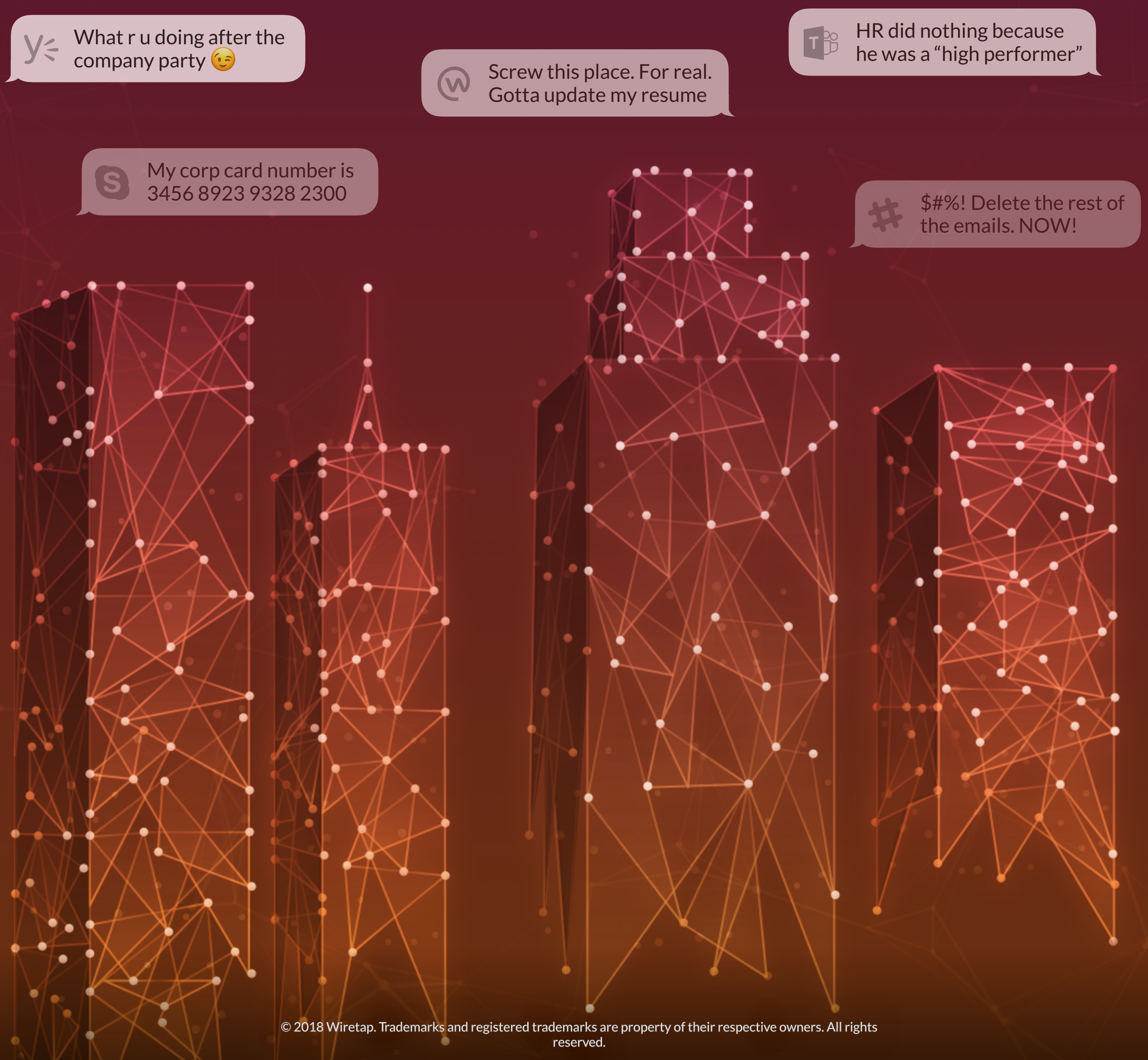
wiretap

JUNE 2018

# The Human Behavior Risk Analysis Report

Discover employee behavior that could be threatening your organization's security, compliance and culture.



What r u doing after the company party 😉

Screw this place. For real. Gotta update my resume

HR did nothing because he was a "high performer"

My corp card number is 3456 8923 9328 2300

$#%! Delete the rest of the emails. NOW!

## TABLE OF CONTENTS

INTRODUCTION

HIGHLIGHTS

SECTION ONE: SENTIMENT

SECTION TWO: TOXICITY

SECTION THREE: INSIDER THREATS

CONCLUSION

NEXT STEPS

## About the Human Behavior Risk Analysis Report

**WIRETAP'S BEHAVIORAL** intelligence team examined more than *a million enterprise collaboration messages* from tens of thousands of authors in order to glean the insights found in this report.

Though this report focuses on aggregate trends across many organizations and industries, Wiretap regularly conducts individualized Collaboration Risk Assessments to help organizations better understand their unique blind spots and areas of risk.

Send us an email to request your own assessment at hello@wiretap.com

**Or for more info:**
wiretap.com/assessment

WIRETAP THOUGHT LEADERSHIP

CONTACT

Aware by wiretap

# A NOTE FROM WIRETAP'S HEAD RESEARCHER

**OPEN, EFFICIENT** communication drives innovation in the modern workplace, where it can facilitate knowledge transfer and problem solving, reduce uncertainty, and break down geographic and managerial hierarchies.

Yet, leaders still hesitate to roll out digital collaboration technologies. After all, these platforms often encourage more informal communication, which can lead to both good and bad behavior.

**EXECUTIVES WORRY** that employees will share confidential information (maliciously or not) with people they shouldn't; that these platforms will become conduits for harassment and other toxic behaviors; or that they will just provide another, needless distraction for employees already suffocating under the weight of email and text messages.

However, the advantages of collaboration platforms greatly outweigh any perceived risk. Furthermore, the risks associated with collaboration platforms are manageable—certainly more so than trying regulate inappropriate banter around the water cooler.

The following report provides an unprecedented glimpse into how employees communicate on enterprise collaboration platforms.

While much of the focus of the report is on gauging risk, the results should also provide encouragement to leaders pushing for broader adoption of collaboration tools. Some of the results highlighted in the study are unsurprising.

For instance, scholars have long known that small groups of heavy users often drive communication networks, and we find the same thing: in our sample, **approximately 25% of users author more than 80% of all messages.**

We also find that toxic behavior is relatively rare and is mostly driven by a small group of employees engaged in private conversation.

Ultimately, this report provides insight that we already know: human behavior is unpredictable. And despite the small population of risky collaboration users, organizations need the ability to identify toxic actors *before* they ruin company culture.

*As the idiom goes, one bad apple can ruin a whole pie, or in this sense, your organizational health.*

Organizations need to track the sentiment and tone of both public and private conversations in order to get a true pulse on the health of their community and assess any areas of potential risk—and they need to do this efficiently without disrupting an already overworked team.

Jason **Morgan, PhD**
VICE PRESIDENT OF BEHAVIORAL INTELLIGENCE

# UNPREDICTABLE HUMAN BEHAVIOR

**LONG BEFORE THE DIGITAL ERA,** major enterprise organizations across the globe focused on one common risk that spanned every size of business and penetrated every industry …

INTRODUCTION

# UNPREDICTABLE HUMAN BEHAVIOR

**TODAY, AS ORGANIZATIONS** continue to undergo a massive digital transformation and seek new ways to connect employees, unpredictable human behavior still weighs on the minds of executives, perhaps even more so than ever before.

