Aware
now part of mimecast

COLLABORATION SECURITY AND COMPLIANCE DATA SERIES

RISK AWARENESS REPORT

What are the risks in your digital communications and collaboration data?

"Leading brands are unlocking the power of their collaboration ecosystems, minimizing risk, eliminating operational friction, and revolutionizing the employee experience through authentic listening and giving employees a voice."

- Aware Marketing Research and Data Science

TABLE OF CONTENTS

03 ABOUT THE RISK AWARENESS REPORT

04 COLLABORATION IS THE NEW WORKFLOW

06 WHY MIMECAST ?

08 EXECUTIVE SUMMARY & KEY FINDINGS

11 TERMINOLOGY

13 MOVING BEYOND CHAT: INTRODUCING THE NEW ENTERPRISE WORKFLOW

16 EMPLOYEES ARE SELF-POLICING

19 THE PROLIFERATION OF CUSTOMER DATA

21 SECURITY POSTURE AND INSIDER THREATS

23 WORKPLACE CULTURE

28 FINAL THOUGHTS AND NEXT STEPS

ABOUT THE RISK AWARENESS REPORT

As the leading AI data platform for Collaboration Security and Compliance, Aware analyzes the state of risk across collaboration platforms such as Slack, Microsoft Teams, Zoom and Workplace from Meta to create awareness around both the risks and opportunities that lie within digital workplace conversations.

Prepared by Aware's in-house team of data and behavioral scientists, this report combines insights from over 6.6 billion collaboration messages with proprietary, purpose-built NLP, Computer Vision, and Machine Learning models that are designed and trained specifically to understand the ways employees collaborate and communicate.

This study delivers the latest insights into the threat landscape of workplace collaboration and the opportunities presented by the fastest-growing dataset across the enterprise today.

If you own collaboration, have been tasked with addressing security risks, or are looking to improve your overall employee experience, this report is both a must read and important industry benchmark to assess your capabilities to leverage collaboration data to mitigate risk, improve your compliance posture, and keep your business and employees safe and secure.

Aware's Collaboration Security and Compliance Research

Aware's industry-leading platform continues to drive innovation in partnership with the world's most iconic brands.

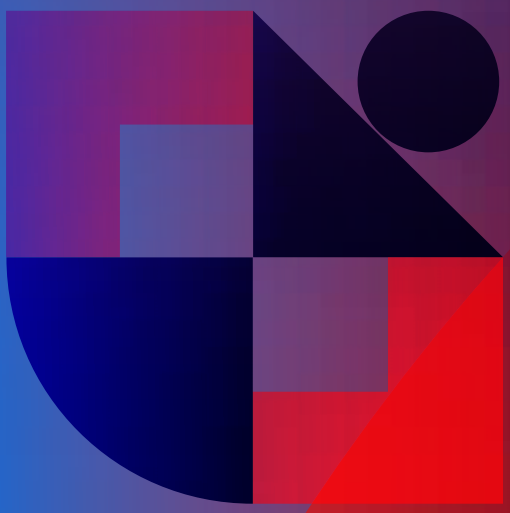
Aware's Behavioral Intelligence Teams are at the cutting edge of insights into employee experience, sentiment, and organizational health.

Leveraging over 7 years of AI models across billions of messages, Aware transforms the way innovative leaders tackle risk and opportunity in the modern digital workplace.

CONTACT US TO REQUEST YOUR OWN ASSESSMENT

CHAPTER 1

COLLABORATION IS THE NEW WORKFLOW



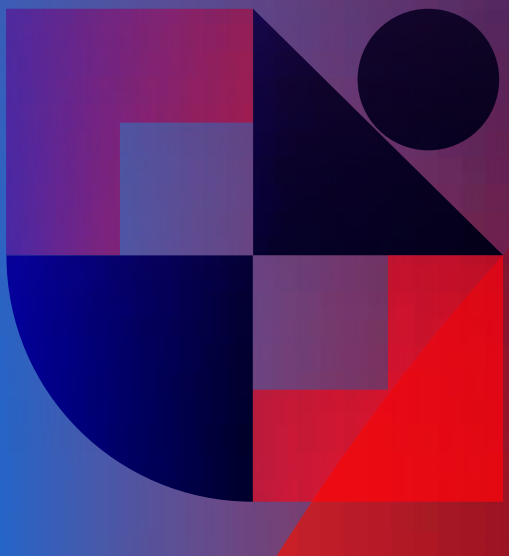
If Enterprises run on conversations, then collaboration platforms are where those conversations happen and work gets done. Tools such as Slack, Microsoft Teams, and Cisco Webex have experienced unprecedented growth over the past decade as the digital transformation, global pandemic, and increased demand for remote and hybrid work schedules have revolutionized the ways we work. Freed from the cubicle, today's employees expect organizations to invest in technologies that enable flexible, collaborative communication and data sharing from any location in real time.

Collaboration platforms are so much more than chat applications where employees exchange pleasantries. They are fundamental to every aspect of the workflow, connecting teams, departments, contractors, customers, and prospects in a real-time environment supported by apps and integrations that facilitate the instant transfer of ideas, insights, documents, code and more.

The growing ecosystem of collaboration platforms continues to evolve, with workplace conversations happening on JIRA, Confluence, G-Suite, Asana and countless other workflow applications. These tools facilitate distributed teams, enhance productivity, and accelerate the pace of innovation, but they also create tangled datasets that represent new risks and opportunities. Collaboration is the new workflow, and bringing order to this dataset is one of the biggest challenges facing executives across the enterprise today.

