smarsh®

How Global Enterprises Can Reduce the Risks of Collaboration Platforms

Considerations for managing regulatory cybersecurity, data privacy and more

New communications technology is a true “equalizer” for organizations, bringing together people from multiple geographies and across demographics. Workers are no longer tethered to a single office, device or time zone. Collaboration and conferencing tools (e.g., Microsoft Teams, Slack, Zoom, etc.) have replaced desk chatter, watercooler conversations and even email.

There are measurable benefits to the digitization of the workplace. Take Microsoft Teams — even before widespread adoption, businesses reported:

- Savings of up to 8 hours per user, per week, by having communications and collaborative features in one platform
- 17.7% improvement in time-to-decision, translating to a 3-year total savings of over $450K
- Microsoft Teams payback period of less than six months following initial deployment

A Forrester Total Economic Impact™ Study Commissioned By Microsoft

For some companies, including Microsoft, Facebook and Salesforce, moving to a remote work model has pushed leadership to rethink the office model altogether.[1] These organizations have taken the opportunity to update processes and infrastructure to support a work-from-anywhere culture.

Of 100 global organizations surveyed by KPMG, only 27% plan to require employees to return to the office as soon as regulations allow.[2]

Not so fast...

Regulated organizations like financial services firms have seen the benefits of collaboration tools. But an enterprise's ability to adapt to a virtual business model overnight is no easy feat. Collaboration tools present unique challenges for compliance and IT departments. Visibility into employee conduct is reduced when people aren’t working from a centralized location and the lines between business and personal communications are blurred.

When most companies were pushed into remote work in early 2020, regulated firms unaccustomed to supporting remote work and digital communications platforms might have chosen to prohibit the use of convenient collaboration tools before they could be securely rolled out. Or, they had to abruptly start using collaboration platforms without the necessary compliance and security protections in place.

Either way, workers are on home networks, potentially using personal devices, or interacting — unwittingly or not — through unauthorized communication apps. This makes the identification and mitigation of risk, and the management of regulatory compliance, exponentially more complex.

[1] https://www.flexjobs.com/blog/post/companies-switching-remote-work-long-term/
[2] https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2020/return-to-work-infographic.pdf

Modern communication platforms are useful, but they must be diligently managed to avoid potential risks:

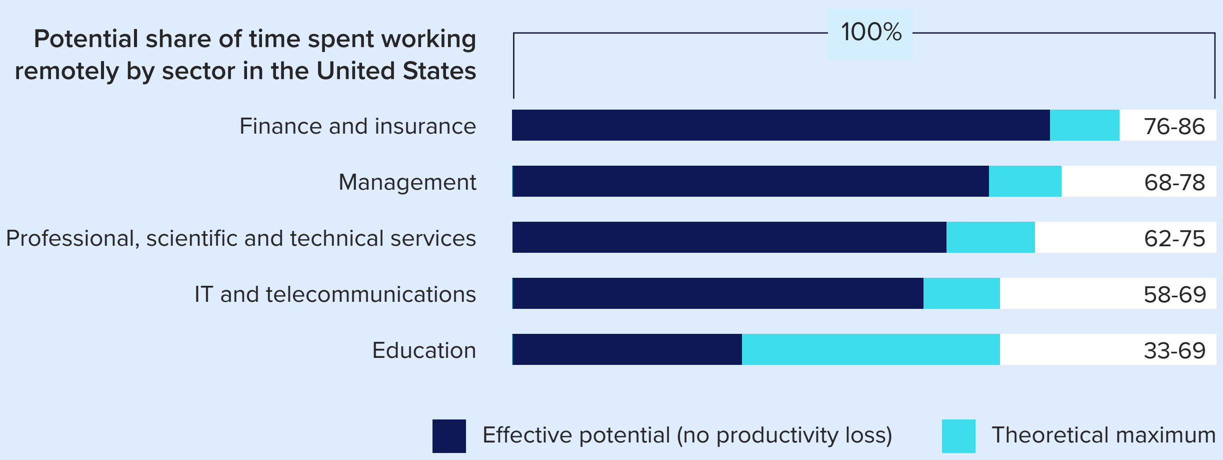
- **Cybersecurity risks:** The use of unsecured home networks and unauthorized devices creates blind spots for IT and security teams, paving the way for increases in fraudulent activity
- **Regulatory risks:** When communications tools are downloaded or deployed before policy controls can be implemented, compliance gaps exist if those communications are not being archived or monitored
- **Data privacy risks:** Privacy complications can arise if collaboration tools are not used exclusively for business purposes
- **Internal policy risks:** New platforms provide a new place for employee misconduct to occur

For financial firms, a distributed workforce isn't merely inconvenient; it's risky. These risks can result in wide-reaching consequences such as loss of intellectual property, regulatory violations, data privacy or legal sanctions, and even reputational or brand damage.

