Kiteworks

2023

Kiteworks Sensitive Content Communications Privacy and Compliance Report

Growing Tool Soup, Malicious Cyberattacks, and Lack of Governance Tracking and Controls Demand DRM

Table of Contents

Foreword

We thank you for downloading the 2023 Kiteworks Sensitive Content Communications Privacy and Compliance Report. We welcome those who walked through our inaugural report in 2022, as well as new readers who found us this year. We are glad you have joined us for this examination of oft-neglected aspects of cybersecurity and compliance—protecting content as it is not only sent and shared internally but also with myriad third parties that an organization does not control.

Protecting content is important because it contains so much of the data that we must safeguard to maintain brand identity, keep customers buying from us, satisfy auditors, and protect our position in the marketplace. Disclosure of personally identifiable information (PII), protected health information (PHI), payment card transaction data, company financials, intellectual property (IP), or non-public information about mergers and acquisitions (M&A) and other legal matters is disastrous for any organization for a variety of reasons.

But for the business to operate, beyond first parties, this same data often must be shared with specific third parties that need the information. And as it turns out, those entities number in the thousands for most organizations. This act of communicating content between stakeholders presents tremendous security and compliance risk for organizations, and the survey on which this year's report is based makes it clear that these risks have not yet been mitigated at most.

The timing of these security gaps is really bad, as risks are growing. More attacks now include data theft than in recent years, with the exfiltration of data now a standard part of ransomware attacks that previously simply locked up systems. At the same time, regulators around the world are tightening their requirements and increasing penalties for noncompliance. And for different reasons, organizations must comply with—and are audited against—frameworks like the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), which seeks to eliminate such protection gaps. For all these reasons, we believe the coming year will be critical for organizations when it comes to the protection of sensitive content communications.

The biggest takeaway from the data insights in the study is the importance digital rights management (DRM) plays in unifying, tracking, controlling, and securing sensitive content communications. And while the report identifies the aforementioned gaps, it also finds that organizations recognize the need for DRM capabilities and have their implementation on the roadmap. When we produce our 2024 report, it will be interesting to discover whether they have progressed in their journey or our findings were merely a mirage.

Sincerely,

Patrick Spencer

Patrick Spencer, Ph.D.
VP of Corp. Marketing & Research, Kiteworks

Executive Summary

If you have ever sent a piece of sensitive content to a third party as a part of your job, this report is for you. When you pressed Send or Share, you likely didn't think at all about the security and compliance implications of what you were doing. But such an action presents increasing risk to organizations every year. The 2023 Kiteworks Sensitive Content Communications Privacy and Compliance Report checks in to see how companies are doing as they share such content with thousands of other entities.

This report is based on a comprehensive global survey of IT, cybersecurity, and compliance professionals at enterprise-level organizations. Respondents represent a wide range of industries, geographies, and job grades. The answers they gave yielded a number of insights about security and compliance of sensitive content communications.

A Complex Web of Recipients, Channels, and Tools

The first insight is that sensitive content communications are complex. The number of third parties with which organizations must share their sensitive content is nothing short of stunning. 9 in 10 organizations exchange such content with *more than 1,000 outside organizations*, and 44% say that number exceeds 2,500.

Equally astounding is the number of tools or systems used to communicate sensitive content: Half of respondents admit they share content using *six or more* channels. Both of these numbers increased significantly compared with an identical question in the survey we conducted for our 2022 report.

Another sign of unacceptable complexity: 85% of respondents use *four or more* tools to track, control, and secure the sharing of such content, and 46% say that number is six or more.

90%

of organizations share sensitive content with 1,000+ third parties

100%

of organizations use 4+ channels to share sensitive content

50%

use 6+ communication tools to send and share sensitive content

85%

of organizations use 4+ systems to track, control, and secure sensitive content communications

A Ways to Go in Terms of Security Maturity

Another insight is the distance many organizations have left to travel for their security efforts around sensitive content communications to be truly effective. Barely one-quarter of respondents say their security measurement and management practices are where they need to be, and a similar percentage reports they have completed a strategic alignment between sensitive content security measurement and management and their corporate risk management strategy. Clearly, a big majority of organizations have a lot left to do.

The result of this incomplete strategic work is that our respondents have a lot of worries. Email, file sharing, and file transfer and automation systems continue to pose huge risks to organizations when used to share sensitive content. But they also recognize the risks posed by emerging channels like mobile apps, texting, and application programming interfaces (APIs). The professionals we surveyed also worry about a wide range of attack methods against every kind of sensitive data—from personally identifiable information (PII) to intellectual property (IP).

Only 27%

say their security *measurement* for sensitive content communications does *not* need improvement

Only 26%

say their security *management* for sensitive content communications does *not* need improvement

Only 28%

say their sensitive content communications security efforts are already aligned with the corporate risk management strategy

More Compliance Requirements With No Additional Resources

Another insight is that compliance remains difficult for the organizations represented in our survey. Europeans are especially under pressure to comply with the EU's General Data Protection Regulation (GDPR), which carries big fines for noncompliance. But most respondents are subject to data privacy regulations for at least one jurisdiction, and most are also audited against at least one industry standard. On top of that, 99% of respondents do business with government entities and must comply with special requirements for those activities.

Unfortunately, this plethora of compliance requirements takes a toll on IT, security, and compliance teams. More than two-thirds of organizations say that compliance efforts for sensitive content communications alone take at least 300 staff hours per year, and more than one-third put that number above 500 hours. And nearly everyone has at least one headcount devoted to this task.

69%

of organizations spend 300+ staff hours annually tracking and reporting sensitive content communications compliance

91%

of organizations dedicate at least 1 FTE for sensitive content communications compliance

Only 27%

say their sensitive content communications compliance efforts are already aligned with the corporate risk management strategy

A Mixed Bag When It Comes to Best Practices

Another insight is that while our respondents tend to have a good understanding of best practices when it comes to sensitive content communications, significant gaps still exist in practice. Important controls like least-privilege access, multi-factor authentication, and data encryption are in place for at least some sensitive content sharing. But protection is not complete at a big majority of organizations.

