knowbe4

CISO STRATEGY GUIDE

Preventing Human Error On Email

Solving Misdirected Emails and Files in Microsoft 365

WWW.KNOWBE4.COM

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | Email: Sales@KnowBe4.com

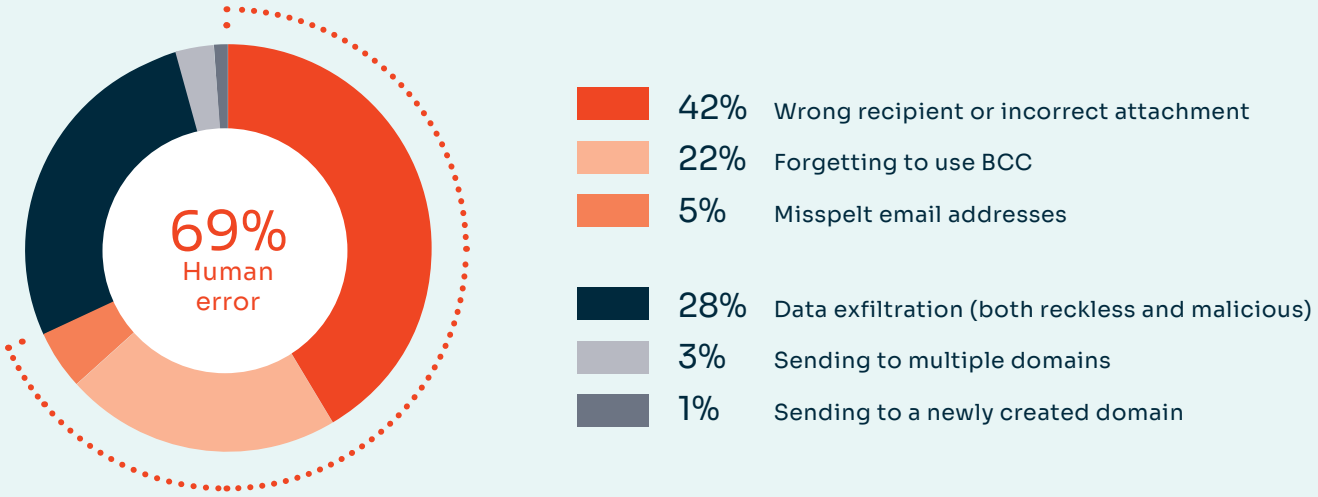
0925US

Introduction

Email has the highest risk of data loss than any other form of business communication. Employees use email more than any other channel, especially when sharing confidential or privileged information,[1] creating a significant surface area for incidents to occur. Email has also benefitted from productivity enhancements, such as Microsoft Outlook autocomplete and integration with mobile devices for round-the-clock, on-the-go communication. While the fast, free-flowing exchange of information enabled by email is critical for businesses, these productivity tools only widen the surface area for risk.

Ninety-one percent of the organizations surveyed for KnowBe4's Email Security Risk Report experienced outbound email data breaches in their Microsoft 365 environment. Platform data from KnowBe4 Prevent reveals that human error is the most common trigger for its real-time data loss prevention (DLP) prompts.

Platform Data From KnowBe4 Prevent Reveals Human Error Is the Most Common DLP Trigger



Human error is virtually impossible to prevent using traditional static DLP rules and solutions, which are too rigid for the fast-paced, flexible way people use email. Consequently, security measures are dialed back in favor of decreasing user friction and increasing efficiency. Additionally, these solutions can over-prompt users, causing click fatigue. Relying on people to detect their own mistakes is also ineffective. By their nature, mistakes are unintentional, so typically the error is detected by the email recipient rather than the sender.

As the reporting loop for email data loss relies on the recipient(s) to notice the mistake and then notify the sender, and then for the sender to notify the organization, the issue is on average 10 times worse than the security team realizes.

1 Independent research conducted for the KnowBe4 Data Loss Prevention Report found that 85% of employees are using email now more than ever, while 80% say they use it to regularly share confidential information.

The Psychology of Human Error on Email

The causes of human error can be broken into four major categories, all of which can lead to email data loss.

Skills-Based Errors

Slip Errors

This is the category people most commonly think of when considering human error and email data loss. Slip errors occur when a person intends to do one thing but instead ends up doing something else. For example, the person sending an email intended to add 'John Smith' to the 'To' field but accidentally selects 'John Small' from the Outlook autocomplete dropdown.