**AND DESPITE THE CLEAR BENEFITS** of digital enterprise collaboration platforms such as Workplace by Facebook, Microsoft Teams, Yammer and Slack, organizations sometimes hesitate to fully implement these technologies. Leaders cite concerns around security against insider threats, regulatory compliance and company policies.

With frequent data breaches and cloud storage infiltration, CIOs and CISOs are rightly concerned. After all, **53% of data security incidents in 2017 resulted from employees**, including factors such as human error[1].

Furthermore, leveraging digital enterprise collaboration creates blind spots within an organization; that is, little to no visibility into areas of shared content and conversations amongst employees. This exposes the organization to potential threats such as data loss, inappropriate workplace behavior (think: Uber) and damage to brand reputation.

### COMPANIES LEVERAGING DIGITAL COLLABORATION GAINED

| | |
|---|---|
| 31% | Faster Time-to-Innovation |
| 25% | Fewer Meetings |
| 20% | Higher Employee Retention |
| 15% | Increased Productivity |
| 10% | Revenue Growth |

Source: McKinsey Study, margolis.co.uk, 2016

[1] BakerHostetler 2018 Data Security Incident Response Report, https://wrtp.me/bhdsir18

## Potential Threats in Digital Collaboration

To better understand the potential threats within organizational blind spots, we examined three overarching categories:

### Sentiment

Employee mood and feelings towards the company, culture, and leadership, both positive and negative

### Toxicity

Unprofessional, harassing or discriminatory behavior that can infiltrate an organization

### Insider Threats

Accidental, negligent or malicious actors who place the organization at risk of a breach

**LET US BE CLEAR.** At Wiretap, we love collaboration and this Human Behavior Risk Analysis Report is **not** intended to scare leaders nor block the full implementation of enterprise collaboration platforms.

The purpose of this report is to expose collaboration blind spots, and illustrate where technology—and rapid advancements in machine learning, in particular—can play a key role in helping to understand and manage collaboration.

**Aware by Wiretap** offers full visibility into public and private messages within enterprise collaboration platforms — helping your organization eliminate blind spots.

Aware by wiretap

HIGHLIGHTS

# OBSERVATIONS & KEY FINDINGS

**COLLABORATION PLATFORMS** continue to gain traction in workplaces around the globe.

**EMPLOYEES TEND** to communicate in a much more casual and candid manner on these tools than on more traditional platforms (e.g. email). This new source of communication data presents your organization an opportunity to not only better understand sentiment, but also to monitor topics, keywords, and shared content that gives your teams the information they need to make better, more informed decisions.

| | | |
|---|---|---|
| Negative Conversations | 1 OF EVERY 190<br>Private Messages | 1 OF EVERY 280<br>Public Messages |
| Passwords Shared | 1 IN 149<br>Private Messages | 1 IN 262<br>Public Messages |
| Confidential Information Shared | 1 IN 135<br>Private Messages | 1 IN 118<br>Public Messages |

## Negative Messages Live in the Dark Corners of Digital Collaboration

43 %
Of all messages are **private**

MESSAGES IN PRIVATE GROUPS

135% More likely to be Toxic than messages in a public environment

MESSAGES IN 1:1 CONVERSATIONS

250% More likely to be Toxic than messages in a public environment

1 OUT OF EVERY 7
People exclusively use **private communication**

EXCLUSIVELY PRIVATE MESSENGERS

160% More likely to be Toxic than messages in a public environment

WORDS ASSOCIATED WITH SEX

1 OUT OF EVERY 170 Messages
And this includes public messages!

## In an Organization With 15,000 Employees …

**MAKE NOTE THAT** the people sending this content could potentially harm workplace productivity and, at worst, cause a major PR crisis and open an organization up to risk of legal action.

9 Alarming Messages Sent Per Day

1 TO 2 Employees Sending Alarming Content Per Day

SECTION ONE

# SENTIMENT

**SENTIMENT IS AN ATTITUDE,** thought, or judgment prompted by a feeling. A sentiment analysis aims to determine the attitude of the author within a given message. On an aggregate level, organizations can audit employee mood and feelings towards the company, culture, and leadership.

## The Impact of Sentiment

**SENTIMENT IMPACTS** companies in profound ways. With an understanding of employee opinion, leaders can better determine where to invest in company culture, development, and workplace conditions, which in turn helps to:

### Reduce Employee Turnover

**EMPLOYEES ARE EXPENSIVE,** especially new hires. Unhappy employees tend to leave companies and, even if not explicitly stated, their digital communications can indicate hints of this sentiment. By understanding employee opinion, companies can implement workplace processes, perks, or changes to keep employee morale high.

### Improve Customer Experience

Sentiment is a strong indicator of employee engagement and engaged employees are more likely to improve customer relationships, leading to a 20% increase in sales[1].

### Boost Brand Reputation

Employees are your strongest brand advocates. They know the ins and outs of your organization and its values. It stands to reason that employees with a more positive opinion towards a company speak more highly of the organization when in the community and within their network.

