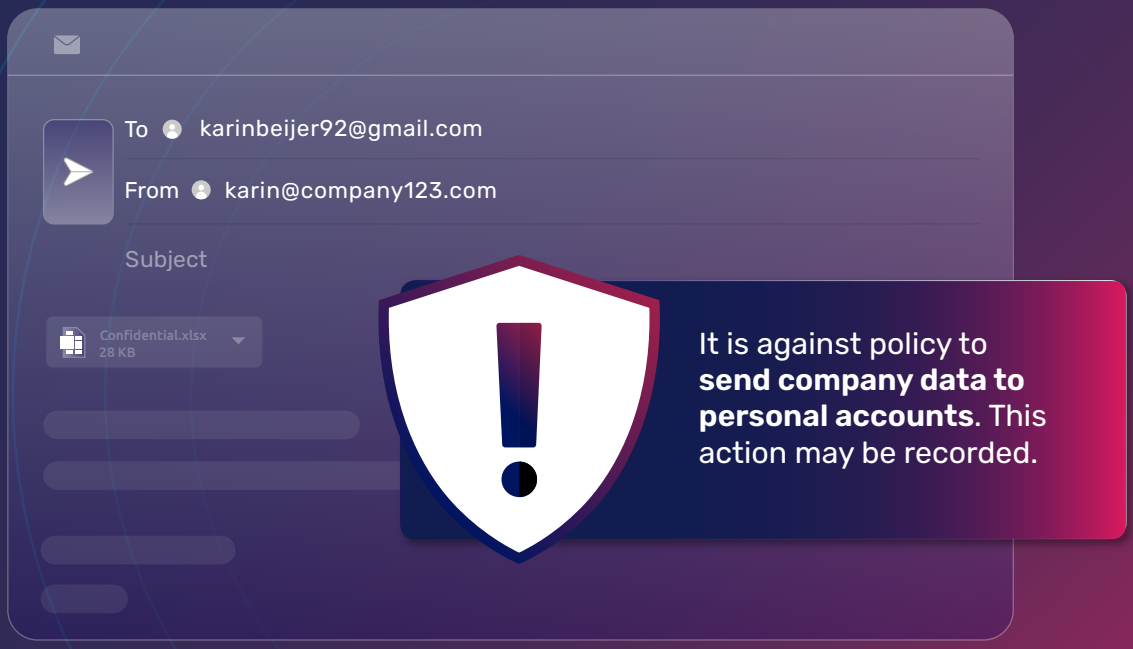
egress
a KnowBe4 company

northdoor
Store IT ◦ Protect IT ◦ Use IT

CISO STRATEGY GUIDE

Data exfiltration over email

How to detect intentional exfiltration in Microsoft 365



The persistent challenge of data exfiltration over email

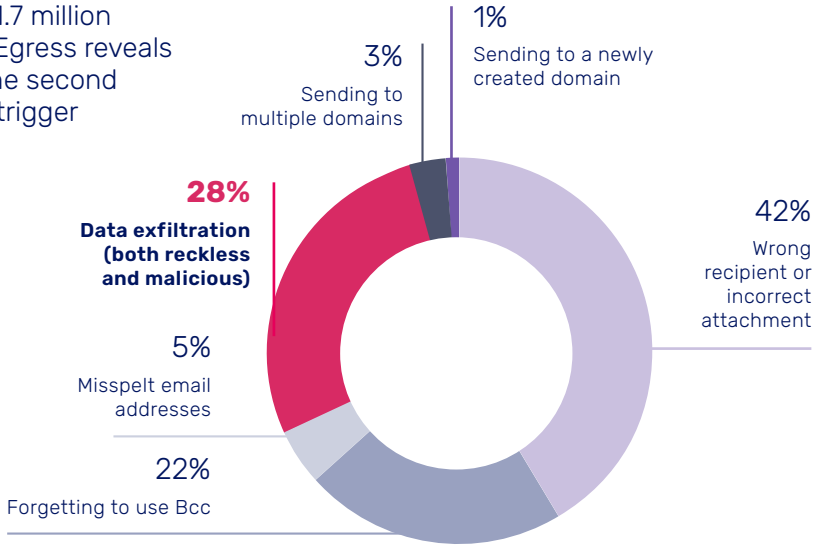
Data exfiltration over email is among the most elusive threats that organizations face, and it's a widespread issue. In fact, Egress' 2024 Email Security Risk Report revealed that 94% of organizations report experiencing data loss and exfiltration within their Microsoft 365 environment, with 91% suffering significant fallout as a result.[1]