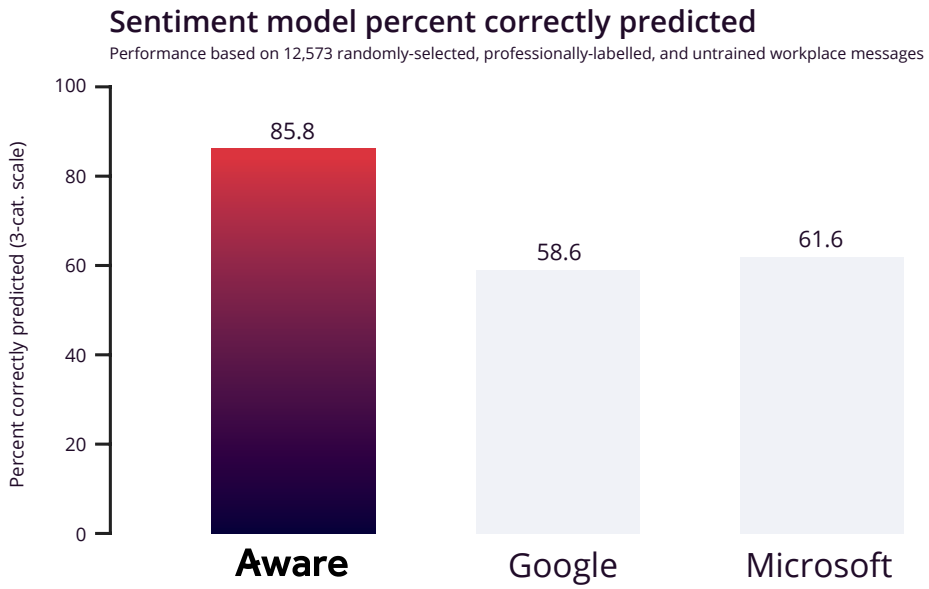
CHAPTER 2

WHY MIMECAST



The Aware platform was built to bring context to digital conversations and help organizations effectively manage the risks and opportunities contained within them.

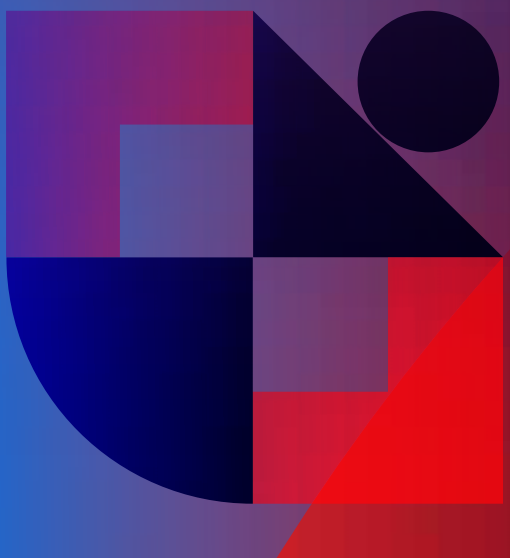
Aware ingests unstructured conversations from any platform, normalizes it, and enriches the data using a purpose-built suite of machine learning (ML), natural language processing (NLP), and computer vision (CV) models. These models deliver the industry's most accurate intelligence using effortless workflow automations, providing forward-thinking business leaders with complete, contextual understanding of their entire digital workplace.



- AI models purpose-built and trained by a diverse, in-house behavioral data science team
- Made for collaboration, using real collaboration data
- Results honed and validated by carefully curated, hand-labeled data
- Sentiment analysis consistently delivers near-human accuracy and far outperforms leading competitors
- Highly targeted models ensure cost-effectiveness and enable near real-time refresh and updates
- Responsible AI delivers representative, trustworthy insights into employee behaviors and key context

