RESEARCH REPORT

Understanding common email fails: **Protecting against the insider threat**

Egress Software Technologies

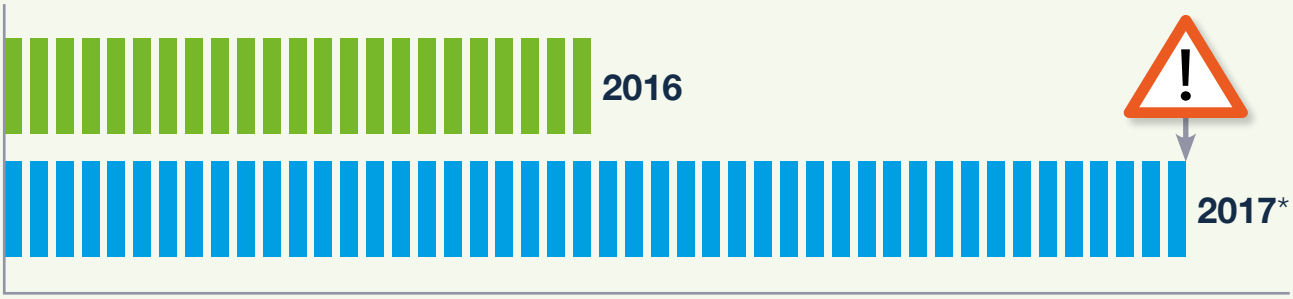
egress®

Introduction

This white paper is about the sinking feeling you get when you realise you've sent an email to the wrong person, attached the wrong file, or uploaded the wrong document to a file sharing site.

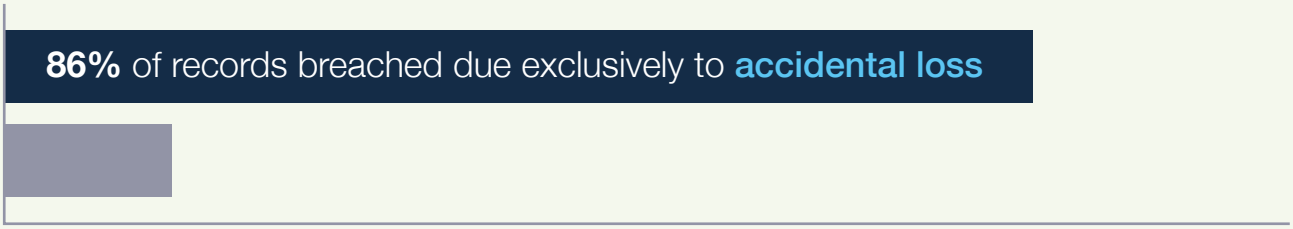
Whether they admit it or not, the majority of people will have experienced this head in hands moment at some point in their careers. The reality is, the easier we make it to share electronic files, the more likely it is that mistakes will happen. At the end of the day, we're only human…

Simple mistakes can have huge consequences. A data breach that results in a regulatory fine, or perhaps even worse, severe reputational damage can have a relatively simple cause - an email sent in error. At the end of the day, how would your customers feel if they discovered you hadn't taken adequate care over their data? Breaches are always serious, whether it's a single citizen's health record or massive amounts of corporate data. In fact, the most recent statistics published by the Breach Level Index, the system used to track global data breaches highlighted that in the first 6 months of 2017 there have been as many breaches, as the whole of 2016. Worse still, 86% of breached records were as a direct result of accidental loss and only four percent of breaches involved any level of encryption.

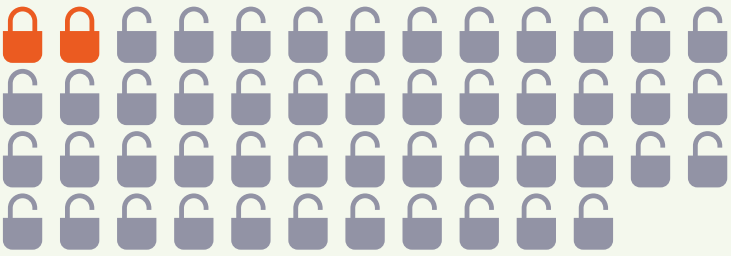


Average number of data records breached per month

*Year to July 2017



Data records breached



4% number of breaches utilising encryption

Every organisation worldwide handles commercially and personally sensitive data every day, so how should they go about mitigating the risk posed by their own people making mistakes?

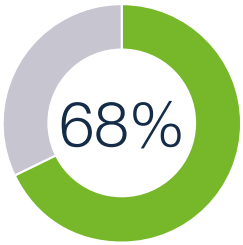
The wrong approach

Rightly concerned about the prevalence of data breaches, organisations everywhere continue to invest in data security solutions that protect their data and help them demonstrate compliance with regulations such as The Data Protection Act and the upcoming EU GDPR. Solutions ranging from firewalls, endpoint security and encryption to malware scanning, anti-virus software and password managers.

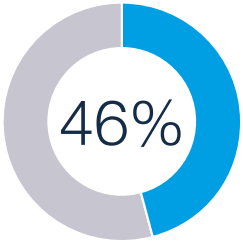
These solutions offer sophisticated security, and yet the data breaches continue to rise. The question is why?