[1] Gallup 2017 State of the American Workplace, https://wrtp.me/gsotaw17

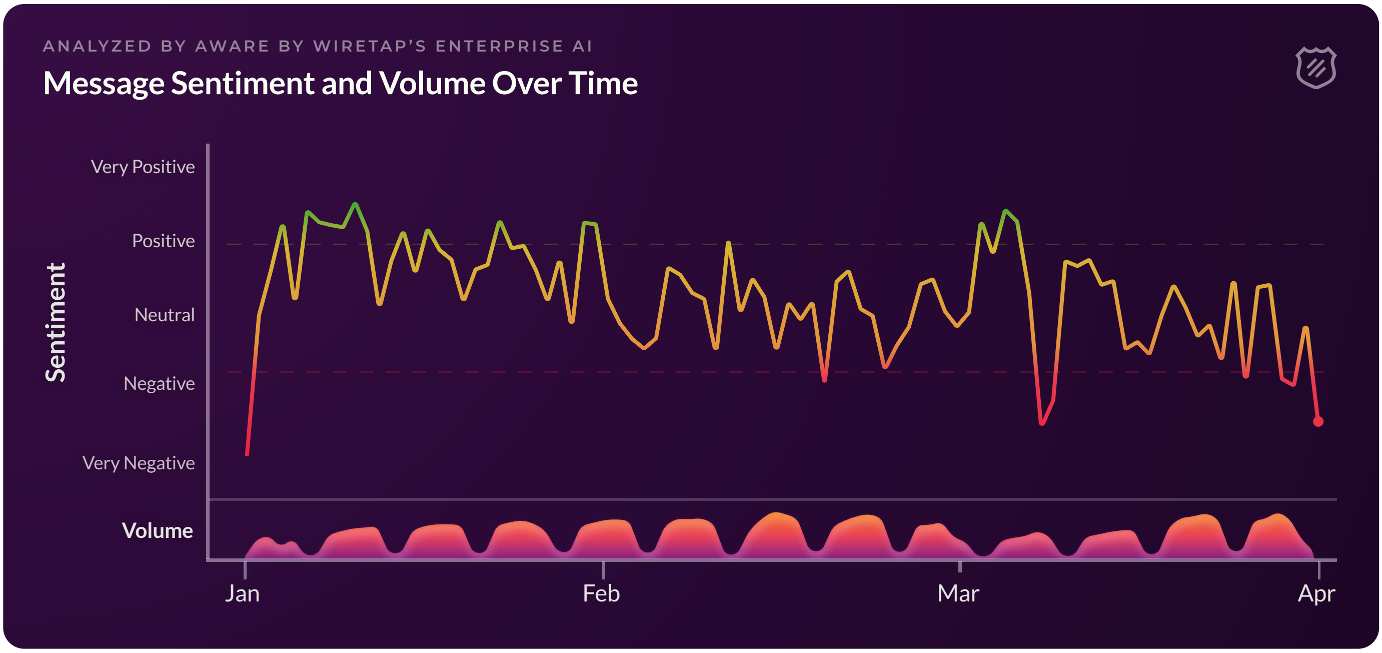
# The Power of Positivity

The majority of messages sent each day remain neutral, as scored by Wiretap's proprietary Sentiment Model. This is expected, as digital collaboration should focus mainly on achieving efficiencies with work.

**HOWEVER,** approximately **1 of every 5** private messages sent each day score positively; this might include messages of praise for an outstanding team or excitement over a recent initiative. This number grows to **1 out of every 3** messages, when looking at public conversations.

When tracked over time, organizations glean valuable insights regarding employee reaction to major announcements. Alternatively, leaders can identify negative trends quickly and search for a possible cause and appropriate solution.

By drilling down to specific business units or work groups, organizations can identify problem areas that might affect the entire company—or find stellar groups to acknowledge and use as role models.



ANALYZED BY AWARE BY WIRETAP'S ENTERPRISE AI

Message Sentiment and Volume Over Time

*Positive messages, such as these, can help boost employee morale and overall productivity.*

### Actual Yammer Message

Fantastic work Team Nash!!! Loving the enthusiasm and passion for our new conversation framework and very much looking forward to seeing you all in person in coming weeks and hearing all about the great customer outcomes you have been delivering :)

### Actual Yammer Message

Thanks John, you've done a fantastic job pulling everything and everyone together. And well done to Casey for producing such great activities. It's going to be a great event, I'm just hoping with all the excitement I remember to keep posting and tweeting!

# Negativity Casts a Larger Shadow

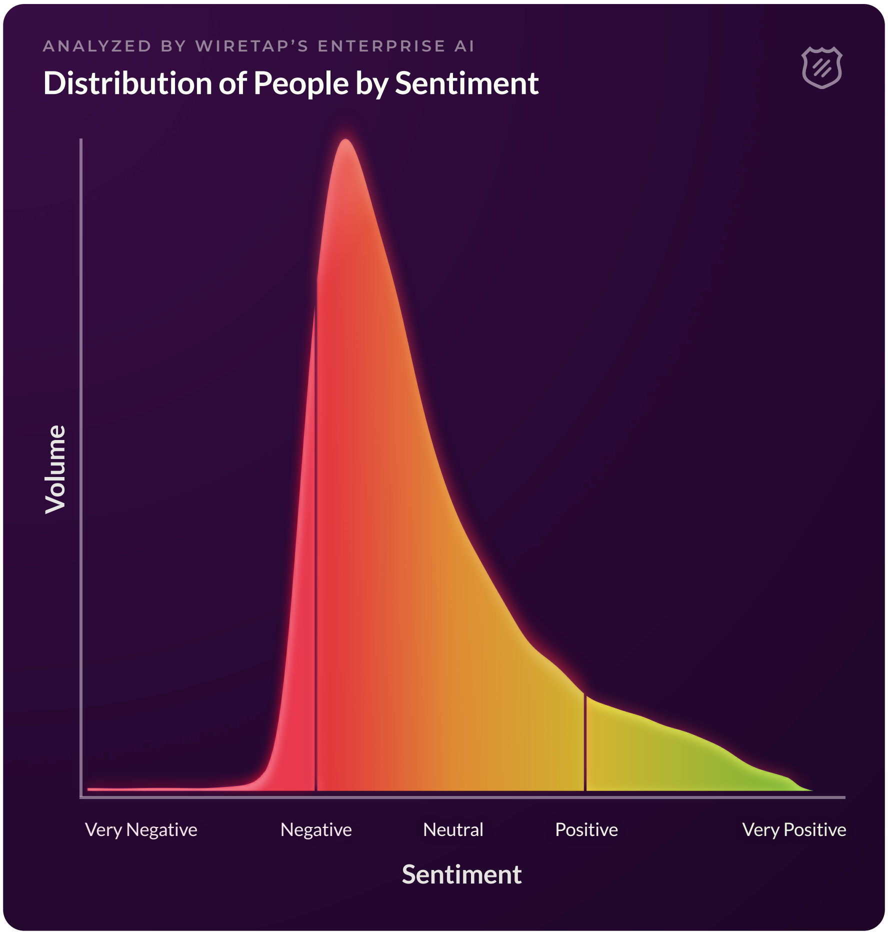
While negative messages comprise just 0.3% of the daily messages sent, they often cast a much larger, darker shadow on an organization.

**LOOKING AT** active contributors (those who sent 25 or more messages), the number of profiles with the most negative sentiment metrics greatly outweigh the users with the most positive sentiment.

The negative messages live in the dark corners of digital collaboration. In fact, only **1 out of every 380 public messages receives a negative sentiment score**. As expected, private groups and conversations are even more likely to skew negatively—in fact, **1.5 times** more likely. But when looking at individuals who only communicate via private messages (**2 out of every 13 individuals**), they are **245%** more likely to send negative messages.

For an organization with 15,000 employees, this translates to approximately **9 negative, potentially-harmful messages a day** within public and private conversations.

Nine messages might not seem like much in the way of volume, but without understanding the context surrounding it, or the content in the message, organizations can't identify the true detriment or cost to the workplace. ●



ANALYZED BY WIRETAP'S ENTERPRISE AI

Distribution of People by Sentiment

ACTUAL MESSAGES

Yes true… just being here shits me… they are all soo f*#king negative.

I'm frustrated that everything I suggest or question I get shut down and made to feel like I don't matter anymore.

This is terribly sad and frustrating. Where is it and what measures were put in place? Unless there is some evidence or strong leads on how the leakage and fraud happened…

WIRETAP THOUGHT LEADERSHIP

# THE CHALLENGE OF THE ANNUAL EMPLOYEE ENGAGEMENT SURVEY

**HUMAN RESOURCES TEAMS** commonly invest in employee engagement surveys annually, in order to better understand employee sentiment and perception of the workplace. However, this process is inefficient, and inherently flawed in a few respects:

> *If you are making informed decisions on old information, you are trying to solve new problems with old data.*

Greg **Moran**
Chief Operating Officer

## Untimely Results, Often Too Late to Take Action

**WITH THESE ONE-TIME SURVEYS,** organizations receive insights from snapshots of a single moment in time. Organizations then leverage this information to make business decisions for a full calendar year.