Often, data exfiltration occurs when reckless or malicious employees send sensitive information such as client lists or financial records to personal email addresses, exposing businesses to severe risk. This type of intentional rule-breaking by employees is frequently cited by Cybersecurity leaders as the leading cause of data loss in organizations. Reflecting this trend, reckless and malicious exfiltration is the second most common Data Loss Prevention (DLP) trigger in Egress Prevent, accounting for 28% of incidents.[2]

Traditional defenses, such as solutions that use static DLP rules, fall short in mitigating this issue. Despite 94% of organizations relying on static email DLP rules, these strategies struggle to scale and fail to detect real-time threats among the thousands of legitimate communications exchanged daily. Consequently, these outdated methods are inherently reactive, depending too heavily on the manual review of audit logs to identify data exfiltration after the damage has already been done.[3]

To protect sensitive information from data exfiltration by email, businesses must adopt more AI-powered defenses that can go beyond relying on static rules alone.

Platform data from 1.7 million emails analyzed by Egress reveals data exfiltration is the second most common DLP trigger



1, 3 2024 Email Security Risk Report, Egress

2 2024 Email Security Risk Report, Egress

The psychology behind exfiltration: Understanding malicious and reckless employee behavior

Unlike human error-related incidents over email, every instance of outbound data exfiltration involves a varying degree of intent, whether it is the mishandling of information by a well-meaning employee or the deliberate actions of a malicious insider.

To understand the intention behind data exfiltration, there are four key psychological factors that need to be considered.

Decision latitude
The level of freedom organizations give employees to make decisions and act independently.

Dunning-Kruger effect
The theory that a person with a small amount of knowledge or training has a heightened level of confidence about their abilities.

Social proof
Copying the actions of others, especially in uncertain or ambiguous situations, or to fit in with the group.

Cost-benefit analysis
Analyzing whether the benefit to the individual or organization is perceived to outweigh the risk.

The malicious insider

This is typically an individual within the organization who deliberately exfiltrates sensitive data to cause harm or exploit it for personal gain. Their motivations can vary widely but may include personal grievances, such as a disgruntled employee seeking revenge or someone looking to sabotage the company's reputation. Additionally, career transitions can drive this behavior, where an employee may exfiltrate sensitive information to gain a competitive advantage in their new job.

Malicious insiders with a high degree of decision latitude can make independent security decisions with minimal oversight, allowing them to exfiltrate data with little risk of detection. Even those with less decision latitude may still attempt to evade notice by leveraging their understanding of technical safeguards to exploit systems and reduce the likelihood of being caught.

They will conduct a cost-benefit analysis, weighing the potential benefits of their actions—such as personal gain or competitive advantage—against the risks of being caught. Their high confidence in avoiding detection often skews this analysis in favor of exfiltration.

The reckless employee

An employee might recklessly exfiltrate data with the well-meaning intention of getting the job done. This can include sending sensitive information to a personal email to work on after hours, aiming to meet tight deadlines or manage heavy workloads.

