proofpoint.

E-BOOK

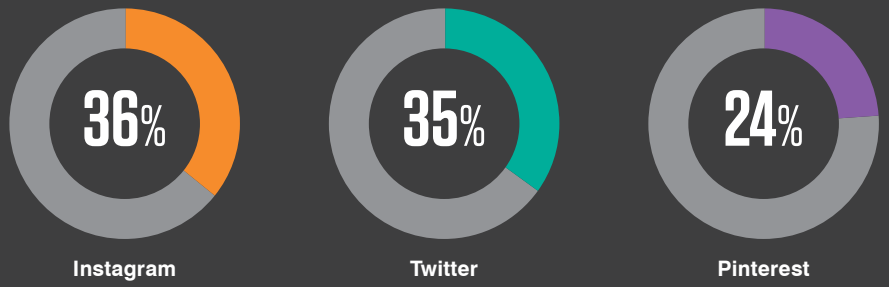
Open Channels, Hidden Threats

How Communication and Social Media Tools Are Changing the Insider Risk Equation for Compliance, IT and Legal Teams

proofpoint.com

Introduction – Two Converging Trends

Share of U.S. audiences who follow brands and companies (Q3 2020)



Source: Statistica

Work-from-anywhere has become the norm for modern business. Whether they're in-office or remote, employees now rely on platforms such as Zoom, Microsoft Teams and Slack to collaborate.

At the same time, teams from sales and marketing to HR and accounting are turning to a growing number of digital channels to stay connected with one another and customers. For many, these channels include public-facing social media platforms. It's no surprise that as many as 85% of respondents to a recent McKinsey executive survey said that their companies have "somewhat" or "greatly" sped up their adoption of digital tools to help employees interact and collaborate.[1]

Has your team considered the risks of insider fraud? In 2018, for example, Goldman Sachs paid $110 million to settle claims that its traders had used electronic chat rooms to share confidential customer information. This disadvantaged clients by enabling rivals to coordinate trades.[2]

[1] McKinsey Global Institute. **What 800 executives envision for the postpandemic workplace.** September 2020.
[2] Matt Levine *(Bloomberg Opinion)*. **"Goldman FX Trader Was Loyal to His Chat Room."** May 2018.

Social media is also changing the game for compliance officers. When Netflix CEO Reed Hastings decided to publish the streaming company's record-breaking monthly viewer count on his personal Facebook page, he triggered an SEC probe.[3]

How well can your organization enforce the HR policies that embody your brand's core values on today's dynamic digital platforms? Claims of widespread "Slack bullying" inside a fast-growing luggage startup drove its CEO to step down in late 2019.[4]

Two converging trends are spawning new legal and compliance risks: social media and enterprise collaboration platforms. As more organizations embrace both, they're creating risks that they may not yet have considered.

Ungoverned, these channels may threaten your brand's reputation or lead to large fines. Many organizations, already struggling with ever-growing volumes of content and changing regulations, just can't keep up.

This e-book explores hidden compliance and information governance risks amid a changing digital business landscape. We'll dive deep into five major areas of risk stemming from social media platforms and enterprise collaboration tools. These include:

- Data Loss
- HR Policy Violations
- Social Media Missteps Causing Reputational Damage
- Insider Fraud
- Legal Issues

We'll also lay out a roadmap for solving these challenges. And we'll show what you need to mitigate legal and regulatory risk without weighing down your staff, budget and business.

Daily active users

Microsoft Teams	Slack	Zoom
115 Million[5]	12 Million[6]	300 Million[7]

[3] United States Security and Exchange Commission Press Release. **"SEC Says Social Media OK for Company Announcements if Investors Are Alerted."** April 2013.
[4] Zoe Schiffer *(The Verge)*. **"Emotional Baggage."** December 2019.
[5] Microsoft. **"Microsoft Teams reaches 115 million DAU—plus, a new daily collaboration minutes metric for Microsoft 365."** October 2020.
[6] Slack. **"Not all Daily Active Users are created equal: Work is fueled by true engagement."** October 2019.
[7] Zoom. **"Zoom Surpasses 300M Daily Meeting Participants, Announces Zoom 5.0 with AES 256-Bit GCM Encryption."** April 2020.

Risk 1 Data Loss

Collaboration platforms like Microsoft Teams and Slack let workers to share content with colleagues. They can send instant messages, share files and team up no matter when and where they work. And most platforms allow users to add third parties to channels, a boom companies with complex vendor ecosystems.

But these platforms also create new data exfiltration risks. Users' behavior isn't always subject to careful oversight.

Whether on purpose or by accident, users may expose data in ways they shouldn't. Departing employees may no longer feel duty-bound to keep confidential data safe. And letting in external partners and vendors opens the door to malicious outsiders. Third-party access to insider-level access to data may also lead to compliance violations.

Most communication and social media platforms don't include data-monitoring features. So they're ripe for abuse by insiders seeking to leak data for personal gain.

The upshot: without the right safeguards in place, these platforms can enable risks that harm the wider organization.

Trio of trouble: people-based data risks

At its core, data loss is a people problem. Here are three types of users and the distinctive risk each poses.

Malicious. Departing or disgruntled employees may no longer feel duty-bound to keep confidential data safe. Others might seek to steal sensitive data, intellectual property or trade secrets for personal gain.

