exclusive REGTECH list helps senior management in financial services filter through vendors in the market by highlighting top companies for data and communication security. Zivver enhances a company's existing email infrastructure by adding a security and privacy layer on top of it. The service can be used with the biggest email clients (Outlook, Gmail, OWA) to increase employee awareness when handling sensitive data. Real time alerts help to prevent data leaks caused by human error, and users can also revoke messages if they do make a mistake.

This is further aided by strong encryption when data is in transit or at rest with zero-access guarantee. Additionally, the service provides out-of-the-box business rules for the financial sector and recipient authentication. All this makes installation, implementation and maintenance realistically achievable in a matter of hours or days, instead of months.

Maximize the ROI and reduce costs

In many cases, working with email data protection specialists can actually reduce costs. Products like Zivver are significantly cheaper than having to upgrade from Office 365 E3 to E5 licenses in order to improve email data protection in your organization. What's more, having these products in place enables you to reduce the costs of file transfer solutions and even cyber security insurance premium costs. The ROI usually lies between 2x-8x. And if you include reducing the use of letters, faxes and couriers, which are still used quite heavily across the financial sector, the ROI can easily be in the double digits.

If that isn't enough to consider working with an email data protection specialist, what is?

Zivver
59-60 Gainsborough House,
Thames Street Windsor,
Berkshire, SL4 1TX
United Kingdom

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

www.zivver.com