For three-quarters or more of organizations, tracking, recording, and access control for sensitive content communications have not yet been extended to all departments, all content types, and all parts of the infrastructure—on-premises and in the cloud.

Only **22%** of organizations **track and record** third-party access across all departments and content types

Only **25%** **restrict access** to sensitive content folders across all departments and content types

Only **22%** **track and control** access to sensitive content at the admin level, on-premises and in the cloud

Way Too Many Exploits

Another somewhat alarming insight: Organizations are experiencing a large volume of exploits, specifically around their sensitive content communications. More than 8 in 10 organizations had four or more such incidents over the past year, and more than one-third had more than seven. More than 6 in 10 organizations suffered financial implications from an attack, and brand impacts and compliance fines were a consequence for more than 4 in 10.

84% of organizations had **4+** sensitive content communication exploits

62% had **financial damage** as a result of such an attack

A Slow Road to Digital Rights Management

The best solution to these problems is a methodology called digital rights management (DRM), in which organizations classify their content, segment it according to risk, and control access according to role—with specific actions on specific types of sensitive content available only to those who need it to do their job—and geography (such as geofencing). While our findings show organizations have a significant distance to go when it comes to DRM, there is good news. Most indicate they aspire to many of the best practices of digital rights management.

More than 9 in 10 organizations already classify sensitive content—something that is motivated by security and compliance concerns around PII and other kinds of sensitive data. Most have users who need offline access to sensitive content—corporate executives, technical field workers, or sales people. And many have put significant thought into their DRM requirements. But barriers like the need for agents to open unencrypted files with external third parties are slowing the process down. Another stumbling block is the need for controls to be customizable for different users, roles, and content types.

93%

of organizations classify sensitive content

However,

55%

say that the need to control according to user, role, and content class is a stumbling block to deploying DRM

Cautious Optimism for the Coming Year

While our survey results reveal that organizations have many gaps in their protection of sensitive content communications, this means they have many opportunities to make improvements in the coming year. Action could not be more urgent, as sensitive content is more vulnerable than ever. Our hope is that organizations will take a holistic approach, using the principles of DRM to improve compliance, protect against insider threats, and protect sensitive content no matter where it comes from or how it is shared.

Introduction: Sensitive Content Communications Is No Longer Just a Lofty Goal

Welcome to the second edition of Kiteworks' Sensitive Content Communications Privacy and Compliance Report! For the second consecutive year, we surveyed almost 800 IT, security, risk, and management professionals to gauge how they are managing privacy and compliance risk as related to sensitive content communications. Not surprisingly, their responses got our attention. Sensitive content is at the core of business and operations at every organization—and a vital lifeblood for many. Unfortunately, whether the content is inadvertently sent or shared with individuals or organizations who should not have access to it, or it is intentionally hacked by malicious cyber actors, the financial, brand, and regulatory implications can be dire.

For individuals who interact with an organization, personally identifiable information (PII), protected health information (PHI), and payment card industry (PCI) data are at risk. For businesses, intellectual property (IP), corporate financial and legal details, and information about mergers and acquisitions (M&A) are vulnerable nuggets for bad actors looking to profit or wreak havoc. And for government entities and related enterprises, exposure of data about national security, critical infrastructure, and criminal investigations could potentially change the course of world history for the worse.

We warn you that some of the contents of this report may induce stress—especially if you're a security, compliance, or risk management professional. But we strive to tell it like it is, and ultimately to inspire organizations to take effective steps to better protect their content in the coming 12 months. Our hope is that next year's report will show improvement in how organizations manage their security and compliance risk when it comes to sensitive content communications. With awareness of the problems and strategic action to address them, such an outcome is fully within the realm of possibility.

Relentless Attacks, Human Foibles, Increasing Costs

It is no secret that cybersecurity accounts for a growing share of any organization's overall risk portfolio. It wasn't so long ago that a firewall, VPN, and antivirus were all that organizations needed for protection. Today, sophisticated attackers, aided by large teams of state-sponsored hackers or black-market managed services providers, make it inevitable that an organization will experience attacks using ransomware, stolen credentials, URL manipulation, or denial of service—among other tactics.

Add to that the increasing theft of content that is a part of these attacks. Research by Mandiant finds that data theft as a percentage of incidents rose from 29% to 40%—a 37% increase over 12 months.[1] File decoding and file deletion are a part of more than one-quarter of attacks, which are carried out by more than 3,500 threat groups—including 900 that were new in 2022.

The 2023 Verizon Data Breach Investigations Report[2] finds that personal data (PII and PHI) played a role in more than 50% of breaches—more than any other confidential data variety. In terms of attack vectors, email continues to be a major security problem for organizations. It ranks closely behind web applications and desktop sharing solutions as a system target. In addition, nearly 60% of social engineering attacks are pretexting and related to business email compromise (BEC).

Beyond the actions of bad actors, human error is also a big factor in the exposure of sensitive content. Verizon finds that 43% of data breach incidents involve misdelivery of data, when it is accidentally shared with the wrong party. On top of that, 23% of incidents are publishing errors, where data is broadcast to the wrong audience.[3]

A Dizzying Array of Data Privacy Regulations

These costs to organizations, individuals, and society are front of mind for regulators in jurisdictions around the world. To build standards to which businesses must adhere, regulators have passed a rapidly growing list of regulations addressing everything from data privacy to cybersecurity standards. And in many places, they have added teeth to those requirements. Organizations that do business across any significant geographical footprint face two challenges: implementing the processes and controls that protect sensitive data in the first place, and doing so in a way that can be easily verified for regulators from a patchwork of jurisdictions.