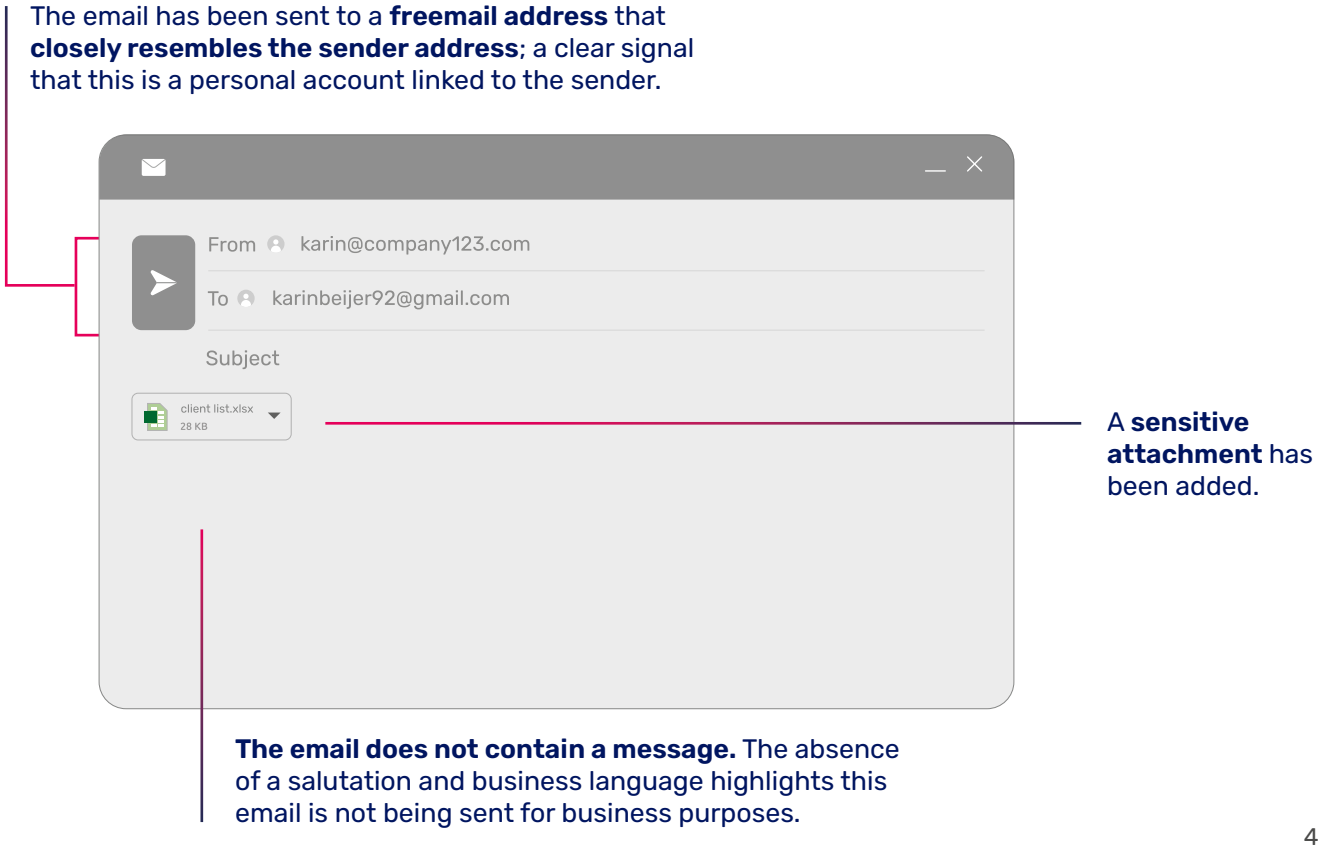
In line with the Dunning-Kruger effect, reckless employees may overconfidently believe they can handle sensitive information securely, without recognizing the seriousness of their actions or that they are violating company policy. They may justify their behavior through social proof, such as observing more senior or long-tenured employees doing the same, or through a cost-benefit analysis, where the benefit of completing the task outweighs the perceived security risk.

This mindset aligns with the findings that one-third (33%) of Cybersecurity leaders said an employee had exfiltrated data 'for work purposes', with the employees likely believing that getting their jobs done was more important than preventing data being sent to personal email addresses.

How data exfiltration happens over email: the risk of sending sensitive data to personal account

Due to the nature of sending information to a personal email, individuals often exhibit subtle behavioral changes compared to how they would behave when sending legitimate business communications.