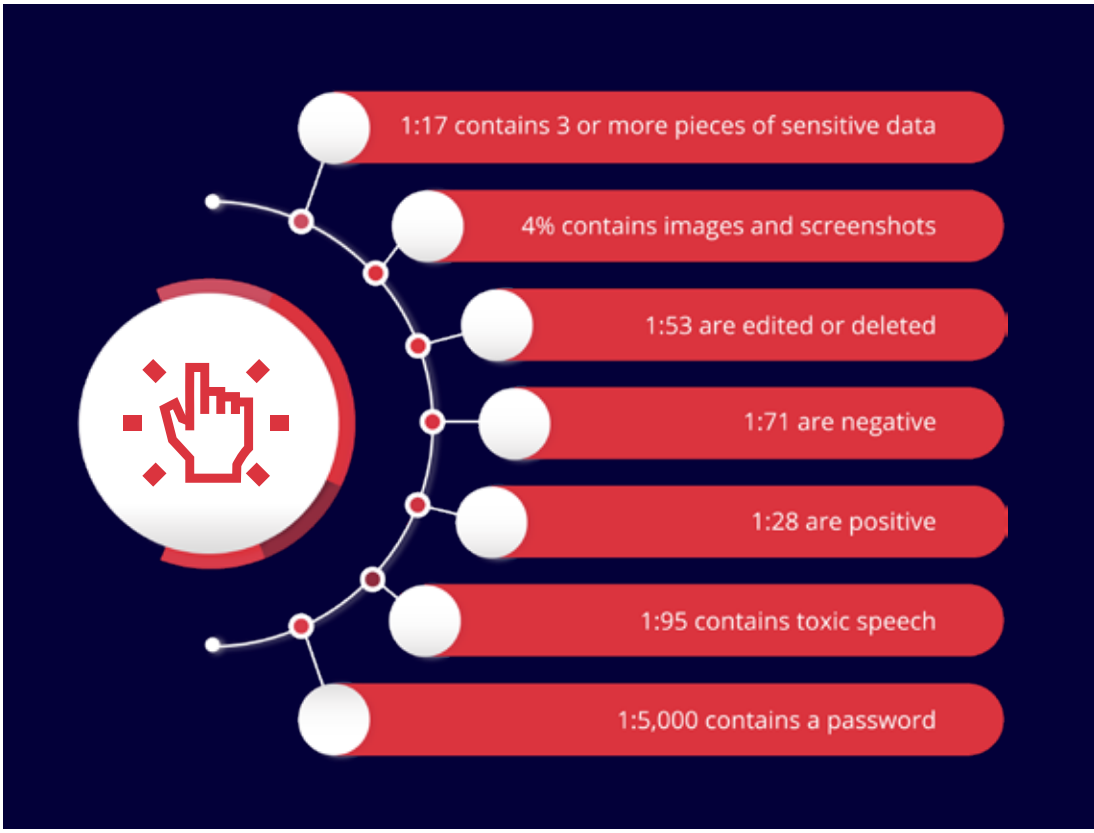
CHAPTER 3

EXECUTIVE SUMMARY & KEY FINDINGS



Key findings

Using Aware's proprietary AI and NLP models, we analyzed over 6.6 billion real messages across a range of collaboration platforms to identify the risk factors leaving organizations exposed to data breaches, insider risks, regulatory fines, no-compliance and impact to the company's reputation. These are the five key trends impacting the digital workplace today.



1. Collaboration is the new enterprise workflow

Employees spend 57% of their day collaborating with coworkers, generating massive amounts of data in the process—in a year, 10,000 employees will send over 90 million messages. Aware research shows that an increasing number of these messages are generated by apps and integrations (15.4%) and external users (1.1%).

The conversations across collaboration span every function of the business. Far from simple chat applications, these tools are functioning as knowledge repositories for critical and sensitive data that must be properly managed and secured.

2. Employees swap security for self-policing

Workplace collaboration users demonstrate a growing understanding that the messages they send may not be secure and often take measures to protect data when transmitting sensitive information, for example using images and screenshots instead of text-based message. Our research team identified an increase in these content types that were statistically more likely to include sensitive data—credit cards appeared in 1:1,113 of them. In addition, Aware continues to train and refine sensitive data detection models to minimize false positive results and ensure that businesses spend less time solving basic information security concerns. The result is dramatic—in 2018, Aware research showed that about 1 in every 262 messages contained a password. Today, that has fallen to 1:5,000.

3. Customer data proliferates

With consumer trust in corporations at an all-time low, it's more important than ever that businesses adequately protect their customers' data. Yet when analyzing collaboration messages, our researchers discovered that 37% of all messages include at least one piece of PII—a startling 1:17 messages contained 3+ pieces. While the majority are innocuous details such as names and dates, messages may also include everything from driver's licenses (1:49 messages) to bank account numbers (1:148) and SSNs (1:892).

This underscores the importance of deploying purpose-built solutions like Aware that can distinguish between different types of sensitive information to minimize false positive results and target the most sensitive data.

4. Insider risk exposure is on the rise

Collaboration tools are filled with blind spots where even administrators struggle to gain visibility. Over 90% of all messages sent in collaboration platforms occur in private or restricted channels. There, passwords, code, intellectual property, and other corporate-sensitive data are stored indefinitely, available for anyone with workspace access to find.

Additionally, Aware research shows that 1 in 53 messages are edited or deleted in the average digital workspace. That rises to 1:14 in private groups and 1:13 messages created in public groups. Without real-time visibility into these revisions, any employee can use collaboration tools to transmit data undetected.

5. Company culture has gone digital

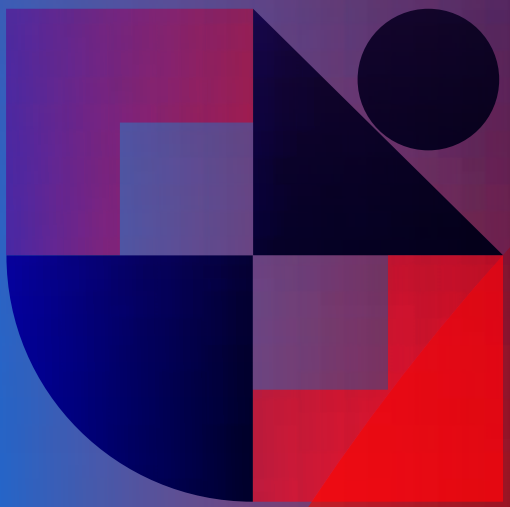
With the rise of remote and hybrid work, modern workplace culture happens increasingly online. Daily fluctuations in sentiment and toxicity don't just give leaders a pulse into the health of the organization but can directly impact productivity and profitability.

Toxic behaviors, including harassment and hate speech, are on the rise. In 2018, just 0.3% of messages (1:380) were negative. Today, that has risen to 1.4% (1:71). Employees express inappropriate (1:125) or offensive (1:500) language and even hate speech (1:2,000) in greater numbers than ever before documented. These increases point to lower morale, greater friction, and elevated risk to the enterprise from lawsuits and regulatory action.

The contrast in productivity and profitability between disengaged employees and engaged employed is material—often 20% or more. Understanding the causes of disengagement is not only good for the employee experience but it is good for the bottom line of the business too.

CHAPTER 4

TERMINOLOGY



As you read this report, several key terms will begin to surface. Gaining an understanding of this terminology will help boost your understanding of the role of technology in assessing collaboration risk factors.

Natural Language Processing (NLP) Models

A subset of artificial intelligence models that are trained to identify, decipher, and make sense of the human language as well as the meaning of words and phrases in conversations.

LLM vs. Targeted LM

A large language model is trained using vast, generic, and often publicly available sets of data, whereas a targeted or curated language model is developed using a more narrow, focused type of data (such as collaboration conversations), designed for greater accuracy in specific applications.

