Aware

WHITEPAPER

SIX CRITICAL DIGITAL WORKPLACE SECURITY RISKS AND HOW TO AVOID THEM.

Avoid inherent risk afforded by unprecedented collaboration across the digital HQ.

INTRODUCTION

THE RISE OF **ENTERPRISE COLLABORATION AND MESSAGING TOOLS**

have brought about unprecedented collaboration opportunities to organizations that embrace them in the growing digital workspace.

Collaboration technology helps break down existing silos of information, people, and processes that slow innovation and kill productivity. However, collaboration platforms come with risk. When an organization's day to day operations occur within a digital workplace, across a variety of platforms, channels, and groups—security gaps emerge. If social networks and collaboration tools are not properly secured and automatically monitored, risk to the organization is high and fallout can be costly. Being familiar with common security risks and knowing how to avoid them is the single best way for organizations to increase their likelihood of success.

What's included in an enterprise collaboration ecosystem?

Not surprisingly, enterprise collaboration is an emerging field of technology that's constantly changing, with varying terminology depending on who you talk to. These tools have evolved into a virtual community where an organization's employees and stakeholders can exchange information and ideas to improve collaboration. Other tools in this space are sometimes referred to as messaging or collaboration tools. Examples of tools that may make up a company's collaboration ecosystem include Slack, Zoom, Microsoft® Teams, Microsoft® Yammer, Workplace from Meta, and many more.

6 Critical Digital Workplace Security Risks: How to Avoid Them and Close the Security Gap

Six common and potentially harmful security risks associated with social collaboration tools in the digital workplace are:

01 Culture Compliance

02 HR Policy Violations

03 Data Leaks

04 Insider Threats

05 Regulatory Compliance

06 IP Leaks

RISK 1

CULTURE COMPLIANCE

Recently, employee emotions and mental health have taken the spotlight at work. Global events and shifts in working conditions throughout the pandemic have blurred the lines between work and life. Executive leaders have more of these concepts top of mind now to maintain culture as a critical competitive advantage for their business.

Many organizations craft and publicize a mission statement and a set of shared values that embody the company culture. But publishing a document with organizational culture ideals may not be enough to assure adherence and reduce risks that may arise from not actually embracing it. The most forward-thinking organizations look inward to ensure their employees are displaying the company values in how they approach getting work done.

RISK 1: Culture Compliance

> If you see success as a zero-sum game, life becomes a series of cut-throat competitions. You reach the top by taking others down. If you see the possibility of a mutual benefit, your goals shift from crushing the competition to making a contribution. You rise by lifting others up.
>
> **Adam Grant**
> Organizational psychologist at
> Wharton Business School

Empathy matters when it comes to organizational culture compliance in employee interactions. Many workplaces state and embrace similar points of view as a way to operate their businesses.

How can leading organizations implement a proactive culture compliance strategy for the mutual benefit of employees and the enterprise?

Proactively look for risks by monitoring for negative sentiment, toxic speech, or controversial topics and themes that pop up in employee conversations. With a proactive strategy, you may uncover problem areas before they get to the point of becoming an official HR policy violation. Use this as an opportunity not always to punish, but to coach undesired employee behaviors. Simultaneously, organizations may uncover positive culture compliance and use the findings as an opportunity to reward and incentivize acts of encouraged workplace behavior. This helps nudge an organization's core values in the workplace moving forward.

Proactively pinpointing areas where there is a lack of empathy, or cultural compliance between employees will decrease burnout and employee turnover, and ultimately help mitigate the other risks that will be discussed in the following sections that can prove to be extremely costly.

76%

of employees believe an empathetic organization inspires more motivated employees.[1]

80%

of CEOs believe that empathy can be learned.[1]

61%

of people with highly empathic senior leaders report often or always being innovative at work compared to only 13% of people with less empathic senior leaders.[2]

RISK 2

HR POLICY VIOLATIONS

HR policy violations are inevitable at large organizations. Often, cases involving sexual harassment, offensive language, and lewd behavior can fester for months or even years before HR or upper management become aware of them. Many harassment cases go unreported, and the violated employee simply leaves, or worse, takes legal action on the company. Meanwhile, the bad behavior of the offender continues unchecked — increasing risk to the organization and its people.

