Aware

An IT Leader's Guide to

Compliance, Legal, and InfoSec Requirements in Collaboration

Everything You Need to Know to Support Your Colleagues and Improve Your Risk Posture

You know enterprise collaboration tools like Slack, Microsoft Teams, Workplace from Meta and Yammer are filled with blind spots and hidden risks. In a dataset that grows exponentially, who knows how much confidential information it contains? How many passwords, restricted files, payment card details or personally identifying information? You probably don't want to know.

However, today's IT leaders have a problem. Courts and regulators have made clear that ignorance of the contents of collaboration data is no excuse. Fines levied against the Fortune 500 for unregulated use of collaboration apps have surpassed $1.8 billion since December 2021.

And courts have already demonstrated they don't care what burden it places on the enterprise to enable eDiscovery within collaboration data.

Getting your arms around this dataset is a must. But how do you know what controls are critical, vs. nice-to-have? Where can you most effectively reduce risk and ensure compliance while remaining within budget? In this guide, we'll explore the top requirements of compliance, legal, and information security departments. By understanding what your colleagues need to keep collaboration safe and compliant, you can make informed decisions about how best to protect the company and your investments.

Fines levied against the Fortune 500 for unregulated use of collaboration apps have surpassed $1.8 billion since December 2021.

Section 01

Compliance

Compliance officers ensure that company datasets adhere to a wide range of regulations, from industry-specific security requirements to data privacy acts.

Industry-Specific Regulations

Highly regulated industries have strict data compliance obligations to meet for collaboration. For example, FINRA or HIPAA noncompliance can cost financial or healthcare companies millions of dollars.

A primary requirement of many industry regulations is for organizations to save and store data for a specific length of time. This includes the data generated by and in collaboration tools. That means you need to implement tools that can archive collaboration messages in real time, capturing revisions or deletions which may prove critical to an investigation down the road.

PII/PCI/PHI

Whatever industry your organization is in, certain information is always considered sensitive and should be protected.

Personally Identifiable Information (PII)
e.g. social security or driver's license number, full name, date of birth, address, phone or email, religion, education and more.

Protected Health Information (PHI)
e.g. diagnoses, treatments, current or former medications, healthcare records, dates or locations of medical appointments and more.

Payment Card Industry data (PCI)
payment card numbers, expiration dates, CVVs, account holder names, account numbers, bank names, PINs and more.

The most effective way to control for this data within collaboration is to deploy real-time intelligent monitoring that uses pattern matching and regular expressions to scan for and remove restricted content the moment it is uploaded.

Top Compliance Requirements for Collaboration Security

01

Visibility and access to both public and private communication data

02

A searchable archive of public and private conversations

03

A well-developed community management strategy to enforce company policy

Data Privacy Rules

The most well-known of these is the European Union's General Data Protection Regulation, or GDPR. However other countries and states have implemented their own versions, such as the California Consumer Privacy Act (CCPA)/California Privacy Rights Act (CPRA).