Negligent. Some users are lax. And even the best workers make mistakes, inadvertently exposing data or storing in in unsafe locations. In some cases, users might sidestep an important data-loss control because it hinders their work.

Compromised. Some users are co-opted by outside threat actors. Their accounts have been taken over or exposed, giving outsiders insider-level access to your data.

INSIDE STORY

Accidental access to the wrong channel leads to data leakage

A massive breach that hit video game publisher Electronic Arts (EA) in mid-2021 can serve as a cautionary tale.

How it happened	The attackers used stolen cookies they bought in an underground marketplace to infiltrate a Slack channel at EA, where they posed as an employee in need of tech support. Claiming that they'd left their phone at a party the night before, the attackers persuaded an IT administrator to give them a multifactor authentication (MFA) token. They then used the token to compromise a development service. From there, they were able to download more than 780 Gb of source code.[8]
The damage	After the criminals' efforts to extort $28 million from EA failed, they posted the stolen source code on multiple torrent sites.[9] The reputational damage EA suffered is hard to gauge. But one thing is clear: its lost intellectual property can never be recovered.

[8] Joseph Cox *(Vile)*. **"How Hackers Used Slack to Break into EA Games."** June 2021.
[9] Catalin Cimpanu *(The Record)*. **"Hackers leak full EA data after failed extortion attempt."** July 2021.

INSIDE STORY

Ex-employee sabotages Cisco's collaboration app

Former employees who retain excess privilege can cause serious harm. Networking giant Cisco learned this the hard way.

How it happened	About six months after quitting, a software engineer used still-active credentials to access the corporate Amazon Web Services (AWS) account that hosted essential support infrastructure for Cisco's WebEx Teams videoconferencing service. He ran a malicious script there that deleted more than 16,000 user accounts.[10]
The damage	It took Cisco more than two weeks to recover the accounts and rebuild its systems. The process cost more than $2.4 million in labor and customer refunds.

Here's a step-by-step account of the incident, pieced together from indictments and news reports.

Sudhish Kasaba Ramesh works in Cisco's platform team from August 2016 to April 2018. His role gave him sanctioned access to the Amazon Web Services (AWS) servers that hosted Cisco's business collaboration app, Webex Teams.

→ Ramesh quits Cisco in April 2018.

→ On Sept 24, 2018, Ramesh allegedly used his AWS access credentials (which were not deactivated when he left Cisco) to access Webex Teams servers.

→ According to prosecutors, he then deploys rogue code that deletes 456 virtual machines running Webex.

↓

The move shuts down more than 16,000 Webex Teams accounts for as many as to two weeks. Cisco spends around $1.4 million in labor costs to restore the accounts.

← Investigators track the incident to Ramesh. The ex-employee reportedly did little to hide his actions. He stored the keys on his personal Google Drive, used a Cisco-provided computer to carry out the attack, and didn't use a proxy.

← Ramesh is charged by U.S. authorities in July 2020. His alleged motives—and why he left such an obvious trail—remain unclear.

[10] Catalin Cimpanu *(ZDNet)*. **"Former Cisco engineer sentenced to prison for deleting 16k Webex accounts."** December 2020.

INSIDE STORY

Microsoft Teams chat content irrecoverable after accidental deletion

Major enterprises aren't immune to these risks. In big four accounting firm KPMG, an administrative blunder deleted the full chat histories of more than 145,000 Microsoft Teams users within the organization.

How it happened	A privileged user reportedly tried to exempt a single user's account from the company's active retention policy. Human error led the change to instead be applied across the entire Teams deployment.[11]
The damage	Though the extent of the losses that KPMG suffered because of this incident have not been disclosed, it served as a wakeup call for CIOs working with the firm. It prompted changes in policy and privilege management within Teams. And the company issued a reminder that Teams chats should never be used to store essential business data.

The average data breach now costs its victim **$4.21 million**.[12]

2,211,396 complaints about internet-associated crime were made to the F.B.I. over the past five years.

These incidents resulted in losses totaling **$13.3 billion**.[13]

[11] Thomas Claburn *(The Register)*. **"IT blunder permanently erases 145,000 users' personal chats in KPMG's Microsoft Teams deployment – memo."** August 2020.
[12] Ponemon Institute. **Cost of a Data Breach Report. 2021**.
[13] Federal Bureau of Investigation, Internet Crime Complaint Center. **Internet Crime Report**. 2020.

Risk 2 HR Policy Violations

67,448
workplace discrimination charges were filed in the United States in 2020.

$535 million
was paid to victims alleging discrimination in the workplace.[20]

According to Microsoft, its enterprise social networking service Yammer enables "open and dynamic communication across the enterprise."[14]

Sometimes, though, apps and platforms like Yammer, Slack, Microsoft Teams and Facebook's Workplace invite conversations that are *too* open and dynamic.

The platforms provide a user experience that closely resembles consumer social media sites. Employees may forget that they need to conduct themselves professionally—and behave in line with corporate policies.

Messages are often short and informal, often filled with emojis and GIFs. People, who think their messages are private and unmoderated, may let their guard down. The result: inappropriate or even illegal conduct.