It's difficult for people to identify slip errors in the moment because they believe they have carried out the action correctly and are entirely unaware of their mistake.

Lapses In Memory

Caused by short-term memory loss, inattention or lapses in concentration. They are not related to training, experience, or motivation levels but are significantly impacted by environmental pressures.

When people are stressed or under pressure, they operate in Type 1 thinking. People in this state act fast and unconsciously, relying on "gut feeling," and therefore are more error prone. Often, people might realize their mistakes later, when they are less pressured and in a more logical frame of mind (Type 2 thinking). As email clients are designed to enable productive, intuitive use, people operating in Type 1 thinking are more likely to add incorrect recipients or make other mistakes because they are concentrating on sending the email by a specific deadline.

Information-Based Errors

Knowledge-Based Mistakes

The person simply does not have enough information to make a better decision. These types of errors are frequently attributed to a lack of training or communication but can also be influenced by whether the person was engaged with the training or communication or told in a way that enabled them to retain this information.

Knowledge-based mistakes lead to unauthorized access to data shared by email because the sender "did not know" the recipient(s) should not receive it.

Rule-Based Mistakes

The person's actions match their intentions, but a security incident still occurs because of the incorrect application of a rule. A rule can be something formally implemented by an organization, something someone was taught or told informally, or something they came up with on their own.

While people can intentionally break the rules, when it comes to human error, rules-based mistakes happen because of a change in the rules (which can be badly communicated or forgotten) or from an inability to apply the rules correctly.

How Does Email Data Loss Happen?

Misdirected Emails

Composing the email message is perceived as the more significant task, so people apply a greater level of cognitive energy to this part of the process. They spend time ensuring tone and word choices are correct and proof-reading for mistakes. Selecting recipients is seen as the “easier” part of the task — after all, from the beginning, the person knows exactly who they want to send the email to. Concentration can lapse and less attention is paid when selecting the recipients.

The role of Outlook autocomplete: While it can save time and prevent errors versus typing full email addresses for each recipient, Outlook autocomplete makes it easier for people to select the wrong address, particularly when choosing between people with similar names.

Misspelt or Mistyped Email Addresses

Closely linked to misdirected emails, these incidents arise when an email address has been manually inputted incorrectly. At best, they are inefficient and result in a bounce back because the email address doesn’t exist. At worst, and particularly when emailing freemail addresses, content is shared with an unauthorized recipient.

These incidents are more common at organizations that have disabled Outlook autocomplete in an effort to prevent misdirected emails.

Mis-Attached Files

In this scenario, the email recipients are correct but the wrong attachments have been selected, or there is other data contained within the attachments that recipients are not authorized to access.

Failure To Use BCC

People use email intuitively, so it is natural to include recipients in the ”To” field as it is more frequently used than the “BCC” field. However, failure to use the ”BCC” field can expose large recipient lists to each others’ email addresses, which can be cross-referenced with content in the email body to link them with confidential information or protected characteristics.

Increased Risk On Mobile Devices

Seventy-two percent of CISOs at organizations using Microsoft 365 think employees are more likely to leak data by email when they are using a mobile device.[2] Small screens make it easier to select the wrong recipient or file, and harder to spot the mistake once it has been made. Additionally, employees accessing emails out of hours are less likely to be fully focused on what they are doing and more likely to be tired, both of which can lead to mistakes being made.