The European Union's General Data Protection Regulation (GDPR), implemented in 2018, is arguably the world's most stringent regulation of personal data. It applies to individuals in 27 EU member states and levies significant fines for noncompliance. But GDPR is by no means the only significant national data protection regulation. The latest count pegs the number at 157 countries—up from 145 countries just 15 months prior.[4] This includes major economies like Australia, Brazil, Canada, China, India, and Japan, among many others.

While the United States has not passed a national regulation like the GDPR, the Health Insurance Portability and Accountability Act (HIPAA) has strict requirements for the protection of PHI specifically. And starting with the passage of the California Consumer Privacy Act (CCPA) in 2018, individual U.S. states are introducing their own regulations, creating an even more frustrating patchwork for businesses operating in North America. At this writing, a total of nine states have passed consumer privacy legislation.[5] Laws in Virginia, Colorado, Utah, and Connecticut will take effect in the last half of 2023, while Indiana, Iowa, Montana, and Tennessee will implement theirs between 2024 and 2026. Further, 10 additional states currently have active bills that are somewhere in the legislative process.

Doing business with the federal government is another trigger for additional regulation for companies operating in the U.S. Over the past decade, the Federal Risk and Authorization Management Program (FedRAMP) standardized cybersecurity practices for cloud services for all U.S. government agencies and their contractors, subjecting numerous private businesses to its requirements. And after launching with fits and starts, version 2.0 of the Cybersecurity Maturity Model Certification (CMMC) now requires 300,000-plus members of the Defense Industrial Base (DIB) to meet one of three maturity levels depending on the type of work they do for the Department of Defense (DoD). The goal is to protect both controlled unclassified information (CUI) and federal contract information (FCI).

And Then There Are Those Pesky Frameworks and Standards!

Beyond government regulations, most organizations now are audited against one or more of an array of cybersecurity frameworks and standards. Compliance with these may be required because of a type of business an organization does, because providers of cyber and other business insurance factor risk management into their underwriting criteria, or because the board of directors or investors insist on compliance with specific best practices with regard to governance.

Regardless of the reason, noncompliance with the Payment Card Industry Data Security Standard (PCI DSS), the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), International Organization for Standardization (ISO) standards such as 27001, 27017, and 27018, System and Organization Controls (SOC) from the American Institute of Certified Public Accountants, and other standards can have consequences for many organizations.

Many Travails in Measuring and Managing Sensitive Content Communications Risk

While compliance with relevant regulations and frameworks is critical for business success, risk management professionals know that noncompliance penalties are just the tip of the iceberg when it comes to an organization's sensitive content risk. Like actual icebergs, it is very difficult to measure what is below the surface of these metaphorical icebergs—or even to understand the nature of what is there. Data breaches can seriously damage an organization's brand reputation, have detrimental repercussions on revenue, and disrupt operations.

One takeaway is that organizations should consider regulatory compliance to be a *floor* above which they build their security infrastructure and practices for sensitive content communications—rather than an aspiration in itself. And while organizations tend to focus significant energy and investment on security for networks, endpoints, applications, and cloud infrastructure, the security of content as it is shared among thousands of first and third parties often falls through the cracks.

Methodology for This Study

Kiteworks' 2023 Sensitive Content Communications Privacy and Compliance Report is based on a comprehensive survey of 781 professionals working in IT, cybersecurity, and risk and compliance management. We report respondents' feedback for the overall cohort, compare it with our survey results from 2022, and cross-analyze it according to various demographic details.

A Diverse Pool of Respondents

The cohort who responded to our survey is a diverse bunch. We limited our survey to employees of enterprise-level organizations, specifically those with more than 1,000 employees (Figure 1). In fact, nearly half of respondents represent entities with more than 15,000 employees, while 86% have more than 5,000 coworkers. Nearly 3 in 10 respondents are from Europe, with 14% from the Asia Pacific region, and 11% from the Middle East (Figure 2). Just under half of respondents are from North America, including 38% from the United States.

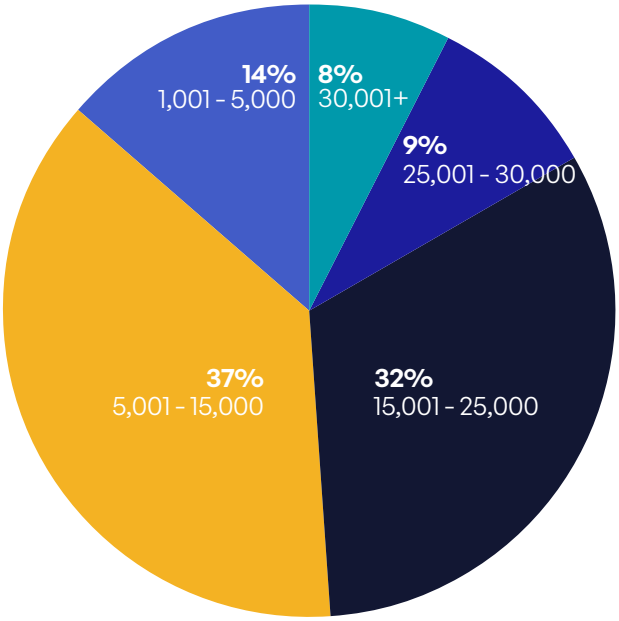


Figure 1: Organization size.

