Kiteworks

2022

2020 Sensitive Content Communications Privacy and Compliance Report

Silos and Complexity Result in Inefficiency, Increased Risk, and Compliance Challenges

Table of Contents

3
Foreword

4
Executive Summary

7
Introduction

8
Methodology for This Study

10
Insights on Privacy and Compliance of Sensitive Content Communications

10
Insight #1: Silos and Inefficiencies Permeate Sensitive Content Communications

14
Insight #2: Security Gaps Increase Attacks and Hamper Incident Response

18
Insight #3: Inconsistent Policies Impede Proactive Risk Management

23
Insight #4: Inconsistent Governance Negatively Impacts Compliance

26
Conclusion

Foreword

Content is at the heart of everyday business at nearly every organization. Information on individuals—personally identifiable information (PII), protected health information (PHI), and payment card industry (PCI) data—can be sold on the black market. Corporate data about financials, intellectual property (IP), and mergers and acquisitions (M&A) are a prime target for state-sponsored competitors seeking business intelligence. And data about national security, critical infrastructure, and criminal investigations from government entities are of intense interest to nation-state threat actors.

Recognizing these risks, regulatory bodies are increasingly focused on the need to track and control access to different types of sensitive data as it moves within and between organizations. This danger is real: Adversaries can exfiltrate content with man-in-the-middle attacks, phishing, spear phishing, network hacks, and web application attacks. In addition, content can get into the wrong hands through exposure by insiders—both malicious actors and well-meaning employees who make a mistake.

For legitimate organizations, protecting sensitive content is a business imperative. The cost of a data breach can be severe, and barring that outcome, fines for noncompliance can be significant. But sensitive data cannot simply be locked down so that it is inaccessible to anyone. Such information is valuable precisely because it is critical for the strategic and tactical operations of the organization. And in the course of everyday operations, sensitive content must be shared with other organizations.

Kiteworks' 2022 Sensitive Content Communications Privacy and Compliance Report highlights that the systems in place to protect sensitive content at most organizations are inadequate to the task. Further, the research finds that compliance is, at best, a work in progress. In fact, more than half of IT, security, privacy, and compliance professionals surveyed admit that they are not adequately protected against third-party risk.

This makes sense given the way content communications is conducted in their organizations. Nearly 6 in 10 organizations admit that they do not even have systems in place to measure third-party risk. One cause is the fact that the typical organization shares sensitive content with hundreds or thousands of third parties over as many as a half-dozen channels. Incredibly, more than half of them fail to take the basic step of encrypting all communications of sensitive content. There is clearly work to be done.

We hope this report is illuminating for you as readers. More importantly, we hope it helps you to identify gaps in your own organization so that you can better protect your sensitive content in the future.

Sincerely,

Frank Balonis
CISO and SVP of Operations, Kiteworks

Executive Summary

For cybercriminals, sensitive data is the crown jewel that they strive to obtain. The rightful owners of this content must protect it against these bad actors—when it is in motion and at rest. According to the Ponemon Institute and IBM, the average data breach in 2021 cost the victim organization $4.24 million.[1] Beyond this existential risk, organizations are faced with regulations that differ from jurisdiction to jurisdiction—but are generally becoming more stringent. As a result, organizations must not only safeguard their sensitive content, but also prove to auditors that they have done so in a compliant way.

The 2022 Sensitive Content Communications Privacy and Compliance Report is based on a survey of 400 IT, security, compliance, and governance leaders. Analysis of the survey findings yields several insights:

51% of organizations are inadequately protected against third-party security and compliance risks related to sensitive content communications. Key causes include failure to encrypt sensitive content communications, lack of content governance controls, and inaccurate and insufficient compliance reporting.

Complexity, Silos, and Inefficiencies of Sensitive Content Communications

The first insight is that content communications is something of a disjointed mess at most organizations. Nearly two-thirds of respondents share content with more than 1,000 external organizations, and all do so with at least five communications channels. Two-thirds use more than four separate systems to track, control, and secure content communications. And dealing with encryption issues consumes dozens or hundreds of hours of staff time per month.

67%	**60%**	**49%**
use 4+ different systems to track, control, and secure content communications	**ask the sender to send an unencrypted file to a shared drive link if an email cannot be decrypted**	**spend 30+ hours of staff time per month dealing with incoming email that cannot be decrypted**

Security Gaps

This complexity makes it harder to provide security for content communications, and respondents identified multiple security gaps. Majorities of respondents fail to scan all incoming communications for viruses and spam and to scan all outgoing communications with a data loss prevention (DLP) tool. Further, encryption of content communications is spotty at best—even when it contains sensitive content.

54%	**88%**	**53%**
do not perform DLP scans on all outgoing email	**do not encrypt all communications with third parties**	**do not encrypt all *sensitive content* communications with third parties**

Risk Management Gaps

These security gaps create significant headaches from a risk management perspective. Most respondents are worried that their organizations are not protected adequately from third-party risk, and even more have not yet deployed the basic step of making it possible to measure such risk. Both the survey's respondents and their board and top executives agree that the most important step in reversing this risk is to centralize content communications under a unified system.

51%

say their organizations are not adequately protected against third-party risk

58%

have not implemented controls to measure third-party risk

49%

of respondents—and of their executive leadership—see unifying management, tracking, policies, and reporting for content communications as a top priority

Compliance Gaps

Respondents must comply with a variety of regulations based on the jurisdictions in which they do business, and most must prepare between four and nine compliance reports per year. Each report consumes more than 20 staff hours at a vast majority of organizations—and more than 40 hours at nearly half. Despite this effort, a large majority of respondents admit that their compliance reports are not fully accurate, and more than two-thirds think that their organization needs to improve its governance when it comes to content communications.

77%

expend 20+ hours per staff time per compliance report

79%

admit their compliance reports are *not* completely accurate

69%

say improvement is needed in governance with content communications

Conclusion

As security threats proliferate and regulations tighten, organizations have no choice but to get serious about securing and controlling content communications. They must replace the current chaos with a unified content communications infrastructure that enables them to track who accesses and shares content, control access to content, and secure it at rest and in motion.

Introduction

The sharing of content is a foundational element of a functioning economy, and much of that content is intended for the recipient's eyes only. In the normal course of operations, businesses share everything from go-to-market plans to financials to personally identifiable information (PII) with third-party partners and suppliers multiple times each day. Governments share top-secret intelligence related to national security, confidential data related to ongoing criminal investigations, and citizens' personal information. Consumers upload tax returns to government authorities—often through intermediaries in the private sector—and many think nothing of sharing personal information on smartphone apps.

Perhaps it is the routine, everyday nature of content communications that makes it easy to forget the security and compliance risks that present themselves when files are shared. Senders and recipients simply want to do their jobs, and they often default to the easiest way to move information to where it needs to go.

Email attachments work well for smaller files, but an organization's ability to protect them while complying with regulations depends on the security of the email systems on both ends of the communication. File sharing services are ubiquitous and easy to use, but do not offer the level of security that enterprises need. This is especially true with consumer-grade personal file sharing accounts, which employees are tempted to use when they encounter an obstacle in sharing content.

Other ways that enterprises share content—managed file transfer (MFT) solutions, application programming interfaces (APIs), and web forms—offer efficiencies and sometimes a modicum of security. But these channels also make content communications more complex by adding to the number of channels over which content is transmitted.

Evolving Security and Compliance Challenges

As the complexity of content communications increases, so does the sophistication of threat actors. In late 2020, the massive compromise of a routine update to SolarWinds infrastructure software[2] impacted as many as 18,000 organizations[3] and highlighted the software supply chain as a top-of-mind security threat. Meanwhile, attackers using ransomware expanded the scope of their attacks to include exfiltration of confidential data—now an element in 80% of attacks.[4]

Regulators responded to this surge in attacks with new requirements of their own. The European Union, Canada, and the state of California placed new restrictions on the use of personal data over the past five years, with costly penalties for noncompliance. And in response to attacks like that on SolarWinds, the White House issued an executive order that places new cybersecurity requirements on entities doing business with the U.S. federal government.[5]

The 2022 Sensitive Content Communications Privacy and Compliance Report provides a snapshot of where secure content communications stands today. It offers insights on strategies organizations can use to reduce privacy and compliance risk and improve efficiency with the sharing of different kinds of content.

Methodology for This Study

This study is based on a global survey of 400 professionals from numerous industry sectors who are responsible for secure third-party content communications for their organizations. Conducted in early 2022, the survey consisted of more than 40 questions with results analyzed for the entire cohort, as well as by industry, job title, organization, geography, and other demographic factors.

A Diverse Pool of Respondents

Respondents tend to be at mid-career; nearly 9 in 10 are between the ages of 35 and 54 (Figure 1). As is typical in technological lines of work, 72% are male (Figure 2). The survey is truly global, with 15 countries represented across the three major geographies (Figure 3). Overall, just over 16% of respondents live in the Asia-Pacific region, 31% come from the Americas, and nearly 53% come from the Europe, Middle East, and Africa (EMEA) geography (Figure 4).

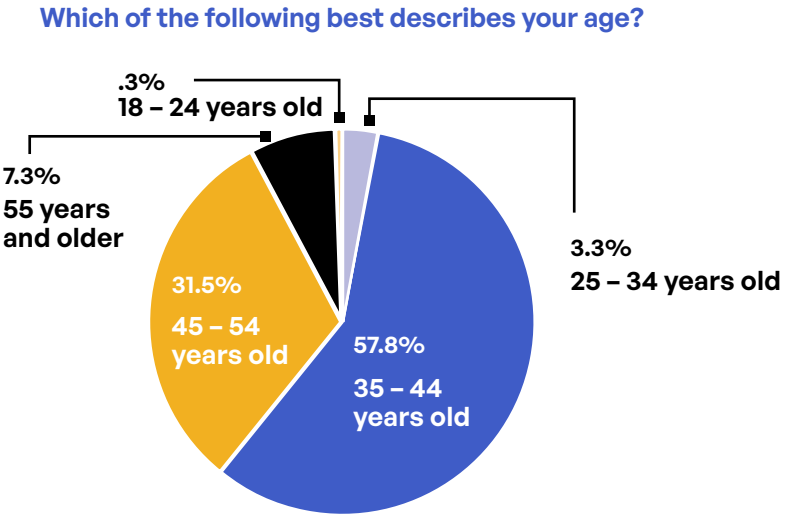

Figure 1

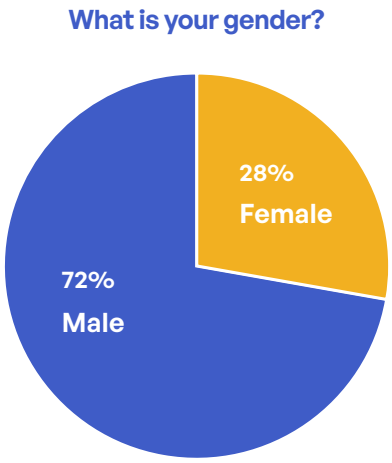

Figure 2

Survey respondents represent a wide range of industries (Figure 5), with financial services, healthcare, and manufacturing topping the list. They hold mostly executive positions (Figure 6), with more than half reporting C-level job titles and nearly one-third identifying as vice presidents. And while organizations of all sizes are represented, more than three-quarters work at companies with more than 5,000 employees (Figure 7).