Spotting the red flags: Signs of data exfiltration to a personal account

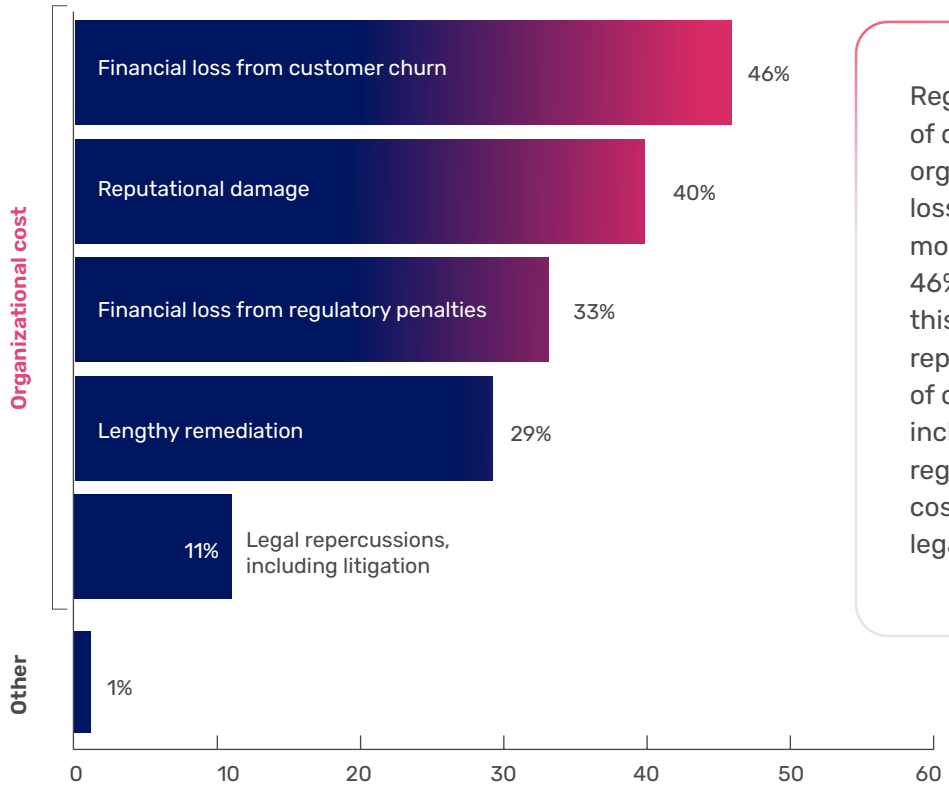


The impact of data exfiltration: how intentional rule-breaking drives data loss

Egress' Email Security Risk Report shows that 94% of the organizations have faced data loss and exfiltration issues within their Microsoft 365 environment, with 91% encountering adverse effects as a result.[4] Although outbound incidents like accidentally sending emails and files to the wrong recipient played a role, Cybersecurity leaders report intentional rule-breaking as the leading cause.

While malicious data exfiltration is less frequent, it can result in substantial damage, with 27% of organizations reporting lost data due to an employee moving jobs.[5] Malicious insiders typically operate within known parameters, leveraging their access to systems and evading cybersecurity measures to enable exfiltration without detection. It is the well-intentioned but reckless employees who pose a more common threat, often exfiltrating data unintentionally while trying to get their jobs done efficiently.

The organizational cost of data loss and exfiltration



Regardless of intent, the impacts of data loss and exfiltration on an organization can be severe. Financial loss from customer churn is the most frequent consequence, with 46% of organizations experiencing this issue. This is closely followed by reputational damage, affecting 40% of organizations. Other ramifications include financial penalties from regulatory bodies, lengthy and costly remediation processes, and legal repercussions.

4 2024 Email Security Risk Report Egress
5 Outbound Email Security Report Egress

Limitations of static rules-based email DLP

Many organizations rely on traditional DLP solutions that only offer static rules to prevent data exfiltration. While commonly used, these technologies come with significant limitations, leading to challenges in effectively managing outbound security threats.

Manual processes that can't scale

One of the primary challenges with static DLP rules is their heavy reliance on manual processes and ongoing administrative oversight. 94% of organizations rely solely on static email DLP rules, and 51% rely on reviewing audit logs to detect potential breaches.[6] This manual approach is a drain on the security team's time, and demands constant adjustments to keep the system aligned with user behavior. Of those Cybersecurity leaders using static rules, 100% expressed frustration with them, citing inefficiencies, high administrative effort, and security gaps as major pain points.

Reactive rather than proactive

The sole reliance on static rules and audit logs means that many organizations are reacting to breaches rather than proactively preventing them. Reviewing audit logs to spot unauthorized data transfers is a backward-looking approach that only flags issues after the sensitive information has already left the organization, failing to stop data exfiltraion in real-time

Blanket policies

A one-size-fits-all approach to data exfiltration isn't practical. Sometimes employees may need to email freemail accounts when communicating with contractors or individuals, while in other departments this practice is unnecessary. Blanket policies can overlook these nuances, and manually adjusting rules for each role or department becomes too granular and unsustainable.

