Insider data breaches in financial services firms

The how, what and why

egress

Inside the report

Introduction

Most financial firms have robust technical measures in place to protect their assets and confidential information from outsiders. However, while it's relatively simple to install and configure a firewall, the people operating from within those technical controls pose a significant risk to your firm.

Insider threats can take many forms but they all fall into three main areas: people get hacked, people make mistakes, and people break the rules

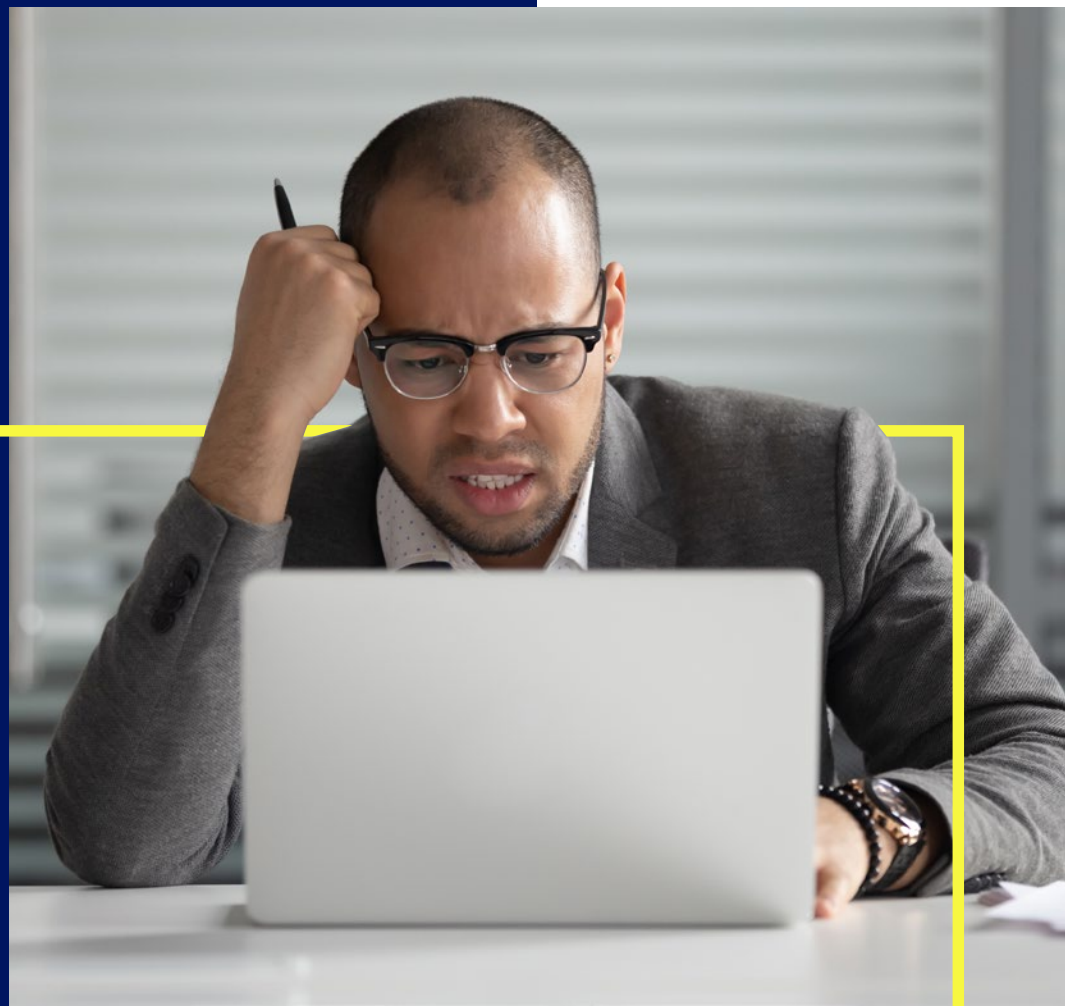
Insider threats can take many forms but they all fall into three main areas: people get hacked, people make mistakes, and people break the rules.