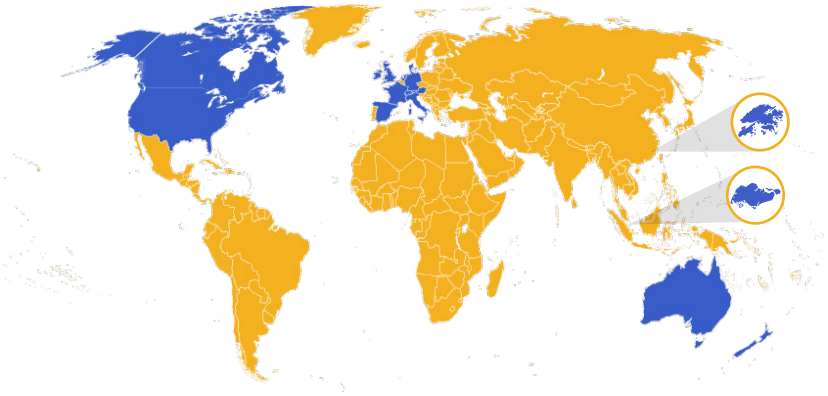

Figure 3

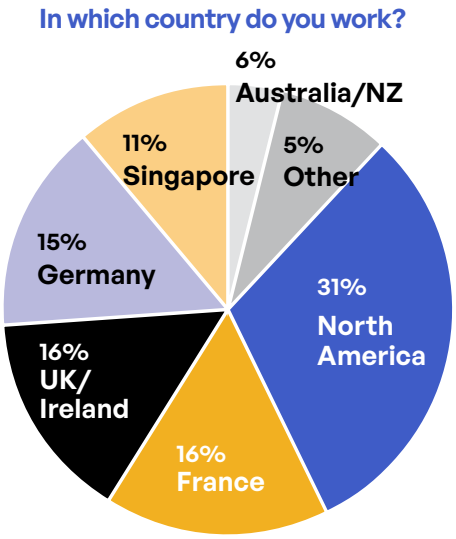

Figure 4

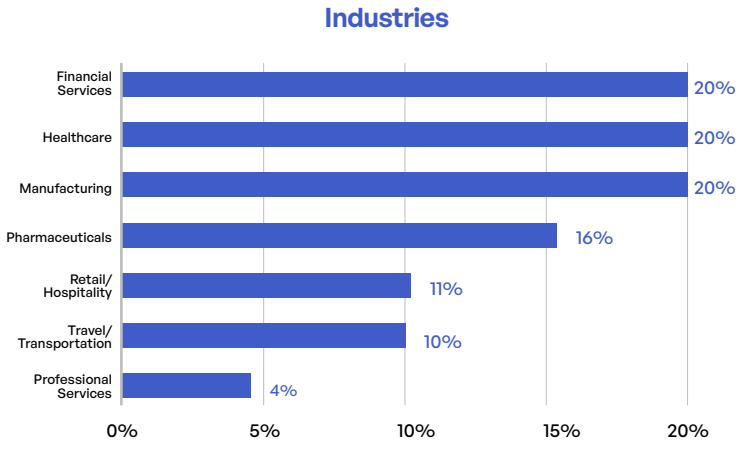

Figure 5

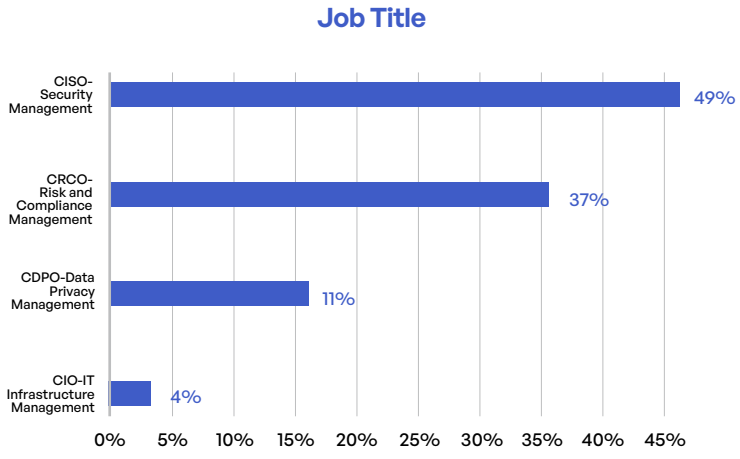

Figure 6

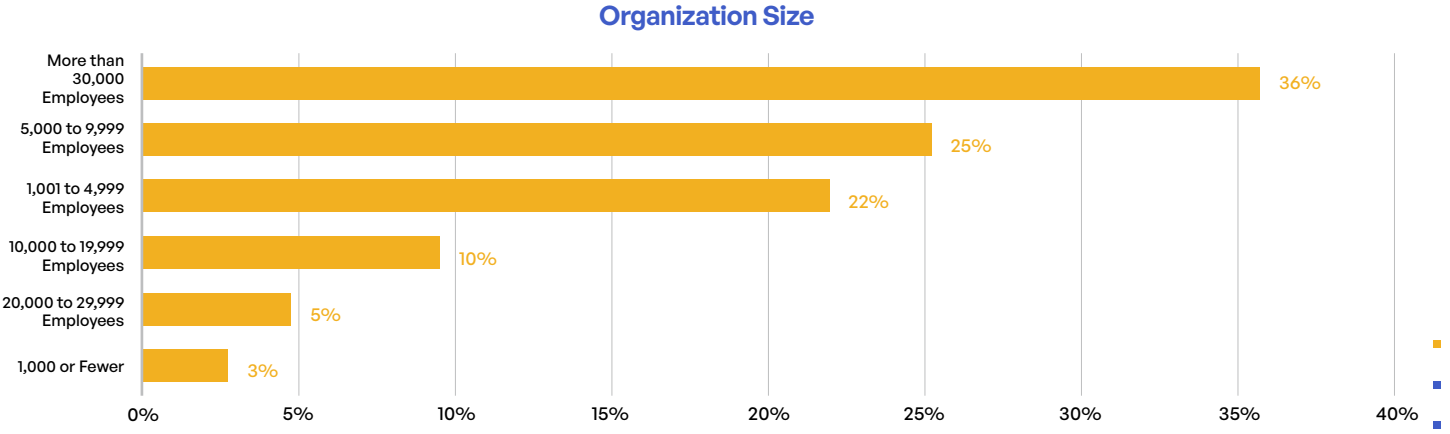

Figure 7

Insights on Privacy and Compliance of Sensitive Content Communications

Analysis of the survey results yielded several insights from the senior IT, security, privacy, and compliance leaders who participated:

Insight #1: Silos and Inefficiencies Permeate Sensitive Content Communications

Overall, respondents report that complexity is the name of the game when it comes to content communications. When asked how many third parties they regularly exchange content with, 62% said more than 1,000, while one-third gave answers above 2,500 (Figure 8). These third parties include vendors, suppliers, contractors, freelancers, auditors, and regulators. These staggering numbers suggest the potential for unwieldy processes and much difficulty in tracking and controlling the movement of content.

How many third parties (e.g., vendors, suppliers, contractors, freelancers, government regulators, et al.) does your organization exchange content with on a regular basis?

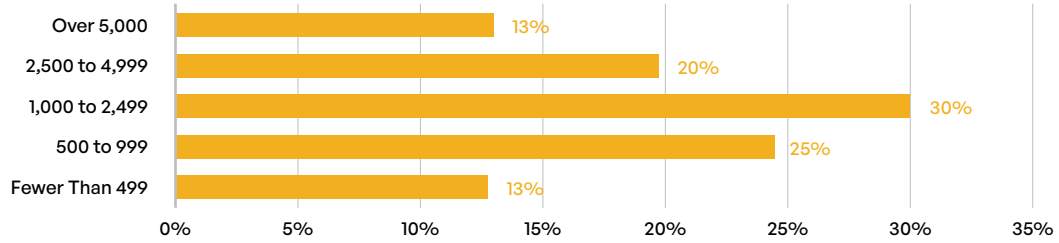

Figure 8

This complexity is compounded by a wide range of methods by which content is communicated. All respondents make at least some use of email, file sharing services, web forms, application programming interfaces (APIs), and file transfer and automation protocols (which consist of MFT, secure file transfer protocol [SFTP], and simple mail transfer protocol [SMTP]) (Figure 9). Not surprisingly, email gets the most use, with 90% of respondents using it for one-quarter or more of all content communications, and 37% using it for 35% or more of content communications. File sharing platforms are second most used, with 45% using this channel for one-quarter or more of content communications.

What is an approximate percentage mix of content communications methods your employees share externally with third parties that are sent, received, and stored over your communications infrastructure?

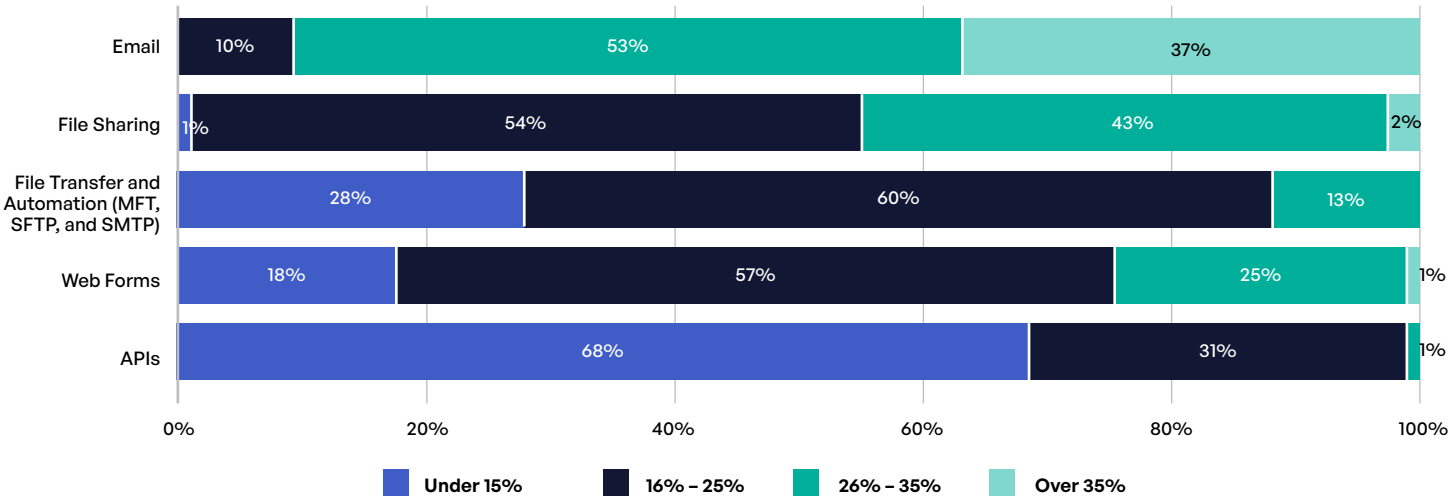

Figure 9

Which content communications methods pose the highest risk for your organization?