Unstructured Data

Often text heavy and filled with irregularities, unstructured data is data that is not organized in a predefined manner, making it challenging to understand.

AI Models

Software programs that have been trained on datasets to perform specific tasks such as recognizing patterns or making predictions.

Computer Vision (CV) Models

A subset of artificial intelligence models that are trained to translate visual data and detect object within images.

Data Platform

An integrated set of tools designed to collect, analyze, manage, and store data to generate key business insights.

Sentiment

The determination of the emotion or attitude behind text, whether positive, negative, or neutral.

Toxicity

The determination of overall health behind text. In Aware's models, toxicity can fall in the categories of healthy, inappropriate, offensive, or hate speech.

Outside Voice

The unfiltered thoughts, feelings, and opinions that employees express outside of a company's digital ecosystem.

CHAPTER 5

MOVING BEYOND CHAT: INTRODUCING THE NEW ENTERPRISE WORKFLOW

The Way We Communicate Has Changed

The popularity of real-time messaging platforms like Slack and Microsoft Teams has made corporate communications more casual and candid than ever before. Emojis, acronyms, short-form, and slang have blurred the lines between work and social media conversations.

These tools have also created a valuable, exponentially growing dataset filled with the real-time thoughts, feelings, and concerns of the entire organization. Analyzing employee voices at scale gives executives new insights that can help them make better, more informed decisions.

How Big is the Challenge?

Employees spend approximately 57% of their day using collaboration platforms such as Slack, Microsoft Teams, and Zoom, sending over 18 trillion messages in 2022—double the volume of the previous year.

An organization with 10,000 employees will produce over 90 million messages this year.

The Majority of Messages Come from a Handful of Authors

The top 20% of authors create 8x more messages than their coworkers, accounting for over 67% of corporate daily messages.

Power users engage in numerous daily conversations and play a key role in connecting people. Losing these top contributors could result in the loss of the networks and knowledge they have accrued. To produce and maintain success, organizations must act to retain their top creators and their knowledge.

SEGMENT	Size (in number of employees)	Ave. Messages per User Daily
SMB	1-700	38
Mid-Market	700-2500	29
Enterprise	2500+	28

SMBs Lead in Collaboration Adoption

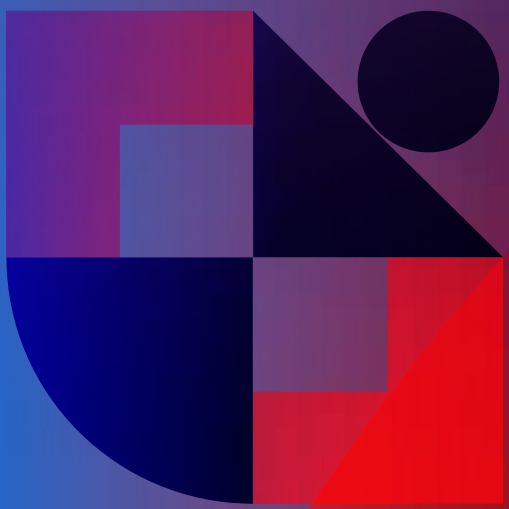
How embedded collaboration tools are in a company culture varies by organization, but some trends became clear when we analyzed message volume by business size.

Smaller businesses rely more on chat tools like Slack and Microsoft Teams for driving business decisions, workflow, and collaboration. In fact, some companies interviewed for this report stated that their organization has “skipped email as a collaboration tool.” Unsurprisingly, the average author at an SMB writes 35% more messages than the average author at an Enterprise.

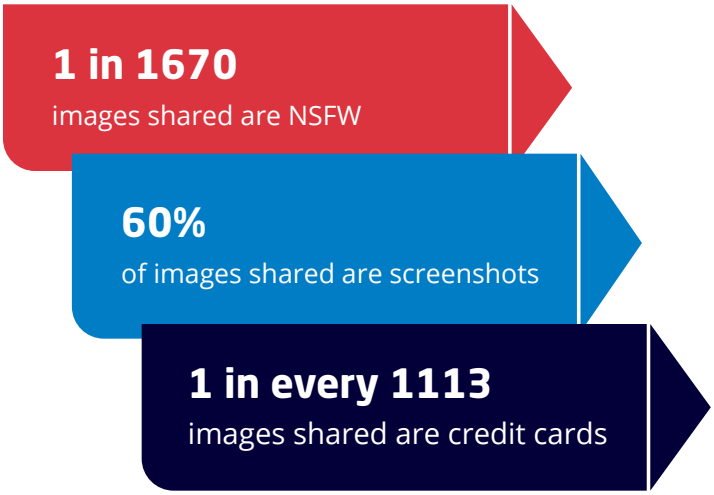
A growing percentage of messages are created by non-employee users, often a strength for email but now another indication that organizations rely less and less on email every day. These include external collaborators (1.1% of messages), and apps and integrations (15.4%) used to facilitate workflow management. As collaboration becomes more embedded within the daily functions of the organization, employees will become more reliant on these automations to help them perform their jobs.

CHAPTER 6

EMPLOYEES ARE SELF-POLICING



Employees are more informed than ever before about the need to protect data while working in cloud-based applications, and collaboration tools are no exception. However, collaboration's convenience makes it tempting to circumvent traditional checks and balances in favor of behaviors that seem safer but may in fact introduce more risk.



The prevalence of password sharing appears to have decreased dramatically within collaboration tools over recent years, and along with improvements to our detection models, that means just 1:5,000 text-based messages contain passwords today. However, Aware data scientists noted that employees were sharing increasing amounts of images and screenshots—around 4% of all content—which are statistically more likely to contain sensitive data. Today's average text-based message contains a credit card number in 1:20,675 instances, but 1:1,113 images are of credit cards.