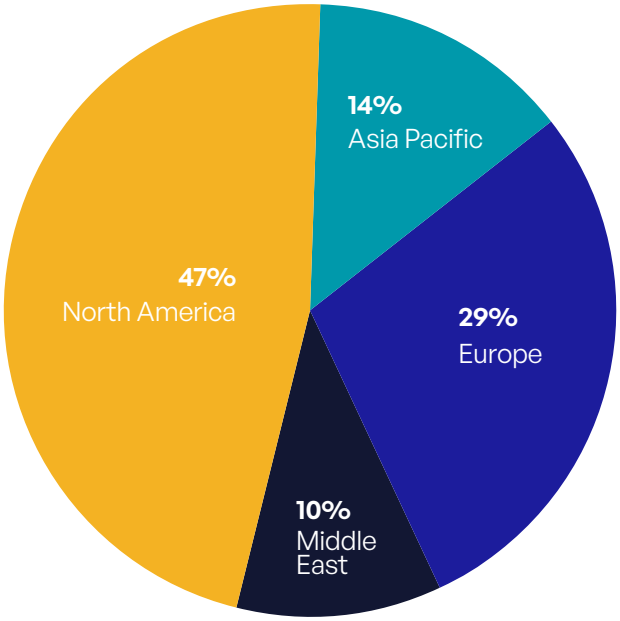


Figure 2: Headquarters of the company.

Respondents come from a wide range of industries (Figure 3), with federal government, security and defense, financial services, and pharmaceutical/life sciences organizations seeing the highest representation. And our survey pool includes a good balance of roles and levels in the organization (Figure 4). Risk and compliance roles represent 45% of respondents, with the remainder falling under IT and security departments. The cohort is also balanced between executive-level (47%), mid-level management (46%), and individual contributor (7%) roles.

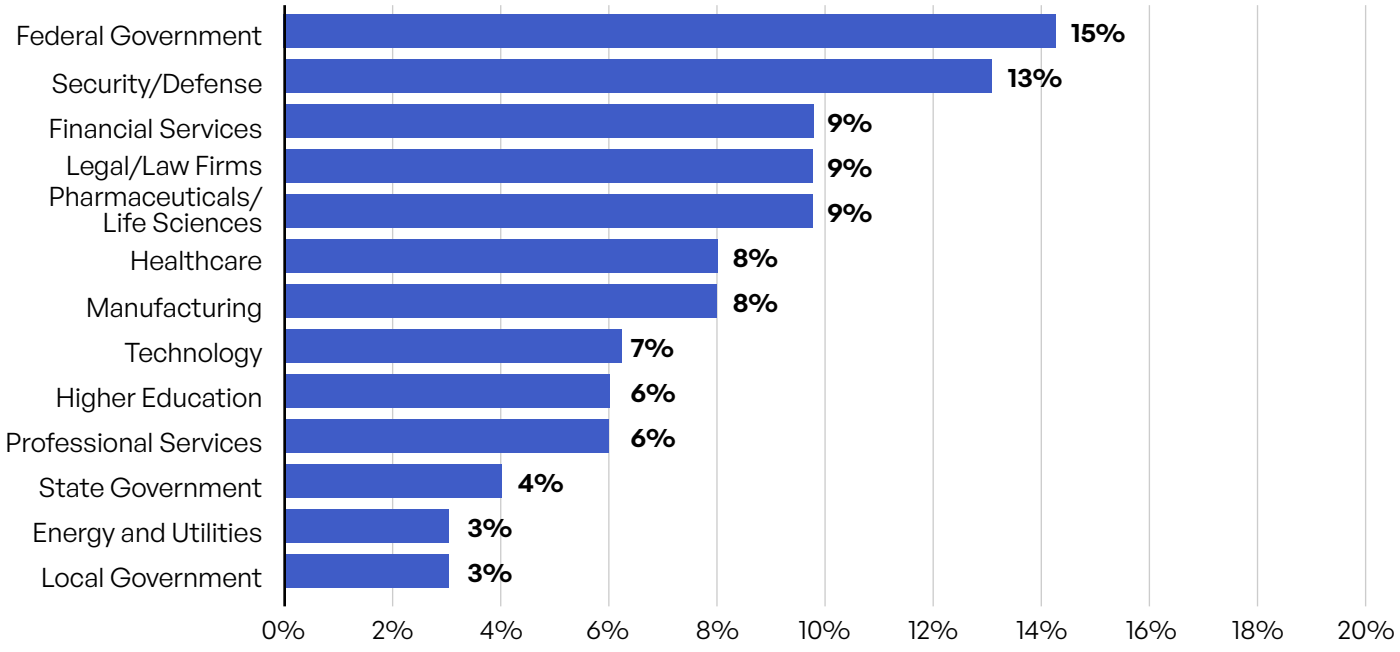


Figure 3: Industry segment.