Employees, contractors, and those with privileged access to user accounts can all be responsible for insider threats. Typically, they're people just trying to do their jobs who are targeted by cybercriminals or accidentally leak data. But whether malicious or not, insider data breaches damage your firm's reputation, sever client relationships and impact your bottom line.

As they have legitimate access to data all the time, insider threats can materialize at any time, making the detection and prevention of these incidents a persistent challenge. As an IT leader, how can you ensure that insider data breaches aren't going undetected?

Throughout this eBook, we'll explore the main insider threats and the risks they present to your firm, and explain how the latest advances in Human Layer Security can keep your people and your firm operating securely.

People get hacked



How does it happen?

According to the *Federal Bureau of Investigation (FBI)*, phishing is one of the most common types of cybercrime.[1] Criminals target individuals via email, telephone or text message, posing as a legitimate person or organization to trick them into carrying out a secondary action, like transferring a payment or providing sensitive data, or even something as simple as opening a malicious attachment that subsequently launches a malware attack.

Financial services organizations are 300 times more likely to be the victim of a cyberattack than other types of companies.[2] They're very attractive targets to cybercriminals as they frequently transfer significant sums of money and hold incredibly sensitive data about their clients. Additionally, financial firms can become targets so cybercriminals can leapfrog into their client base to defraud them. If targeted by ransomware, firms are likely to give in to cybercriminals' demands in attempts to preserve their reputation and resume business as normal.

Employees most commonly fall victim to email scams, with 96% of phishing attacks arriving via email inboxes.[3] Since email phishing is constantly evolving, more people are being caught by attacks, while Security teams chase after a moving target.

Of particular concern are Business Email Compromise (BEC) attacks, which are notoriously hard to detect because hackers use compromised corporate email accounts from known and trusted individuals to trick the recipient into believing they're speaking with a legitimate contact. Not only do they look very convincing to the human eye, they go under the radar of traditional secure email gateways (SEGs) and anti-phishing filters.

Let's imagine for a moment that Bob from Company A receives a phishing email with a malicious link. Bob, believing the email to be legitimate, clicks on the link and enters his credentials into a website. The hackers now have his username and password to access Bob's corporate account, which they use to learn that he regularly sends invoices to Alice at Company B. They can now pose as Bob to send Alice an invoice, which she may unknowingly pay directly to the hackers while thinking she's transferring money to Bob.

Financial services organizations are 300 times more likely to be the victim of a cyberattack than other types of companies

Why hacking is difficult to detect

Like it or not, cybercriminals are innovative, constantly devising new ways to bypass traditional anti-phishing technologies. In fact, 98% of all phishing cases rely on social engineering, where victims are manipulated into supplying confidential information to a supposedly legitimate sender.[4]

SEGs are unable to detect this level of sophisticated attack. Firstly, they usually depend on IT Administrators to update them, primarily by adding to lists of keywords. The constant requirement to update keyword lists creates an unmanageable amount of work in today's rapidly evolving threat landscape, meaning firms are usually on the backfoot and enabling many sophisticated phishing emails to go undiscovered before it's too late.

Secondly, SEGs tend to look for set criteria within emails to determine whether they're fraudulent, including subject lines, the age and trust score of the sender's domain, and whether it includes certain blocked keywords. Although these technologies will catch some phishing attempts, hackers know these criteria and therefore are engineering more advanced scams. For example, they can simply leave the subject line blank or take time "ageing" their domains to fool those tests.

As a business leader, what can you do to protect against this? It may seem like an impossible task, but there are systems and processes that you can put in place to defend your firm.

Cybercriminals looking to phish employees are banking on them being too tired or busy to properly take in information. They use pressurizing social engineering tactics, such as urgent requests and consequences for non-compliance, to block employees' logical thought processes. That's why it's essential to have the right technology in place that can detect the suspicious signs your employees may be missing.