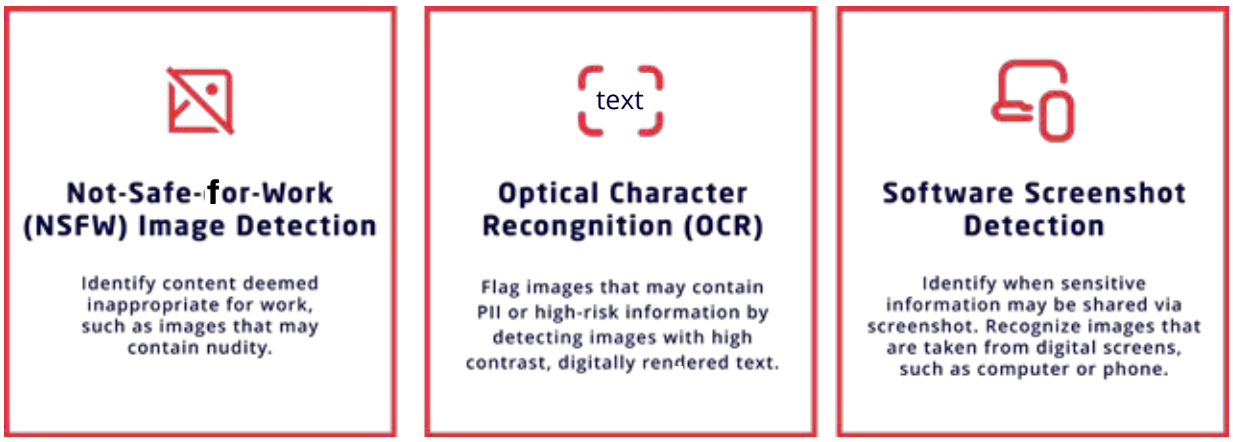
While employees might be forgiven for thinking images are less searchable, and therefore a safer way to share confidential information, Optical Character Recognition software can instantly recognize and read an image of a password or credit card. Screenshots and images may also create more risk from human actors, as many collaboration tools allow users to filter messages by attachment, making images some of the easiest content to find.

With the current volume of messages shared publicly and privately over chat, it is essential that businesses have technology to detect and mitigate this kind of information sharing.

How Aware Leads in Image Detection and Management

Aware uses advanced Computer Vision models trained to detect unauthorized and inappropriate content in any images uploaded to workplace collaboration platforms. Aware specializes in the detection of NSFW images and includes OCR to detect high-risk information and PII.

Computer Vision is trained to detect various objects within images



Edits and Deletions Present New Challenges

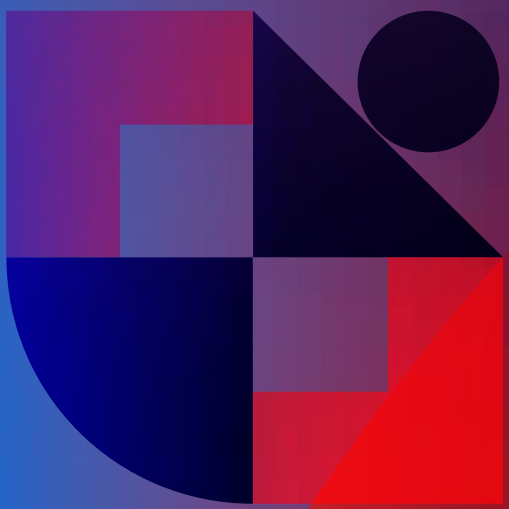
One of the most popular features of collaboration platforms like Slack and Microsoft Teams is the ability for users to edit or delete their messages. In most instances, this enables employees to correct simple typos or mistakes, or walk back a comment where they may have lacked full context before speaking. However, this feature also provides cover for both malicious and accidental data exfiltration to go unnoticed by workplace administrators.

Aware research shows that 1 in 53 messages are edited or deleted in the average digital workspace. That rises to 1:14 in private groups and 1:13 messages created in public groups. Higher prevalence of revisions in public makes sense—after all, fewer people are concerned about a typo in direct messages than they are in front of the whole company. But there could also be incidents where employees accidentally upload a confidential document or mention a restricted project and remove the evidence without giving infosec leaders the opportunity to understand that a potential breach occurred and mitigate the damage.

The only way to grasp the true extent of risk exposure from revisions and deletions is to capture a complete record of all messages as they happen. Without real-time oversight of collaboration tools, there is nothing to stop malicious actors from sending and deleting harassing messages, or exfiltrating confidential files and immediately removing the evidence.

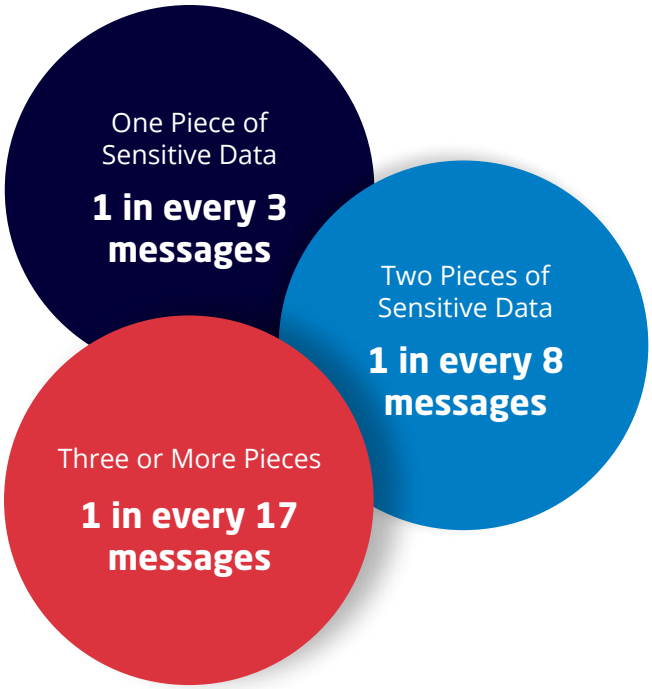
CHAPTER 7

THE PROLIFERATION OF CUSTOMER DATA



Nearly all organizations deploy security and data loss protection (DLP) for email and internet, and most are beginning to recognize the blind spots created by unmanaged collaboration tools. The rapid growth of data across these tools makes it difficult for IT to fully understand their threat surface and remediation. Further, permissions involved in collaboration systems are typically less restrictive, making it easier to share sensitive information undetected—which employees do with alarming regularity.