RISK 2: HR Policy Violations

The normalcy of remote and hybrid work has put a heightened lens on policy violations due to a lack of culture compliance. Recent studies show that over one-third of US workers were subject to harassment while working remotely.[3] In leaving the physical workplace, there is a lack of oversight, absence of presence from others, and the extension of a digital workplace that facilitates more asynchronous communication, more privacy between employee communications, and somewhat of an invisibility factor. These circumstances may lead others to take advantage of power dynamics. There is even a term for this, the online disinhibition effect. The online disinhibition effect is the understanding that, while online, some people may self-disclose or act out more frequently, or intensely than they would in person.[4] **24% of US workers have claimed they believe that remote environments may increase, or worsen, harassment in the workplace.**[2]

This premise holds true with numerous HR policy violations and issues — including discrimination, bullying, and employee disengagement. The best security platforms allow organizations to specify granular policies against which information traveling through systems are monitored. This eliminates the inefficient time lags that typically exist between a policy violation occurring, it being noticed and responded to, and eventually being resolved. As a result, the organization and its people are better protected, and safe and ethical collaboration can be supported.

Some common workplace harassment scenarios may include sexual harassment, disability harassment, racial harassment, sexual orientation & gender identity harassment, and ageism.[5] In addition to leveraging technology to monitor for bad behavior, consider the bigger picture in addressing toxicity in your collaboration platforms. Consider how to identify and evaluate behavior that is contributing to toxicity, build a shared code of conduct for interactions within tools such as Slack and Teams, properly communicate that code to the organization, and enforce it across the entire collaboration ecosystem.

IN 2020

67,448
workplace discrimination charges were filed in the U.S. in 2020.

$535.4 M
was secured for victims of discrimination.[6]

RISK 3

DATA LEAKS

Most collaboration platforms come with some level of security that provides certain types of protection to the organization, but many companies don't realize that the embedded security may not be enough to properly protect them from accidental or intentional data leak.

Additionally, more collaboration tools are being leveraged not simply for employee conversations, but for a comprehensive collaboration network between employees, vendors, partners, and customers. For example, Slack Connect, the extended version of Slack Shared Channels that enables communication with people outside the organization through channels and direct messages (DMs), experienced 200% year over year growth in 2021. **77% of Fortune 100 companies today are using Slack Connect in some capacity**.[7]

RISK 3: Data Leaks

The premise of tools like Slack Connect is to facilitate partner or customer conversations as easily as employee conversations organically happen. Adding new external contacts to an existing Slack Workspace is a quick process that simply requires an account admin to approve an addition.[7]

This expansion of use cases across collaboration datasets may alarm security and compliance leaders, but the truth is, it's good for business. In fact, **83% of users believe that losing access to working with partners in Slack Connect would negatively affect their ability to get work done**.

Microsoft Teams has a similar tool available to enable external conversations. Its governance, however, is not as straightforward. Admins behind the scenes must navigate a variety of admin consoles and separate policy engines to track governance as well as implement some security protocols.