Harassment from co-workers, corporate leaders and third parties on Slack

In the wake of the uptick in Slack usage since the start of the pandemic, employment lawyers have seen an increase in harassment complaints involving the platform.[15]

Bari Weiss, an opinion editor at the *New York Times* who resigned last July, is a prime example. She said the news organization's Slack channel had become a place where her "work and character… [were] openly demeaned."[16]

And Steph Korey, CEO and co-founder of fast-growing luggage startup Away, stepped down after a former employee described "Slack bullying" as a pervasive element of the company's culture.

"In my experience there, it was extensive and relentless," the ex-employee said.[17] Though Korey later backtracked on the resignation, the incident continues to on the company's brand.[18]

Harassment concerns among Slack users became so far-reaching that Slack delayed the rollout of a planned direct-message feature. When a user invited someone to communicate with them one-on-one in the app, they could send a customized, possibly abusive, invitation message.

And another new feature, ConnectDM, let users send that invitation to people outside their organization. There was no way for recipients to block unwelcome invitations.[19] Slack disabled the feature amid worries that people might misuse it to harass or abuse other users.

Bad behavior isn't easy to police or block

Unlike consumer-oriented social media platforms, Slack doesn't offer any means of directly blocking other users within the same organization. For employees on the receiving end of abusive comments, the only recourse was to contact that channel's administrator or leave the channel.

At the same time, employees can create private channels, making it easy to ostracize others or share inappropriate or unwanted content.

[14] Microsoft. **Yammer Overview**. Accessed September 2021.

[15] Chip Cutter and Aaron Tilley *(The Wall Street Journal)*. **"Slack Has Made Remote Office Communication Easier. It Can Also Be Less Civil."** August 2020.

[16] Jeffrey A. Trachtenberg and Lukas I. Alpers *(The Wall Street Journal)*. **"Bari Weiss Quits New York Times Opinion, Alleging Hostile Work Environment."** July 2020.

[17] Zoe Schiffer *(The Verge)*. **"Emotional Baggage."** December 2019.

[18] Charity L. Scott *(The Wall Street Journal)*. **"Chief of Online Luggage Seller Reverses Course on Resignation."** January 2020.

[19] Kate Cox *(Ars Technica)*. "Slack pledges update to **"Connect DM" after realizing harassment exists."** March 2021.

[20] United States Equal Employment Opportunity Commission, **Enforcement and Litigation Statistics.** 2020.

Risk 3 Social Media Missteps Causing Reputational Damage

If an employee unwittingly exposes protected information in a social media post or responds poorly to a customer's complaint in a public forum, it can damage the company's reputation and dampen customer loyalty.

More and more companies let employees engage with customers and prospects over social media. Beyond marketing teams, technical support and customer service reps now use social media regularly. Meanwhile, workers in highly regulated industries (such as financial advisors and insurance agents) are growing their presence on Facebook and Twitter.

Ensuring that everything posted about a company is compliant and embodies the brand's values is a growing challenge. It's no wonder that so many organizations struggle to police the growing volume of social-based content has grown so complex.

Deleting an errant post is easy—recovering from it is harder

A wide range of employee actions on social media can harm an organization. The issue could be something as simple as someone accidentally clicking "like" in response to offensive or inappropriate content. An employee might share content that conflicts with corporate values and standards. Or a bad actor might take over a brand's social media account to sabotage it.

In any of these cases, the fix isn't as simple as just removing the offending content. All too often, people take screenshots. And in many instances, poorly thought-out attempts at cover-up look worse than the original offense.

INSIDE STORY

Credit reporting company sends customers to phishing site in the wake of massive data breach

Many social media mistakes are nothing more than embarrassing missteps. But in other cases they can cause lasting harm to customers and to the brand's image. Consider the example that a major credit bureau set in the wake of a large-scale data breach that affected more than 147 million of its customers.