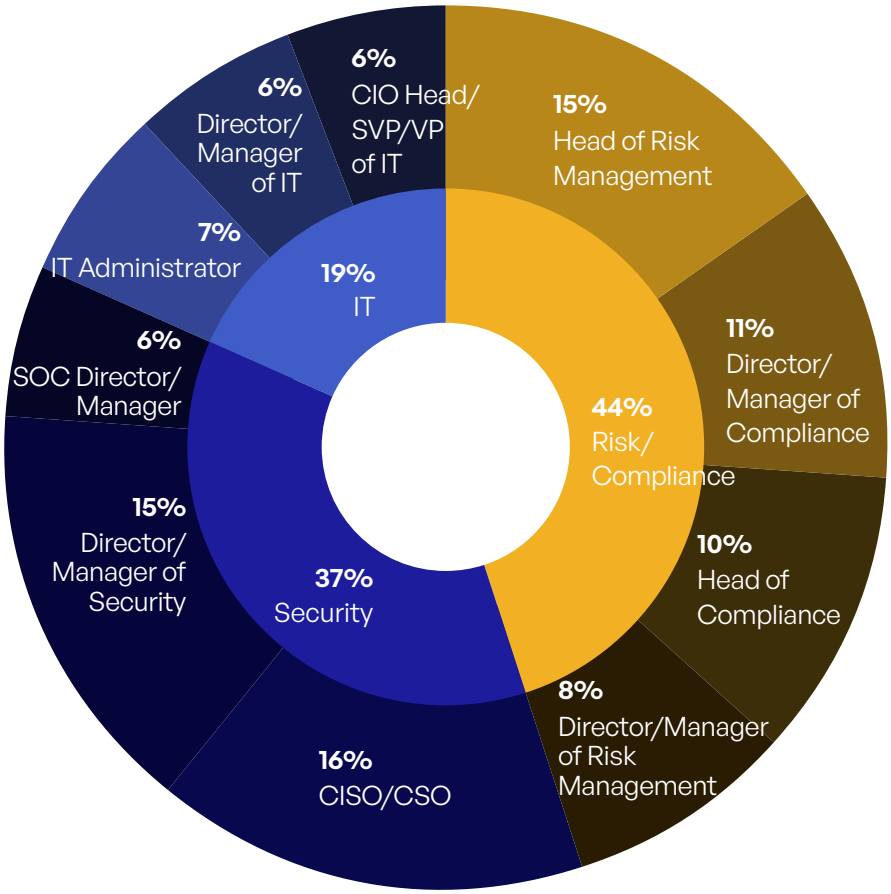


Figure 4: Job title and responsibility of respondent.

Insights on Privacy and Compliance of Sensitive Content Communications

Our respondents bravely fielded more than 40 questions related to how they manage and secure sensitive content communications. The result is the combined wisdom of many decades of experience and diverse expertise. When we distilled the survey results, several areas of clear insights emerged:

Complexity

Insight: Organizations Share Content With a Growing Number of Third Parties Using Multiple Channels, and This Is a Problem

If there is a single question in our survey that gets to the root of the problem, it is the simple question of how many third parties with which organizations share content. A comparison of 2022 and 2023 findings reveals the problem is getting worse. This year, 90% of respondents say they exchange content with more than 1,000 outside organizations, and 44% say that number is above 2,500 (Figure 5). These numbers are significantly higher than 2022, when 63% had more than 1,000 third parties and one-third had more than 2,500.

Not surprisingly, larger firms tend to exchange content with more third parties overall, with 65% of firms with more than 30,000 employees exchanging content with more than 5,000 third parties. But even in smaller enterprises (fewer than 5,000 employees), 93% had more than 1,000 third-party recipients of content. More than half of respondents in the financial services, manufacturing, pharmaceutical/life sciences, professional, and security and defense industries report more than 2,500 third parties with which they exchange content.

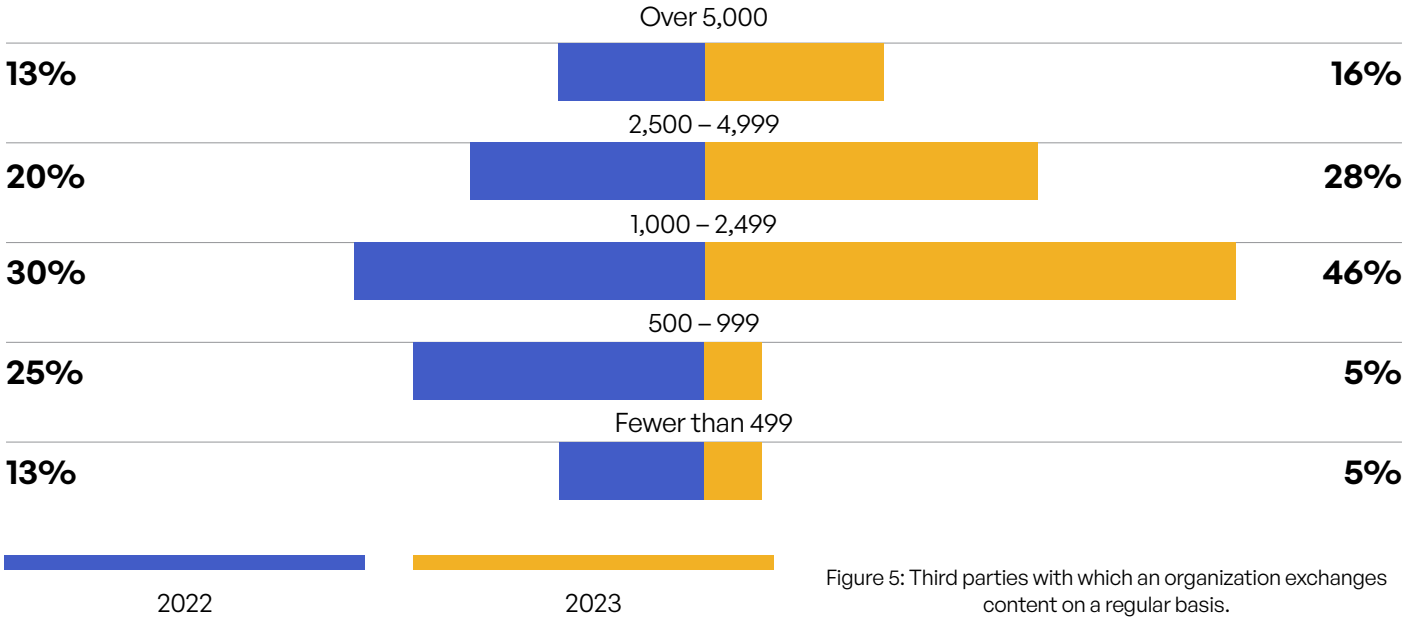


Figure 5: Third parties with which an organization exchanges content on a regular basis.

An Overwhelming Array of Communication Channels

The second biggest element of the problem is the number of tools or channels used to transmit content—a number that is growing in our survey as well. Half of all respondents in 2023 say they use six or more tools for sensitive content communications, and all respondents report four or more (Figure 6). Last year, "just" two-thirds used more than four tools and only one-quarter used more than six! "Whac-A-Mole" just became exponentially more difficult.

The problem is even worse in financial services and healthcare, which have specialized applications over which content can be transmitted. In those industries, well over two-thirds of respondents report more than six tools in use for sensitive content communications. The largest enterprises also employ disproportionately more tools, with 92% of organizations with more than 30,000 employees using six or more.