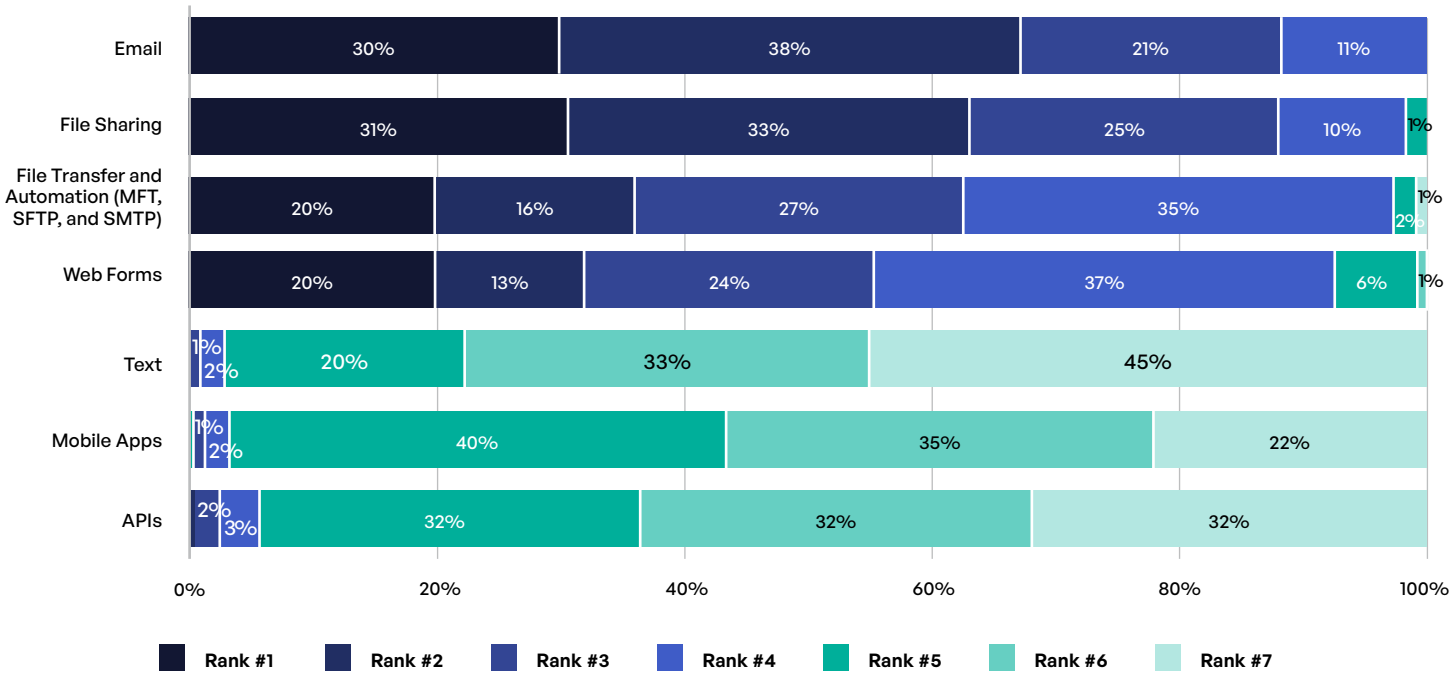

Figure 10

Looking at this question by industry, three industries stand out as heavy users of email for content communications. Among respondents in the financial services, retail/hospitality, and professional services industries, nearly half (between 46% and 50%) use email for 35% or more of their content communications. Two of those industries—retail/hospitality and professional services—also make much more use of web forms than the other industries.

Not surprisingly, the most used communication methods are also seen as the riskiest (Figure 10). Respondents most commonly rank email (68%) and file sharing (63%) among the top two risks. Conversely, risks posed by content communication by text message, mobile apps, and APIs rank very low for respondents.

How many different systems does your organization use to track, control track, control, and secure content communications with third parties?

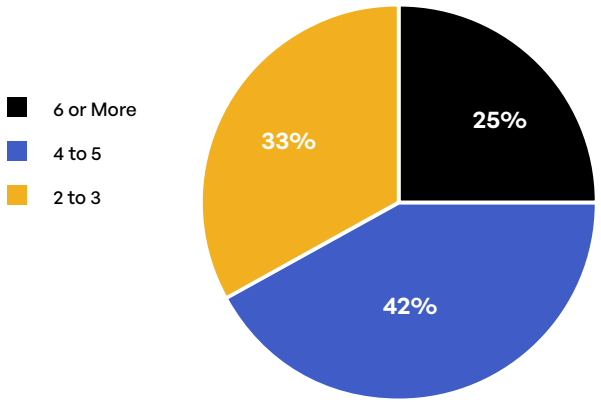

Figure 11

The complexity is compounded yet again by the number of different systems used by respondents to track, control, and secure content communications with third parties (Figure 11). Two-thirds of organizations use more than four separate products, and one-quarter use six or more. These tracking and security systems often are siloed by communication method, and it is likely that at least some are not integrated with other parts of the security and compliance architecture.

The high number of disparate tools suggests that many enterprises have made one-off security investments over the years—rather than integrating security and compliance tools with each other and with secure content communications tools. Even organizations that want to change this may face financial pressure to wait until existing investments have expired before purchasing new, more integrated solutions.

Inefficiencies With Email Encryption

Encryption introduces a further element of complexity to the mix. The major email encryption protocols—S/MIME, TLS, and OpenPGP—are incompatible with each other, complicating content communications with third parties that use another protocol internally. When encrypted email arrives that cannot be decrypted onsite, 60% of respondents admit to asking the sender to resend unencrypted files through an unpublished—but presumably unencrypted—shared drive link (Figure 12). The remaining 40% ask the sender to transfer a password-encrypted zip file.

How does your organization address encrypted email that you cannot decrypt?

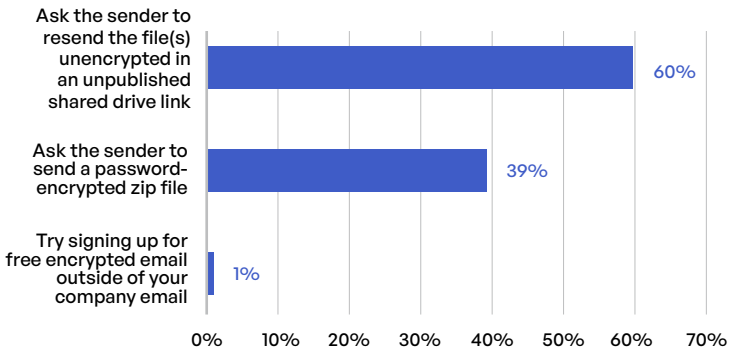

Figure 12

How much time is spent dealing with encrypted email and files from third parties that your employees and contractors cannot open each month?

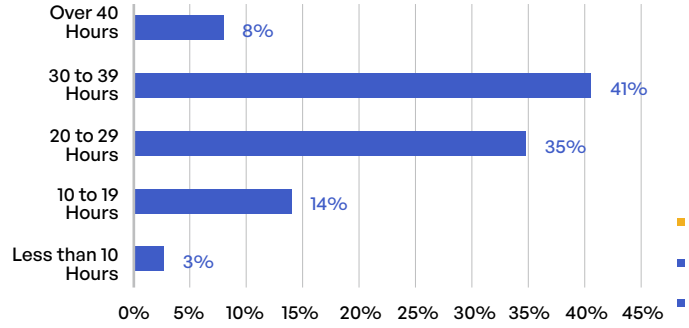

Figure 13

Regardless of the method used, one result of encryption incompatibility is a lot of wasted time. Nearly half (49%) of respondents spend 30 or more hours of staff time per month dealing with encrypted content that internal users cannot open (Figure 13). And for organizations whose email encryption requires public key infrastructure (PKI), more than half (51%) of organizations expend at least 20 hours per month supporting this element of the architecture (Figure 14).

Plugins are another source of inefficiency for email encryption systems, and most solutions require them. Nearly half (49%) of organizations report that managing plugins requires at least 30 hours per month of staff time (Figure 15). And with systems where users must manage their own encryption keys, more than two-thirds of respondents (68%) report that this task requires at least one hour per month for each user (Figure 16)—an inefficiency that can add up dramatically in a larger organization.

When encrypted email cannot be decrypted,

60%

of organizations ask the sender to send an unencrypted file to a shared drive link.

For email encryption that requires PKI, how much time is spent supporting encryption of third-party emails?

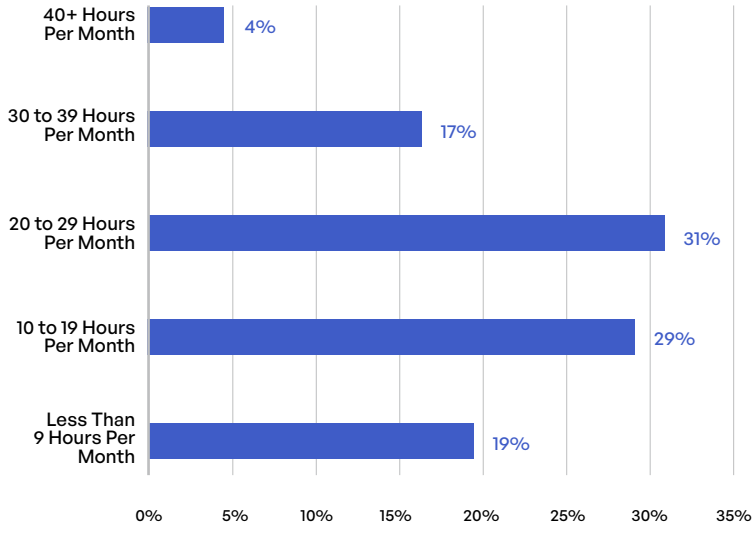

Figure 14

For email encryption that requires plugins, how much time is spent supporting encryption of emails (plugins, remediation, etc.)?

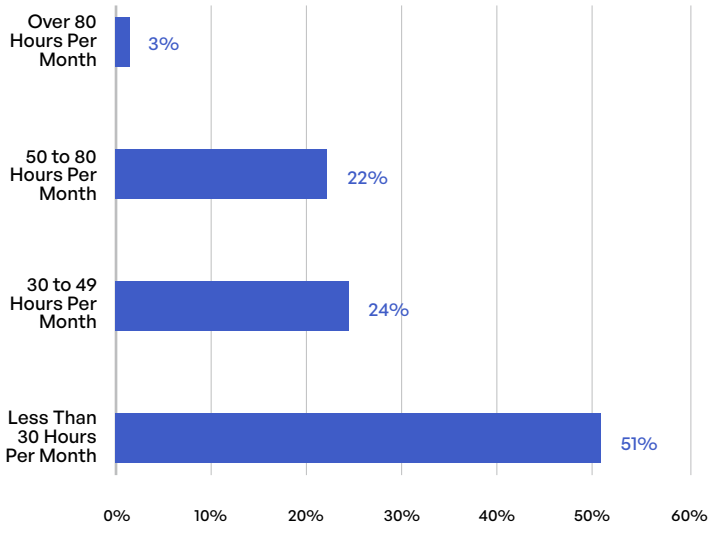

Figure 15

If your organization uses email encryption that requires users to manage encryption keys, how much time do those end users spend on encrypting and decrypting third-party emails, including managing keys and getting problems remediated?