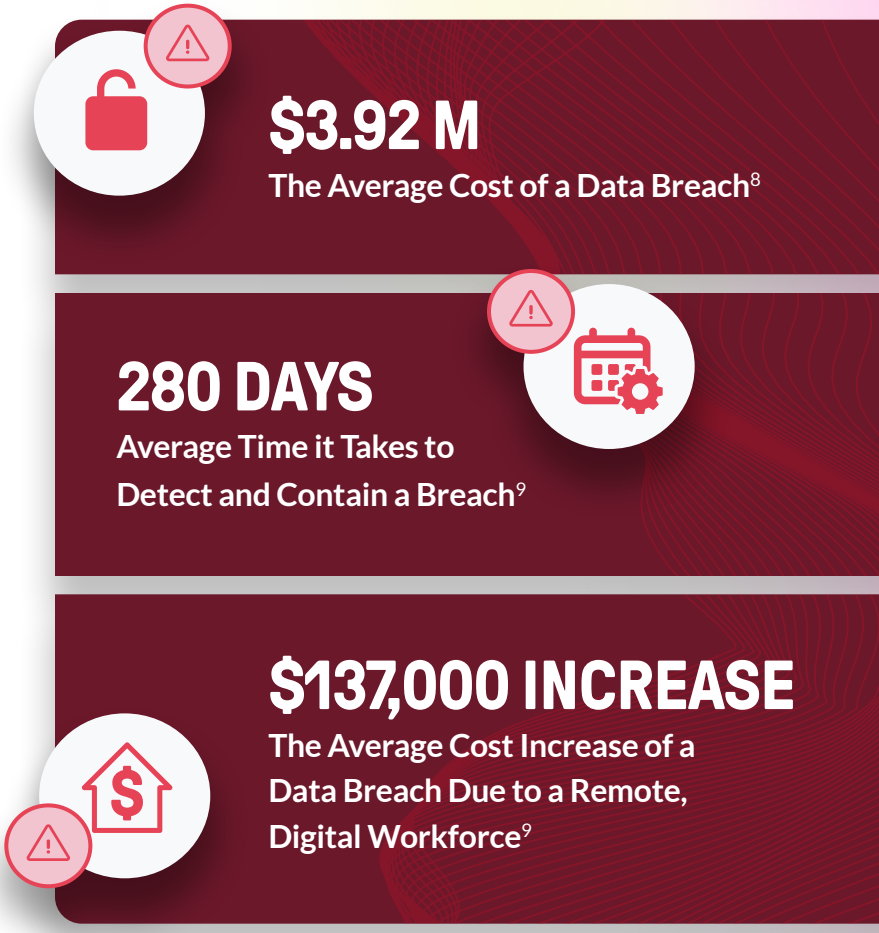
In addition, some vendors who now offer employee monitoring focused on productivity tracking for well-being, may innocently expose employee calendars or other types of data that they may inadvertently expose sensitive information that is not meant for certain audiences.

So, what does this mean for data leaks? Data Leaks have always been a concern within internal collaboration tools. As collaboration platforms evolve into a primary source of business communication, the probability that data leaks will occur increases, as does the likelihood that those leaks find their way — accidentally or unintentionally — into third party communications with an external audience. If they do happen, it can be very time consuming and costly to contain without the right risk management, monitoring, and policies in place. As shared access and guest channel functionality expands across native collaboration solutions, there are more gaps and complexities of managing usage, access, reporting, and monitoring abilities for the application administrators.

Prevent Leaks by Securing Your Collaboration Platforms

Many potential data leak woes can be avoided if you have a single, highly secure platform to monitor the entire collaboration ecosystem. By setting policies once, a single security platform can oversee multiple business social networks and tools to hold them to the same security standards.

With automatic 24/7 monitoring of information shared both internally and externally, security gaps can be eliminated, and rogue usage thwarted. **In addition, predictive analysis can provide visibility into potential issues before they grow into costly problems**.



RISK 4

INSIDER THREATS

Enterprise organizations have always faced insider threats from employees and business partners, either with ill intent or simply acting carelessly. But today, insider threats have emerged as one of the biggest risks to corporate data — and workstream collaboration tools have given employees and partners new and greater access to sensitive information that can be used against the company.

The magnitude and scope of this problem is alarming. **61% of companies had an insider threat attack reported in 2020 and 60% of organizations had more than 20 incidents of insider attacks a year.**[10] The actual figures are probably much higher due to the amount of security breaches from the inside that go unreported.

