proofpoint.

E-BOOK

The Future of Email DLP

Stopping human-centric data loss with a modern approach to email DLP

Introduction

An employee accidentally emails a spreadsheet with personal information for 130 employees to 65 other coworkers.[1] A bank employee sends highly sensitive financial details about a scam victim to the wrong email address.[2] Sensitive U.S. military information is sent in accidental emails to Mali.[3]

Each of these real-life examples shows what human-centric data loss looks like. When a person unintentionally exposes, mishandles or exfiltrates sensitive data, the consequences can be devastating.

Modern organizations know that email security is critical. That's why they are spending more than ever on cybersecurity solutions to protect their most sensitive data. Despite this, data breaches are at an all-time high. Rightly, security teams focus on the technological vulnerabilities that lead to successful phishing attacks, malware installation and stolen credentials. However, a significant percentage of data breaches are caused by people.

This e-book explores human-centric email data loss and why it's so difficult to stop. It also describes the most effective way to solve this problem by taking a modern approach to email DLP that includes an adaptive, behavioral solution.

1%

of users are responsible for 88% of data loss events[4]

85%

of organizations experienced one or more data loss incidents in the past years[5]

38%

of organizations have a "mature" DLP program[6]

1. Fisher Philips. "One Employee's Accidental Email Leads to a Significant Data Breach Ruling in Federal Appeals Court." May 2021.
2. *The New Zealand Herald*. "Privacy Breach: Banking Ombudsman Scheme Sends Highly Sensitive Details about $300k Scam Victim to Wrong Email Address." June 2024.
3. *Military Times*. "Sensitive U.S. Military Info Exposed in Accidental Emails to Mali." July 2023.
4. Proofpoint. *Data Loss Landscape Report*. 2024.
5. Ibid.
6. Ibid.

Introduction

Human-centric data loss is on the rise ●

Types of human-centric data loss

Why email data loss is hard to stop

What it means to modernize email DLP

Conclusion

Human-centric data loss is on the rise

In recent years, the nature of work has transformed. Today's employees collaborate from everywhere, causing email data security to grow more challenging. What follows are a few reasons why people are often behind the biggest email data loss incidents.

Employees have access to highly sensitive data

Today, nearly every employee, contractor or partner—regardless of their role—has some access to an organization's data and key systems. They might have direct access to sensitive data. Or they might interact with software tools and platforms that manage this data. This increased accessibility allows for greater efficiency and collaboration. However, it also significantly increases the potential risks to data security.

Human behavior remains a significant vulnerability

Advancements in technology and security tools can only protect organizations so much. Human behavior can be difficult to protect against because people are unpredictable. Human risks fall into three categories:

1. **Careless.** These users often create risk because they're distracted, not paying attention to details or not following established security protocols. The most common careless mistake is accidentally sending emails to the wrong address.
2. **Compromised.** An employee who has been compromised—whether through a cyberattack or coercion—is one of the most dangerous threats to email data security. Attackers often use their stolen credentials to access systems while appearing to be legitimate, trusted employees.
3. **Malicious.** Malicious employees often use email to exfiltrate sensitive data. This typically involves forwarding confidential client data, intellectual property or financial records to themselves or third parties. By using email, they can bypass firewalls or other perimeter defenses that would typically block unauthorized data access.

The high cost of human-centric data loss

Human-centric data loss can have a huge impact on organizations, and the consequences go far beyond money.

1. **Brand impact.** If sensitive customer information—like credit card details, Social Security numbers or health records—is accidently leaked, it can tarnish a company's reputation. What's more, customers often lose trust.
2. **Operational disruption.** Email mistakes often require a substantial amount of time and resources to correct. This leads to inefficiencies in administrative time, delays and increased operational costs.
3. **Regulatory fines.** Companies in industries like healthcare and finance must follow strict regulations like HIPAA, GDPR and CCPA. When laws for mishandling data or transmitting sensitive data are violated, there can substantial fines and penalties.

Types of human-centric data loss

Email data loss that's caused by humans is usually either unintentional or intentional.