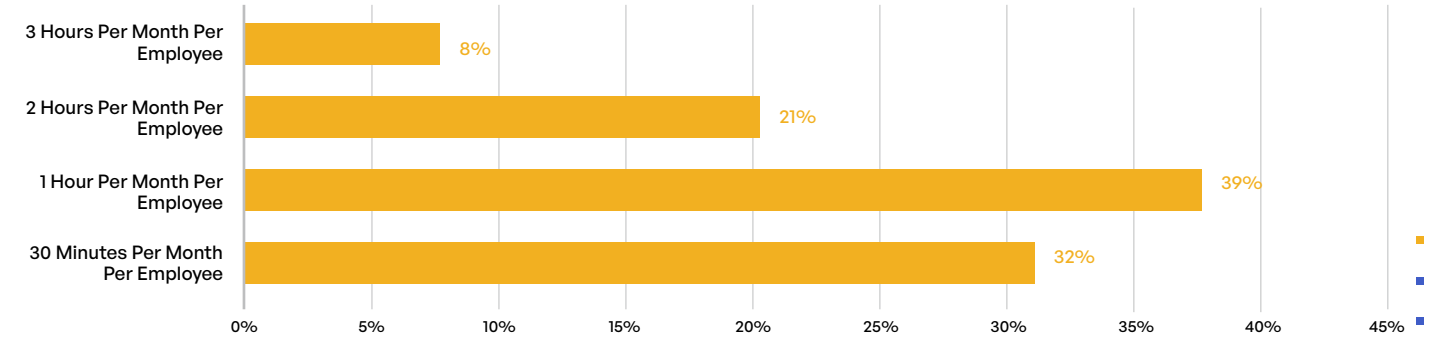

Figure 16

Insight #2: Security Gaps Increase Attacks and Hamper Incident Response

Another problem with complexity in content communications is the almost inevitable security gaps that such a setup can cause. When asked about their top concerns with having multiple content communications systems, security issues with external and insider threats were by far the most common answers (Figure 17). Insider threats, including well-intentioned employees who fall for a phishing attack or accidentally send sensitive content to the wrong person, ranked as the number one concern for more than one-quarter of respondents. And external threats, including malware, ransomware, and distributed denial-of-service (DDoS) attacks, were among the top two concerns for 59% of respondents. Two other common concerns relate to the governance of sensitive content and compiling compliance reports on content communications.

At 68%

of organizations, managing encryption keys consumes one or more hours per month per employee.

What are your top concerns in managing multiple content communications systems and how sensitive information is shared and stored internally and shared with external third parties?

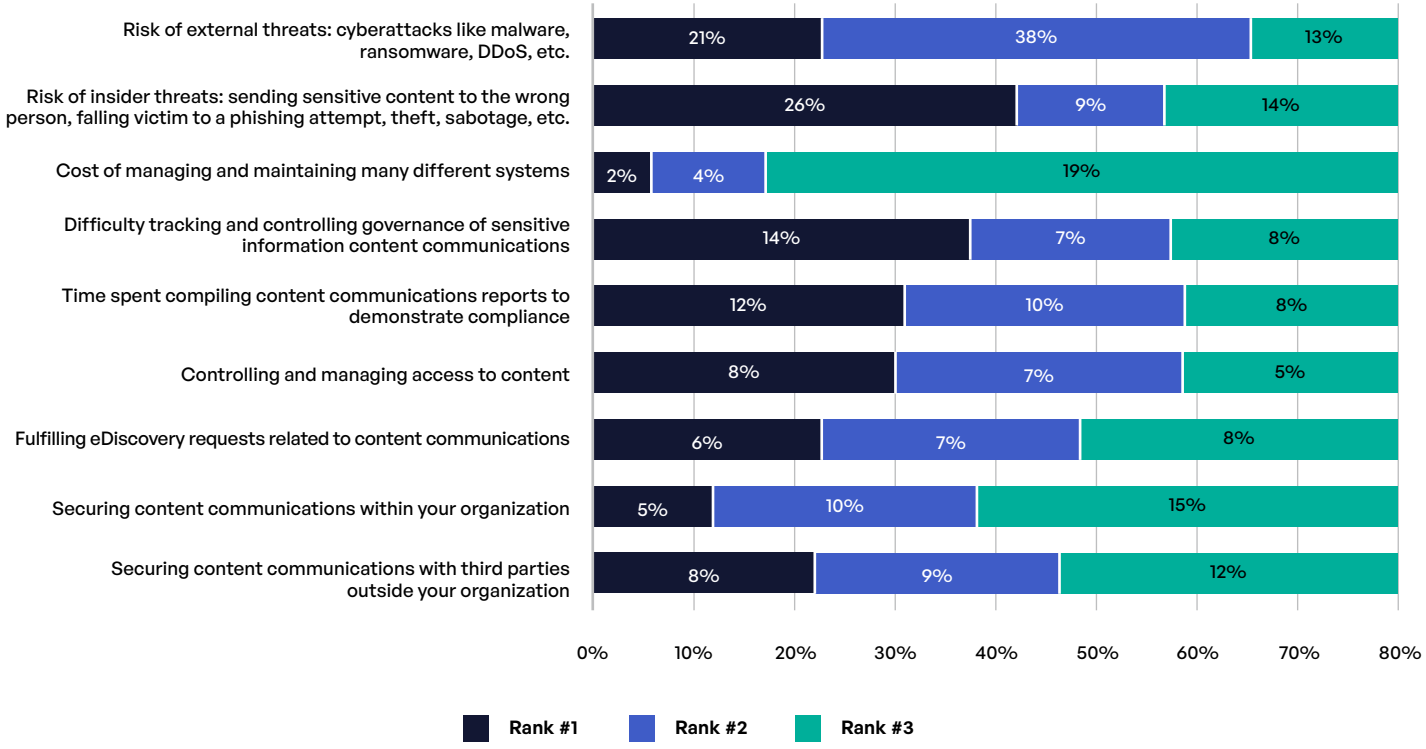

Figure 17

Inconsistent Security Protocols

These worries about internal and external cyber threats are not unfounded given the security gaps identified in the survey. For example, 56% of respondents admit that not all incoming communications are scanned for viruses and spam (Figure 18). This figure is especially high in the pharmaceuticals and manufacturing verticals, where 64% and 62%, respectively, do not scan everything.

Scanning of outbound content is also inconsistent. 54% of respondents—67% in the retail/hospitality industry—admit that they do not scan all outgoing email with a DLP tool (Figure 19). Moreover, 57% of organizations fail to perform DLP scans for all file sharing and MFT transfers with third parties (Figure 20). Professional services (69%) and travel/transportation (71%) are especially prone to this latter security gap. One of the reasons for these gaps relates to the complexity of the siloed approach to content communications, which brings a high likelihood of missing protections across the network.

Do you employ anti-virus/ anti-spam technologies for all incoming communications from external third parties?

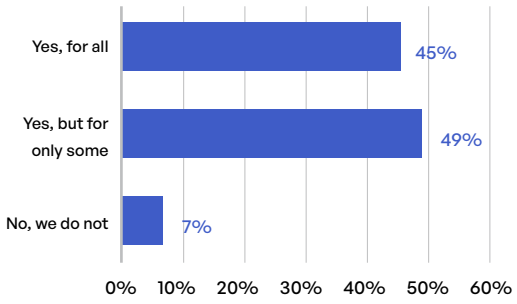

Figure 18

Do you employ data loss protection (DLP) for email sent to third parties outside of your organization?

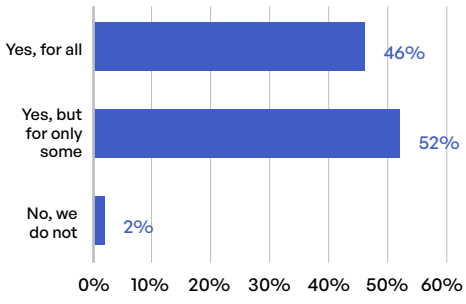

Figure 19

Do you employ DLP for file sharing and MFT with third parties outside of your organization?

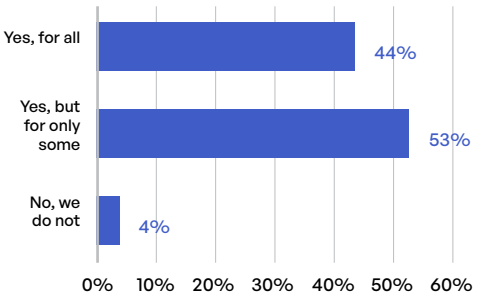

Figure 20

And while adhering to a zero-trust security model can help mitigate security gaps like the ones we have discussed, respondents also report an inconsistent application of this principle at their organizations (Figure 21). While everyone adheres to zero trust for email and a vast majority (83%) do so for file sharing services, fewer consider it a critical component in risk management for file transfer and automation solutions (46%), web forms (35%), or APIs (17%).

Does your organization consider zero trust as a critical component in managing third-party risk related to sharing and storing sensitive content?

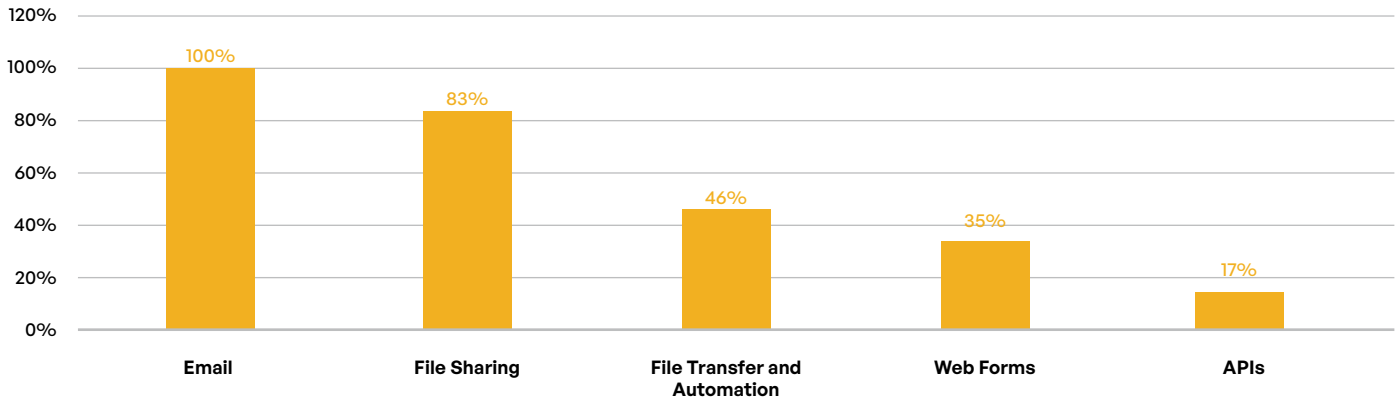

Figure 21

Gaps in Encryption and Access Control

Encryption of communications is another area where coverage is inconsistent. Only 12% of respondents claim that all communications with third parties are encrypted at their organizations, and half of them admit that less than three-quarters of such communications are encrypted (Figure 22). Encryption is especially uncommon in smaller organizations, with just 25% of organizations with between 1,000 and 4,999 employees encrypting most or all communications. Retail/hospitality and professional services fared the best with encryption, with 75% or more of both verticals encrypting most or all third-party communications.

Only 40%

do DLP scans on all emails sent outside the organization.

What percentage of your communications with third parties is encrypted?