2 KnowBe4 Data Loss Prevention Report

The Impact of Email Data Loss

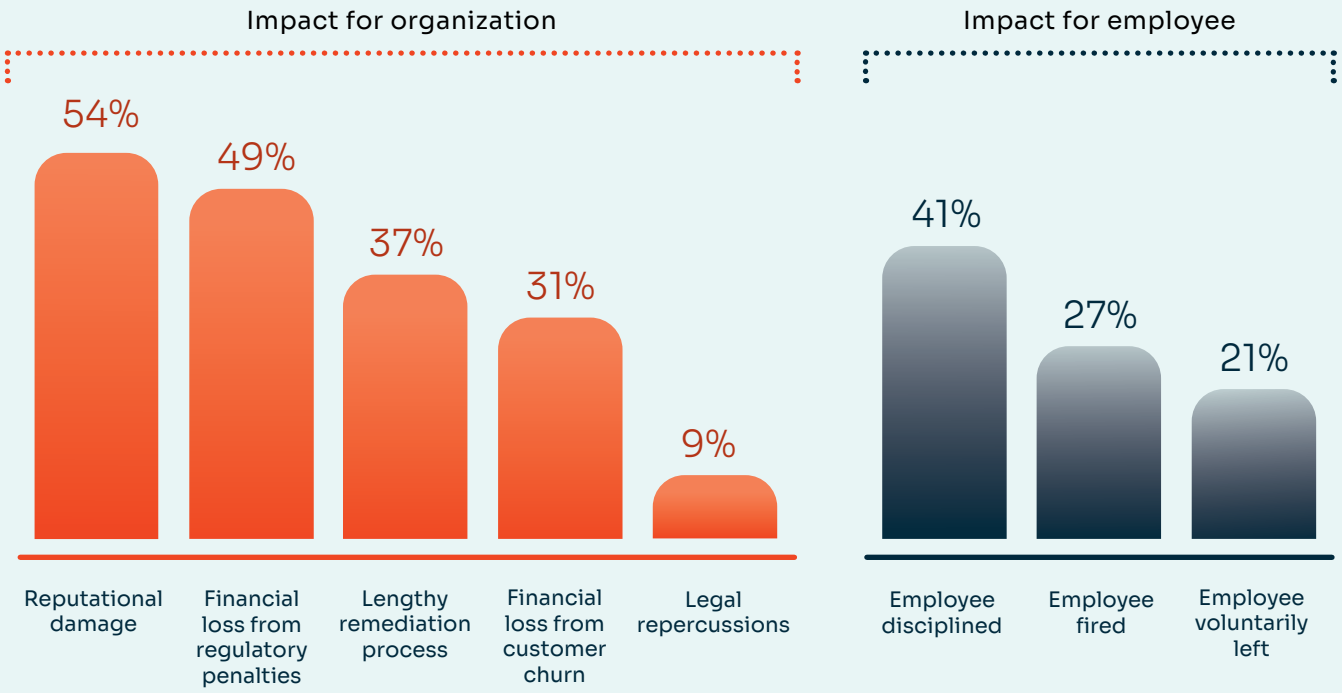
Independent research shows that 86% of organizations have suffered negative impacts following an outbound email data breach. These impacts affect both the organization as a whole and the individual employee involved.

For over half of organizations (54%), the most common impact was reputational damage. Even when security incidents are kept out of the headlines, clients and data subjects must be informed. While human error is universal to every organization, outbound email security incidents are often interpreted as careless or negligent because keeping email communication private is a fundamental, basic requirement of supplier-client relationships. In competitive markets, reputation is key to securing clients' investments and misdirected emails can damage trust and lead to churn, which happened in almost one-third of organizations (31%).

For the employees involved in these security incidents, disciplinary action was the top standalone outcome. While organizations need to respond to deliberate acts and even repeat offenders who make the same mistake, punishing human error can often have an adverse effect on security culture. If people believe they will be disciplined for owning up to a mistake, they can delay notification or underplay the severity of the incident, impacting response times, or even not report the incident altogether.

Email data loss also results in a loss of talent. Employees left 48% of the surveyed organizations as a direct result of an outbound email security incident, either through dismissal (27%) or because they voluntarily left (21%), with organizations needing to fill skills gaps that arise from simple mistakes.

Cybersecurity Leaders Share How Outbound Email Security Incidents Have Impacted their Organizations



The Limitations of Static Rules-Based Email DLP

Traditional email DLP solutions rely on static rules to prevent data loss. These solutions, however, take a data-led approach to security, rather than a behavior-based approach, and therefore cannot dynamically respond to the way people use email on a day-to-day basis. Unable to take context and individual behavior patterns into account, rules-based DLP solutions lead to either sprawling and unworkable policies, or a dialing back of security to reduce user friction and increase efficiency. Alternatively, they push detection onto the user, for example prompting them to acknowledge every recipient and every email they send.

They Cannot Scale To Provide Granular DLP Across the Organization

Static DLP rules can only be implemented across groups within an organization, rather than on an individual level. The rule must work for everyone or it works for no-one. Administrators cannot be expected to create and maintain multiple rules for each individual, but instead can only apply blanket policies.