The fact is that these solutions can't do anything when someone mistypes an email address, accidentally or intentionally sends an email to multiple recipients using To/Cc instead of Bcc, or adds the wrong person to a group email. This is because existing solutions don't interpret user behaviour, and so when someone inside the business makes a mistake (unintentional or otherwise) – there is no safety net, and indeed no way of even alerting them or an administrator that a mistake has been made.

1/3 of workers admit to sending an email to the wrong person



email send mistakes caused by **rushing**



email send mistakes caused by **autofill**

Research carried out by OnePoll on behalf of Egress Software Technologies shows the scale of the problem. More than one in three workers admitted to sending an email to the wrong person, whilst nearly half (46%) have received information clearly intended for someone else. Of those making mistakes, 68% listed rushing as the reason, whilst 46% explained that autofill caused the error.

The research shows that not all leaks are accidental. In fact, one in four admitted they had maliciously leaked business data, whilst half of respondents said they either had or would delete emails from their sent folders if they had sent information somewhere they shouldn't.

25% of workers have **maliciously** leaked business data

50% of workers would **delete emails** to hide evidence

The facts about misaddressed emails

35%
have sent to the wrong person

One in four workers have **maliciously leaked** business data

20% increase in data sent by email to the incorrect recipient

Half of respondents admitted they had or would **delete emails** if they had sent data somewhere they shouldn't

Over 1.6bn records stolen as a result of accidental breaches in the first half of 2017 (**86% of all records taken**)

<1% of lost records were encrypted

One in two have received information clearly intended for someone else

42% of mistakes were caused by the **autofill on email**

More records were lost in the first half of 2017 than the **whole of 2016**

40% accidentally sent emails containing an **insult** about the recipient or a **rude joke**

In the UK, the number of records breached **rose by 130%** from H2 2016

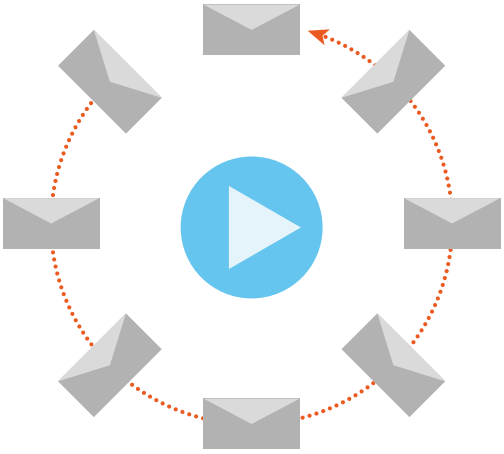
68% of mistakes were down to **rushing**

Sources: 2017 Global Breach Level Index, OnePoll survey and ICO Data Security Trends 2016-17

The right approach

So that's the scale of the problem, but what can we do about it? Accidents happen. How can we prevent something caused by human error and therefore unpredictable, related to whether a user has had enough sleep, or if it's near lunch time?

What's key is the realisation that while accidents do happen, people get things right most of the time.



Step one: Gather historic data

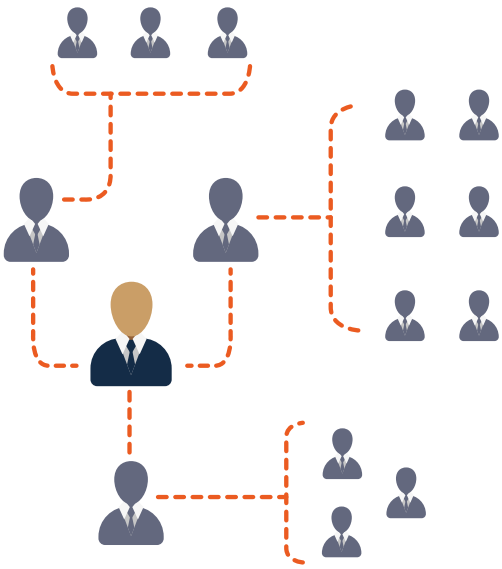
Looking at a user's past email and file sharing behaviour can provide an insight into when they've sent data to the right people with the right protection applied.

Once you understand this, you can start to tackle the insider threat by gathering and analysing data on who people usually send emails to and share files with, including multiple recipients in group contexts.

You need a system that captures the metadata of these email interactions, both feeding in historic data and recording it in real-time. Useful metadata includes senders, recipients and groups that appear in email threads together regularly (think the company board, or the finance team). This email metadata, appropriately stored, is a vital source of information for predicting future user behaviour.

Step two: Build a network

You can use information about who has been sharing with whom to build a network of interactions.



Using big data analysis tools and machine learning techniques, crunch the numbers and create a network showing common interactions and contexts, for example, the fact that Bob1, Alice and John email each other often, but Bob2, Alice and John are never found in an email thread together.

Big data analysis helps construct these networks by taking in the historic user data and aggregating it. Machine learning comes in when you need to build probabilities around how people share. For example, working out how probable it is that Alice and John would include Bob2 in an email, compared to when they would include Bob1. The answer: not very probable.