In every organization, sensitive customer data is being extensively shared over workplace chat platforms, including everything from names and addresses to Social Security Numbers and credit card details. Almost two-thirds (63%) of all sensitive data shared in collaboration constitutes personally identifiable information, putting customers at risk of identity theft in the instance of a data breach.



- 1 in 583 messages contains an Email Address
- 1 in 258 messages contains a Phone Number
- 1 in 120 messages contains a US Bank Number
- 1 in 48 messages contains a US Driver's License
- 1 in 892 messages contains a US SSN

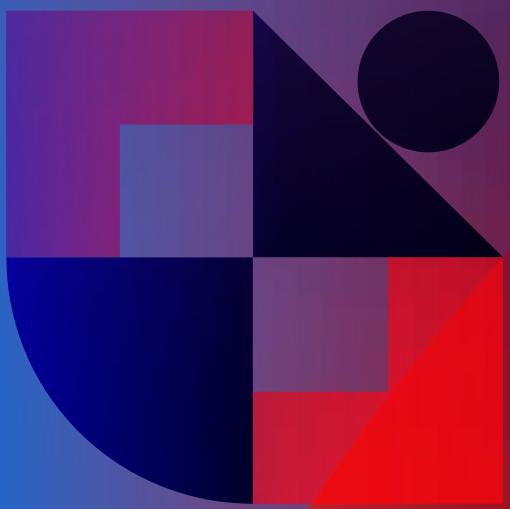
Notably, employees tend to share sensitive data during the workweek, indicating that most of this activity occurs within work hours and through work-related conversations.

This risk is particularly prevalent in organizations with large front lines that routinely handle customer data, for example banking or health insurance call centers. Employees in these locations often deal with multiple restricted systems that secure sensitive data, but collaboration tools can become an attractive alternative if they allow them to work faster.

Improperly securing customer data can have disastrous consequences for businesses. Alongside a damaged brand reputation and loss of consumer trust, companies may face regulatory action and costly fines and penalties.

CHAPTER 8

COLLABORATION SECURITY AND INSIDER THREATS



Data breaches have emerged as one of the most pressing challenges faced by companies in today's digital landscape, and those caused by insider threat are among the most devastating. According to IBM Action Guide, the average data breach cost $4.45 million in 2023. This was a 2.3% increase from 2022 and a record high. Each year, 34% of businesses globally experience some form of an insider attack (Forbes).

It's tempting to believe, "We hire good people here! We trust our employees." However, the truth remains that almost every organization will encounter an employee not acting in the company's best interest. Therefore, proactive measures against such risks are essential to safeguarding organizational integrity and success.

Collaboration Tools are Packed with Valuable Data

Our research shows that 0.5% of all messages contain file uploads, which might not sound like a lot but in a single month, 10,000 employees will share over 27,500 files. Those files contain everything from memes and pet photos to corporate strategy and payroll details, confidential customer list, or the roadmap for a new product. When Rockstar Games' Slack was hacked, a malicious actor exfiltrated and published footage from their upcoming, highly anticipated, Grand Theft Auto VI video game.

While what constitutes confidential data and IP fluctuates for each business, Aware research showed that information flagged as private, restricted, sensitive, and for internal eyes only was shared at a rate of 1 in 1,501 collaboration messages. Aware's contextual intelligence analysis and OCR technology make it faster and easier for security leaders to identify and mitigate confidential data in collaboration attachments by scanning image files to detect text, code, and NSFW material.

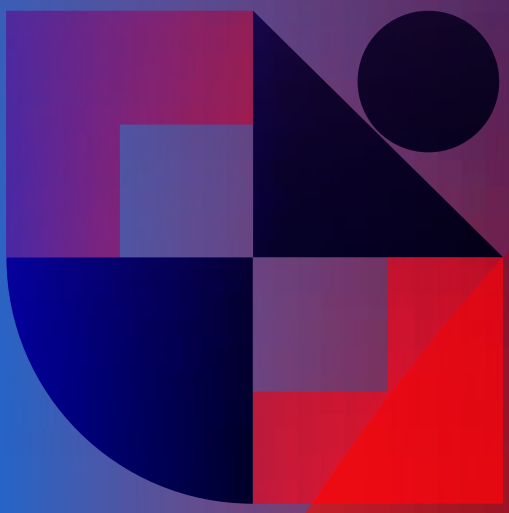
Mitigation Requires Tools that Understand Context

Employees must be able to share confidential information somewhere. To effectively address this critical issue, organizations must adopt compliance monitoring technology that differentiates between appropriate use and potential data leaks by understanding the context in which data is shared.

By proactively assigning value to the data contained within a collaboration tool, enforcing appropriate archiving and retention policies, and tracking messages in real time to identify unauthorized data sharing, organizations can reduce the risk of an insider data breach.

CHAPTER 9

WORKPLACE CULTURE



Aware scores every message on two scales: Sentiment and Toxicity. Sentiment refers to how negative, neutral, or positive a message is. Toxicity measures the presence of offensive or inappropriate language or hate speech. Even when negative in sentiment, messages in a healthy workplace should not be toxic.