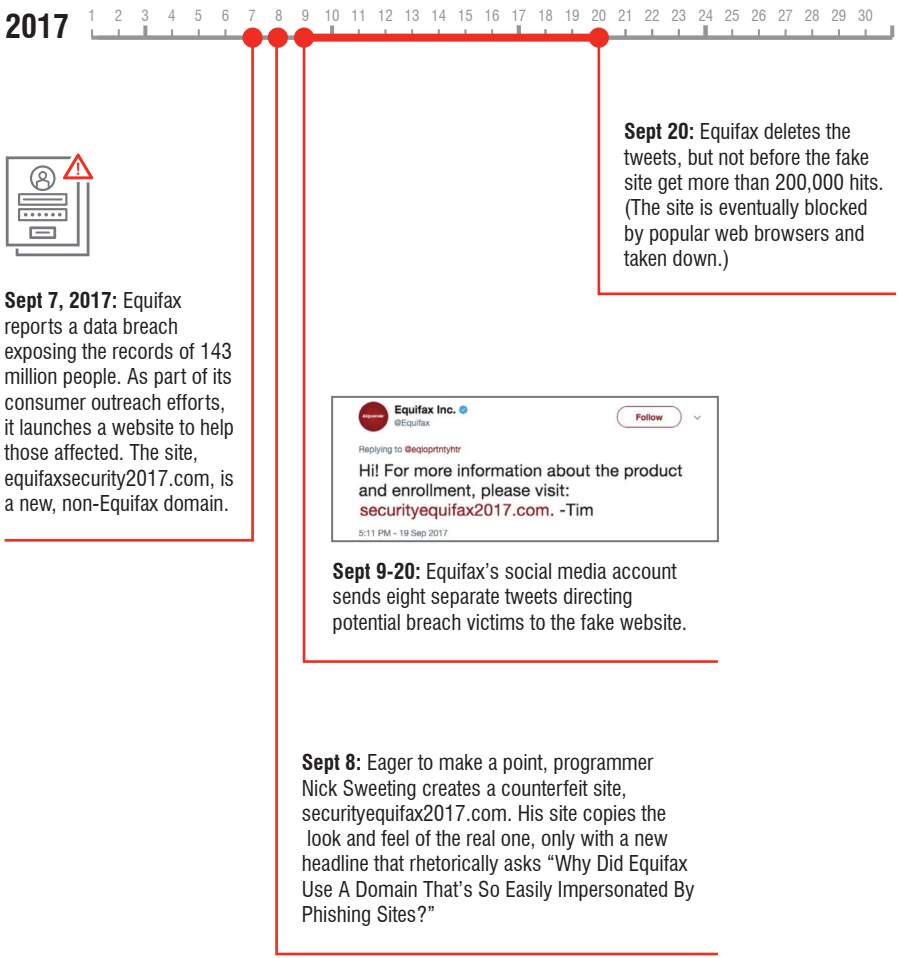
How it happened

Tweets sent from the company's official Twitter account, purportedly signed by one of its employees, steered customers concerned about the breach to a fake website instead of a real one the bureau had set up to inform and reassure them. The phony site mocked the company for choosing a domain that was so easily spoofed.[21]

The damage

Though the offending tweets were quickly removed, the gaffe drew major media attention—the last thing the company needed as it struggled to recover from the breach. And there's no telling how many customers fell victim to cyber criminal activities related to the spoofed site. Unfortunately, Equifax's mistake isn't unique. Hotel giant Marriot used an easy-to-spoof domain to help those affected by a 2018 data breach. Fortunately, cybersecurity experts bought up lookalike domains to keep them out of the hands of cyber criminals.

Here's a timeline of the blunder:



[21] Sarah O'Brien *(CNBC)*. **"Equifax tweets sent victims to phishing site."** September 2017.

Risk 4 Insider Fraud

91%

of companies with 100 or more employees use social media for marketing purposes.[22]

83%

of financial advisors use social media for business purposes.[23]

13%

of Americans say they've been the victim of social media account takeover.[24]

Social media networks have instant global reach. They are anonymous and easy to use—and ripe to be exploited by criminals. At the same time, enterprise collaboration tools can be a ready source of information for ill-intentioned insiders looking to cash in their knowledge.

Collaboration platforms are left unmonitored in many organizations. As a result, they're often perceived as a safe place to share customer data or other intelligence that shouldn't be made public. In recent cases, they've even become a place where malicious insiders looking to commit fraud. Information can be exchanged in milliseconds, enabling insiders to cash in on their advance knowledge to set up shady deals and trades.

Chat rooms and WhatsApp used for insider trading schemes

In 2018, Goldman Sachs agreed to pay $110 million in fines for foreign exchange trading fraud. Traders from several large banks took part in chat room conversations where they shared confidential information about customers' upcoming trades. This allowed the traders to collude at customers' expense.[25]

More recently, an employee of a Northern California-based bank paid civil penalties to the Securities and Exchange Commission for sharing insider information about upcoming acquisitions with his employer's clients.[26] The employee sent encrypted messages on WhatsApp to a friend. The friend then bought stock in the target companies just before the deals were announced. The U.S. Attorney's Office for the Northern District of California is now pursuing criminal charges.

The social side of money laundering

Social media has grown into a popular place to recruit money laundering mules. These can be innocent victims who supply bank account information at the request of a cyber criminal. Some unwitting accomplices may reply to seemingly legitimate job offers. Others are lured by promises of romance. Still others are responding to pleas for help from strangers pretending to be in crisis. And sometimes, the accomplice is fully aware of the fraud, attracted to the prospect of turning a quick profit.

In the aftermath of the global COIVD-19 pandemic and ensuing economic shocks, this activity may become more prevalent. Social media's wide reach—along with the fact that direct messaging on most platforms isn't monitored—makes it a near-perfect place to recruit new money mules.

Data-privacy rules make money mule schemes hard to detect. It's near impossible to trace individual payments once they're left one bank for another. That means no single financial institution can see the end-to-end path that a payment takes as it flows through the banking network.

[22] Statista. **"Social media marketing usage rates in the United States from 2013 to 2022."** August 2021.
[23] Putnam Investments. **"The Putnam Social Advisor Survey."** 2019.
[24] Pew Research Center. "**Americans and Cybersecurity."** January 2017.
[25] Matt Levine *(Bloomberg Opinion)*. **"Goldman FX Trader Was Loyal to His Chat Room."** May 2018.
[26] United States Security and Exchange Commission Press Release. **"SEC Charges San Francisco Bay Area Finance Employee and Friend with Insider Trading."** June 2021.