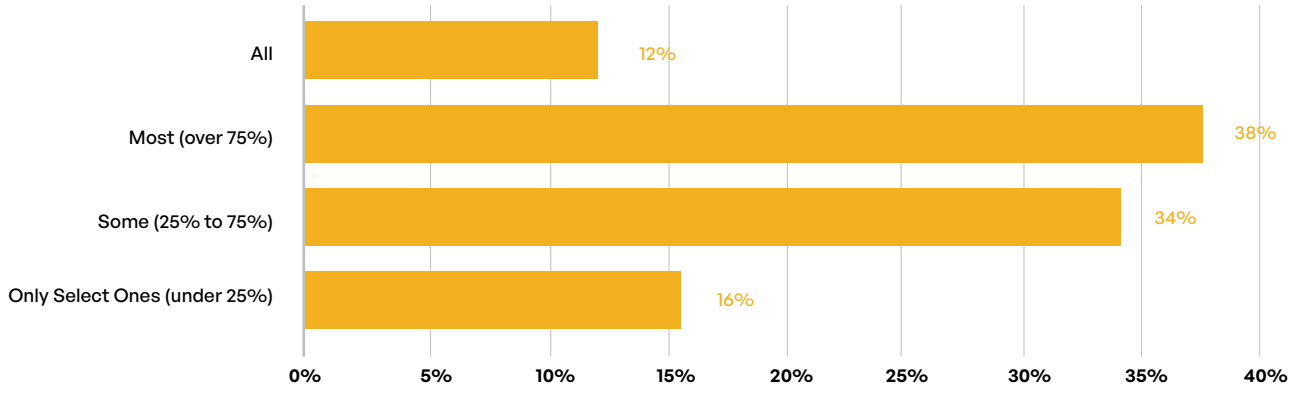

Figure 22

What percentage of your sensitive content email communications with third parties is encrypted?

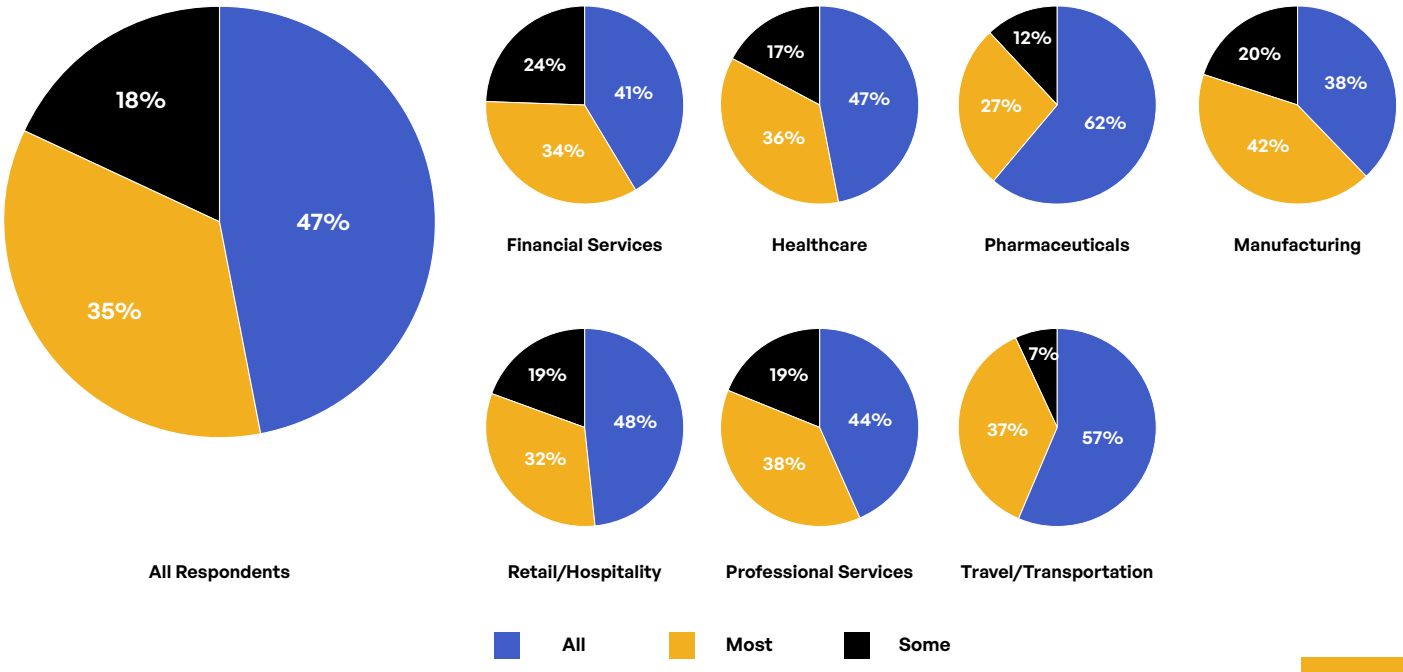

Figure 23

Some might counter that email without sensitive content does not need to be encrypted. But when specifically asked about sensitive content email communications, less than half (47%) of respondents encrypt everything (Figure 23). The situation is even worse with manufacturing (38%) and financial services (41%) firms, while pharmaceuticals (62%) and travel/transportation (57%) are doing better than average. The largest enterprises struggle with this element of security and compliance: Only 40% of companies with more than 30,000 employees encrypt all sensitive content communications.

Gaps in Third-party Content Access

Encryption does little good if unauthorized parties can access a piece of content on the corporate network, and third-party access is another area where significant gaps exist at the organizations represented in the survey. Only 43% restrict third-party access to folders using capabilities such as content permissions, expiration, locking, and versioning (Figure 24). Moreover, only 49% of respondents say they track and record which documents are viewed by specific third parties and when this occurs (Figure 25).

Do you manage or restrict third-party access to folders with capabilities such as content permissions, expiration, locking, and versioning?

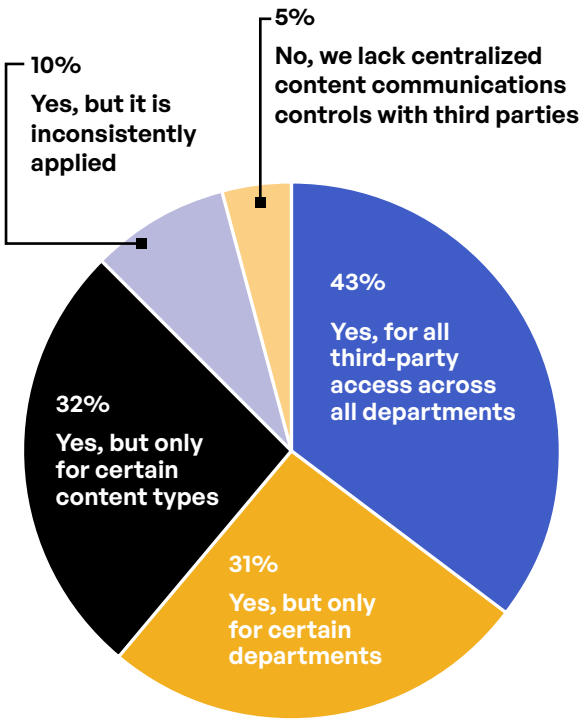

Figure 24

Do you track and record on third-party access to sensitive files and folders such as who viewed a document and when, who accessed the document and when, who downloaded a document and when, and who shared a document and when?

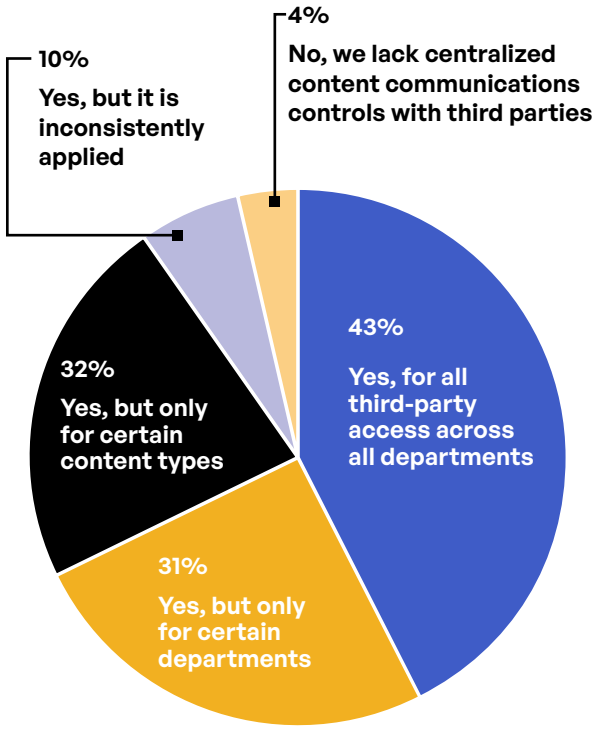

Figure 25

Insight #3: Inconsistent Policies Impede Proactive Risk Management

Another consequence of a disaggregated and siloed content communications infrastructure is that it complicates risk management. Most respondents (51%) say their organization is *not* well-protected against third-party risk. More than 70% of chief data privacy officers and risk and compliance managers answered in the same way. And professionals in the United Kingdom (63%) and Germany (65%) respond more negatively than the overall cohort.

51%

of respondents say their organizations are *not* adequately protected against third-party sensitive content communication risks.

Looking at what needs to be done to improve risk management, only 16% say no improvement is needed in their organizations' risk management strategy when it comes to content communications (Figure 26), whereas 41% want to see significant improvement or even a whole new approach. Respondents in healthcare and retail/hospitality—two industries that bore the brunt of the turmoil of the past two years—were especially adamant, with 60% saying that at least some improvement is needed. And more than 80% of executives and managers in the data privacy space across all industries say such improvement is needed.

When asked what would give them more confidence in their risk management efforts, two answers stand out: more systems and more training (Figure 27)—one of which is the first choice of 86% of respondents. More than 6 in 10 (62%) retail/hospitality respondents want more systems, while 56% in professional services favor more training.

What is your level of satisfaction with your organization's risk management and protection of third-party communications?

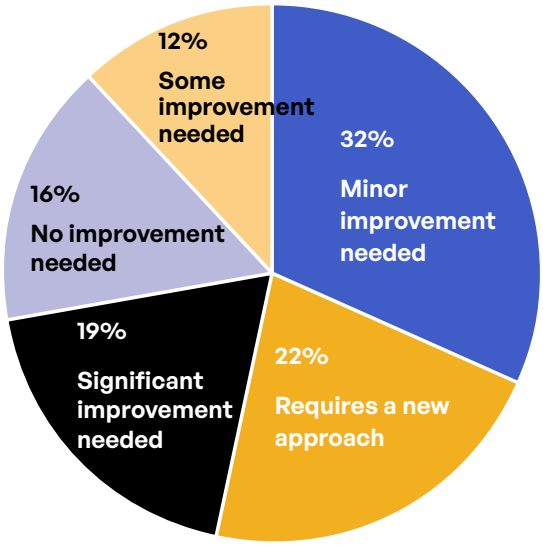

Figure 26

What would give you more confidence?