Understanding these two scales is essential for capturing a complete picture of the health of your company culture and can provide an early warning system, alerting leaders to enhanced risk of insider threat action. Further, Aware normalizes results for each individual organization, delivering a more nuanced understanding of each company's unique culture. What is normal for a tech startup may be considered abnormal in a highly regulated corporate setting, for example.

Neutrality is the Norm, But Toxicity Fluctuates by Segment

The average sentiment is neutral across all business sizes, suggesting a balanced distribution of positive and negative messages. However, when taking the volume of messages into account across business segments, SMBs stand out as:

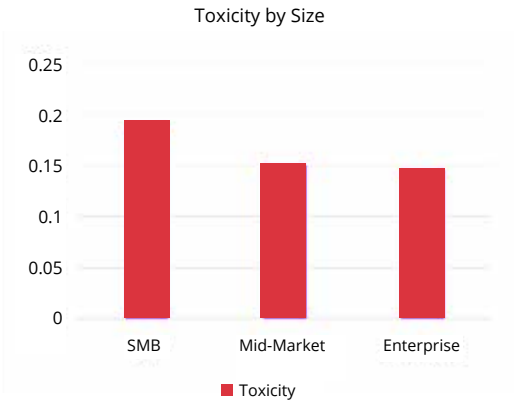
28% more toxic than Mid-Markets and

31% more toxic than Enterprises.

Employers at smaller companies must note that with an increase in toxic speech comes increased risk, which must be dealt with accordingly.

The Disproportionate Impact of Negativity

Although the average sentiment across all segments is neutral, that doesn't mean employees post positive and negative messages in equal measure. In the average workplace, 1:28 messages are positive, but only 1:71 messages are negative. Despite individual messages being 2.5x more likely to be positive, the impact of negativity is so profound that in aggregate they cancel each other out. This can affect employees' mental health, self-esteem, and overall performance. The entire company and its culture suffers.



Scale also matters. 10,000 employees author a remarkable 1.1 million negative messages annually, exerting a tangible influence on a company's cultural fabric.

Identifying negative trends and their causes is crucial for leaders, as it allows them to swiftly investigate potential triggers and implement appropriate solutions. Executives must also lead by example to foster an environment where employees feel valued, supported, and motivated to perform at their best. By proactively addressing negative conversations, organizations can cultivate a healthy and thriving workplace where employees can thrive and contribute positively to the organization's success.

Positivity

Positive conversations promote a thriving work environment, improve employee well-being, and amplify overall organizational success. High rates of positive communication signal that employees are satisfied with their jobs, engaged with their work, and collaborating productively. Messages with positive sentiment may include praise for an outstanding team, excitement over a recent initiative, or gratitude towards another employee, and they all contribute to a healthier and happieremployee base.

> Thank you! I am totally inspired and proud of our associates and customers. We raised over $120,000 for our local children's hospital during this fundraiser! The time, passion, and focus that goes into this is amazing. Great job to everyone who volunteered, organized, or participated in this great cause, you should be proud.

> I am very proud of you! You are an amazing young man and I am so excited to see what is in your future! You are truly destined for greatness!

Toxic behavior Poses the Biggest Risk

Sexual harassment, bullying, racial slurs—all are examples of toxic behaviors. These behaviors make peers feel unsafe, isolated, and violated. And a toxic employee who engages in these activities is one of the worst things that can infiltrate the workplace.

Inappropriate Language

A message that contains language that is not appropriate for the workplace, such as off-color jokes or innuendo, but does not contain a direct target. These messages could be considered non-toxic if evaluated outside a workplace environment.

Offensive Language

A message that is not appropriate for the workplace and is targeted towards a specific person or group of people. However, the message is not motivated by personal bias.

Hate Speech

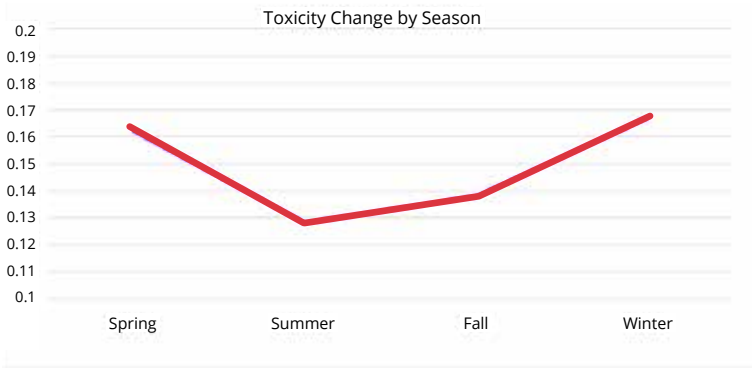
The message expresses strong dislike or bias against a person or group, often containing racial, religious, or sexual slurs. These messages create hostile work environments, particularly if targeted toward a coworker.

Our data reveals 1 in 95 messages contains toxic speech, including inappropriate, offensive, and hate speech. Toxicity can be impacted by both external and internal factors. Seasonally, toxicity peaks in winter and is lowest in summer. And even day-to-day, there is a 7.5% increase in toxicity from the weekdays to the weekends.

Metrics like these shed light on crucial workplace trends and employee dynamics. For example, the winter season may introduce unique stressors and increased responsibilities that are not present during summer. A study from the American Psychological Association revealed that 38% of people experienced a surge in stress during the holiday season.