In reality, organizational sentiment ebbs and flows depending on events and the mood of the organization. For example, a survey distributed soon after a company culture event might yield very different results than if employees took the same survey after a large lay-off. And over a year's time, the accuracy of these surveys inevitably diminishes.

Furthermore, the initial insights are even naturally delayed. Surveys need time to collect employee responses once distributed. Then, it takes additional time to compile and analyze the responses. Human resources teams receive the results several weeks or months later, further diminishing the value of the survey outcomes.

## Biased and Inaccurate Responses

**IN LARGE ENTERPRISE ORGANIZATIONS,** traditional culture surveys often tie directly or indirectly into employee evaluations and bonus pay.

The availability of bonus dollars or other incentives sometimes depends on an increase in positive sentiment at the company, or even overall improvement within a small workgroup, for example. This leaves a lot of space for influence and bias, as teams encourage each other to respond to surveys in a positive manner. As such, employees may choose not to respond honestly.

These surveys also utilize questions shaped by Human Resources professionals and can lead to confusing language. Misinterpretation of the questions may lead employees to answer inaccurately, further skewing the results. Lastly, organizations must determine if the survey even asks the right questions in order to get an accurate pulse of employee opinion towards the workplace.

# How Natural Language Processing AI-Technology Can Change the Face of Sentiment Analyses

With a *natural language processing* solution, an AI-powered technology that analyzes human language, organizations can leverage the communication data in their own ecosystem.

For example, by analyzing the patterns in public and private messaging on Yammer or Workplace by Facebook, organizations can glean more accurate and relevant employee insights than the traditional annual survey process.

## Near Real-Time Insights Allow for More Timely Response

**BY MONITORING** and analyzing communication data within your tech-stack, leaders pull insights whenever needed, analyzing the metric in near real-time. With this insight, leaders can identify when sentiment starts to slip, determine potential causes based on context, and respond before the situation inflames.

AWARE ENTERPRISE AI AT WORK · QUIET · AWARE ENTERPRISE AI AT WORK · QUIET ·

*Led by Dr. Jason Morgan, Aware by Wiretap's artificial intelligence models were built for the exclusive purpose of analyzing enterprise interpersonal dynamics from real enterprise social graphs.*

## Collaboration Platforms and Sentiment Analysis: A Powerful Combination

**COLLABORATION PLATFORMS CONTINUE** to gain traction in workplaces around the globe. Employees tend to communicate in a much more casual and candid manner on these tools than more traditional platforms (e.g. email).

This new source of communication data presents your organization an opportunity to not only better understand sentiment, but also to monitor topics, keywords, and shared content that gives your teams the information they need to make better, more informed decisions.

**Aware by Wiretap's** AI-driven, proprietary sentiment model analyzes workplace communication and delivers a real-time sentiment metric informed by both message content and context. Therefore, leaders need only to check a dashboard to keep a pulse on organization sentiment.

If they see an issue, they can investigate—bias free. With shared content monitoring functionality, the team can also pull relevant messages and leverage additional context to identify the root of the sentiment change.

SECTION TWO

# TOXICITY

**SEXUAL HARASSMENT,** bullying, racial slurs—all of these are examples of toxic behaviors. These distracting behaviors make peers feel unsafe, isolated, and harassed. And a toxic employee, one whom engages in these activities, is one of the worst things that can infiltrate the workplace.

## Toxicity is Contagious

**TOXIC EMPLOYEES** have a way of spreading their behavior to others' around them, similar to a nasty virus; crippling others morale, performance, and productivity. While not all employees are toxic, all employees are capable of adopting toxic behaviors and people who are close to a toxic employee are more likely to become toxic themselves.

### Unprofessional

The message uses harsh language, slurs, phrases or innuendo that is not appropriate for a work environment, but wouldn't necessarily qualify as inappropriate in a personal setting.

ACTUAL MESSAGES

WTF? Why is this greaseball goon now involving himself in politics?

P.S. I think everyone has the xmas shits luvbahahahahahaha

### General Harassing

The message contains off-color jokes or content that might offend a person or group; the message includes sexual innuendo that may be offensive to others, but is not targeted at the message recipient.

...I feel like I'm always compared to that f**kwit.

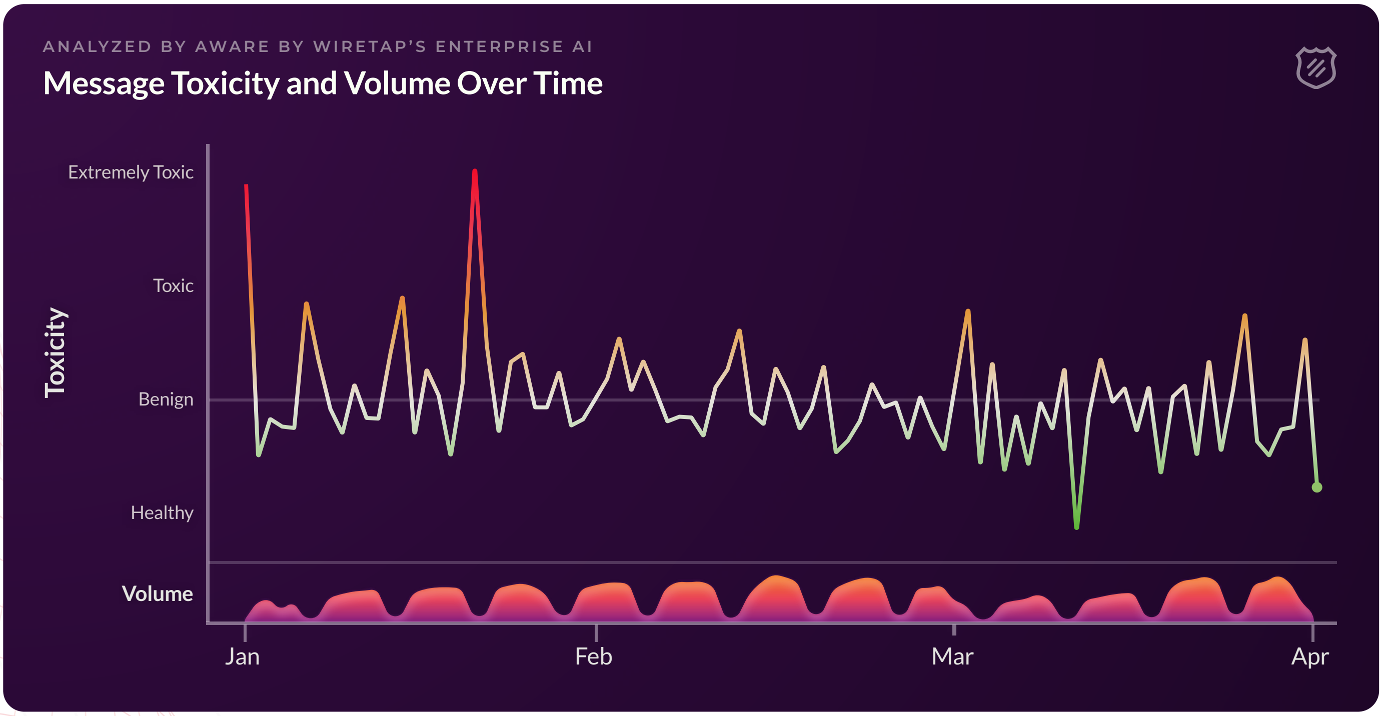
### Discrimination

The author expresses strong dislike of a person or group of people; the message contains racial, religious or sexual slurs towards a person or group; the message creates an unpleasant or hostile situation, possibly sexual in nature, particularly if the message is targeted at the recipient or coworker.