The finance team, for example, might have freemail domains blocklisted but the sales team frequently contact clients on these email addresses. As soon as the policy becomes unworkable for even one person within the finance team, however, it is usually scaled back or removed entirely rather than create individual exceptions.

They Create User Friction

Rules that negatively affect employees' productivity create friction. If, for example, the organization blocks emails to a specific domain but an employee has a legitimate reason for contacting someone on that domain, business productivity is impacted while the rule is amended. Too many scenarios like this occurring results in a lowering of security measures across the organization.

They Cannot Predict the Unpredictable — or, They Are Only As Good As Their Inputs

Human error is unpredictable, which is why it remains a problem we have not solved. It is implausible for solution vendors and organizations' administrators to correctly anticipate and map out the myriad different ways data can be leaked via email for each individual organization to implement static rules. Consequently, there will always be use cases they do not cater for.

They Lead To Click Fatigue

Solutions that push detection onto the users by prompting them on every email they send lead to click fatigue. People may initially engage with the prompt to check their recipients, however the more frequently they approve correct recipients, the less attention they will pay to the prompt. Over time, they will become unconsciously biased about the correct recipients they included in their previous emails and consequently over-confident that they have not made a mistake this time. People may also click through prompts when in a rush or under pressure, not taking the time to check their recipients.

They Are Admin-Intensive

Building and maintaining rules, keyword libraries and data classifications and tags takes time and resources. Combined with static DLP's inability to scale across an organization, these solutions become a drain on security teams without offering sufficient assurances or benefits.

Strategic CISO: Deploying AI in the Inbox To Stop Human Error

Protecting organizations from outbound email security incidents caused by human error requires a new approach that leverages intelligent technology.

Machine Learning for Dynamic Risk Analysis

Combining unsupervised and supervised machine learning enables organizations to deliver email DLP at scale across the organization, accounting for a significantly higher number of security use cases than static rules-based solutions can deliver.

Unsupervised machine learning analyzes and clusters data created as people use email. A self-leaning technology, it can understand patterns in email use to detect anomalies in real time. The technology is informed by the context in which people send emails, including the recipients and groups of recipients they contact, and the content they share.

Supervised machine learning leverages policy engines and organizational rules set by administrators to increase the number of use cases that unsupervised machine learning can meet on its own. This supervision also mitigates the likelihood that the unsupervised machine learning will be incorrectly informed by users.

Behavior-Based Email Security That Can Account for Context

Unlike static rules-based solutions, intelligent email DLP can understand each individual user's behavior to deliver security at a granular level. Social graph databases are used to analyze each user's relationships, establishing their strength and interaction patterns, to enable identification of new or abnormal behaviors as an email is being composed.

In-the-Moment Prompts When Risk is Detected

Prompts should only be delivered when risk is detected, reducing click fatigue and increasing the solution's value to employees. These real-time alerts "nudge" people away from risk, allowing them to correct their mistakes before an email is sent and a security incident occurs, and provide in-the-moment education that augments security awareness and training programs.

Stop Outbound Email Data Breaches With KnowBe4 Prevent

Learn how KnowBe4 Prevent uses machine learning to protect an organization's most sensitive assets by ensuring only the right data is sent to the right person and with the appropriate level of security.

Want to Learn More About How To Prevent Human Error in Your Organization?

Request Your Personalized Demo

Request Demo

See How We Stop Misdirected Emails

Learn More

About KnowBe4

KnowBe4 empowers workforces to make smarter security decisions every day. Trusted by over 70,000 organizations worldwide, KnowBe4 helps to strengthen security culture and manage human risk.

KnowBe4 offers a comprehensive AI-driven "best-of-suite" platform for human risk management, creating an adaptive defense layer that fortifies user behavior against the latest cybersecurity threats. The HRM+ platform includes modules for awareness and compliance training, cloud email security, real-time coaching, crowdsourced anti-phishing, AI Defense Agents and more.

As the only global security platform of its kind, KnowBe4 utilizes personalized and relevant cybersecurity protection content, tools and techniques to mobilize workforces to transform from the largest attack surface to an organization's biggest asset. For more information, please visit www.KnowBe4.com

knowbe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com