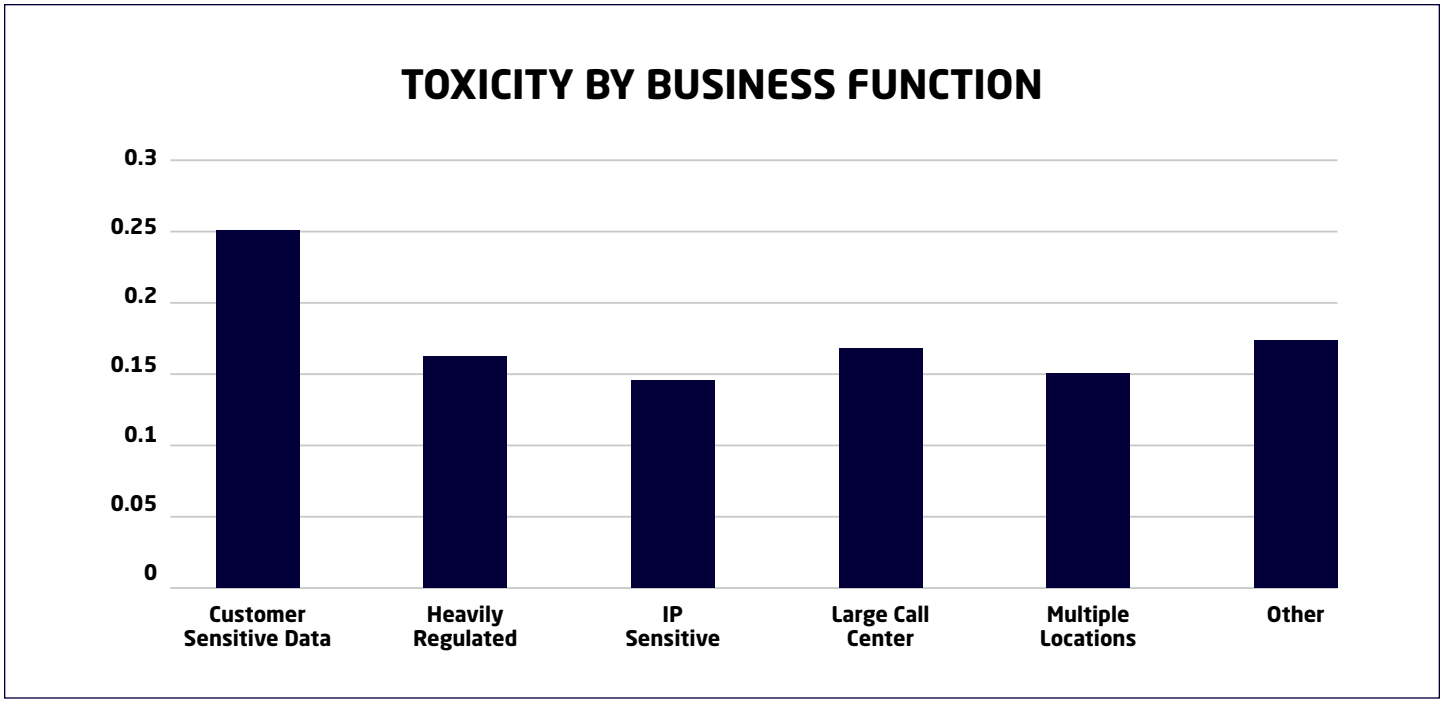
It's also no secret that some industries and job roles are more toxic than others. Aware research found that workplaces with large front lines handling customers' sensitive data are on average 70% more toxic than companies with other primary business focuses. This is highly concerning as toxic work environments decrease employee loyalty and increase the likelihood of a legal or security incident, putting the data they handle at risk.

Benefits of Managing and Reducing Toxicity in the Workplace



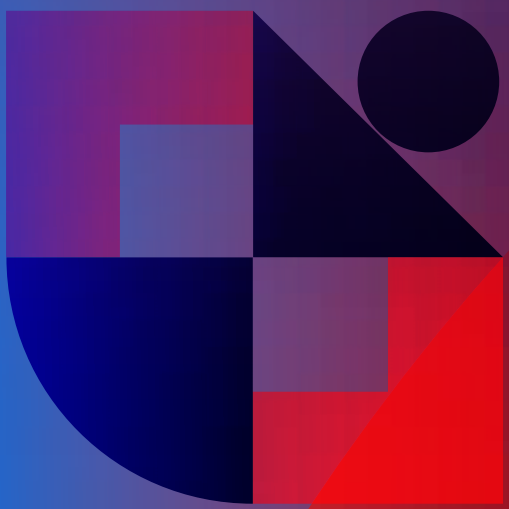
Company leaders must take initiative to unveil and understand workplace toxicity. Unnoticed, toxicity will continue to cause harm to both their organizations and employees.

Decreasing toxic speech and behavior helps to improve company culture, decrease voluntary turnover, and mitigate the risk of a disgruntled employee becoming an insider threat.



CHAPTER 10

FINAL THOUGHTS & NEXT STEPS



Emerging technologies always expose organizations to some inherent risks alongside the opportunities they represent. Cloud-based, real-time collaboration platforms provide a vehicle for more informal, frequent conversations between coworkers but the sprawling datasets they create must be managed and controlled to mitigate the potential harm they could cause.

In addition, collaboration tools give business leaders the opportunity to move beyond biased, infrequent, expensive employee engagement surveys and tap into a real-time, continuous stream of insights from all across the enterprise. Using the very latest in groundbreaking AI designed for and trained exclusively on this dataset, leaders can take a daily pulse of the topics that matter most to their employees.

Attain Actionable, Near Real-Time Insights

Enterprise leaders deserve tools that provide value, making decision-making simpler. That's why the Aware platform not only enables enhanced visibility, but also leverages proprietary AI Models to offer truly actionable insights from the vast amount of unstructured data generated whenever—and wherever—employees talk.

Get started with Aware

Protect your company, enable employee success and transform business outcomes.
www.mimecast.com


Aware
now part of mimecast