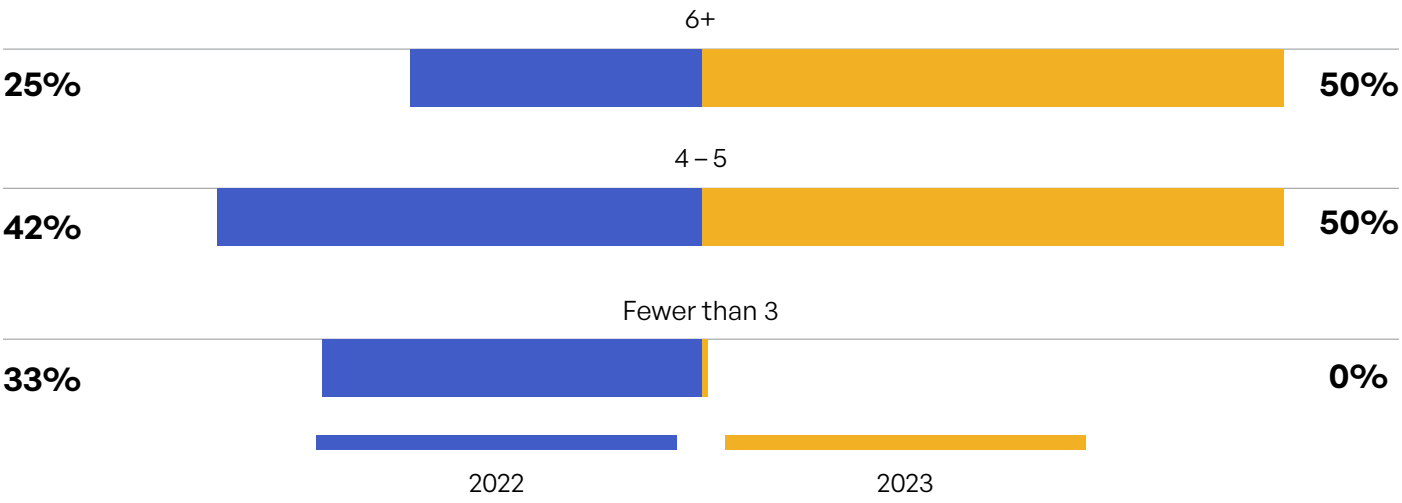


Figure 6: Tools/systems used for sensitive content communications.

Huge Complications in Tracking and Controlling Content Access

Returning to the iceberg metaphor, it is no surprise that with so many third-party partners and so many channels over which content is shared, what lies below the surface is even more difficult to discern. Adding to the complexity, organizations use multiple tools to track, control, and secure content communications with third parties. In fact, 85% use four or more systems, while 46% use six or more (Figure 7). Disaggregated sources of data from all these tools add to staff time in reporting on the security posture and demonstrating compliance—and inevitably leave gaps in visibility.

And while many cybersecurity measurements have only indirect impact on the bottom line, the cost of this tool soup is a discrete line item in the budget. Given this plethora of solutions, it is not surprising that 69% of organizations pay more than $250,000 in licensing per year (Figure 8). More than one-quarter of higher education and pharmaceutical/life sciences organizations spend more than $500,000, while well over half (57%) of financial services firms spend more than $350,000.

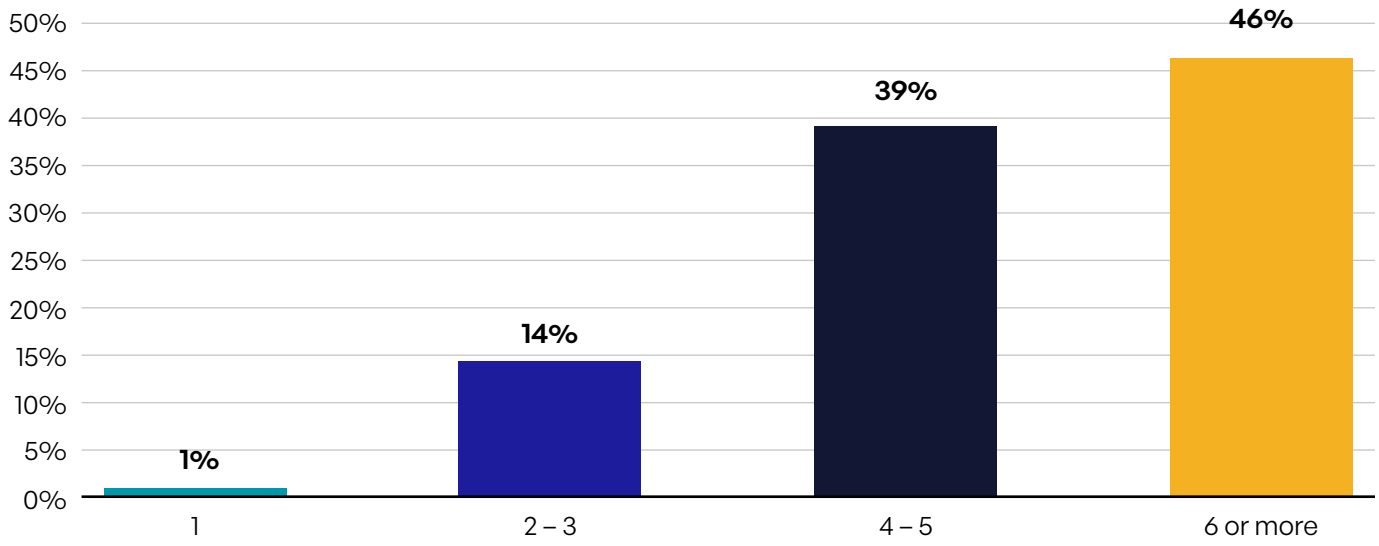


Figure 7: Systems and tools used to track, control, and secure third-party content communications.