I hope your halo doesn't fall off when you're riding the f*** out of my big fat c***.

# The Impact of Toxicity in the Workplace

Most organizations want to track and understand toxicity in the workplace. Toxicity causes both the organization and the employees to suffer.



**POORLY MANAGED** work groups are generally **50% less** productive and **44% less** profitable according to Gallup. And men who worked for toxic managers were **60% more likely** to suffer a heart attack[1].

Tracking individual employee toxicity over time can help identify and differentiate habitually toxic employees from those who begin to trend more toxic than previously.

Using these insights, organizations can dig deeper to understand why an individual might suddenly exhibit toxic behaviors by looking into the context around the toxic messages.

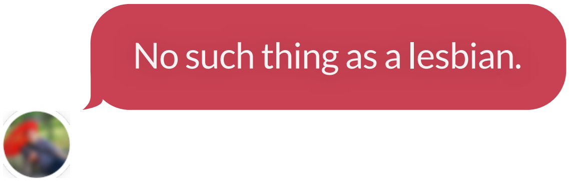
[1] Gallup 2017 State of the American Workplace, https://wrtp.me/gsotaw17

# Toxicity in Private Messages

At one organization an individual revealed his or her sexual orientation and was subsequently harassed via private messages from colleagues.

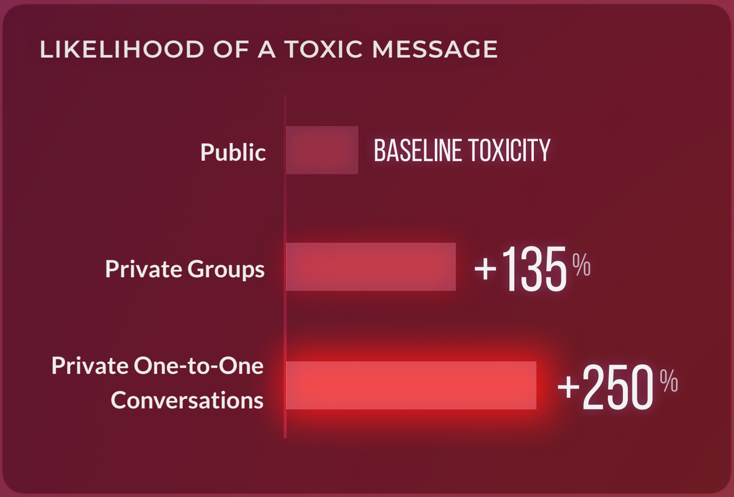
**USING THIS SCENARIO,** if the harassment continues over time and goes unaddressed, the victim might begin to feel unsafe and unwelcome in the workplace, leading to disengagement and potentially toxic behavior.

However, if an organization quickly identifies the harassment, or begins to see that the victim is trending negatively, leaders can intervene appropriately.



No such thing as a lesbian.

*Actual message a person sent to an openly gay employee*



**OUR DATA REVEALS** that messages in private groups are **135%** more likely to be toxic & *messages in private, one-to-one conversations are **250%** more likely to be toxic than messages in a public setting.*

Additionally, individuals who *only* communicate in private groups or conversations are **160%** more likely to send toxic messages.

# Drugs, Sex and Other Not-Safe-for-Work Topics

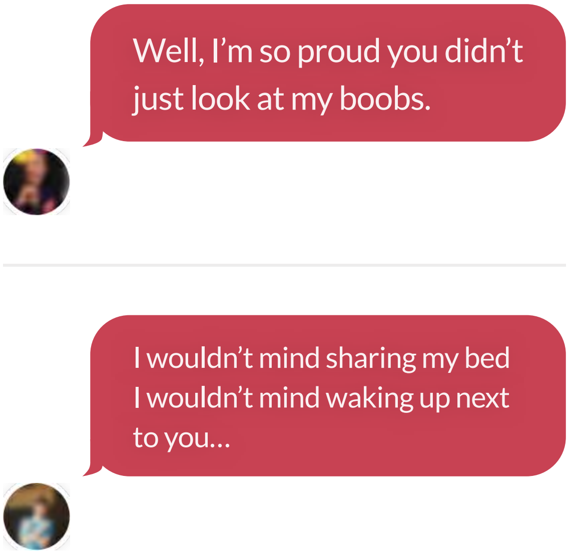
With **43%** of all messages occurring in private groups or conversations, organizations face the potential for toxic messages to proliferate out of control.

**IN ADDITION TO HARASSMENT,** employers must also deal with toxic behaviors such as drug usage, discrimination, sexual misconduct and more. As expected, private messages are **nearly 160%** more likely to contain words associated with illicit and pharmaceutical drugs.

Somewhat surprisingly, though, **1 out of every 170 messages**, including public messages, contains words associated with sex.

In fact, **1 out of every 132** individuals sent a not-safe-for-work (NSFW) or toxic message within the first quarter of 2018. ●

ACTUAL MESSAGES



Well, I'm so proud you didn't just look at my boobs.

I wouldn't mind sharing my bed
I wouldn't mind waking up next to you...

## In an organization with 15,000 employees ...

This translates to over **130 individuals per quarter** who sent a message that could potentially harm workplace productivity, and at worst, cause a major PR crisis and open an organization up to risk of legal action.

Aware by wiretap

WIRETAP THOUGHT LEADERSHIP

# THE DAMAGE OF A TOXIC EMPLOYEE

**RARELY A DAY** goes by without a headline that reveals misconduct or poor culture at a major enterprise organization. Depending on the offense, the impact of toxic behavior varies widely, but regardless the potential damage is significant.

## Lower Morale

80%

In a Gartner study, **80%** of employees experienced less commitment to their workplace because of a toxic employee.

## Higher Turnover

12%

Gartner found that **12%** of employees have left an organization entirely due to a toxic coworker.

## Performance Decline

30–40%

With the contagious nature of toxicity, having just one toxic employee in a group can bring down team performance by **30% to 40%.**

## Increased Risk

Overlooked toxic behaviors, such as bullying or harassment, can open a company up to legal risk. Unfortunately, companies like Uber, Fox News, or Nike know all too well the repercussions of turning a blind eye to toxic behavior.

## Damaged Brand Reputation

If a situation escalates to legal action or becomes a press nightmare, organizations face both financial and organizational costs to deal with litigation, public relations, crisis management and brand reputation management.

**IN MARCH 2018,** Nike's boys-club culture and the shortcomings of the human resources department was a topic of the national conversation regarding how to address and expose these important issues[1].

**EARLY IN 2018,** 100 Google employees organized to combat cyber bullying against employees. The group demanded more well-defined rules for internal forums, enforcement of rules, and protection for targeted employees[2].