RISK 4: Insider Threats

The typical insider threat actor may not be the original profile you imagine when you think of an insider risk. The employee most likely to be an insider threat risk is one who may be more aware of the risks than the average employee. **IT users, those who often hold the most privilege when it comes to data and access, account for up to 63% of insider risk incidents. Managers with sensitive information, contractors, and consultants are also likely culprits in over 50% of insider risk scenarios**.[10]

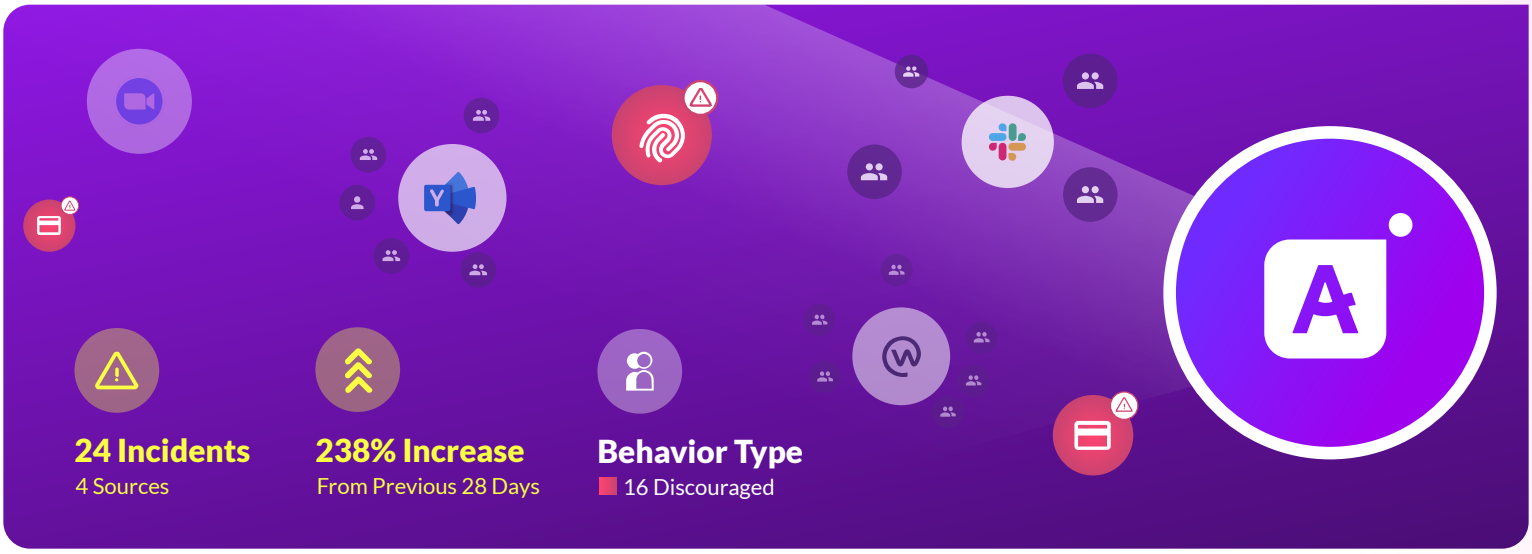
There can also be two different types of insider threats, the malicious and the negligent user. Negligent insider threats are unintentional. The risk they introduce to an organization may result from carelessness or mishap. An employee may not be fully up to date on their company's security policies and need coaching, or they may have ignored them. Malicious insiders take intentional actions to put their company at harm for personal gain or grievance. Both types of insider risks are likely to be lurking in your collaboration ecosystem, and the remediation costs are substantial. **Remediation costs due to incidents tied to an employee, can reach $6.6 million annually and almost $500,000 per incident**.[11]

Stop Insider Threats Before They Occur

To succeed with collaboration data, organizations must safeguard against insiders exploiting or carelessly misusing their access to sensitive enterprise information. When collaboration ecosystems are not secure, a malicious employee can simply post what they want to a private group and easily move valuable information outside the enterprise, without notice. Without the proper security controls in place, employees might find it easy to leverage the organization's social network to garner data, customers, partners, and staffing — all on the company's dime.

The best way to prevent malevolent insider attacks and careless activities is to plug the security gaps and tighten controls. To do this, companies need a highly customizable security platform that oversees all business social networks and collaboration tools within the extended enterprise.

The security platform selected should continuously monitor all social content and activity it oversees and send targeted notices so that the appropriate personnel can take action. It should also have analytic capabilities to spot patterns of suspicious behavior, enabling it to predict likely future activity and prevent potentially damaging incidents before they occur.