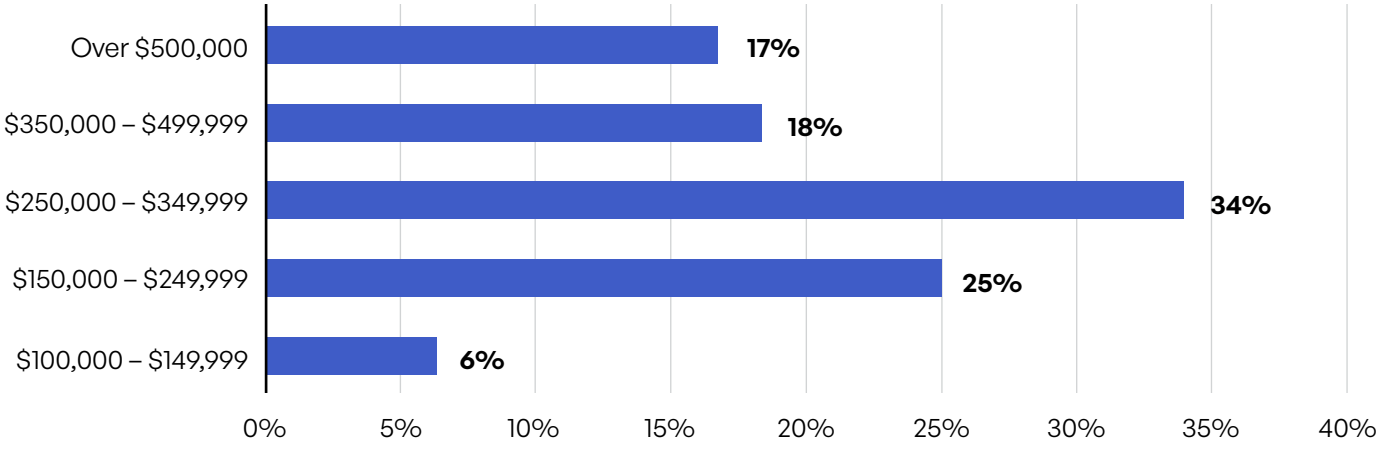


Figure 8: Annual licensing cost for content communication tools and systems.

So Many Organizational Priorities!

When respondents are presented with eight important aspects of secure content communications and asked to rank their top four in terms of importance, their answers are all over the map. This is not necessarily a bad thing, as all eight are important priorities and each organization may accomplish them in a different sequence.

When we weighted the answers to give more points to higher rankings,[7] two priorities bubble to the top: tracking content permissions, expiration, locking, and versioning; and unifying management, tracking, policies, and reporting (Figure 9). A close third is protecting content in motion—an important priority when sensitive content is shared so widely internally and externally.

Not surprisingly, eDiscovery got more number 1 answers in law firms (21%) and healthcare organizations (23%). Tracking content permissions was a bigger deal in state government (29%) and professional services (20%). Unifying all systems was a priority in security and defense companies (29%). Regardless of the immediate priority at each organization, all eight of these priorities are very important for sensitive content communications.

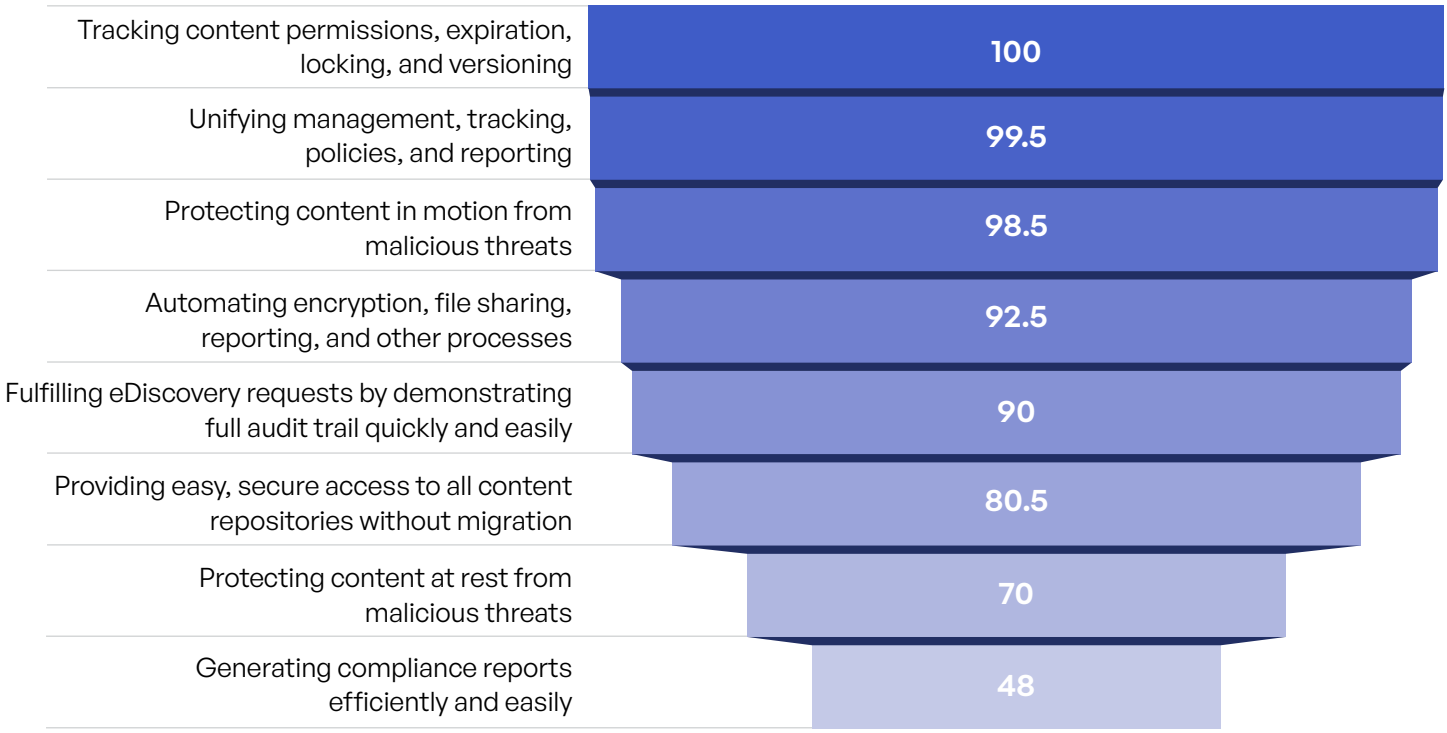


Figure 9: Weighted scores: Top priorities for sensitive content communications (rank top 4).