[1] Wall Street Journal, "Inside Nike, a Boys-Club Culture and Flawed HR," https://wrtp.me/wsjnike

[2] Reuters, "Exclusive: Google Employees Organize to Fight Cyber Bullying at Work," https://wrtp.me/googbully

# Artificial Intelligence and Toxic Behaviors

The cost of a wounded culture cannot be understated, leading to increased turnover, reduced productivity, and decreased brand sentiment. Protect your organization, and its culture, by investing the time and resources to minimize and remove toxic scenarios.

## Identify, Address Toxic Behaviors

**FIRING A TOXIC EMPLOYEE** can prove difficult due to the lack of "hard evidence" exposing the behavior, yet these employees hurt the business.

By leveraging artificial intelligence, human resources teams can revolutionize the way they deal with toxic employees.

For example, they can monitor employee digital communications—such as private or public messages in Microsoft Teams or Workplace by Facebook—and automatically flag violations of predetermined company policies.

This saves teams a significant amount of effort searching for evidence of a violation and creates more time to determine an appropriate response.

## Determine an Action Plan

**IN A DIGITAL SITUATION,** some tools, such as Aware by Wiretap, allow automation when violations or other incidents occur.

For example, organizations can set messages with a high level of sexual content to notify a human resources representative for follow up.

Alternatively, content with foul speech can trigger an automated communication coaching the employee that the transmitted word choice is inappropriate for work.

Each organization is unique, and therefore must determine the most appropriate response based on existing corporate culture. Most importantly, though, leaders must consistently communicate that the organization will not tolerate toxic behavior. ●

SECTION THREE

# INSIDER THREATS

## Accounting for the Cost of an Insider Breach

Insider threats are one of the most prevalent threats in an enterprise environment, and are difficult to mitigate.

**MANY OF THESE BREACHES** result simply from human error or negligence, rather than a malicious incident. According to Ponemon[1], the global average cost of a data breach is **$3.62 million**, regardless of if the incident stemmed from an intentional or accidental act.

Furthermore, an article in the Harvard Business Review estimates that **80 million insider attacks** occur annually[2], a cost that amounts to more than **$10 billion** in fines, penalties, or operational disruption[3]. That doesn't even account for the unquantifiable damage to an organization's brand and credibility.

### "But ... We Only Hire Good People in My Organization"

**WIRETAP CHIEF OPERATING OFFICER,** Greg Moran says that "it is an inconvenient truth that not everyone inside an enterprise is trustable, despite all efforts to hire trustworthy employees."

It's tempting to fall in the trap of thinking, *but we hire good people here!* We trust our employees. However, the truth is that nearly every organization will have an employee that is not acting in the best interest of the company.

**Private conversation messages are:**

**144% MORE LIKELY**
To contain confidential information

**165% MORE LIKELY**
To contain identification numbers

**6x MORE LIKELY**
To use 'password' keywords

[1] 2017 Ponemon Cost of Data Breach Study, https://wrtp.me/ibmbreach

[2] Harvard Business Review, "The Danger from Within," https://wrtp.me/hbrdanger

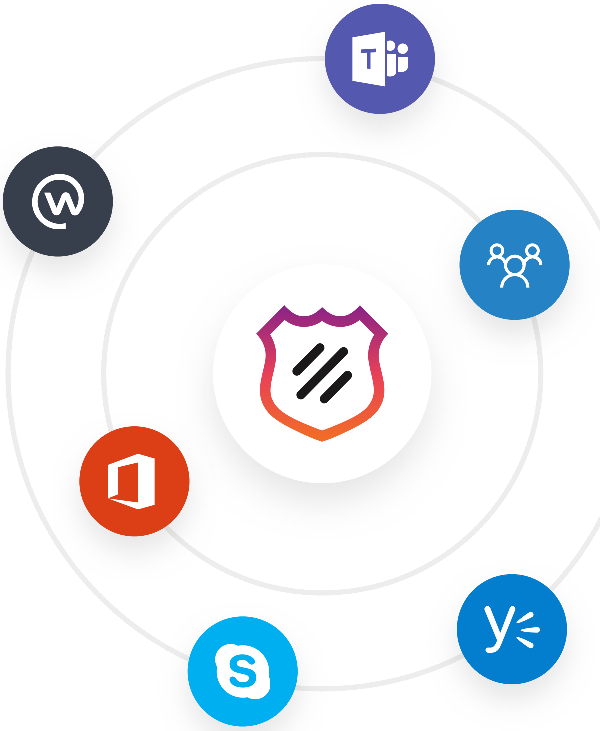
[3] CSO from IDG, "Reading Between the Lines: The Real Impact of Insider Threat," https://wrtp.me/csoinsider

# Information Sharing Is Easier, and More Reckless, Than Ever

**AS EMPLOYEES** become increasingly dependent on digital tools for day-to-day communication, the interactions become more casual and, at times, careless. This creates even more space for breaches or sensitive information sharing.

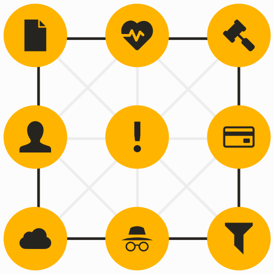
More and more organizations continue to adopt digital collaboration platforms, but the real-time sharing of unstructured data within these tools creates a critical gap in the overall business security fabric.

While nearly all organizations deploy security measures and data loss protection (DLP) for email and internet usage, few realize the blind spot created by using collaboration tools without proper monitoring and governance in place.



## Symantec’s 2018 Shadow Data Report

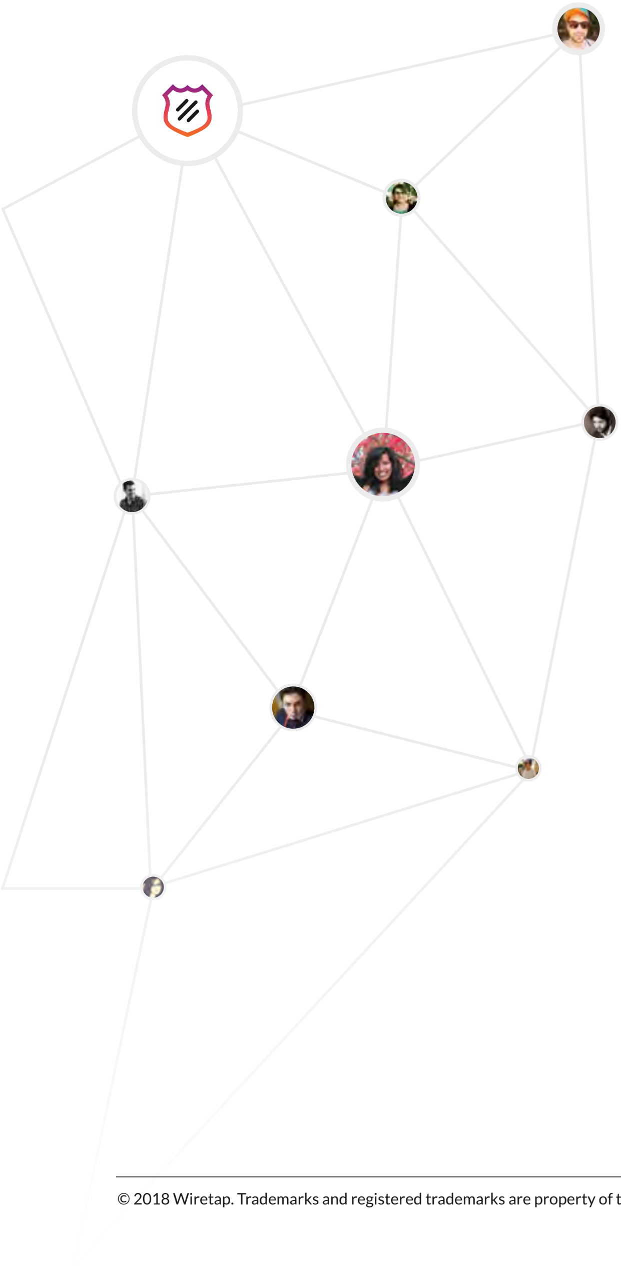
- **13%** of all files stored in the cloud are broadly shared, and **1%** of these files contain compliance related data
- **18%** of all PII, **13%** of all PCI and **56%** of all PHI shared in the cloud is overexposed
- **68%** of organizations have some employees who exhibit high-risk behavior in their cloud accounts (activities such as data destruction, data exfiltration, and account takeovers)