This guide will help you navigate the benefits and risks of collaboration platforms and how to adjust your policies, technology and employee training to enable the future of work and stay ahead of risk.

Financial services and insurance have the highest potential (i.e., lowest productivity loss) for remote work.

Top 5 Sectors for Remote Work Potential



McKinsey Global Institute: *What's next for remote work: An analysis of 2,000 tasks, 800 jobs, and nine countries*

What's so great about collaboration platforms?

Collaboration tools such as Slack, Microsoft Teams and Zoom help organizations stay more connected, interactive and responsive to business needs. These platforms take elements of instant messaging, audio/video conferencing, file sharing and social media, and bundle them into a single, cohesive, easy-to-use package. The ability to interact with colleagues and clients is easier and instantaneous, facilitating internal collaboration and enhancing customer service.

These benefits have proven invaluable for companies that have transitioned to a remote-first or hybrid working model. Executives support the use of collaboration tools because they enable productivity, efficiency and quick decision-making, which translates to a return on their investment. Employees like them because they can communicate with coworkers and clients in real time and across devices while working remotely.

Technology moves quickly, and new communication channels are introduced every day. But many of these tools are not built with the retention and oversight needs of highly regulated industries in mind. Requirements for collecting, preserving, supervising and producing communications are made more difficult when the content that's generated:

- Includes different types of messages: private chat, group chat, channel messages
- Incorporates file sharing: internal documents, images, contracts, video
- Includes activities that generate contextual metadata: edits, deletes, joining or leaving a conversation
- Is created through multiple devices: work computer, personal computer, mobile devices, etc.

All these elements are critical to understanding the context of conversations and are uniquely challenging to capture, preserve and supervise.

Do you prohibit the use of these tools and hope to avoid risk, or do you enable collaboration tools and manage risk?

Competitive organizations don't have much of a choice anymore. That means enterprises must embrace these technologies and new ways of working. New challenges for managing risk and meeting ongoing regulatory obligations will be profound — and inevitable.

Adopting a new channel to meet employee and customer preferences does not come with a simple on-and-off switch. An organization now needs to be able to manage many communications sources and data to ensure they meet their legal, technical and regulatory obligations. It takes a strategic approach that encompasses:

1. **Policies and governance**
2. **Unified, future-proof technology**
3. **Ongoing education and training**

Let's explore recommendations for each of these areas of risk mitigation.

RISK MITIGATION TIP #1

Strategic policies and governance

To stay ahead of compliance risks, firms must develop policies and procedures for collaboration platforms that have been thoughtfully considered, and then follow those guidelines. We recommend starting with the following policy and governance practices:

Install a cross-departmental communications governance council

Involving stakeholders from cross-departmental functions (legal, compliance, IT, etc.) is one way to collectively make decisions about communications technology and the implied risk across the business. Each new tool requires a thorough assessment of its impact. This requires an understanding of the platform itself, which functionality will be supported, how and where electronic communications data is being archived, how it is being secured, and how it could be accessed in the event of a legal or regulatory inquiry.

Implement communications policies

Regulated firms are required to establish Written Supervisory Procedures (WSPs) for the use of electronic communications. To support compliance with WSPs, we also recommend outlining internal usage policies and code of conduct guidance. These include a list of permissible communications methods and an explanation of the possible consequences of noncompliance. Include guidance for every channel your employees are permitted to use—be specific. Consider communications etiquette guidance, and whether to include confidentiality and non-disclosure clauses to ensure the security and confidentiality of customer records and information.

Define mobile policies

Whether your company uses company-issued mobile devices, or you enable a bring-your-own-device (BYOD) policy, employees should be aware of and understand how content generated on their phones or mobile devices is governed. Rules should be updated to account for any new mobile applications that employees are using to communicate. Document your mobile device policies, be explicit about which mobile applications are allowed or prohibited and share mobile policies with staff regularly.