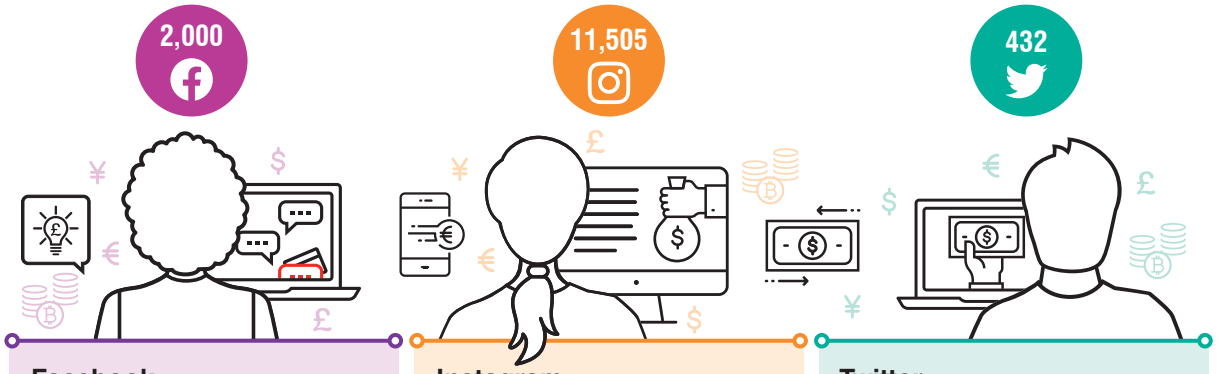
Instagram influencer Hushpuppi and worldwide money-laundering networks

The 37-year-old Instagram influencer known as Hushpuppi was arrested in June 2020 on multiple counts of money laundering, wire fraud and other internet scams. Born poor in Lagos, Nigeria, the social media star allegedly amassed a multimillion-dollar fortune through business email compromise (BEC). These schemes diverted wire transfer payments into bank accounts controlled by criminals. Hushpuppi is alleged to have recruited co-conspirators around the world to help him launder the money.[27]

Recently the average age of participants in these kinds of schemes has tumbled. The number of 14- to 18-year-olds who have allowed their bank accounts to be used for funds diversion has increased by 73% over the past two years. In September 2020, the Secret Service seized $140,000 from a 19-year-old who was serving as a money mule for a criminal group.[28]

But it's not just teens who get involved in criminal activity. A Maryland man recently pleaded guilty to conspiracy charges after laundering more than $6.2 million. The money was collected in a fraudulent romance scam that targeted victims on social media and dating sites.[29]

Using four basic search terms our research identified potential money-mule activity on three social media platforms. There was some crossover of followers between accounts.
Based on the simplicity of the search terms used and the obvious (and at times overt) reference to money muling activity, it is our assessment that the use of social media platforms by money mule gangs is systemic to the gang's success and ability to identify and recruit mules.



Facebook

- 5 out of 100 accounts identified via the search terms appeared to conduct money mule activity.
- There was one specific group with 2,000+ members that in our opiniont, strongly suggested that money muling was involved.

Instagram

- Instagram searches returned 8 accounts with followers amounting to 11,505 with some follower cross-over between accounts.
- Instagram had the most accounts assessed as linked with money muling activity. This is likely due to the graphical nature of content that can be used to draw in followers, targeting the demographics of the users and the ease of setting up accounts.

Twitter

- 4 separate accounts were identified via the search terms ranging from 20-225 followers with a total of 432 followers.
- There were more potential money muling accounts on Twitter than was expected given the nature of the platform and the time spent developing a following.

Source: Fintrail, **"How Social Media is Used to Further Financial Crime – Part 1,"** March 2020.

[27] Michael Kaplan *(New York Post)*. **"Influencer to Criminal: the rise and fall of Instagram star Hushpuppi."** September 2020.
[28] Gary M. Shiffman *(Wall Street Journal)*. **"Money Mules in Sheep's Clothing."** January 2021.
[29] AP News Wire. **"Man pleads guilty to laundering $6.2M in 'romance scheme'."** August 2021.

Risk 5 Legal Issues or Compliance Violations

62%
of compliance leaders expect that more time and resources will need to be devoted to risk issues within the next twelve months.[31]

In 2020, regulators around the world issued

67,125 alerts

—a new high.[32]

The number of channels and platforms that employees use to communicate has exploded in recent years. Organizations must ensure that employees aren't publishing inappropriate content or running afoul of regulators.

Today's social media networks and collaboration platforms make it easier to share information. But data privacy and information-security rules are as stringent as ever. With more communication channels than ever, companies must still be able to apply policies that align mandates such as HIPAA, FINRA, FDA, SEC, SOX and others. And they must be able to do so consistently and demonstrably.

Data privacy protection challenges

If you are in a highly regulated industry, you must adhere to strict rules governing what information you share with the public and how you share it. The same holds for publicly traded companies. (Companies in both categories, such as publicly traded banks and healthcare companies, have the biggest challenges of all.)

Expecting all employees to understand all the nuances of the law just isn't realistic. Inadvertent disclosures on social media are always a risk.

Organizations face similar challenges ensuring that access to internal communication platforms is granted to only the right people at the right time. Employees may not know which colleagues or business partners have access to which channels. And they may not realize that they're sharing regulated data with people who shouldn't be included.