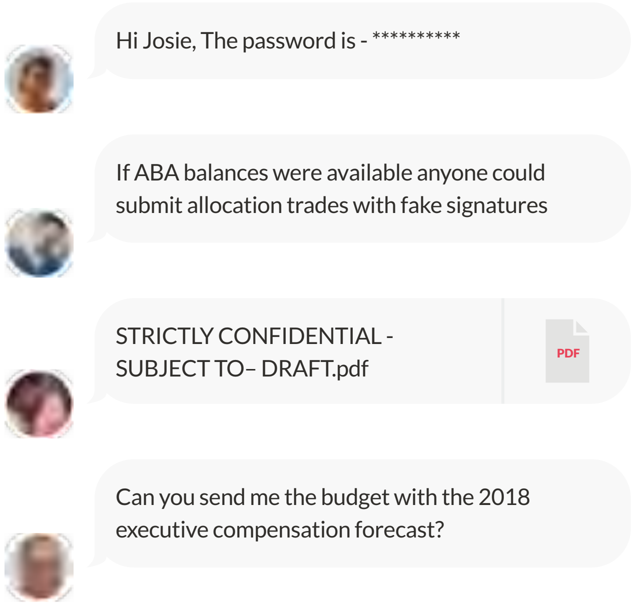
Symantec.

# Information Is Shared Privately *and* Publicly

**WHILE SOME** of these messages might adhere to industry regulations and company policy, your organization can't distinguish appropriate use versus potential leaks without some form of monitoring capability in place—specifically for collaboration platforms. ●



ACTUAL MESSAGES



Hi Josie, The password is - **********

If ABA balances were available anyone could submit allocation trades with fake signatures

STRICTLY CONFIDENTIAL - SUBJECT TO– DRAFT.pdf

Can you send me the budget with the 2018 executive compensation forecast?

## How Often is Sensitive Information Shared?

| | Private | Public |
|---|---|---|
| Confidential Information | 1 in 135 | 1 in 118 |
| Passwords | 1 in 149 | 1 in 262 |

Aware by wiretap

WIRETAP THOUGHT LEADERSHIP

# INSIDER THREATS AND WORKPLACE COLLABORATION PLATFORMS

**AN INSIDER THREAT** is a risk of breach that comes from individuals within a given organization (e.g. employees). The risk level with this type of threat is especially high given the amount of access, knowledge, and autonomy employees possess.

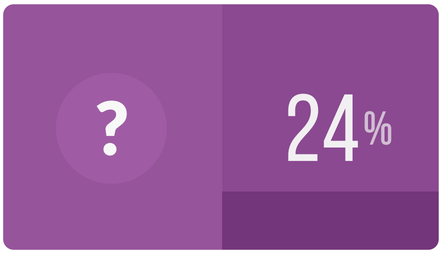
The truth is, inconveniently, people act one way in formal meetings and another way on their company's digital collaboration network.

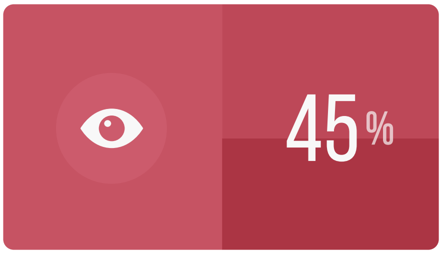
And this inconvenient truth can add a layer of risk, or a blind spot, for the organization.

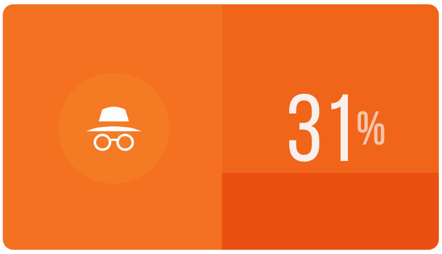
# The Different Kinds of Insider Threats

As the technology of collaboration platforms continue to gain traction, the concern for insider threats grows.

**NOT ALL INSIDER THREATS ARE THE SAME,** though they all present a danger to the organization. The three basic types of threats inside the workplace, and their allocation percentage, include[1]:







## Inadvertent Actors

**EVEN WHEN** it comes to benevolent employees, there is still the risk of insider threats simply from employee negligence. Often, employees don't understand when their behavior, such as sending a sensitive document over a public company channel, is risky.

These well-meaning employees benefit from trainings regarding safe workplace behaviors.

## Outsiders

Outsiders could include 3rd party contractors who possess some degree of access to the workplace networks. Unfortunately, some of the most devastating data breaches in recent years happened via third party vendors.

For example, in April of this year, hackers targeted third-party sellers on Amazon.com to post fake deals and steal cash[2].

## Malicious Insiders

These are the evil-doers that we often picture when speaking about insider threats. These employees either enter an organization with the intention of causing some sort of breach or damage, or become a disgruntled employee who commits the act on their way out the door.

[1] IBM Security Intelligence "The Threat Is Coming From Inside the Network: Insider Threats Outrank External Attacks," https://wrtp.me/sicsi

[2] Wall Street Journal, "Amazon's Third-Party Sellers Hit By Hackers," https://wrtp.me/wsjamz3

# Mitigate the Risk of Insiders With Workplace Monitoring

The casual, threaded communications on collaboration platforms continue to gain traction and, in some scenarios, replace email completely.

**COLLABORATION PLATFORMS** offer many positive attributes, such as cross-functional communication, quick distribution of information, and increased workplace connectivity—all of which can lead to increased productivity and profits. However, it's time to take the inherent risks of these communication platforms seriously.

There are more casual and chatty conversations in a Yammer multi-company group or Workplace private message setting than in an email conversation, for example. This creates a scenario where inadvertent actors may accidentally and negligently share sensitive data because they put something in writing they wouldn't ordinarily email to a colleague. Unfortunately, this also creates more space for malicious insiders to pray on those inadvertent actors.

Today, nearly all organizations monitor employee email communications with some sort of data loss prevention (DLP) solution. In fact, as of April 2017, **78% of major companies** now monitor employees' use of email, internet, or phone[1]. It's time now to add a monitoring and compliance solution created specifically for the unique ecosystem of digital collaboration.