Update supervision and content monitoring practices

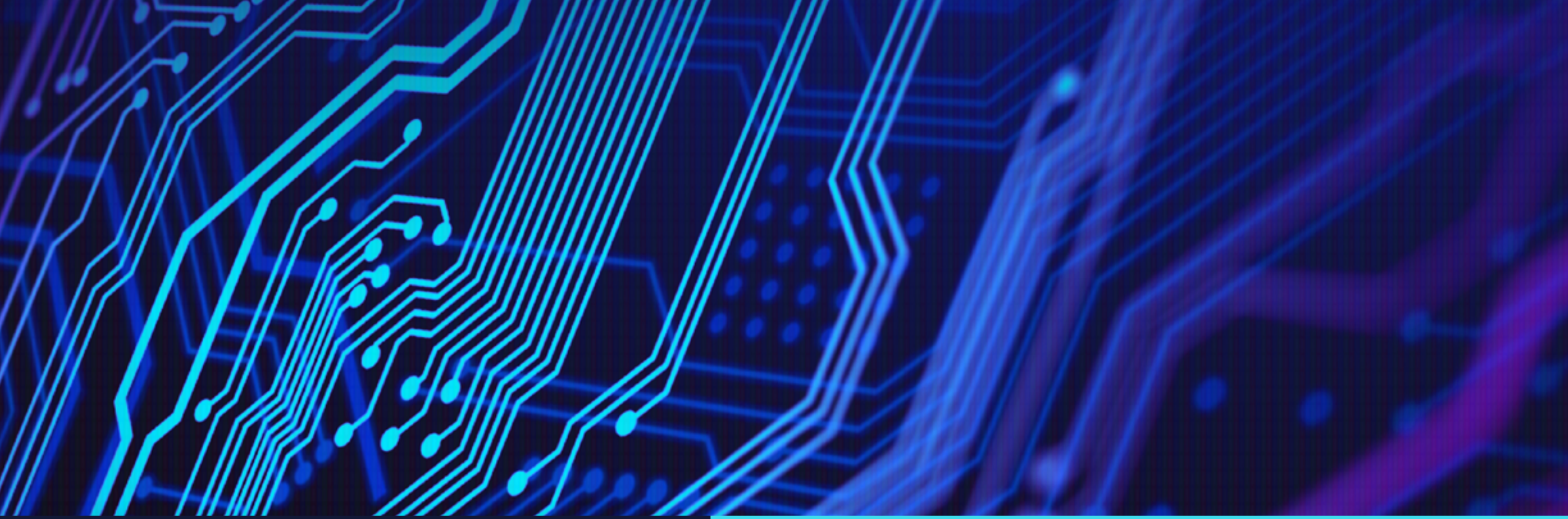
Be prepared for regulatory examinations to include requests for content generated through collaboration platforms. Assess your organization's practices, policies and procedures to confirm they address regulatory obligations for investment advisers and registered representatives working remotely. Check and double-check your systems for vulnerabilities and to ensure the communications are being captured for retention, with a particular focus on mobile devices.

Don't forget data privacy

Across the world, laws and regulations to protect consumer data are being established. Multi-national organizations must contend with differing requirements across regions. Compliance with data privacy protections requires a comprehensive understanding of existing and emerging regulations and requisite policies to avoid fines, litigation or a loss of consumer trust.

LEARN MORE

Managing Global Data Privacy Laws and Communication Regulations in Financial Services



RISK MITIGATION TIP #2

Unified, future-proof technology

Every day employees are requesting to use applications like Microsoft Teams, Slack and other collaboration tools for work. Prohibiting the use of these tools doesn't mean they won't be used. One result of prohibition policies is that you won't be able to preserve and monitor communications on those platforms. When these unapproved communications platforms are inevitably used, an organization runs the risk of fines from regulators. Technology to manage compliance and cybersecurity can help you enable employees and customers to communicate through their preferred means, but do so in compliance with regulatory requirements. Such technology creates a system for diligent recordkeeping and supervision of these communications.

Install a robust archiving solution

To keep up with evolving electronic communication demands and exponential data growth, large financial organizations should implement context-aware, scalable, cloud-based solutions for capturing, preserving, supervising and producing large volumes and types of communications content. It should work reliably across all global regions with no downtime, with high-availability and disaster recovery functionality. Having a powerful archiving solution doesn't mean you have to allow every content channel that's requested. But with an enterprise-first solution, you can support and monitor all the channels employees and clients across the world want to use — and manage risk.

Take advantage of AI/machine learning for supervision and surveillance

One of the biggest challenges with today's supervision systems is separating real risk from "noise." Review teams are required to sift through a vast and often unmanageable number of false positives to get to relevant and targeted content. Many systems rely exclusively on a lexical approach to risk identification. This approach is suitable for a limited set of risk scenarios. However, in most cases, supervision systems lack the ability to consistently filter out less precise matches, creating a large volume of irrelevant alerts. Supervision can be enhanced with AI and machine learning capabilities to drown out noise, make review queues more precise and make the process more efficient. Surveillance for employee misconduct is also a major concern for global organizations. A combined supervision and surveillance solution provides a proactive, single line of defense for regulatory inquiries and misconduct issues.