Solutions that employ natural language processing (NLP), machine learning and social graphing technologies together can detect when a sender isn't legitimate. This type of technology is especially useful for defending against BEC and impersonation attacks because it won't allow the usual social engineering tactics to pass its rigorous test.

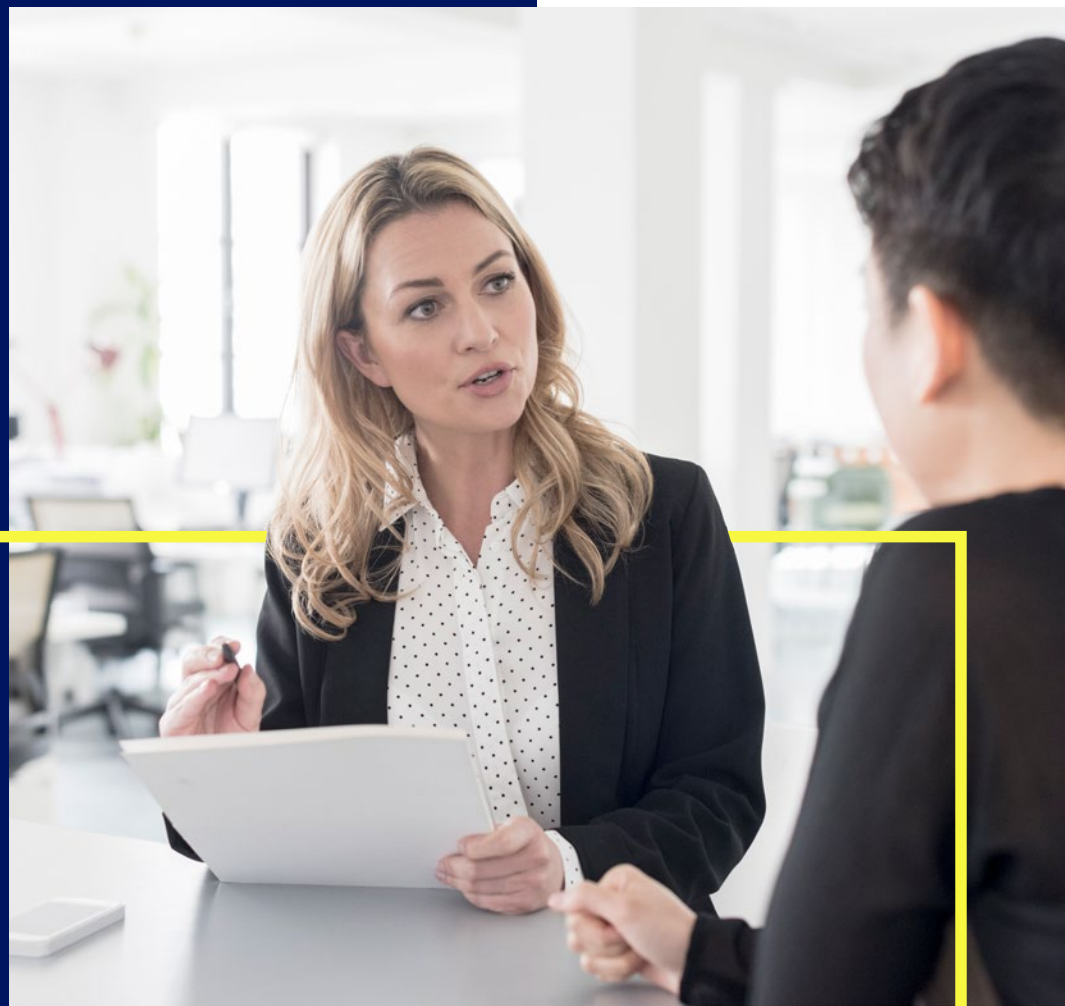
[1] Federal Bureau of Investigation: Internet Crime Report 2020. 2020_IC3Report.pdf

[2] Security Boulevard. 10 Statistics that Summarize the State of Cybersecurity in Financial Services - Security Boulevard