[2] Wall Street Journal, "Amazon's Third-Party Sellers Hit By Hackers," https://wrtp.me/abc78

CONCLUSION

# COLLABORATION TOOLS & HUMAN BEHAVIOR RISK

**AS WITH ANY** emerging technology, introducing tools like Microsoft Teams, Yammer or Workplace by Facebook exposes organizations to some inherent risks.

**THESE PLATFORMS** house more informal, frequent correspondences in both private and public forums. Our research very clearly shows that employees do, in fact, behave differently in a public versus private digital environment, and this does introduce a new set of potential risks to the enterprise security ecosystem.

The most unpredictable risk of them all impacts both company security and organizational health: **human behavior.**

## Choose Secure Collaboration

**WE'LL BE THE FIRST TO SAY**—at Wiretap—we *love* collaboration and are exhilarated for the future of the digital workplace. We believe in the impact of increased cross-functional communication, enabled innovation, and real-time information sharing.

Sometimes the task of problem-solving for risk mitigation makes it tempting to say no to adopting collaboration tools. However, that could ultimately cost your organization greatly in lost productivity. That's why we seek to serve as collaboration 'unblockers' for enterprises around the globe and refuse to let risk halt innovation and progress.

At Wiretap, we believe in this so strongly that we created a solution that mitigates human behavior risk, while also tapping into a plethora of employee collaboration content in order to offer real-time insights to the organization.

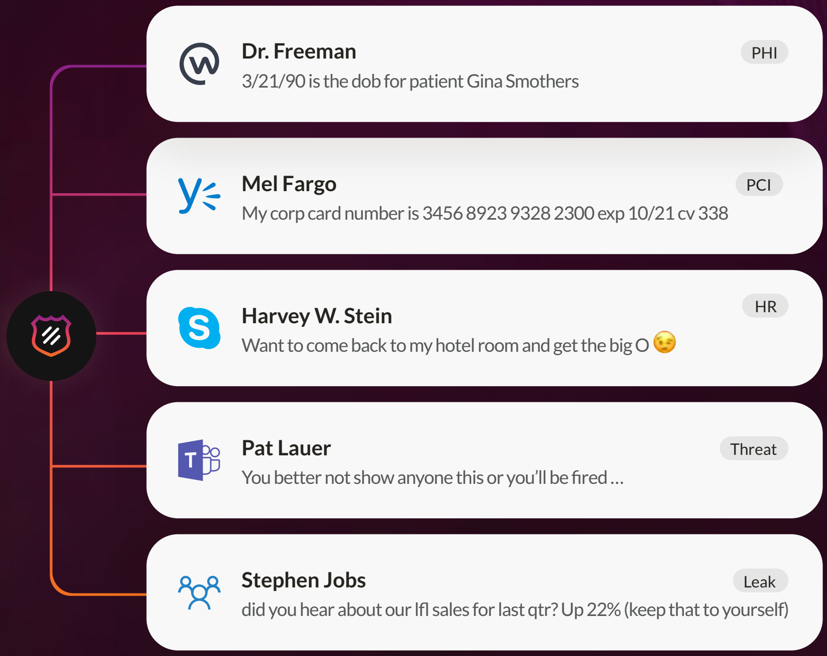
Aware by wiretap

GAIN VISIBILITY INTO EMPLOYEE COMMUNICATIONS

# THE MONITORING & COMPLIANCE SOLUTION FOR ENTERPRISE COLLABORATION

**AWARE BY WIRETAP** seamlessly integrates with Microsoft Yammer, Teams, and Workplace by Facebook.

The solution delivers exceptional visibility into shared employee content (both private and public); enables compliance with regulations such as GDPR, HIPPA, and FINRA; and facilitates safe collaboration by monitoring shared files and materials for insider threats, harassment and more.



Dr. Freeman PHI
3/21/90 is the dob for patient Gina Smothers

Mel Fargo PCI
My corp card number is 3456 8923 9328 2300 exp 10/21 cv 338

Harvey W. Stein HR
Want to come back to my hotel room and get the big O 😉

Pat Lauer Threat
You better not show anyone this or you'll be fired ...

Stephen Jobs Leak
did you hear about our lfl sales for last qtr? Up 22% (keep that to yourself)

# 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 a proprietary AI-infused model to offer truly actionable insights from the vast amount of unstructured data housed within an enterprise collaboration program.

### Insights come from behavior metrics like:

#### Sentiment Score

A measurement of the mood and feelings of employees towards the company, culture, and leadership.

#### Toxicity Score

A measurement of distracting behaviors that make peers feel unsafe, isolated, and/or harassed.

#### Insider Threat Score

The level of risk presented by individuals within the organization of a potential breach; this includes both inadvertent or malicious actors.

### Respond Effectively

**WITH A DATA BREACH** or workplace toxicity, it's not enough to simply know of the issue. An appropriate, timely response can make or break your organization's reputation.

That's why **Aware by Wiretap** allows leaders to configure custom policies in order to identify and respond to incidents within the collaboration environment.

This might include automatically deleting sensitive file-sharing (e.g. information breach), alerting a leader of inappropriate content (e.g. sexual harassment), or simply sending the offending employee a pre-composed coaching communication regarding the infraction. ●

Aware by wiretap

NEXT STEPS

# Get Unprecedented Insight Into Your Collaboration Platforms

## See how your enterprise stacks up with these benchmarks.

**REQUEST A FREE** Collaboration Risk Assessment to gain visibility into employee interactions and identify potentially harmful or inappropriate communications on your organization's collaboration platform.

Empower your organization to collaborate with confidence with enhanced monitoring, visibility, governance and culture protection.

Get an Assessment Now

Aware Collaboration Risk Assessment
For Your Collaboration Tools

ARE YOU AWARE?

## Get Your Free Collaboration Risk Assessment

Find out if individuals are putting your organization at risk.

844.433.3326 hello@wiretap.com wiretap.com/assessment

# About **Wiretap**

**WIRETAP'S FLAGSHIP** platform, Aware by Wiretap, delivers secure collaboration, monitoring and governance for enterprise organizations deploying today's leading collaboration and messaging platforms, including Microsoft Teams, Microsoft Yammer®, and Workplace by Facebook.

**Aware by Wiretap** encourages and facilitates safe collaboration and compliance by monitoring files and conversations, as well as preventing communication that could place organizations at risk.

The editors of Columbus Business First recently named Wiretap one of the Best Places to Work in Columbus, and leading research analyst firm CB Insights cited Wiretap as a leading early stage cybersecurity startup to watch in the Insider Threat Detection category.

FOR MORE INFORMATION, VISIT:

**Our Website |** wiretap.com
For up-to-date details on products, case studies and blog posts.

**Twitter |** @AwareByWiretap
Get timely articles and conversations around collaboration and security.

**LinkedIn |** linked.com/company/wiretap
Follow for networking opportunities, job openings and industry news.

**Press Contact |** marketing@wiretap.com
Email us to receive additional media assets or to schedule an interview.

**Other Inquiries |** hello@wiretap.com
Contact us for product demos, partnership opportunities, and sales.

**Wiretap HQ**
111 Liberty Street, Suite 102
Columbus, OH 43215-5656