RISK 5

REGULATORY COMPLIANCE

The explosive growth of data — compounded by the big data boom — has increased the regulatory burden on nearly every large organization today. On average, every employee has access to 11 million files today.[12] This rapid growth of data, shareable content, and digital conversations across corporate tools can become overwhelming, particularly for the most regulated industries. From banking and financial services to insurance and healthcare, to legal and global consulting, no industry has gone untouched. What they all have in common is that their compliance challenges are growing and changing all the time, increasing risk and cost to the enterprise.

While the cost of compliance is high, the cost of noncompliance can be much higher. Fines and penalties for non-compliance can reach tens of thousands of dollars a day in some industries. **According to Ponemon Institute, the average costs for organizations that experience non-compliance problems is $14.82 million**. These high costs are due to business disruption, revenue loss, and fines. **Depending on how regulated the industry is, average costs can reach upward to $30.9 million**.[13]

RISK 5: Regulatory Compliance

Knowing this, an overburdened compliance team may be skeptical of a collaboration tool since it can mean additional data and activities to be monitored. This can keep some companies from deploying it, causing them to miss out on valuable benefits. Others might restrict features so much that the tool becomes unusable and unable to scale to the point where it benefits the company. This may backfire on a company.

In late 2021, JP Morgan was fined **$200 million** after admitting it failed to archive employee messages about work-related matters.[14]

The SEC mandates that financial institutions keep records of communications in case the agency needs access for investigations down the road. In this instance, a struggle to keep up with an influx of business conversations across a variety of channels, including those outside of official corporate channels, resulted in a costly mistake. There is no need for this to happen. Organizations need to have a clear understanding of their business communications toolset and employ a security platform that proactively monitors, supports compliance, and improves audit readiness across their entire collaboration ecosystem.

Increase Compliance & Improve Audit Readiness

Uncovering regulatory and compliance matters in a collaboration tool can be like finding a needle in a haystack. But with a security platform that automatically monitors collaboration data 24/7, non-compliant data and activities are brought to the surface quickly, authorized personnel are notified immediately, and non-compliant employees can receive real-time coaching on appropriate behavior — mitigating risk and speeding resolution.

Since state and federal regulations can change frequently, it is imperative that the security platform allows administrators to select from a set of pre-defined policies, as well as easily set and customize detailed, industry-specific compliance policies that enable productive collaboration. What's more, organizations should be empowered to limit certain functions for specific users that may be in highly regulated roles.

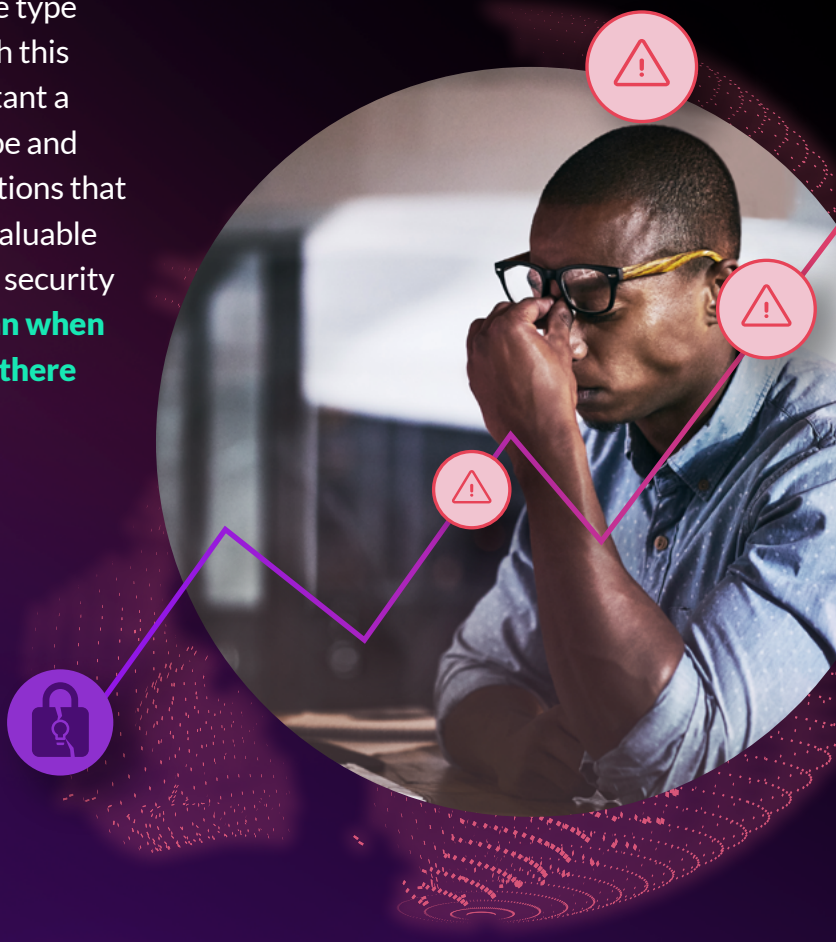
In addition, companies should pay special attention to records retention requirements. Administrators should be able to set up and control an orderly records retention and purging system — one that is customized to the organization's needs and modifiable as those needs change and grow.