[3] Expert Insights. 50 Phishing Stats You Should Know In 2021 | Expert Insights

[4] CloudAlly. Social Engineering: 2020s Top Cybersecurity Threat (cloudally.com)

People make mistakes

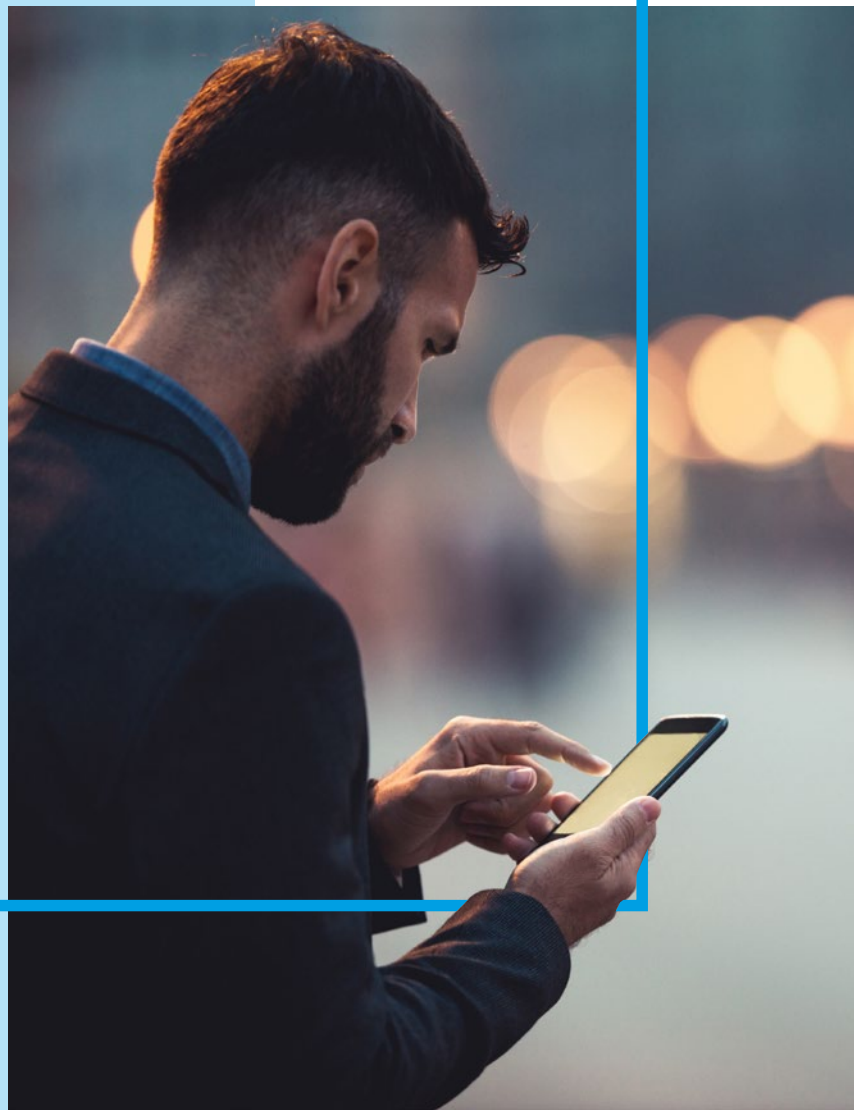


Why mistakes are so common

As the saying goes, 'to err is human'; in other words, we all make mistakes. In today's connected world, there are more opportunities for employees to make honest mistakes than ever before.

Most workers now have access to their corporate emails at the office, at home and on the go. As a result, employees can share sensitive data and privileged information from anywhere across multiple devices. Unsurprisingly, worker negligence - such as sending sensitive information to the wrong recipient - accounts for 30% of all data breach cases.[5] In some employees' cases, they may not even be aware that there's a problem until it's too late because of their poor cybersecurity knowledge.