"Shadow IT" also poses risks. Workers often sign up for free versions of collaboration tools instead of IT-sanctioned platforms. If people like Slack more than Microsoft Teams, they might turn to an unmonitored Slack channel instead of the corporate instance of Teams. With shadow IT, there's no guarantee of corporate data or employee privacy.

Information Governance Problems

More and more work-related discussions happen in real time over chat rather than email. This shift makes compliance difficult for organizations that don't monitor and retain content from all the channels their people use. Many companies still haven't enacted information governance policies that cover today's most popular tools and platforms. Running afoul of regulators is all too easy.

Even firms that aren't regulated may find themselves losing their "institutional memories" if they don't have some way to retain content.

E-discovery requests and litigation

If your organization is involved in litigation or any legal investigation, you'll need to produce any non-privileged information deemed relevant to the case. This may include business communications. It may also include email messages, social media posts and many other types of digital communications. If you aren't retaining this content, you aren't litigation-ready.

Improper financial disclosures

In 2013, Netflix CEO Reed Hastings decided to publish the company's monthly online viewer count on his personal Facebook page. This act triggered an SEC investigation.[30] Ultimately, the SEC decided that companies can make financial disclosures (or disclosures with financial implications) on social media as long as investors are alerted beforehand.

Investors must be told which social platforms will be used to publish information. SEC Regulation Fair Disclosure (FD) still applies to social media disclosures. They must take place "in a manner reasonably designed to get that information out to the general public broadly and non-exclusively."

In practice, social media's widespread adoption has made it much easier for employees to bypass corporate policies and due process when making such announcements.

[30] United States Security and Exchange Commission Press Release. **"SEC Says Social Media OK for Company Announcements if Investors Are Alerted."** April 2013.
[31] Thomson Reuters. **Cost of Compliance 2021: Shaping the Future.** 2021.
[32] Ibid.

How to Make Communication Tools and Social Media Platforms Secure and Compliant: A Four-Step Plan

To mitigate these risks in today's virtual-first world, a people-centric approach to compliance and security is critical. Collaboration takes place online. Your customers and prospects expect to be able to engage with you on social media. Thus, you must be able to capture, manage, retain, supervise and govern content across multiple tools and platforms.

STEP 1

Capture business communications

You need to be able to capture non-persistent communications across all of the channels that your employees use. These likely include chat, collaboration platforms, social media and more.

You cannot rely on the platforms alone to perform this on your behalf. Many can't. Even in those that can, maintaining connectors from every platform to a centralized data store can be difficult.

To be able to analyze the content—or search it for e-discovery purposes—it needs to be normalized into a standardized format. Otherwise, your team can end up spending hours on manual review. If each platform must be searched individually, the content may have changed by the time it's surfaced for e-discovery, which isn't forensically sound.

Today, it's essential to extend the same supervisory capabilities across social media in real time. This way, you can monitor content at its point of capture and remove risky or non-compliant content quickly—in some cases before it's even published.

Finally, you'll need to be able to verify that all captured content is received by downstream storage services. This makes it possible to find and close any hidden gaps. This is essential for full compliance with e-discovery and regulatory rules.

Content capture for compliance: key questions to answer

- How do your employees communicate?
- Are you confident that you're able to capture and manage data from every one of these sources?
- Are you equipped to manage new data sources as soon as they come into use?
- How is the content packaged and processed?
- Are there any gaps and inconsistencies in your content delivery and archiving workflow that could result in costly compliance violations?

For compliance officers, corporate counsel and teams who manage information governance, security or insider risk

To meet regulatory or corporate governance mandates, you must capture content from all the tools employees use to communicate. Look for a solution that:

- Supports all relevant platforms
- Can capture data regardless of the user's device type or location
- Normalizes content using a consistent and well-documented format
- Integrates with archiving, e-discovery and supervision solutions

STEP 2

Retain and supervise business communications

For easier and more effective compliance, e-discovery and information governance processes, you'll need to supervise communications efficiently. This is the case whether those exchanges take place within your own network or on third-party platforms.

This means capturing messages in their original form. You should include contextual details such as file attachments. The same goes for context around what came before and after the messages within the conversation thread. Ensure that you can capture attributes that are unique to each channel as well.

After all, compliance is about people. When you can see what messages looked like in their original form, you can understand what your employees likely intended. You can also see what the tone and context of the conversation was like—no matter which social platform or collaboration tool they were using.

This is where insider threat management and compliance can reinforce one another. By working together to create a visual timeline that shows who did what, and when, the two tools provide critical context for understanding what happened and the intent behind the action.

For retention, accuracy is key. If you are retaining information for litigation, internal investigations or audits, you must store content in a secure and compliant archive. To guarantee the information is accurate, the archive must be immutable. This is critical for preserving the chain of custody for evidence should you ever need to prosecute an insider or former employee.

You should also have accurate and efficient discovery capabilities. Orchestrating e-discovery workflows simplifies the assignment, search and review process. It also makes it easier to give your legal team, outside counsel and courts any requested information quickly.

With the right tools, you can narrow your search results and better uncover insights. To that end, consider a solution powered by machine learning. A modern solution will find the most relevant content within your searches efficiently and minimize false positives.