RISK 6

INTELLECTUAL PROPERTY LEAKS

Intellectual property (IP) is a highly valuable asset for any large organization. It drives innovation, competitiveness, and business growth, and sustains the organization over time. **IP is so important in fact, that according to Deloitte, it can constitute more than 80% of a single company's value.**[15]

Not surprisingly, the risks and costs associated with IP leaks are substantial. A single leak can cost an organization millions (if not billions) of dollars, depending on the type of IP stolen and how it is used. As we move through this period of "the Great Resignation", now is as important a time as ever for organizations to consider the scope and impact of intellectual property leaks. For organizations that work heavily with personally identifiable data or valuable intellectual property, it is critical to put the proper security protocols in place. **From April to June 2021, a span when employee resignations were at an all-time high, there was a 61% increase in data exposures.**[16]



RISK 6: Intellectual Property Leaks

Data exfiltration often arises during employee resignations. The likelihood of a misappropriation of data by an employee who is preparing to leave a company is elevated as they may maliciously collect data or simply not understand that collecting the data could be considered a crime. Companies who value their intellectual property should consider their data protection policies and not leave this up to chance.

Two of the most common sources of IP leaks *(both intentional and unintentional)* are employees and business partners, and their business interactions are increasingly growing in tools like Slack and Teams. As asynchronous employee communications expand in these platforms, the volume of intellectual property that lives amongst disparate locations is expanding. Therefore, IP is much more likely to fall into the hands of the wrong person or outside of the organization. This is another reason that securing an entire collaboration ecosystem is mission critical.

Protect Against IP Leaks by Planning for Them

Any collaboration security platform should allow administrators to create specific internal and external sharing policies and set policies for immediate, targeted alerts to be sent when suspicious incidents occur. Continuous, automated monitoring of all activity and content on collaboration tools can shut down potential IP leaks before they happen. There are many ways this type of security plays out, day after day. **Here are just a few examples:**

- A file accidentally posted to a collaboration group that contains sensitive merger information is immediately deleted, never reaching the unintended recipients.
- A chat regarding future business plans between an internal buyer and a trusted vendor is flagged for review.
- A file marked “R&D: Confidential” is blocked from being shared outside the R&D work group.
- An image of a product concept is blocked from being posted to an innovation group where images are not allowed.

When these protective actions occur, users can be alerted and informed about internal and external compliance rules, so they are less likely to repeat the behavior — educating both themselves and other employees.