Unintentional email data loss

This type of data loss is usually caused by careless users. These users make honest mistakes or take risky actions, like sending emails to the wrong people, attaching the wrong files, or sending sensitive data to personal email accounts for work purposes.

While these types of incidents may seem benign, their consequences can be severe. This is especially true in cases when sensitive or confidential information is shared with the wrong individual, customer or vendor. Unfortunately, they are hard to predict, difficult to detect and can go unnoticed until significant damage has been done.

33%

of employees send 1-2 misdirected emails per year[7]

40%

of workers email the wrong person[8]

[7] Proofpoint platform data, 2024.
[8] Proofpoint. *Psychology of Human Error*. 2022.

Misdirected emails

Perhaps the most common form of unintentional data loss is misdirected emails. This is when a person accidentally sends an email to the wrong recipient. These are common reasons for why they happen:

- **Autocomplete errors.** When typing a name or email address, email clients often suggest previously used contacts. In a rush, a user might choose the wrong recipient from the list.
- **Simple mistakes.** A slight misstep when typing an address, such as an extra letter or omitted part of a domain name, could result in a message going to the wrong recipient.
- **Group emails.** Sometimes, the confusion over recipient lists (especially in large organizations) leads to emails being sent to people outside of an intended group.

50%

of error-related breaches are caused by misdirected emails[9]

48h

the average time it takes to detect and remediate an incident caused by a careless employee[10]

33% of employees send at least 1-2 misdirected emails a year

USERS	MISDIRECTED EMAILS	MISATTACHED FILES	EMAIL EXFILTRATION PREVENTIONS
5,000	3,408	178	751
10,000	6,816	356	1,502
20,000	13,632	712	3,004
50,000	34,080	1,780	7,510

Proofpoint data about types of email data loss.

[9] Verizon. *Data Breach Investigations Report*. 2024

[10] Ponemon Institute. *Cost of a Data Breach Report*. 2022.

Misattached files

This refers to when a person sends an email with the wrong file, the wrong version of a file or a file with sensitive data. Misattached files typically happen for these reasons:

- **Inadvertent sharing of sensitive files.** An employee may accidentally send an internal memo or financial report to a customer.
- **Hidden or unknown information.** A user might send a spreadsheet that has hidden content or data, unknowingly exposing sensitive data that's not intended for the recipient.
- **Loss of valuable data.** A user may send an incomplete version of a report or presentation that lacks key data, which damages their credibility and client trust.

Intentional email data loss

This type of email data loss is caused by malicious users who might be employees, business partners, contractors or other third parties. These individuals have access to sensitive data and critical systems. They may intentionally leak or steal data for personal gain, to harm the business, or both.

Losing sensitive data can be highly disruptive and damaging. In the Proofpoint *2024 Data Loss Landscape* report, 85% of surveyed companies said that they had experienced a data loss incident. For 50% of that group, the incidents caused business disruption.

Email data exfiltration

This is of the most serious types of data loss from email communications. Email data exfiltration occurs when someone with access to privileged data emails it to their own personal account or to an unauthorized third party.

$4.9M

the average cost of a data breach by a malicious insider[11]

Various factors can motivate an individual to exfiltrate sensitive data. Here are a few examples:

- Leaving to work at a competitor
- Business changes like mergers and acquisitions and divestitures
- Resentment due to job changes or conflict with a supervisor
- Disgruntled leaver
- Fear of job loss
- Poor job performance
- Extortion
- Corporate espionage

[11] Ponemon Institute. *Cost of a Data Breach Report*. 2022.

With data exfiltration, the type of data stolen can be highly sensitive. Here are just some examples:

- Intellectual property
- Financial documents
- Legal documents
- Engineering schematics and production data
- Customer lists and data
- Passwords
- Board meeting notes
- Personal identifiable information (PII)
- Personal health information (PHI)

Often, hundreds of large attachments of highly sensitive data are taken. The consequences of these types of breaches can be severe, especially for industries that are heavily regulated like finance, healthcare, legal and manufacturing.

72h

the average time it takes to remediate an email exfiltration incident[12]

[12] Ponemon Institute. *Cost of a Data Breach Report*. 2022.