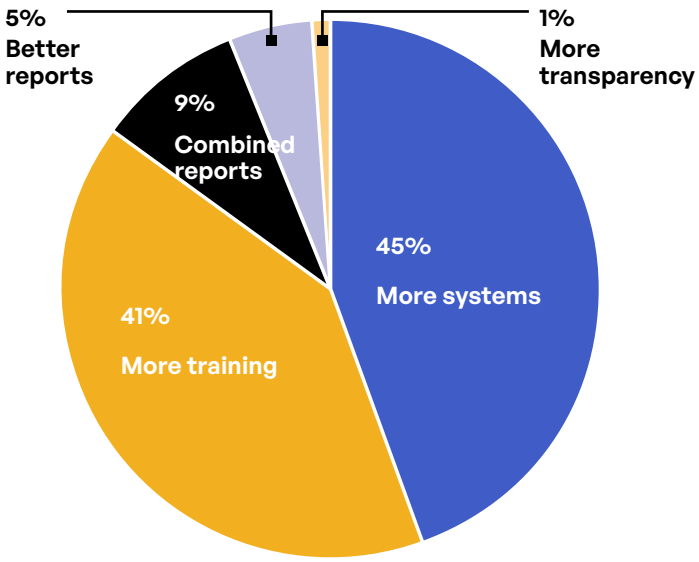

Figure 27

Priorities of Top Leadership Versus the Rest of the Organization

As organizations look at ways to improve their risk management when it comes to content communications, different groups do not always have the same priorities (Figure 28). Respondents reported that their executive management and board of directors most cited tracking content permissions (42%), unifying management (49%), and providing easy access to all content repositories (43%) in their top two priorities. Tracking content permissions is a top-two priority among an even higher percentage of leaders in the professional services (57%) and retail/hospitality (51%) verticals.

Respondents themselves had slightly different priorities (Figure 29). They agree with their executives on the need to unify management, tracking, policies, and reporting for content communications (49% cite this among their top two priorities). But beyond that, their priorities are more diverse, with interest in protecting content in transit (41%), tracking content permissions (29%), and automating processes (21%).

What does your company's leadership and board list as top priorities around third-party content communications?

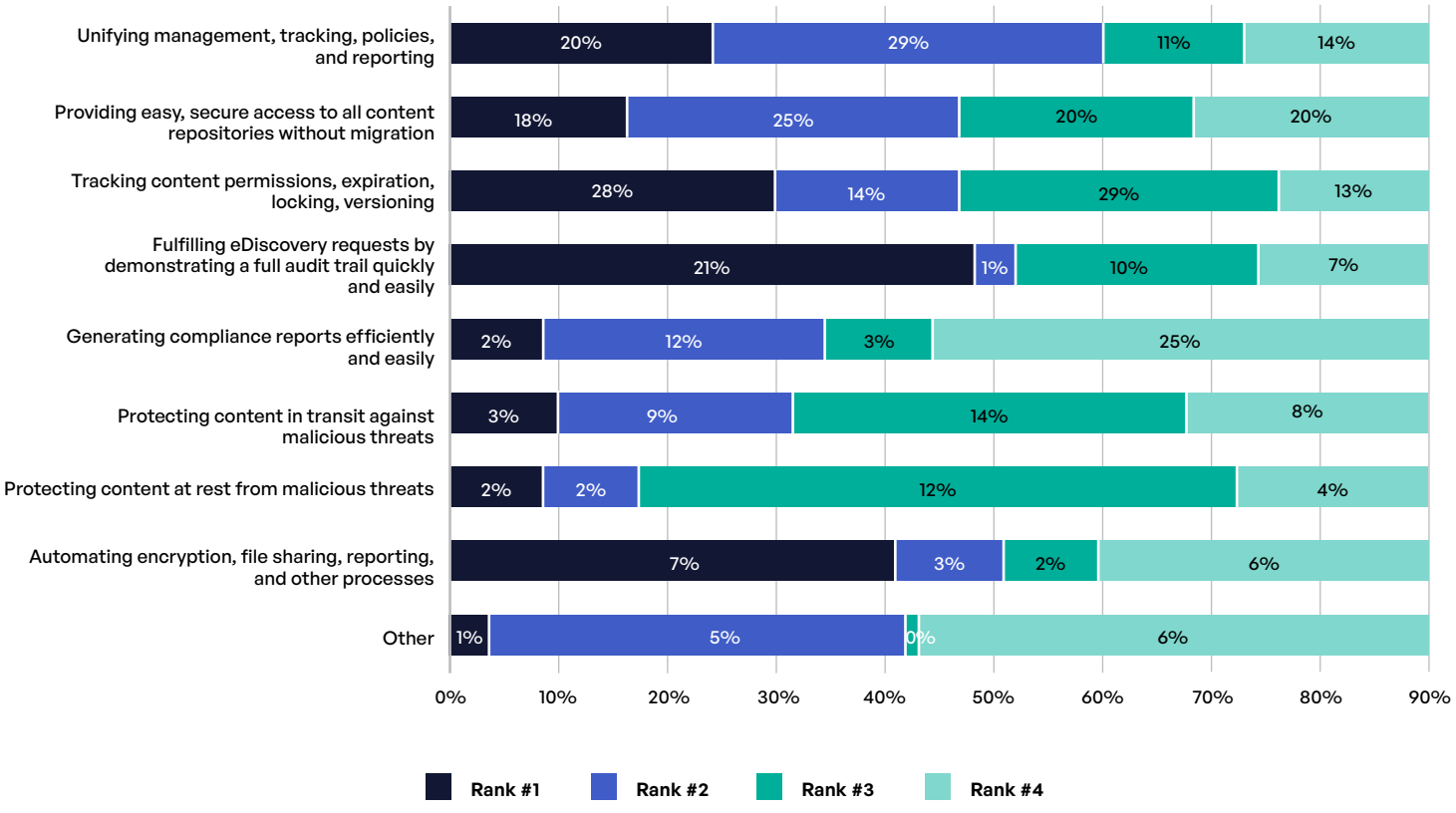

Figure 28

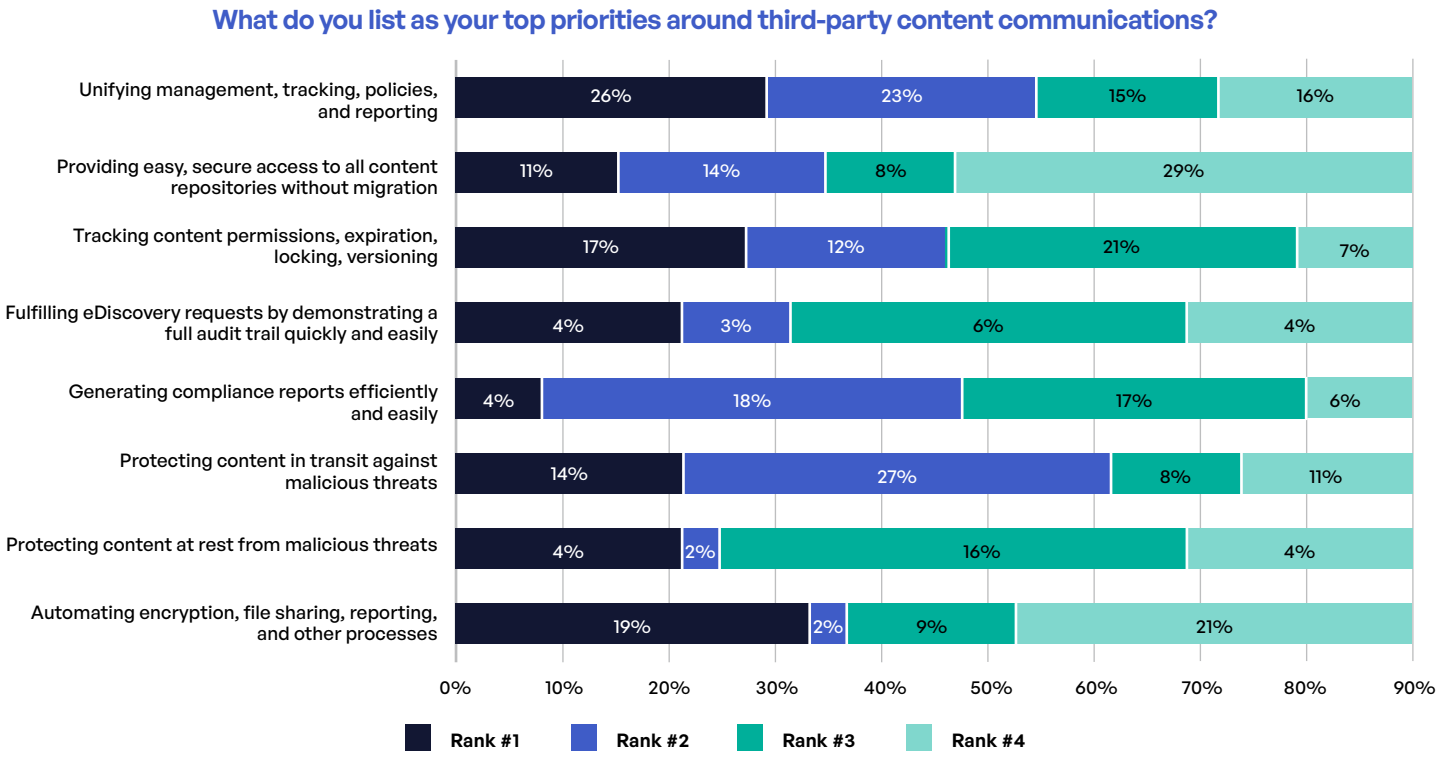

Figure 29

Risk Management Strategies

When asked about specific strategies that might result in more effective risk management around third-party content communications, survey responses were equally spotty. Significant majorities of respondents reported having a formal risk management program to vet vendors and suppliers for email (68%), file sharing (65%), and web forms (63%) (Figure 30).

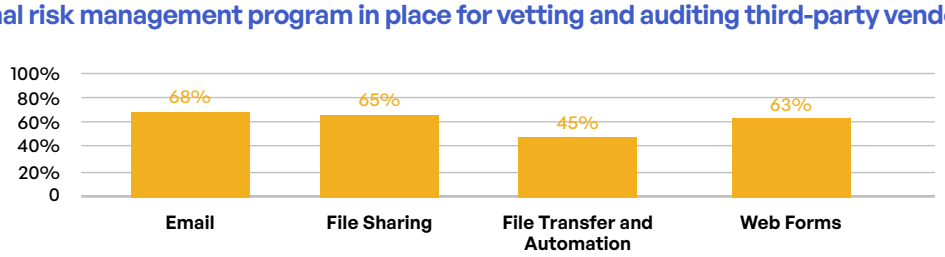

Figure 30

Despite this, only 42% of all organizations report having implemented controls to measure third-party risk (Figure 31)—and it is difficult to imagine a formal risk management program being successful without the ability to measure risk. Even fewer organizations in the United States (38%), the United Kingdom (37%), and Germany (27%) can do such measurement. Unfortunately, critical industries like financial services (35%), retail/hospitality (36%), and healthcare (37%) are also deficient in this regard compared with the overall cohort.

Has your organization implemented controls for measuring risk associated with third-party content communications?