CONCLUSION

YOUR ORGANIZATION'S **COLLABORATION ECOSYSTEM REPRESENTS GAME-CHANGING OPPORTUNITIES**

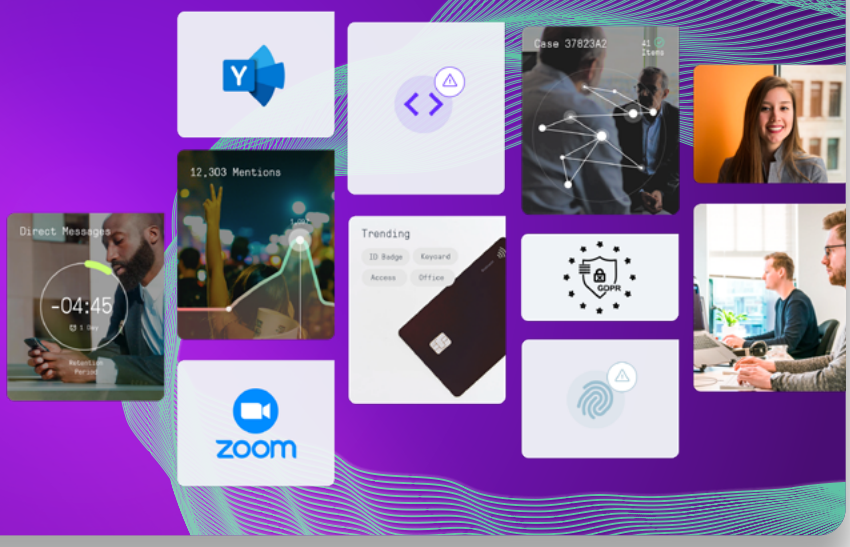
including seamless collaboration across work groups and locations, faster time-to-innovation, and increased productivity.

At the same time, the nature of this work contains security gaps that bring significant risk to the organization. To realize the benefits and prevent the risks of business social networking, companies must employ a security platform to oversee all social networks and collaboration tools within the enterprise.

The Aware platform is an enterprise-grade, collaboration governance platform making sense of human behavioral data. Aware's holistic approach to collaboration data governance transcends business silos and enables the alignment of key stakeholders across your organization to reduce risk while adding valuable knowledge to each business unit. By continuously collecting and normalizing digital conversations from multiple sources — the Aware platform provides AI-enriched governance, search, monitoring and analytics, purpose-built for the nuances of collaboration data. For security, compliance and IT leaders, proactive data loss prevention, compliance and content monitoring across your organization's collaboration ecosystem is made possible with Aware.

Aware

For more information on how Aware can help enable your successful adoption of next-gen collaboration, visit **AwareHQ.com**.



SOURCES

[1]https://www.businessolver.com/workplace-empathy-executive-summary#:~:text=Building%20a%20culture%20of%20empathy%20cannot%20take%20a%20back%20seat,said%20the%20same%20in%202019

[2]https://www.catalyst.org/reports/empathy-work-strategy-crisis

[3]https://www.morningbrew.com/hr/stories/2021/11/01/the-workplace-went-virtual-the-harassment-stayed-real

[4]https://news.crunchbase.com/news/remote-workplace-harrassment-how-to-prevent-claire-schmidt-allvoices

[5]https://www.hracuity.com/blog/workplace-harassment

[6]https://www.jdsupra.com/legalnews/eeoc-fy-2020-statistics-eeoc-s-recovery-9089875

[7]https://slack.com/blog/transformation/fortune-100-rely-slack-connect-build-digital-hq

[8]https://www.csoonline.com/article/3634869/top-cybersecurity-statistics-trends-and-facts.html

[9]https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures#:~:text=According%20to%20their%20reports%2C%20the,%2411.1%20million%20to%20%2413.3%20million

[10]https://financesonline.com/insider-threat-statistics

[11]https://www.ciodive.com/news/insider-threat-malicious-negligent-employee/617715/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-01-26%20CIO%20Dive%20%5Bissue:39333%5D&utm_term=CIO%20Dive

[12]https://info.varonis.com/hubfs/docs/research_reports/2021-Financial-Data-Risk-Report.pdf?utm_content=146358482&utm_medium=social&utm_source=twitter&hss_channel=tw-21672993

[13]https://www.globalscape.com/resources/whitepapers/data-protection-regulations-study

[14]https://nypost.com/2021/12/17/jpmorgan-fined-200m-failed-to-monitor-employee-communication

[15]https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html

[16]https://www.code42.com/blog/incydr-scoop-data-exposure-jumps-as-employees-head-for-the-doors