Why email data loss is hard to stop

Humans are unpredictable. This makes it difficult to write policies or create security procedures that cover every possible data loss scenario. But that's not the only reason why stopping human-centric email data loss is difficult. Here's a list of the biggest challenges:

Lack of visibility

Sometimes human-centric email data loss isn't immediately visible to systems or monitoring tools. That's because it can look like normal work emails. If there's no auditing or adaptive behavioral monitoring in place, these mistakes often go unnoticed.

Evolving human behavior

Unlike automated processes or algorithms, human behavior is difficult to predict or write rules around. This unpredictability makes it hard to build systems that can catch human-centric data loss in real time. What's more, insiders often have legitimate access to sensitive data. Security systems often can't tell the difference between normal and malicious behavior.

Lack of awareness

Without regular reminders about data protection policies and the risks of email-based breaches, employees may not always follow best practices.

What it means to modernize email DLP

You can significantly enhance your email data protection strategy by using both a content-driven email DLP solution and a behavioral-focused, adaptive email DLP solution. This is the modern approach to email DLP.

Content plus behavior equals comprehensive protection

The key is to protect known content-based risks as well as unknown behavioral-based risks in email. When you do this, you get a more comprehensive, behavior-based approach to preventing email data loss.

- **Traditional email DLP tools** focus on content. They provide rule-based protection against known risks such as sensitive data being sent by email. They're very effective at protecting known, well-defined structured data. This includes PII, credit card numbers and more.
- **Adaptive email DLP** looks at behavior and context. It extends the coverage given by traditional email DLP products to also protect you against unknown and evolving threats. It uses behavioral AI and machine learning (ML) to detect unusual user behavior. So it can detect when a user sends sensitive data to an unintended recipient, shares files in an unusual pattern or sends an email to an unauthorized account.

The value of behavior-based email DLP

A behavior-based email DLP solution uses behavioral AI, ML and relation graphing (RL) to learn from, adapt to and predict human behavior. It detects potential data loss incidents even when the data isn't well defined. It continuously learns and evolves as user behavior evolves. This makes it the ideal approach for combating human-centric data loss.

Here's why a behavior-based email DLP solution is so useful.

Validate recipients

Behavior-based email DLP solutions can intelligently validate the recipient of an email before it's sent. By analyzing normal email behaviors and patterns with ML, these systems can flag emails that are being sent to the wrong recipient. It doesn't matter if it's an internal or external contact. This is especially helpful in preventing misaddressed emails.

Scan attachments

These solutions automatically scan email attachments to ensure that they are the correct versions and that they don't contain any sensitive data. They also use RL to check that attachments are typically associated with the intended recipients. If an attachment is missing, or being sent to a user not typically associated with it, then the sender is notified before they hit "Send."

Analyze context

Contextual awareness means that the content and context of emails are analyzed for potential risks. For example, if an email contains sensitive data, behavioral AI can assess whether it is appropriate to send that data to the recipient based on their context, like their role within the organization or whether they have communicated on the subject or project before.

Perform historical benchmarking

ML can analyze an organization's historical email patterns. It can then benchmark normal email sending behaviors and predict potential errors before they happen. This enables the system to suggest corrections in real time based on past behaviors and common mistakes.

Provide real-time alerts and coaching

These solutions provide real-time feedback to users. If an email appears to contain sensitive information or is being sent to the wrong or unauthorized recipient, the system will alert the sender immediately. This gives them a chance to correct the error before it's too late and increases their email security awareness in the moment.

Conclusion

To effectively address all forms of email data loss, you need to take a holistic approach to email security. To do this, you need both a content-based email DLP solution combined with an adaptive behavioral email DLP solution.

This modern, multilayered approach to email data security ensures that you have robust protection against known risks. Plus, you benefit from dynamic, intelligent detection of unknown human-centric data loss threats. You get enhanced data protection, improved user compliance, reduced operational overhead and a stronger overall email data security posture.

Learn more about how Proofpoint can help you deploy modern email DLP.

Visit https://www.proofpoint.com/us/products/adaptive-email-dlp.

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations’ greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 85% of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

Connect with Proofpoint: LinkedIn

DISCOVER THE PROOFPOINT PLATFORM →