To mitigate the risk of an accidental breach, you must be aware of the common mistakes employees make and what you can do to prevent them.



Outlook autocomplete

Productivity tools are developed to make our lives easier. However, these tools also have the potential to backfire if not used with care.

Outlook autocomplete is a good example; it was designed to detect sent and inbound email addresses and suggest them as recipients for future emails. Users begin typing the first few letters in and autocomplete does the rest.

The only problem is, it doesn't always select the right recipient. Let's say you want to send an email to john.smith@companyA.com; it may instead suggest john.jones@companyB.com. Employees in a rush might not spot this and hit send on an email containing sensitive data before realizing what they've done.

Some financial firms try to mitigate this risk by disabling Outlook autocomplete entirely; however, this can open new avenues for error or, at the very least, inefficiency. Ultimately, you're still relying on the sender to input the correct recipient whether that's via free typing, an address book or a list of email addresses saved elsewhere (such as in a spreadsheet stored locally). Particularly with free typing, which employees typically resort to for efficiency, there's significant potential to mistype an email address. Some errors may result in a bounce back but others can be sent to the wrong recipient.

Attaching the wrong files

It's estimated that the average office worker sends and receives around 121 business emails each day.[6] The margin for error is significant. Of course, not all misdirected emails result in data breaches, but emails containing incorrect attachments often cause the most headaches for IT managers. Generally, attached files tend to contain more confidential or sensitive information than a standard email.

Unfortunately, in the case of a wrong attachment, the problem may not disappear simply by asking the unintended recipient to delete the email. Once an email is sent, the sender has lost control of it for good. Unencrypted attachments can be downloaded, copied and shared by anyone. This is an issue for all financial firms, but can be particularly damaging when sharing files relating to trading, acquisitions and mergers, or high-net-worth individuals who have wide interest appeal.

Reply all

A 'Reply all' faux pas can damage a lot more than an employee's personal pride. If the email in question contains sensitive information, potentially hundreds of people have access who shouldn't, causing a widespread data breach. These data breaches usually happen as the result of the sender failing to notice that more people have been added to the Cc field than there was earlier in the conversation.

Another variation of this is when a user sends an email to multiple recipients by including their email addresses in the To or Cc fields instead of Bcc. Exposing people's email addresses in the To/Cc field not only breaches their privacy but the subject of the email can do further damage, for example if sensitive financial information ends up being linked to specific people or businesses on the circulation list.

Why mistakes are difficult to prevent

Preventing human error is notoriously challenging because there are so many ways it can occur and it's impossible for the human mind to predict. Until recently, static email DLP technologies have formed the main defense against this type of risk. However, 100% of IT leaders in financial firms that deployed these technologies have become frustrated by them, finding they are unworkable in practise and create user friction.[7]

Advances in contextual machine learning and social graphing technologies offer a better alternative by deeply understanding an individual's behavior and alerting them when they're about to make a mistake. This includes analyzing the context and content of every email, as well as the recipient(s) it's going to. Intelligent DLP can also notify the sender when abnormal behavior is detected, such as a wrong file being attached or the wrong recipient being included.

Preventing human error is notoriously challenging because there are so many ways it can occur and it's impossible for the human mind to predict

[5] CNBC. A surprising source of hackers and costly data breaches (cnbc.com)

[6] Review42. How Many Emails Are Sent per Day in 2021? [And More Thrilling Stats] (review42.com)

[7] BusinessWire. An Alarming 85% of Organizations Using Microsoft 365 Have Suffered Email Data Breaches, Research by Egress Reveals | Business Wire

People break the rules

Rule-breakers don't always want to cause harm

Let's take a look at the non-malicious rule-breakers first. These employees haven't set out to harm the firm, but they're aware their actions go against cybersecurity policy and there's a level of beneficial "payoff" for them, usually efficiency gains.