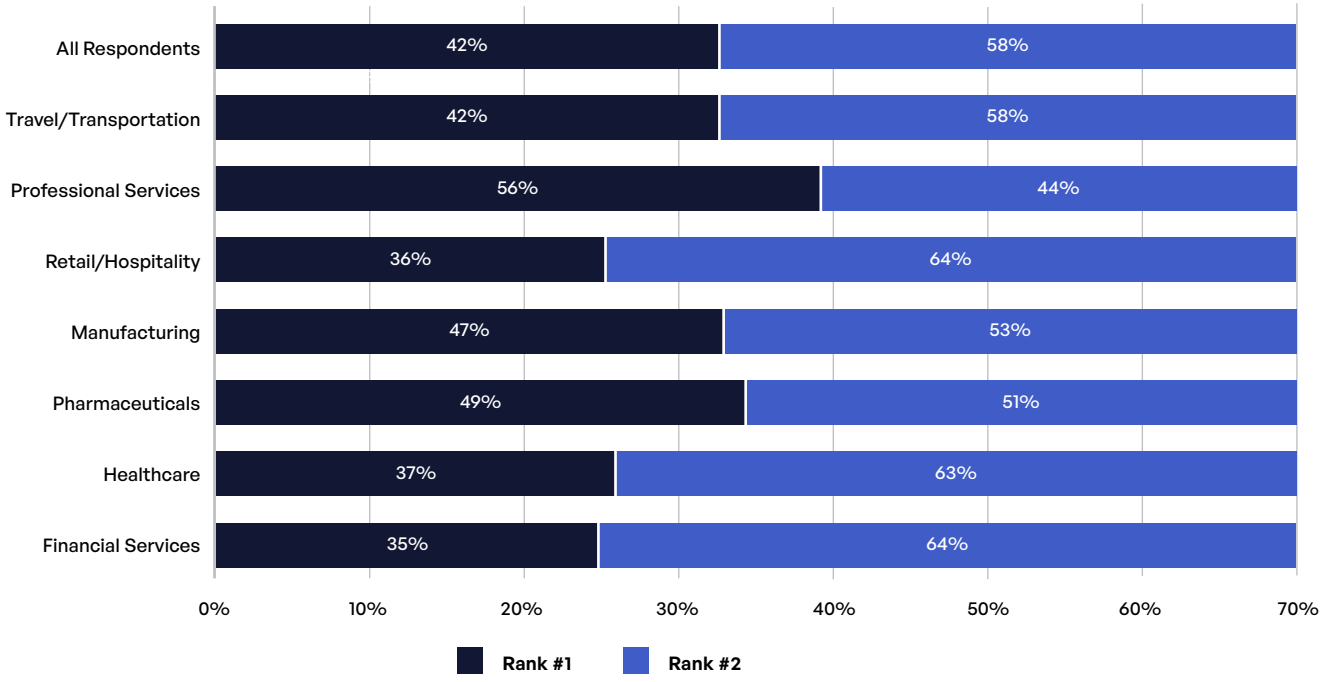

Figure 31

When asked about the barriers they experience to investing in risk management, the complexity of implementing and managing such a system was the number one factor for 45% of respondents, while the high cost of such a solution was among the top two factors for 81% of them (Figure 32).

What are the biggest barriers for your organization when it comes to investing in systems for managing compliance, governance, and protection of third-party content communications?

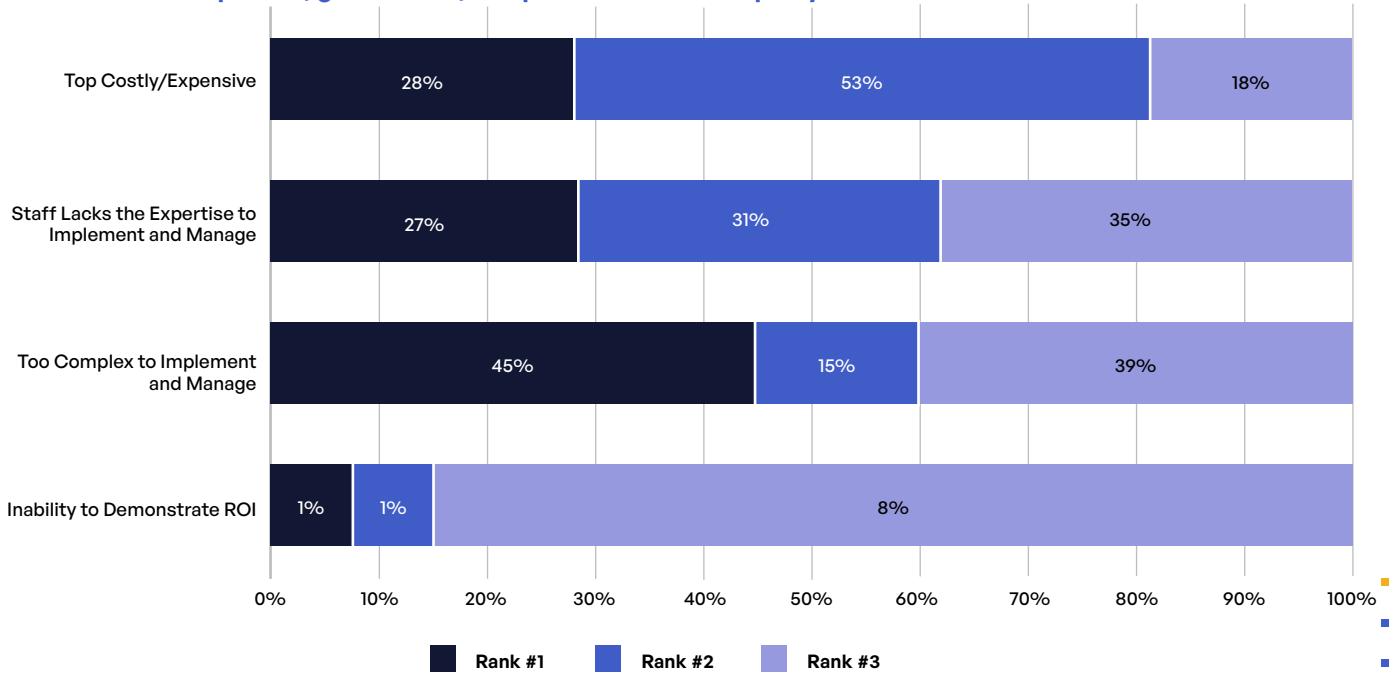

Figure 32

Cyber Insurance

Cyber insurance is an increasingly common way for organizations to mitigate the risks brought about by an increasingly complex threat landscape. An overwhelming majority of respondents (84%) say their organizations carry cyber insurance that covers third-party content communication breaches (Figure 33). For 59% of respondents, this policy covers at least $1 million in losses (Figure 35). And 86% of organizations require the third parties with which they exchange content to carry cyber insurance of their own (Figure 34).

However, with the average cost of a data breach reaching $4.24 million last year, up from $3.86 million the year before (a 10% jump), the average cyber insurance policy covers only a portion of the overall cost of a data breach.[6] Thus, even though most organizations have some form of cyber insurance in place, the final cost of a data breach to their organizations is still significant.

Do you have cyber insurance and does the policy cover content communications (sent, receipt, storage) with third parties?

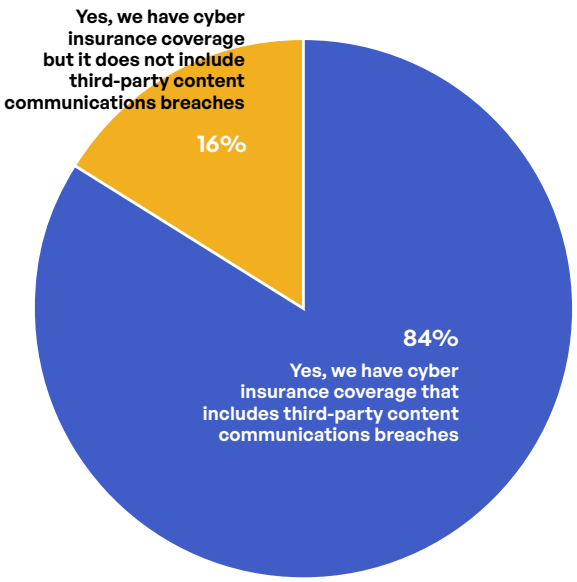

Figure 33

Do you require your third parties to have cyber insurance coverage that includes communications content breaches?

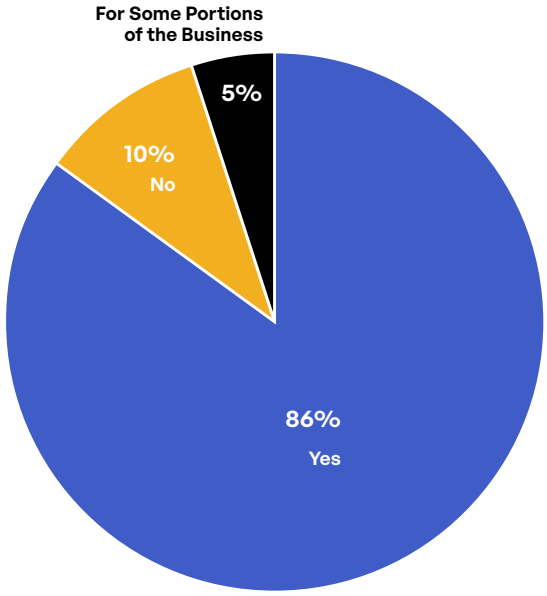

Figure 34

About how much does your cyber insurance cover in the event of a third-party content communications breach?

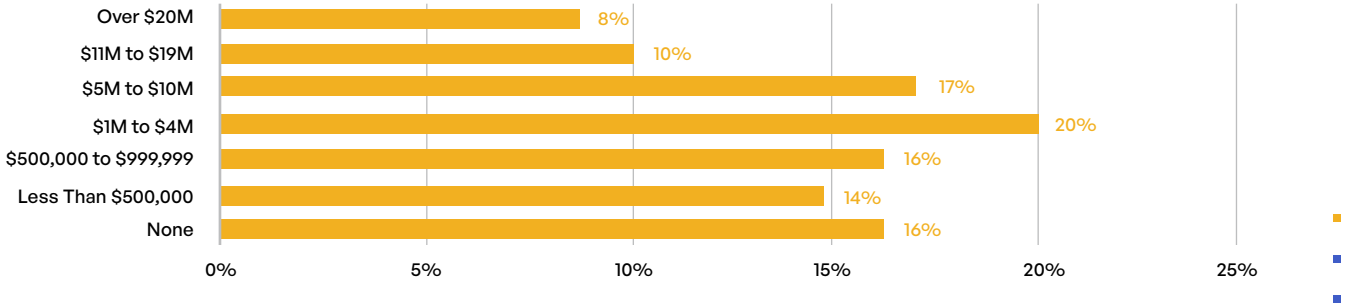

Figure 35

Insight #4: Inconsistent Governance Negatively Impacts Compliance

Compliance with regulations and other standards is a requirement for all organizations. It is closely related to risk management, as the intent of most regulations is the reduction of risk. However, the need to demonstrate compliance to regulators and auditors requires organizations to move beyond reducing risk to *proving* that risk reduction.

The mix of regulations that govern organizations' content communications for this global cohort is not surprising (Figure 36). Nearly three-quarters (74%) of respondents must comply with GDPR—more than any other. More than half of respondents must comply with the Payment Card Industry Data Security Standard (PCI DSS; 54%), the United States' Health Insurance Portability and Accountability Act (HIPAA; 56%), the Data Protection Act (DPA) in France and the United Kingdom (58%), and the California Consumer Privacy Act (CCPA; 52%).

