REPORT

egress

## EMAIL DLP 2020 INSIGHT REPORT

# Your guide to the latest breach mitigation technology

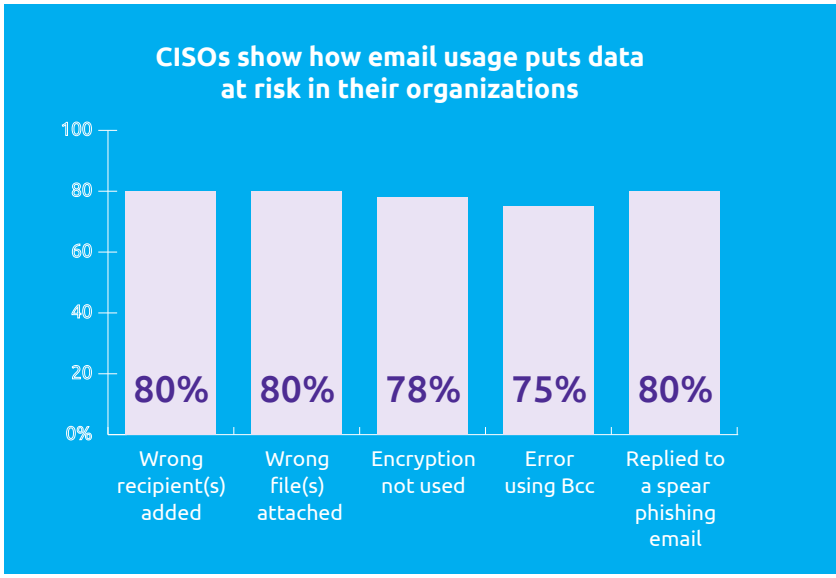
Data breaches caused by outbound email are prolific. In the last 12 months, 93% of organizations experienced security incidents where email use has put sensitive data at risk. And these aren't one-off occurrences. In fact, an organization of just 250 employees experiences an average of 180 incidents per year that put sensitive data at risk. That's one every 12 working hours.

### Why do people cause data breaches when using email?

Outbound email data breaches are driven by people's behavior. Research shows that there's no one leading cause of incidents, but an alarmingly high number across a variety of use cases – and most of the time, they're happening as people simply use email to get their jobs done.

Some of these instances are purely accidental, while others have a level of non-malicious intent behind them.

At the top of list are three common mistakes:




#### 1. Adding the wrong recipient(s)

Ironically, the productivity tool autocomplete, found as default in popular email clients like Microsoft Outlook, is a major culprit behind misdirected emails, where the sender adds the wrong recipient. Adding recipients is normally perceived as the easiest part of sending an email versus crafting the message itself, and these incidents usually frequently occur when employees are tired, stressed or rushing.

#### 2. Attaching the wrong files

Similar to adding incorrect recipients, these breaches occur when content is shared with unauthorized recipients. This can include attaching the wrong file outright or the sender forgetting to check different tabs or hidden cells in a spreadsheet. Again, attaching documents is often seen as a straightforward part of sending an email and not something that requires a great amount of attention to detail, so there's significant margin for error.

> "An organization of just 250 employees will have 180 incidents per year. That's one every 12 hours."
>
> OUTBOUND EMAIL SECURITY REPORT 2020

### 3. Replying to a spear phishing attack

As spear phishing attacks are, by nature, often highly targeted, these incidents often happen to newer employees (who are eager to respond to requests from "senior managers" or those who have access to the most valuable data (for example, HR or Finance personnel). Use of mobile devices that don't display full screen names can exacerbate this issue, with recipients unable to see who they're replying to.

"Ironically, the productivity tool autocomplete is a major culprit behind misdirected emails."

## Static DLP can't mitigate outbound email data breaches

With 93% of organizations experiencing these security incidents every year, and an average of 180 breaches taking place in businesses of only 250 employees, it's clear to see that the approach taken to date is unable to properly mitigate human-activated risks caused by people's behavior.

Traditional email DLP technologies are built using static rules based on security policies, designed to either force encryption of sensitive information or prevent it leaving the organization altogether. For example, in law firms, policies could be linked to a client ID or a specific case matter number. The problem is that these approaches focus predominantly on data sensitivity, rather than the context of an individual sharing information, potentially with the wrong recipient.

Thinking about this in context, we can create a scenario where Person A from Company 1 needs to regularly share sensitive data with Person B at Company 2, but on this occasion, accidentally adds Person C from Company 2 instead because they have a similar name or email address as Person B. Unfortunately, Person C isn't authorized to see the data that's been shared with them and a security incident has occurred.

Static rules wouldn't work at scale across Company 1 to prevent this incident.

Rules can be set up to allow Person A to share data with Company 2's domain – but as both Person B and Person C work there, the rule would allow this email to be sent. It's possible, but not practical, for Person A's IT administrator to create allow / block lists that are tailored to Person A – but the level of granularity required make this an impossible overhead to manage.

Alternatively, Person A could receive a prompt to approve their email recipient(s) every time they send any emails or share certain types of data. However, solutions that utilize this functionality rapidly create "click fatigue" within their uses bases, who naturally begin to operate on autopilot and approve requests without thoroughly checking them.

The same principles apply across various scenarios that lead to email data breaches – from adding a recipient into an email chain that contains sensitive data they're not authorized to see further down, to forwarding emails, attaching the wrong documents, or replying to a spear phishing attack.

Static email DLP technologies were never designed to mitigate risk at the volume we currently use email or what we use it for.