Smarsh uses AI to reduce false positives by up to 10x and reduce the volume (7.7x) of alerts needing review.[3]

[3] https://www.smarsh.com/guides/smarsh-enterprise-conduct

RISK MITIGATION TIP #3 Ongoing education and training

The importance of employee training that is specific to new collaboration tools cannot be understated. Clear, unambiguous guidelines that are updated at a regular cadence are critical to keeping employees informed and aware of their role in minimizing risk.

Develop a training program

Explicit training should define acceptable and prohibited uses of communication channels and devices for every job role across the organization. This is a great chance to share your newly minted communications, mobile and supervision policies. Require signed attestations from employees at the end of each training session. Include training in onboarding processes for all new staff, calling out specific guidance for registered reps.

Share rollout plans for new communications tools

This will be most effective with reinforcement from your communications governance council. Once you've gone through due diligence for a new communications tool and have documented appropriate use policies, update employees with your rollout plans. Pay close attention to the use of these tools and provide opportunities for feedback from staff.

Update policies and training on a regular cadence

Once scalable technology has been adopted, and compliance and supervision policies and procedures are in place, ongoing staff training is key to maintaining efficiency and ROI — especially as new platforms emerge. Regularly engage with users to stay on top of new tools that best equip staff to do their jobs. Stay up to date on cybersecurity and data privacy issues and what's happening in the regulatory landscape to keep policies and training fresh.

For wealth management firms under the watchful eye of regulators, employee involvement in unauthorized outside business activities (OBA) like the GameStop debacle could have serious consequences. In fact, in FINRA's 2021 Examination and Risk Monitoring priorities letter, OBA was elevated as a critical issue to which firms should be paying careful attention.

Recommended Reading: *How to Inspect Communications for Outside Business Activities*

Enabling communication today to manage risk in the future

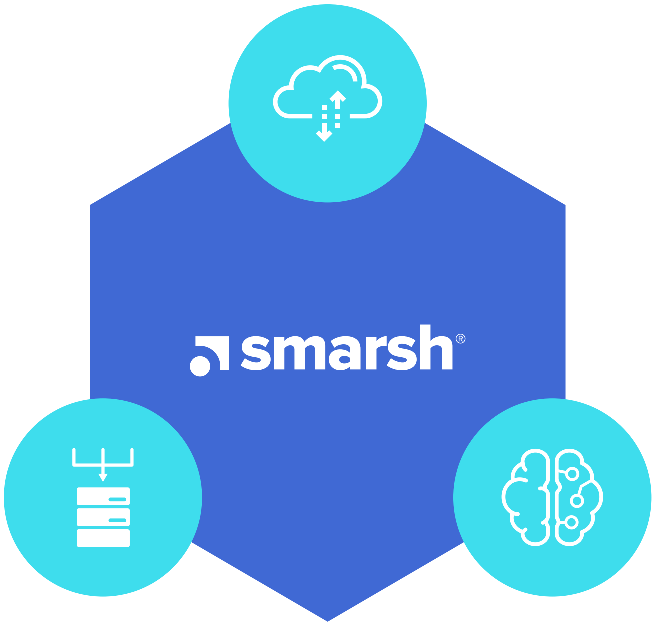
Ultimately, this examination of new collaboration technologies is not just about mitigation of risk. It's about enabling your employees to be more effective in the way they engage with clients and each other. We've gotten used to the many features of collaboration and conferencing tools — gathering with multiple people, sharing links or documents we would have once emailed, even moving from desktop to mobile device — all during a meeting.

Communication is fluid, and the tools that people use to collaborate will continue to evolve. This puts regulations and resulting data capture, archiving and supervision needs in an ongoing state of flux. Lessons learned from early transitions to remote work can serve as a guide to prioritize updated policy, technology and training — and better prepare for the next set of features and collaborative networks that continue to emerge.

How does the Smarsh Enterprise Platform work?

The Smarsh Enterprise Platform is the first-of-its-kind SaaS platform that is AI-powered, cloud-native and built to scale to meet communication data needs of modern global enterprises.

It works by securely processing all relevant communications, in key languages, at your company's scale. To maximize business value, this requires tight integration of three top-level components: communications capture, information archiving and end-user applications that work with communications data.