The ground-breaking aspect of machine learning technology is the fact that it automatically improves over time. The more data that is fed into the system, the better the system becomes at analysing behaviour patterns and predicting when mistakes are about to be made. So the more often people send emails accurately, the better the system gets at understanding what incorrect recipients look like.

Step three: Engage the user

Once the system has discovered a potential mistake, basing the decision on historic data, it's vital then that the end-user is alerted before they hit Send. A warning and a recommendation of an intended recipient (in this case Bob1) is enough to help the user make a better decision and address the email or file share to the right people. This could be a relatively innocuous email discussion, but it could also be sharing highly sensitive data. Engaging the user in an unobtrusive way is key here.

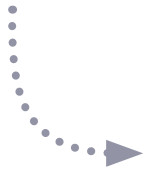
It's true, the concept of machine learning has been mentioned a lot recently as the Next Big Thing, and buzz words have a tendency to overpromise and underdeliver. The problem of misaddressed emails though, is a scenario where we can finally fulfill the potential of machine learning technology, providing real results and tackling a previously insurmountable problem.

Crucial parts of this solution are methods for securely storing email metadata even if the email has been encrypted, an advanced machine learning system that gets better over time, and an engaging interface for end-users that provides both alerts and accurate recommendations.

Five types of email sending mistakes, and how the right technology can prevent them

1. Accidental send

Sending to the wrong person in a certain context. Based on the other recipients in the message or file share, effective machine learning can highlight where a user has accidentally added the wrong recipient, perhaps someone with the same first name as the intended recipient. This common mistake, often due to autocomplete features in email clients, would be impossible to fix without a system that can effectively analyse and model historic interactions.

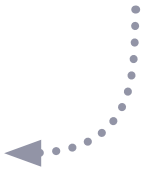


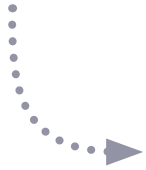
2. Mistyped recipients

It's all too easy to spell names wrong when addressing emails, whether it's the recipient name or email domain name. While it often might simply lead to a bounce-back, one can envisage a situation where a phishing attack has used a slightly modified domain name and pretended to be an internal employee (Bob.Smith@company.com vs Bob.Smith@conpany.com). Luckily, if a user goes to reply to an email of this kind – perhaps a request for financial details – the system could recognise the mistake and warn the user.

3. Forgotten recipients

If you usually send to a specific group of people (e.g. the company board or a customer and third-party stakeholder) but forget to add someone, effective tech can let you know and recommend the right person to add.





4. The first send to an unknown recipient

Obviously, if this machine learning solution bases its decisions on historic data, sending to a new recipient wouldn't have any past data to draw on. Hence, if you're sharing with a specific recipient for the first time, there should be an option to warn the user before they send, encouraging double-checking of the recipient address. Again, this would be effective in cases where a user is about to inadvertently reply to a potential phishing email.

5. Using To and Cc instead of Bcc

When sharing data with multiple recipients it can be vital to put the recipients in the Bcc field, rather than To or Cc. A recent example of a failure to do this involved sending a newsletter about sensitive medical topics to multiple recipients but leaving the recipients in the To field, revealing the identities of all the recipients to each other. Large fines were levied, but probably more damaging was the media coverage and ensuing reputation loss. This error could have been avoided by simply alerting the sender to the fact before they sent the email, a warning as simple as "Have you thought about putting these recipients in the Bcc field?" Of course, it may not be necessary to use Bcc if all the recipients are known to each other – if they are in the same company – but appropriate technology can analyse the recipient domains and suggest Bcc in cases where many different recipient domains are present.

These mistakes probably cause a wince of recognition in most, if not all, email users. However, the fact that there is a way to avoid the embarrassment, fines and reputational damage should be very encouraging, especially when considering the new challenges that data protection reform presents for data security and compliance.

Stop sending emails to the wrong people, start achieving compliance

That sinking email you get when you realise you've sent an email to the wrong person? With the advent of EU GDPR in 2018, that feeling is about to get worse.

Financial penalties in case of a data breach are set to increase to up to 4% of annual worldwide turnover or 20 million euros, whichever is greater. It will also be mandatory to report these data breaches to the relevant authority, and that's before the incident becomes reported in the media.

Investing in solutions that stop external attackers from stealing sensitive business and citizen data is the right thing to do, but it's not the whole story. When the stakes are this high, minimising the threat posed by an organisation's own employees is crucial, and preventing the accidental send should be high up the list of any organisation's data security priorities.

Despite the difficult nature of the problem, with intelligently applied machine learning and big data analysis, misaddressed emails and the insider threat can become a thing of the past.

GDPR penalties

4% of worldwide annual turnover

€20 million euros

Egress Software Technologies Ltd

Egress Software Technologies is the leading provider of security services that protect shared information throughout its lifecycle, delivered using a single platform: Egress Switch.

The award-winning Switch Platform includes email and document classification, email and file encryption, secure managed file transfer, secure online collaboration, and secure email and file archiving.

www.egress.com

info@egress.com
0844 800 0172
@EgressSwitch