E-discovery, monitoring and supervision: key questions to answer

- Can your teams easily find messages from specific people? What about conversations between pairs or groups of people?
- Can you surface messages created during a given time period? Can you search message content by topic or platform?
- Can your content capture solution map the content consistently across all the platforms that your employees use to communicate?
- Do you have access to complete litigation hold capabilities?
- Can your organization monitor all relevant social media platforms in real time to detect compliance or policy violations that occur within corporate accounts and employees' personal accounts?
- How quickly can you remove problematic content?
- Do your content supervision solutions provide a holistic view of communication throughout the organization in one place, with a single-pane-of-glass dashboard view?

For compliance officers, corporate counsel and teams who manage information governance, security or insider risk

Want to ease compliance, reduce risk and simplify the e-discovery process? You need a solution that can:

- Provide broad, native support for a wide array of digital communication tools and platforms
- Simplify monitoring by enhancing visibility
- Demonstrate compliance with supervisory review capabilities
- Store communications in a secure, accessible and fully compliant archive
- Use machine learning to streamline e-discovery and supervision workflows

STEP 3

Prevent data loss and detect employee misconduct quickly

Negligent and malicious insiders can put your sensitive and confidential data at risk. So can employees whose accounts have been compromised by an outside attacker.

To protect your data and intellectual property from accidents, mistakes, cyber attacks and insider threats, you must detect misconduct in seconds. And you should be able to do so across all the communication channels and platforms that your employees use. These include cloud services, email and websites and endpoint-based file shares.

Because today's communications happen across so many channels, you need a combined, holistic view to get the full story.

Easing the burden

You need to tackle the full spectrum of people-centric data loss scenarios. Just as important, you need to do so in a way that doesn't impose a huge administrative burden. Be sure your process won't take too much of your team's valuable time.

A solution that can apply common DLP classifications across multiple channels helps you enforce compliance and data protection rules with just a few clicks. At the same time, security and compliance teams can accelerate reviews and speed response times by investigating alerts from the cloud, email, the web and endpoints within a single, unified interface. Together, these capabilities reduce DLP costs so that you get more value from the solution, faster.

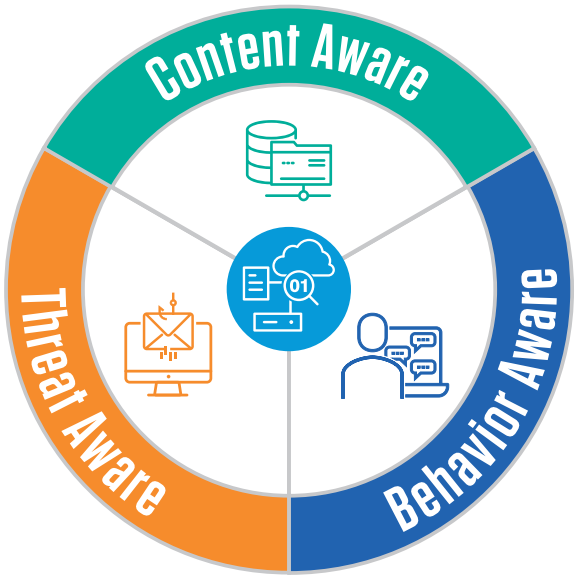
Every organization's data privacy and compliance needs are unique. Meeting them all demands tools that are flexible and adaptable. Your data will continue to grow, and laws will continue to change. You need a solution that can evolve with you.

Data aware, behavior aware and threat aware

Detecting the full range of data risk types can be complicated. To address all use cases relevant to your organization, choose a data loss prevention (DLP) solution that's:

- Content aware, so that it can accurately identify sensitive or regulated data
- Behavior aware, so it can determine which user behaviors are risky, which are likely indicators of malicious intent, and which types of access are unusual
- Threat aware, so it can identify compromised accounts or tell when users have fallen victim to a phishing attack

Together, these three areas can help you understand the "who, what, where, when and why" behind every user action.



Data loss prevention: key questions to answer

- Can your organization identify all sensitive and regulated data in your environment, no matter where it resides?
- How accurately can you identify compromised user accounts?
- How quickly can you remediate post-compromise malicious activities on cloud applications, websites and endpoints and with your sensitive data?
- How long does it take your security and compliance teams to investigate a DLP alert? Can your teams keep up with all the alerts you receive?
- Can you accurately and efficiently identify sensitive data across channels that your employees use?
- Does your current DLP solution use behavioral and contextual information to uncover user intent? How well does it calculate risk levels?

For compliance officers, corporate counsel and teams who manage information governance, security or insider risk

Data doesn't lose itself. To protect your organization from the full range of people-centric data loss risks, you need a solution that can:

- Address the full range of risks that your data faces, including those from negligent, compromised or malicious users
- Save time and reduce administrative hassle by building DLP policies once, then applying them across all applicable channels
- Protects your users from threats to their credentials, corporate applications and your sensitive data
- Enable faster responses and investigations by security teams

STEP 4

Exercise good governance over cloud platforms and apps

If you don't know how your employees communicate, you can't monitor their conversations. Nor can you protect your data.

Unfortunately, "shadow IT" is an ever-present risk. If your security and compliance teams don't know what tools people are using, they can't be sure they are secure. Insecure public platforms, competitors' products and third-party apps that contain malicious source code are all real risks.