"Static DLP focuses predominantly on data sensitivity, rather than the context of an individual sharing information."

## What's the impact of static DLP not mitigating these risks?

When sensitive data is put at significant risk due to outbound email, there are impacts for both the organization and the individual sender.

At an organizational-level, one-third of CISOs have reported that their company suffered financial repercussions from fines and customer churn; 26% reported reputational damage; and 26% also reported their business was investigated by a regular, consuming their Security team's time in remediation.

> "Static email DLP technologies were never designed to mitigate risk at the volume we currently use email or what we use it for."

For the senders themselves, almost half (46%) received a formal warning or reprimand; in 27% of incidents, the employee responsible was fired; and in 28%, legal action was taken against the employee.

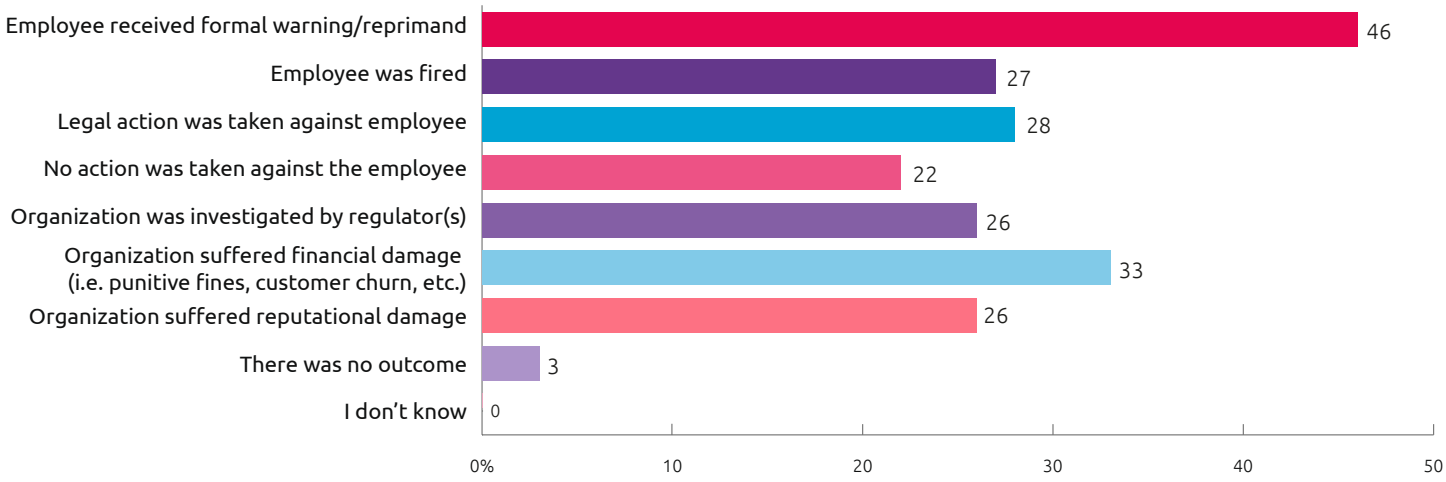
At the frequency with which outbound email data breaches occur, serious incidents and their impacts mount up to create significant operational and security risks to businesses.

## Contextual machine learning is the new face of email DLP

Advances in machine learning have revolutionized email DLP technology over the last few years. By being able to deeply understand an individual user's behavior and relationships when using email, and by inspecting the content contained in message body and attachments, this technology can create context around authorized data sharing scenarios and those where abnormal behaviors put data at risk.

This is all carried out in real time, meaning the solution is constantly learning and adapting based on users' interactions, with new rules being created without administrative overheads.

**CISOs reveal the outcomes of their most serious email data breach in the last 12 months**



## Stopping email data breaches before they happen

Egress Prevent part of the Egress Intelligent Email Security Platform utilizes contextual machine learning in three core areas to:

### Continuously understand a user's behavior

**We use Bayesian inference models to continuously update our risk assessments as more information about users becomes available, which means we're able to build genuine context around who employees communicate with and what data they should be sharing.**

### Assess relationship strength

**We deploy graph databases to map out and interrogate the strength of a user's relationships in order to detect anomalies, such as adding an incorrect recipient or attaching the wrong document.**

### Monitor time patterns

**With Gaussian mixture models, we're able to understand access patterns that are specific to each user, and flag when their behavior deviates from "the norm" and a breach is about to occur.**

## Your next steps to stop outbound email data breaches

### Analyze your risk with Egress Investigate 365

A completely free audit tool, Investigate 365 plugs into your Microsoft 365 or Exchange environment to analyze 12 months of email data, detecting misdirected emails (incorrect recipients and attachments), DLP policy violations, and instances of unverified TLS.

### Talk to the team about Egress Intelligent Email Security

The Egress Team would be happy to discuss how we can help your organization. Our technology wraps a protective layer around individual users to stop human-activated data breaches before they happen. Our Intelligent Email Security prevents accidental and intentional security incidents, protects sensitive data relative to risk, and equips CISOs and their teams with the detailed reporting required for compliance purposes.

## About Egress

Our vision is for a connected world in which people communicate efficiently and securely. To achieve this, we wrap a protective layer around individual users to stop human-activated data breaches before they happen. Our patented technologies are built using leading-edge contextual machine learning and powerful encryption that mitigate modern risks in ways that other solutions simply can't achieve.

**www.egress.com** | info@egress.com | 1-800-732-0746 | @EgressSoftware