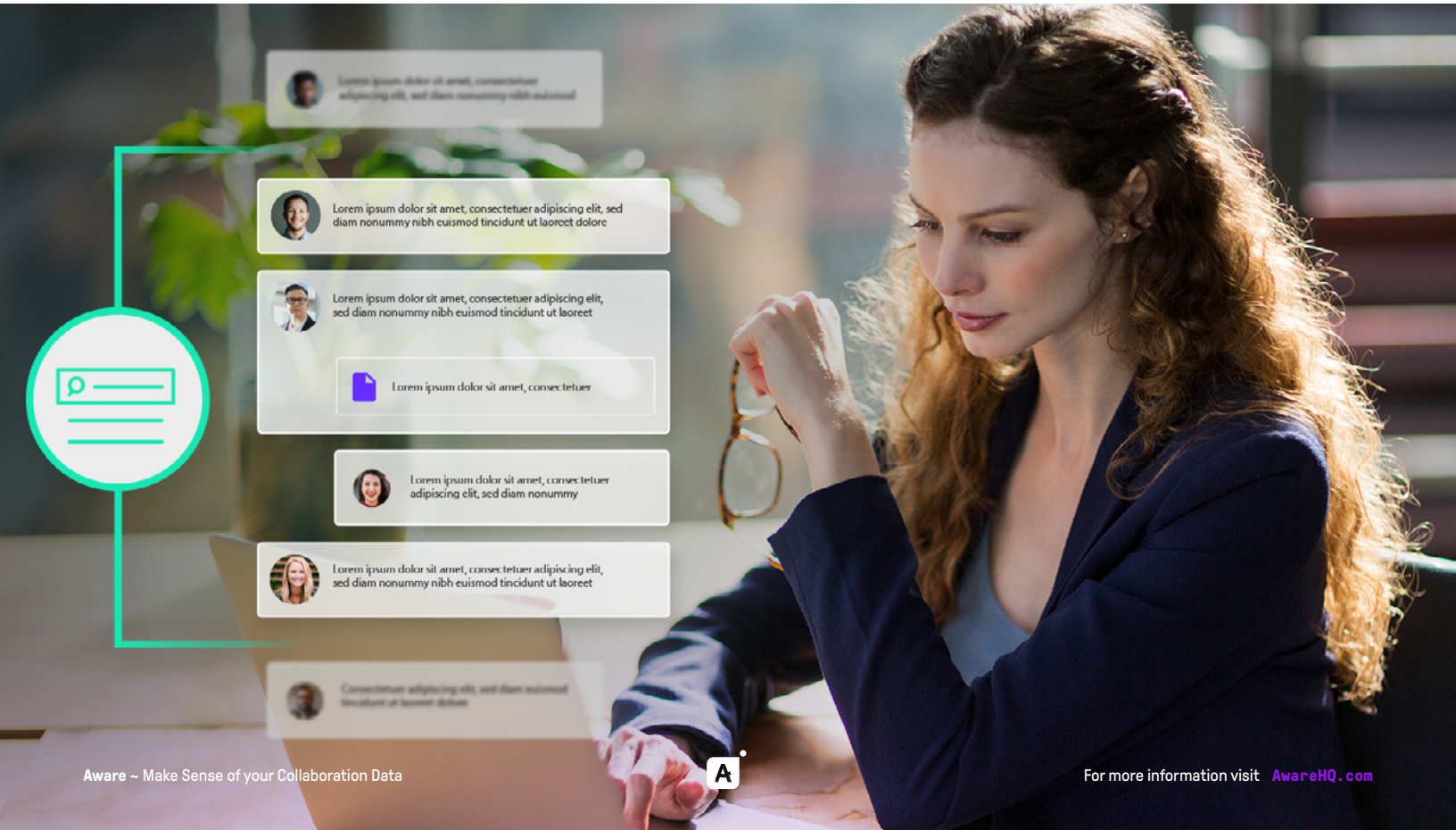
Data privacy legislation hinges around two key rights: the right to access the information held on an individual, and the right to be forgotten. These rights apply to employees as well as customers. That means you need to be able to search for user data within collaboration, determine the ownership of that data based on context, and erase user-owned data upon request.

When it comes to the digital workplace, the best way to control legal risk is to select a data management tool that can efficiently capture and export all conversations and communications to/from an individual in the event of a data subject access request. You also need a tool that can delete all the user's data from both the platform and any archives in the event of an erasure request or to comply with company retention policies.

Internal Compliance Policies

Aside from industry or federal regulations, each organization also has its own policies and guidelines for appropriate behavior. For example, generally employees sign a code of conduct that states they will treat fellow employees with respect and dignity. Yet, we see headline after headline of harassment or discrimination within the workplace.

Workplace collaboration tools offer coworkers a more casual and faster way to communicate with each other, but also open the door for conversations that are not necessarily appropriate in the workplace. Ease concerns of both your compliance leaders and human resources by implementing a real-time monitoring solution that specifically looks for inappropriate behavior which could lead to psychological or legal risk.



Section 02

Legal

Legal departments must be able to access a full history of collaboration messages and associated context to conduct early case assessment and gain a true picture of an organization's risk exposure.

To prepare for pending litigation, legal teams need to gather all relevant data that might prove useful for a case prosecution or defense. This can include financial data, email communications and phone records, as well as public and private conversation content.