This type of third-party app compromise recently took place when online workflow management platform Monday.com was part of a supply-chain attack.[33] This risk is especially grave if the third-party apps can use OAuth permissions. OAuth can give the apps access to data and other critical resources.

Good governance in today's cloud-based IT environments means enforcing identity-and role-based access controls—and applying policies in real time. This is critical no matter where your users work or what type of device they're using.

Also essential is real-time behavioral monitoring. If a user takes an action that's risky or raises suspicion, you should make them re-authenticate. This prevents account takeover attacks from progressing into larger breaches.

Remain aware: what infrastructure-as-a-service (IaaS) accounts and resources does your organization own? You can prevent compromised or malicious users from doing harm by monitoring all cloud resources and actively managing your cloud security posture. Cut off access for departing employees right away. And always make sure that current employees aren't granted privileges they don't really need.

Cloud platform and application governance: key questions to answer

- How accurately can you assess the risk that a given account has been compromised?
- Do you have an accurate inventory of all the cloud apps, web apps and resources your people use?
- Do you discover and track new applications in your environment used by your users?
- How well can you keep track of OAuth-connected third-party apps within your environment?
- Can you apply adaptive access controls across applications and users in real time, not just during the first login? Can you make users re-authenticate in cases where they take unusual or risky actions mid-session?

For compliance officers, corporate counsel and teams who manage information governance, security or insider risk

Today's employees work from anywhere, anytime. And today's IT ecosystems no longer sit behind a firewall or within the network perimeter. Look for a solution that can:

- Protect users, accounts and data from advanced threats, whether they're in the cloud, in the data center, or on an employee-owned device
- Integrate threat detection and access control across email, cloud and the web
- Incorporate user behavior analysis and multi-factor authentication (MFA)
- Monitor for and control access to unauthorized cloud applications

[33] Ax Sharma (BleepingComputer). **"Codecov hackers gained access to Monday.com source code."** May 2021.

Other considerations:

Compliance and security are intertwined. That's why you need to take a holistic, people-centered approach to both.

Work-from-anywhere is the norm and employment is more flexible than ever. In this new normal. you cannot understand data risk without a full understanding of user risk. A single incident can have ripple effects for multiple teams and business units.

- Imagine your team geting an alert that a user has mishandled sensitive information. The team must:
- Open a ticket within security operations to identify and remediate a compromised user's account
- Launch an investigation within legal and HR departments to see whether an insider has behaved in ways that were deliberately inappropriate or malicious
- Assign user training to ensure that the same issue doesn't take place again by mistake
- Revamp business processes that weren't well designed to safeguard regulated data

Each of these response processes can occur independently from the others. But all of them can be enhanced with multi-functional solutions that speed response. The best solutions can provide clear visibility into:

- What has occurred
- When it happened
- Who and what data was involved
- What the risks are

Not all insider risks are created equal. Some users pose a greater risk than others. To assess insider threats accurately, you must be able to figure out where the greatest risks lie based on all the relevant factors. Soon-to-depart employees and contractors whose engagements are ending, for instance, may be less motivated to protect your organization. Anyone with elevated privileges inherently poses more risk.

Risks stemming from social media and collaboration platforms go hand-in-hand with other aspects of data privacy and security. Addressing them all together with an integrated and unified solution is critical. With an integrated approach, you can enhance visibility across your organization's entire information ecosystem.

In the same way, email, cloud and endpoint security are also interrelated. You can't effectively protect one of these resources without protecting the others too.

A holistic, people-centered approach will give you enhanced visibility, detection and response capabilities by incorporating the following components:

- DLP
- Insider threat management
- Access controls
- Threat protection that enables you to prevent, detect and quickly respond to threats

A unified solution that includes multiple capabilities inside a single platform can lower your IT and security costs while simplifying management.

Conclusion

Even as organizations adjust to remote and hybrid work, success hinges more than ever on effective collaboration across departments, distances and time zones.

Many are struggling to support friction-free communications while balancing security and compliance mandates.

Collaboration platforms and social media networks used in today's organizations demand modern compliance and security architecture. You must capture, manage and supervise content from many sources for compliance. You must detect, prevent and respond intelligently and quickly to protect from data breaches for security. Ideally, you want to consolidate vendors, manage one platform and get unified analytics across the risks. That's why a holistic, integrated approach is key.

Why Proofpoint?

Proofpoint offers a full suite of people-centric compliance, data

loss prevention and insider risk solutions for enterprise communication tools and social media networks.

Proofpoint Solutions:

- **Proofpoint CASB** secures cloud application access, protects users against advanced cloud threats and provides granular controls for cloud data at risk.
- **The Proofpoint Compliance Platform** helps you capture, discover, retain and supervise critical business communications everywhere they happen.
- **Proofpoint Enterprise DLP** prevents data loss across email, endpoint, cloud, on-premises and cloud.
- **Proofpoint Insider Threat Management (ITM)** protects IP, sensitive and regulated data from malicious and negligent users—without compromising endpoint performance.

And our archiving and compliance solutions help you capture, retain and supervise critical business communications everywhere they happen.

To learn more about how Proofpoint can help secure your communication tools and social media platforms, visit **proofpoint.com/us/products/information-protection/enterprise-dlp**.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at **www.proofpoint.com**.

proofpoint.

0501-008-01-01 10/21