This group of rule-breakers may do the following:

- Send files to their personal email address to print at home
- Share video conferencing invites (with attachments) to their personal devices to join a meeting
- Not encrypt an email or use a secure portal to send messages if they know their client will push back on the friction it creates

Commonly, these employees feel they are too busy to follow procedures. In their cost-benefit analysis, they see all the cost residing with them and the benefit of data protection belonging to the firm.

Alternatively, they feel social pressure from colleagues, particularly those senior to them or who have been at the firm for longer, to work in insecure ways, with the pay-off being acceptance into the group. Finally, they might be overconfident in their abilities and cybersecurity knowledge, disbelieving that there really is a risk to data.

Malicious data breaches

Now let's look at the intentionally malicious rule-breakers. Not only does this type of data breach take the longest for financial services organizations to resolve at an average of 55.1 days, but it's also the most costly. Typically, firms pay around $243,101 to resolve malicious insider data breaches.[8] Malicious actors are motivated by personal gain, but they're not considering any level of benefit to the firm; they're in it for themselves and present a tremendous risk.

Malicious insiders come in many forms and have various motives, for example:

The 'hard-worker'

The 'hard-worker' has usually built up a long list of customer contact details and a strong knowledge of various projects during their employment. When they accept a new job, these employees may email this information to their personal email address and take it with them. In the financial sector, the new job will commonly be at a competing firm.

Many people believe that they are entitled to take data to a new job because of the hard work they put into obtaining the information

Many people believe that they are entitled to take data to a new job because of the hard work they put into obtaining the information. The *Insider Data Breach Survey 2020* reports that 41% of employees don't believe organizations have any ownership over their data.[9]

The resentful worker

Employees can become resentful if they don't feel like they are valued. Resentment can breed spite, which begets malicious action. In this case, they may steal company data to sell on the dark web as a means of 'getting back' at the business or are more likely to respond to requests for data from competitors.

The disloyal worker

Disloyal employees either don't feel a sense of loyalty to the business, or their loyalty to themselves outweighs everything else. So, when a cybercriminal offers them the opportunity to help commit a crime in return for a pay-off, they take it. In 2020, 71% of malicious insider breaches were financially motivated.[10]

Why rule breaking is difficult to detect

In malicious breaches, people understand the boundaries of the security measures the firm has put in place, figure out how to circumnavigate, and mask their true intentions until the damage has been done (or potentially for some time after as well).

Mandatory security training can go some way to curb intentional behavior, particularly for rule breakers. But IT managers can't rely on this alone, as it won't prevent intentionally malicious behavior.

Most of the technologies that organizations currently use only look for the most obvious signs of phishing, but they don't monitor user behavior and consider existing data. As such, they can't verify when a user is doing something they shouldn't be - whether that's deliberately or unintentionally.

For ultimate protection, organizations should consider implementing a technology that takes a 'zero trust' approach to all emails, both in and outbound. A technology that couples this with human-led natural language processing can detect the signs of sinister activity and protect your business against potential data breaches.

[8] Security Boulevard. 10 Statistics that Summarize the State of Cybersecurity in Financial Services - Security Boulevard

[9] Insider Data Breach Survey 2020. egress-insider-data-breach-survey-2020_uk.pdf

[10] Security Boulevard. Even Low-Level Malicious Insider Threats Cause High-Level Damage - Security Boulevard

The consequences

Regardless of how an insider data breach is caused, there will be serious consequences for your business in the form of reputational damage, client relationship deterioration, non-compliance sanctions and financial harm.

A real-life example of an insider data breach

In 2011, a former Bank of America employee sold customer data - names, addresses, PINs, birth dates, and other sensitive information - to cybercriminals, who used it to commit fraud and identity theft.

One victim was hit especially hard by the scam. The cybercriminals used the victim's information to order and cash checks from Bank of America, and had all of his calls forwarded to their cell phones so he wouldn't be alerted. As a result, the victim lost over $20,000.

Bank of America reportedly offered to reimburse the victims and provide two years' credit monitoring for free. However, the breach severely damaged customer trust in the organization.