Pair your collaboration tool with a solution that allows legal teams to build an archive of all content (including revisions!), enact legal holds to preserve the content from individuals of interest and easily extract relevant content by author or keyword.

Design collaboration with legal needs in mind

In creating a digital space for employees to share ideas, innovate and work through challenges, you also provided a tool where intellectual property and sensitive information can be shared and stored.

Cut your legal team a break by purging conversation data you don't need. That way they don't have the burden of discovery if they are performing early case assessment and prevent lingering conversations that no longer offer value to the business from getting in the wrong hands.

Simplify collaboration management through platforms with bi-directional retention capabilities that apply purge and preservation rules to live datasets and archives simultaneously.

Top Legal Requirements for Collaboration Security

01

Robust retention policies that limit liability from stored data

02

Preservation of edited and deleted message content

03

eDiscovery enablement for messages and context

Manage your people

You can help control liabilities within collaboration tools by proactively managing your digital community. Introduce norms that protect employees, customers and IP. Educate staff on sensitive information sharing and the risks of regulatory noncompliance. Foster a sense of co-ownership of collaboration security from the bottom up.

Enforce your standards

In tandem with encouraging appropriate use of collaboration, include ways to enforce your community management policies. Pair collaboration with a monitoring solution that scans public and private areas of communication for keywords or patterns of concern. This will surface unsafe sharing and you can notify your legal team of potential risks in real time.

Section 03

Information Security

The essential responsibilities of information security are consistent across organizations: reduce IT risks, safely store and protect company, employee and customer data, and develop possible breach scenarios along with corresponding reaction and response plans.

Collaboration tools represent new challenges for infosec leaders. By design, they democratize and simplify data sharing and open new avenues for exfiltration. Within their complex datasets, insider risk can proliferate from both negligent employees and malicious threat actors. That makes enterprise collaboration security a new risk frontier and top priority for your colleagues in information security.

Take a human approach to collaboration security

It's the unpredictable *human behavior* that introduces risk into these collaboration networks. The informal, chatty nature of these platforms creates an environment that is ripe for sharing sensitive or confidential information with the wrong individuals, intentionally or unintentionally.

According to the Ponemon Institute, the average annual cost of mitigating insider threats was

$15.4M

in 2022.

To mitigate risk of insider threats, proactive community management is necessary. As the collaboration application owner, you need to present a solution to keep sensitive material safe and out of the wrong hands.

That starts with educating employees, but a human approach should be augmented by intelligent learning solutions for maximum effectiveness. Smart automations use AI/ML-infused insights and rules-based monitoring to scan collaboration in real time and flag unsafe communications for further review.

Top InfoSec Requirements for Collaboration Security

01

Proactively uncover and mitigate potential avenues for data exfiltration

02

Detect indicators of insider risk and alert infosec in real time

03

Reduce shadow IT uptake by empowering full functionality of authorized tools

Properly manage, store and secure conversation data

Collaboration platforms generate huge amounts of unstructured data without adequately considering where or how that data is stored. To reduce liability, you need to deploy a data retention policy to purge information that no longer holds business value.

Making informed, deliberate decisions about the value of data not only ensures regulatory compliance but reduces your overall risk surface area. Any information that remains within a collaboration archive without adding value only creates risk. Identifying and removing it limits exposure in a data breach scenario.

Limit shadow IT with viable collaboration options

Shadow IT — unsanctioned applications and programs in use across the enterprise — often takes hold when employees have unmet needs that help them work more efficiently. These unregulated, unmoderated tools represent a significant information security risk to the organization.

The good news is, collaboration platforms can help to reduce reliance on shadow IT by providing employees with a properly regulated and sanctioned tool that meets all their coworking needs. In organizations with bring your own device (BYOD) policies, collaboration further insulates sensitive information and corporate communications within enterprise-grade apps. This limits the risk of data exfiltration.

To achieve the highest uptake of enterprise collaboration tools and limit shadow IT exposure, look for monitoring and management solutions that have the least impact on the end user. Having to continually reauthenticate activity or navigate through third-party login portals will cause employees to look elsewhere for communication solutions.