Human behavior and malicious insiders

Whether due to reckless oversight or malicious workarounds, data exfiltration stems from the choices people make. Consequently, incidents are difficult to anticipate and even harder to prevent. While training is a good step in mitigating well-intentioned rule-breaking, it is unlikely to deter a malicious insider who is aware of data exfiltration policies but is eager to disregard them.

Limited visibility and scalability

Many employees who exfiltrate data often know how to circumvent existing policies to move sensitive information outside the organization. This makes data exfiltration one of the most challenging outbound threats to prevent and effectively monitor, so it is crucial for security teams to have visibility of incidents before the occur.

However, relying on reviewing audit logs to detect outbound security breaches offers limited visibility into real-time threats and is not a sustainable solution for any business. Ultimately, static rules are fundamentally unworkable at scale, as manually identifying data exfiltration incidents among thousands of legitimate business communications is both impractical and prone to error.

6 2024 Email Security Risk Report Egress

Strategic CISO: Intelligent detection of data exfiltration over email

Protecting organizations from behavior-based email security incidents requires a proactive approach that leverages intelligent technology, while still allowing the creation of rules for organization-wide policies that remain consistent across all users when necessary.

AI-driven detection of data exfiltration over email

Recipient analysis to detect exfiltration attempt
Organizations should leverage AI to analyze recipients and detect signals of exfiltration, including identifying whether a recipient's account is a personal one linked to the sender. To accurately identify data exfiltration, the analysis must incorporate contextual machine learning, social graph analysis, and pretrained deep neural networks.

Attachment analysis
It is essential that any solution used for detecting data exfiltration can analyze attachments for sensitive content. This ensures that attachments are thoroughly checked for confidential data and that their integrity is verified against the intended recipients. By doing so, it guarantees that sensitive documents are accessible only to authorized individuals.

Message body analysis
As data exfiltration may be indicated by subtle behavioral changes, organizations need a solution with natural language processing (NLP) that can analyze email message bodies for key signals, such as unusual language patterns and contextual clues.

Total visibility and adaptive flexibility for administrators

Every organization has a unique risk appetite, so they need flexible solutions for managing data exfiltration while maintaining full visibility without extensive manual intervention.

Depending on a business's individual policies, security administrators need the option to automatically block activity, prompt individuals when they are about to violate policy, prompt an administrator to review, or even monitor activity silently in the background. This automated approach eliminates the need to spend hours reviewing manual audit logs and provides a clear picture of the overall threat .

To truly mitigate the risk of data exfiltration, CISOs must shift from reactive, manual processes to intelligent, adaptive solutions that can proactively address evolving security threats and human behavior.

Stop outbound data exfiltration with Egress Prevent

Learn how **Egress Prevent** uses machine learning and NLP to detect and block exfiltration of personal and company data over email.

Egress Intelligent Email Security Suite

Egress Defend

Detect and defend against targeted phishing attacks

Learn more

Egress Prevent

Stop data breaches before they happen

Learn more

Egress Protect

Send and receive secure, encrypted email

Learn more

Inbound threat protection

Outbound threat protection

Want to learn more about how to prevent data exfiltration in your organization?

Request demo

About Northdoor

Northdoor helps organisations harness the full power of their data throughout its lifecycle. Northdoor helps clients manage all aspects of data—keeping it organised, governed, protected, compliant, accessible by both people and applications, and always ready for high-speed analysis. Northdoor provide solutions across consultancy, applications, security, hybrid infrastructure, analytics, AI, and managed services. Northdoor partners with the biggest and best vendors in global IT, and maintains deep technical skills to help clients overcome any challenges.

northdoor
◦ Store IT ◦ Protect IT ◦ Use IT ◦

About Egress

As advanced persistent threats continue to evolve, we recognize that people are the biggest risk to organizations' security and are most vulnerable when using email.

Egress, a KnowBe4 company, is the only cloud email security provider to continuously assess human risk and dynamically adapt policy controls, preparing customers to defend against advanced phishing attacks and outbound data breaches before they happen. Leveraging contextual machine learning and neural networks, with seamless integration using cloud-native API architecture, Egress provides enhanced email protection, deep visibility into human risk, and instant time to value.

egress
a KnowBe4 company

www.egress.com