The most common frequency of required reports is biannual, although a plurality of those who must comply with GDPR must file quarterly reports. Overall, 90% of organizations must prepare between four and nine compliance reports every year (Figure 37).

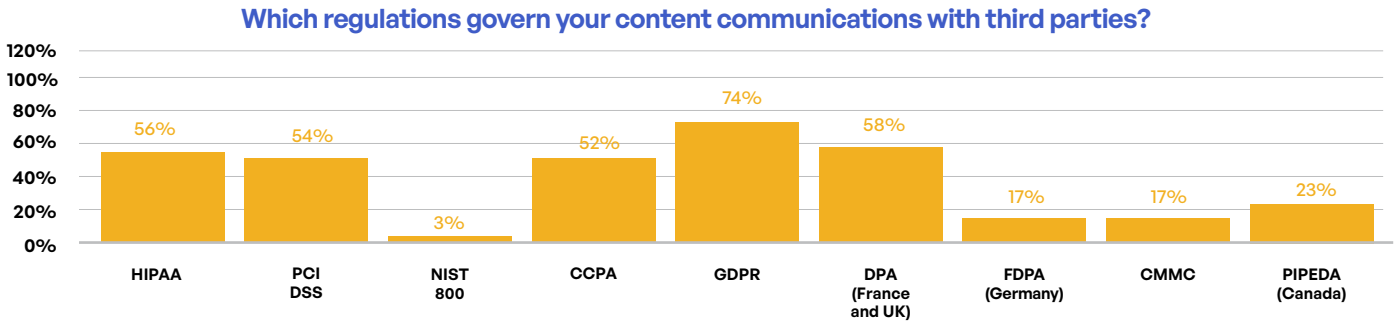

Figure 36

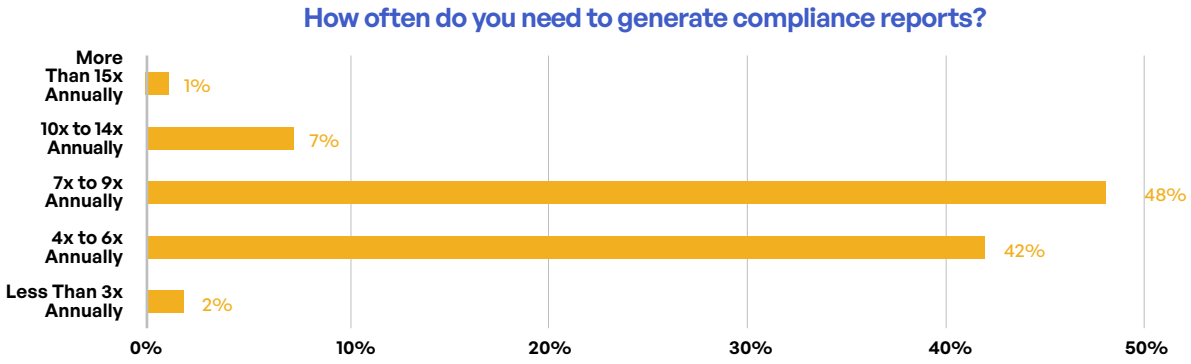

Figure 37

Hours of Time Consumed, Limited Accuracy

When asked about the amount of staff time required to compile information for each compliance report, 77% of respondents report more than 20 hours, and 45% say more than 40 hours (Figure 38). Yet despite the many hours spent on these reports, their accuracy leaves much to be desired. Only 21% claim their compliance reports are fully accurate (Figure 39). This figure is even lower in the United States (19%) and Germany (12%), while the United Kingdom (32%), Switzerland (50%), and Spain (67%) do better—but even those countries have room for improvement.

This lack of full accuracy is concerning not only because incorrect information may be submitted to auditors and government regulators, but also because it suggests that many organizations' risk management efforts may be based partly on incorrect information.

How much staff time is spent compiling information for each compliance report?

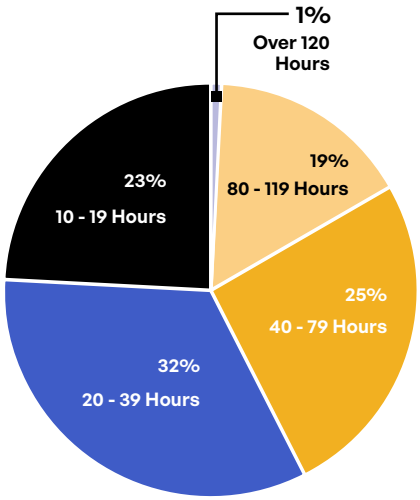

Figure 38

What is the level of accuracy of your compliance reports?

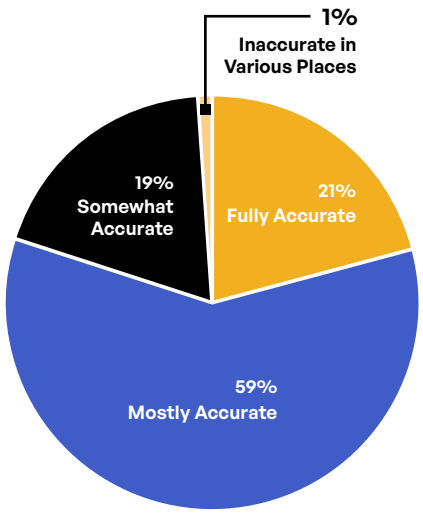

Figure 39

Do you have governance, compliance, and protections in place for sensitive content communications (e.g., PII, PHI, IP, etc.) in the cloud?

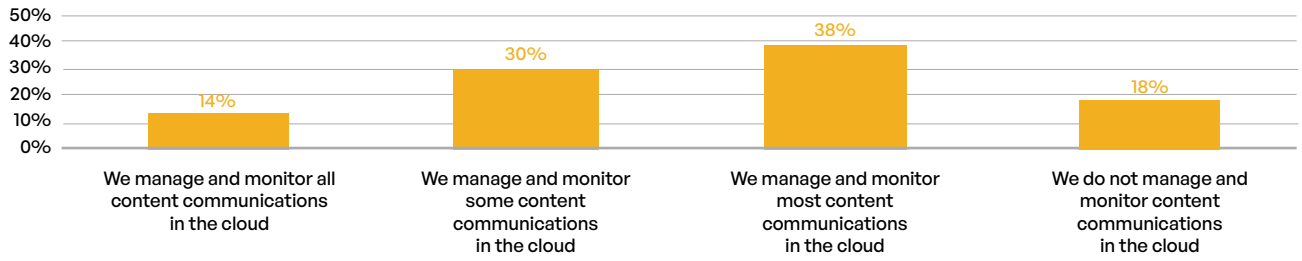

Figure 40

One reason for this startling level of inaccuracy may be a dearth of governance protections in place at many of the organizations represented in the survey. For example, only 14% claim that they manage and monitor all sensitive content communications that take place in the cloud (Figure 40). Cloud computing has expanded virtually every organization's attack surface in recent years, and many organizations clearly have not gotten on top of their cloud infrastructure when it comes to secure content communications. Another factor behind the inaccuracy of compliance reporting is that many of these standards and regulations consist of hundreds of compliance areas.

Governance That Leaves Much To Be Desired

Given the struggles with compliance reporting experienced by survey respondents, it is no wonder that they express dissatisfaction with the current state of governance at their organization, specifically around third-party content communications. Well over two-thirds (69%) say that at least some improvement is needed, and 35% say that significant improvement or a whole new approach to governance is required (Figure 41).

79%

of respondents say their compliance reports are not fully accurate.

What is your level of satisfaction with your organization's governance and protection of third-party content communications?

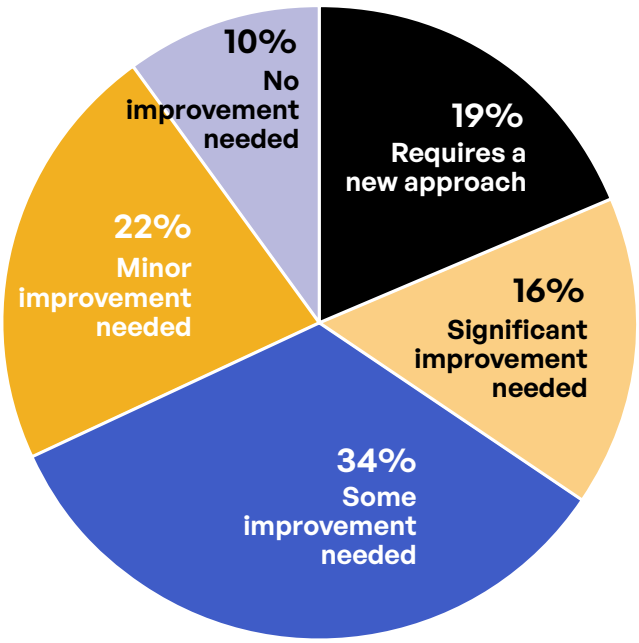

Figure 41

Conclusion

In many ways, the 2022 Sensitive Content Communications Privacy and Compliance Report paints a worrisome picture about the state of content communications. Organizations share content with hundreds or thousands of third parties using multiple transmission methods. Security checks are inconsistent for both inbound and outbound content, and encryption is inconsistently applied.

Too often, the communication of content is siloed according to the method of sharing, the type of content, or the department that sends or receives the content. Security and compliance solutions are frequently siloed in similar ways. And monitoring of when and by whom sensitive content is accessed is spotty or nonexistent at most organizations—again, partly due to the silos that exist.

But as the threat landscape becomes more complex, compliance requirements are tightening. Jurisdictions around the world have enacted tougher controls in recent years over how protected content can be used and transmitted—and how quickly the public must be notified when there is a data breach. Organizations now have no choice but to bring content communications under control. In a nutshell, they must:

- *Unify* the content communications infrastructure under a centralized system. This enables organizations to standardize the way that content is shared and simplify the audit trails by which content communications is monitored.
- *Track* content, user, and system activity across all content communications channels. This enables organizations to have an enterprise view of all third-party access and easily meet regulatory compliance reporting requirements.
- *Control* content access according to functional roles, inside the organization and with third parties. Having these controls in place enables organizations to change policies in response to changes in the threat landscape.
- *Secure* content through encryption at rest and in motion. This protects against accidental and deliberate exposure of sensitive information to malicious bad actors.

As content becomes increasingly important to businesses and other organizations, it is imperative that they think in terms of a private content network that manages and monitors the movement of all content that is shared internally and externally. Protecting this content must become a priority on par with securing networks, endpoints, and databases. At many organizations, content communications may be the biggest security and compliance gap that needs to be addressed.

References

[1] "Cost of a Data Breach Report 2021," IBM and Ponemon Institute, July 2021.

[2] Michael Novinson, "SolarWinds Hack 'One Of The Worst In The Last Decade': Analyst," CRN, December 17, 2020.

[3] Michael Riley, et al., "Russia-Linked SolarWinds Hack Snags Widening List of Victims," Bloomberg, December 18, 2020.

[4] Jaycee Roth, "Data Exfiltration in Ransomware Attacks: Digital Forensics Primer for Lawyers," Kroll, September 16, 2021.

[5] "Executive Order on Improving the Nation's Cybersecurity," The White House, May 12, 2021.

[6] "Cost of a Data Breach Report 2021," IBM and Ponemon Institute, July 2021.

Kiteworks