In addition to the severe reputational damage caused, the data breach cost Bank of America $10m to resolve.[11]

38% of IT leaders believe that reputational damage has the most extensive impact after an insider data breach.[12] When you consider the knock-on effect a damaged reputation can have, usually in the form of severed customer and client relationships, this statistic isn't surprising.

In fact, a survey showed that 65% of customers lost trust in an organization following a data breach. A further 27% discontinued their relationship with that company.[13] Losing customers and clients will have financial ramifications, but unfortunately, it doesn't stop there.

The cost of a cyberattack is highest in the banking and financial services industry, reaching an average of $18.3m annually per company.[14] In addition to falling share prices and loss of business, a breach often includes costs such as:

- Help-desks and compensation for affected customers
- Investigations into the incident (hiring a third party or paying staff overtime)
- Regulatory penalties

Regulatory penalties are, by far, the largest cost following a data breach. The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to safeguard sensitive data and explain their information-sharing practices to customers. Under GLBA, penalties for non-compliance can include fines of up to $100,000 per violation, with fines for company officers and directors up to $10,000 per violation. Plus, the provisions can include criminal penalties of up to five years in prison and the revocation of licenses.[15]

If your business offers goods and/or services to the EU, then it is also subject to the General Data Protection Regulation (GDPR). Non-compliant companies could be fined up to €20m ($24.3m) or 4% of their global annual turnover, depending on which is greater.[16]

---

[11] Computer World. Insider data theft costs Bank of America $10 million | Computerworld

[12] Internal Data Breach Survey 2019. Insider Data Breach survey 2019 (scoop-cms.s3.amazonaws.com)

[13] Ponemon Institute. ponemon_data_breach_impact_study_uk.pdf (centrify.com)

[14] Ponemon Institute. Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf

[15] SmartVault. GLBA Compliant Document Management & File Sharing Solution | SmartVault

[16] IT Governance. The damaging after-effects of a data breach - IT Governance UK Blog

The ideal solution

Egress Intelligent Email Security

Clearly, insider data breaches are extremely hard to detect, making them one of the most substantial risks to businesses and the most complex cybersecurity challenge to solve. So how are IT leaders supposed to protect their organization from data breaches and keep up with cybercriminals' ever-evolving tactics?

The answer lies in Human Layer Security, which utilizes intelligent technology to identify and prevent abnormal human behavior such as carrying out actions as part of a sophisticated phishing attack, or accidentally or intentionally leaking data.

Egress offers the only human layer security platform that defends against both inbound and outbound threats.

Our intelligent technology uses contextual machine learning and natural language processing to detect and prevent abnormal behaviour such as targeted phishing attacks, misdirected emails, and data exfiltration. This combined with powerful end-to-end encryption allows us to comprehensively protect the highly sensitive financial data shared via email.

Our analytics technology accurately demonstrates risk reduction through using Egress, as well as areas for targeted remediation, and enables administrators to run thorough compliance reporting.

1

Egress Defend

Detect and defend against targeted phishing attacks

This email shows very strong signs of phishing

2

Egress Prevent

Stop email data breaches before they happen

You wouldn't normally include janed@gmail.com with the other recipients on this email

3

Egress Protect

Send and receive secure, encrypted email

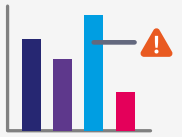
Unprotected

Encrypt email and attachments

4

Egress Respond

Understand, monitor and report on the security of your network.



About Egress

Our mission is to eliminate the most complex cybersecurity challenge every organization faces: insider risk. We understand that people get hacked, make mistakes, and break the rules. To prevent these human-activated breaches, we have built the only Human Layer Security platform that defends against inbound and outbound threats. Using patented contextual machine learning we detect and prevent abnormal human behavior such as targeted phishing attacks, misdirected emails, and data exfiltration.

Used by the world's biggest brands, Egress is private equity backed and has offices in London, New York, and Boston.

www.egress.com | info@egress.com | @EgressSoftware

egress