CAPTURE: Smarsh capture solutions support 100+ channels retained in the channel's native format and context. Email, mobile, social, IM & collaboration, video and voice channels are all captured with solutions deployed to meet your unique needs in the cloud. Smarsh natively captures and manages the widest variety of communications and includes APIs for the ingestion and enrichment of content.

ENTERPRISE ARCHIVE: Enterprise Archive is the compliant storage solution that covers the most stringent communications retention and immutability regulations, including FCA, MiFID II, IIROC, SEC, FINRA, and GDPR.

ENTERPRISE WAREHOUSE: At the core of the Enterprise Platform is the Enterprise Warehouse. With petabyte scale and elastic compute, the warehouse provides a centralized location to retain, analyze and enrich your communications data.

ENTERPRISE CONDUCT: Take your communications data monitoring and analytics to the next level with Enterprise Conduct. Utilizing battle-tested technology, Enterprise Conduct empowers your teams to work more efficiently by reducing false positives. Reveal intent within language at scale, uncover truth faster, and augment the expertise of your risk mitigation teams.

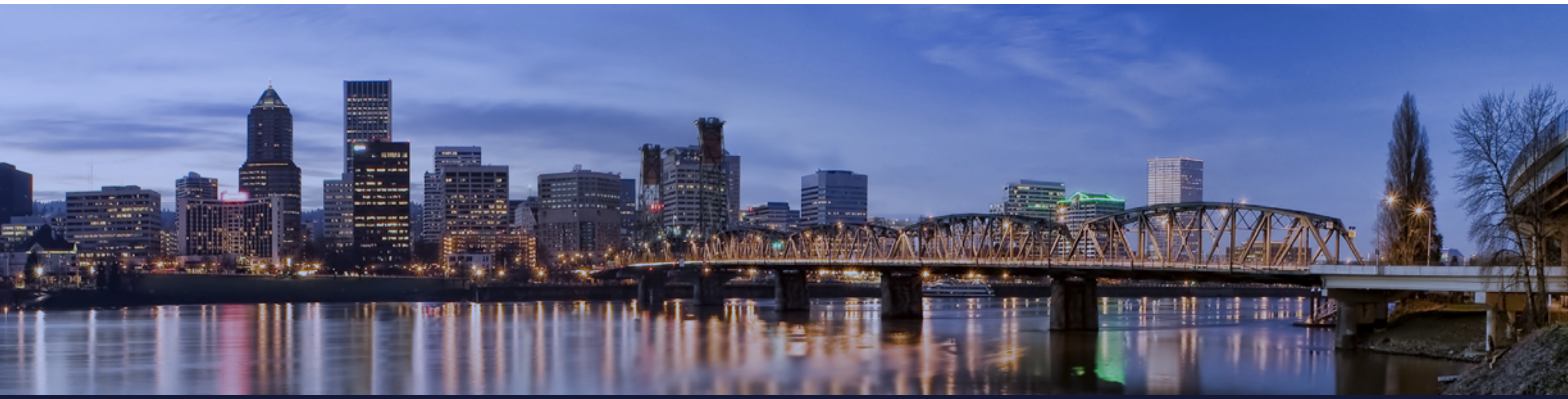
ENTERPRISE DISCOVERY: Built for demanding legal workflows, Enterprise Discovery helps you identify, preserve, review and export your electronic communications data at speed. Save time and money in your e-discovery and investigations by placing legal holds quickly, reviewing all communications in native format and reducing the need to over-collect prior to export for outside counsel and third-party review tools.

Why it's important to future-proof your communications strategy now

It is predicted that by 2025, the total volume of data created and shared worldwide will reach 181 zettabytes — a 1068% [4] increase from 2015. That ten-year span has also seen the advent of widely popular communications tools such as Microsoft Teams and social media apps like TikTok, WhatsApp and WeChat, the emergence of cryptocurrencies as a viable financial product, retail investing applications, and fully remote or hybrid global enterprises.

The tools we use have changed, the financial markets have changed, the very structure of the corporate office has changed. As we look to the future, it's important to lay the foundation for your infrastructure now to stay prepared for shifting sands.

[4] Amount of data created, consumed, and stored 2010-2025, https://www.statista.com/statistics/871513/worldwide-data-created/



Smarsh provides marketing materials for informational purposes only. Smarsh does not provide legal advice or opinions.
You must consult your legal team regarding your compliance with applicable laws and regulations.

Guide - 01/23

☎ 1-866-762-7741 www.smarsh.com @SmarshInc SmarshInc Company/smarsh