Security Risk

Insight: Security of Sensitive Content Communications Is No Longer an Afterthought

We are going to put on our risk management hat for a moment and take you on a tour of two distinct kinds of risk when it comes to sensitive content communications—security risk and compliance risk. As we have said, regulatory compliance should be seen as a minimum requirement, and organizations should go beyond compliance requirements to address overall security risk.

Regardless of this distinction, mitigating both areas of risk involve two components—measuring that risk and managing it. As the old saying goes, "What gets measured can be improved." Unfortunately, when it comes to both measurement and management of security, our cohort as a whole understands that improvement is needed. Barely one-quarter of respondents claim that no improvement is needed in these two areas at their organizations (Figure 10). Interestingly, a higher percentage (37%) says that *significant* improvement is needed in security management than in security measurement (29%).

Energy and utilities companies are much more confident in their *measurement*, with 52% saying no improvement is needed (Figure 11). At the same time, 44% of local government respondents believe significant improvement is needed in their measurement, while 46% in state governments believe no improvement is needed. When it comes to management, local government is by far the most confident vertical, with 52% saying no improvement is needed (Figure 12)—despite their lack of confidence in their security measurement.

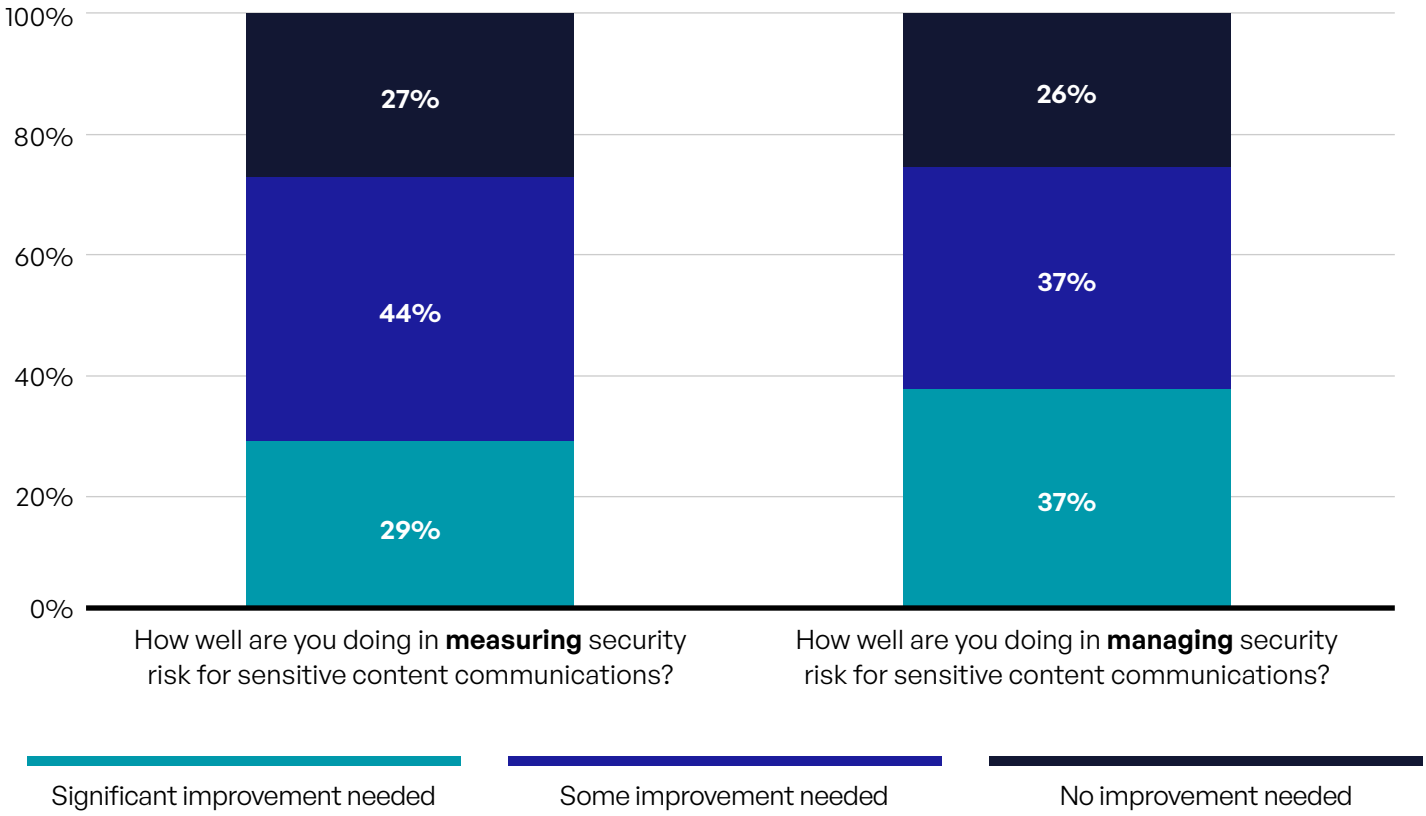


Figure 10: Maturity level of organization measuring and managing security risk.

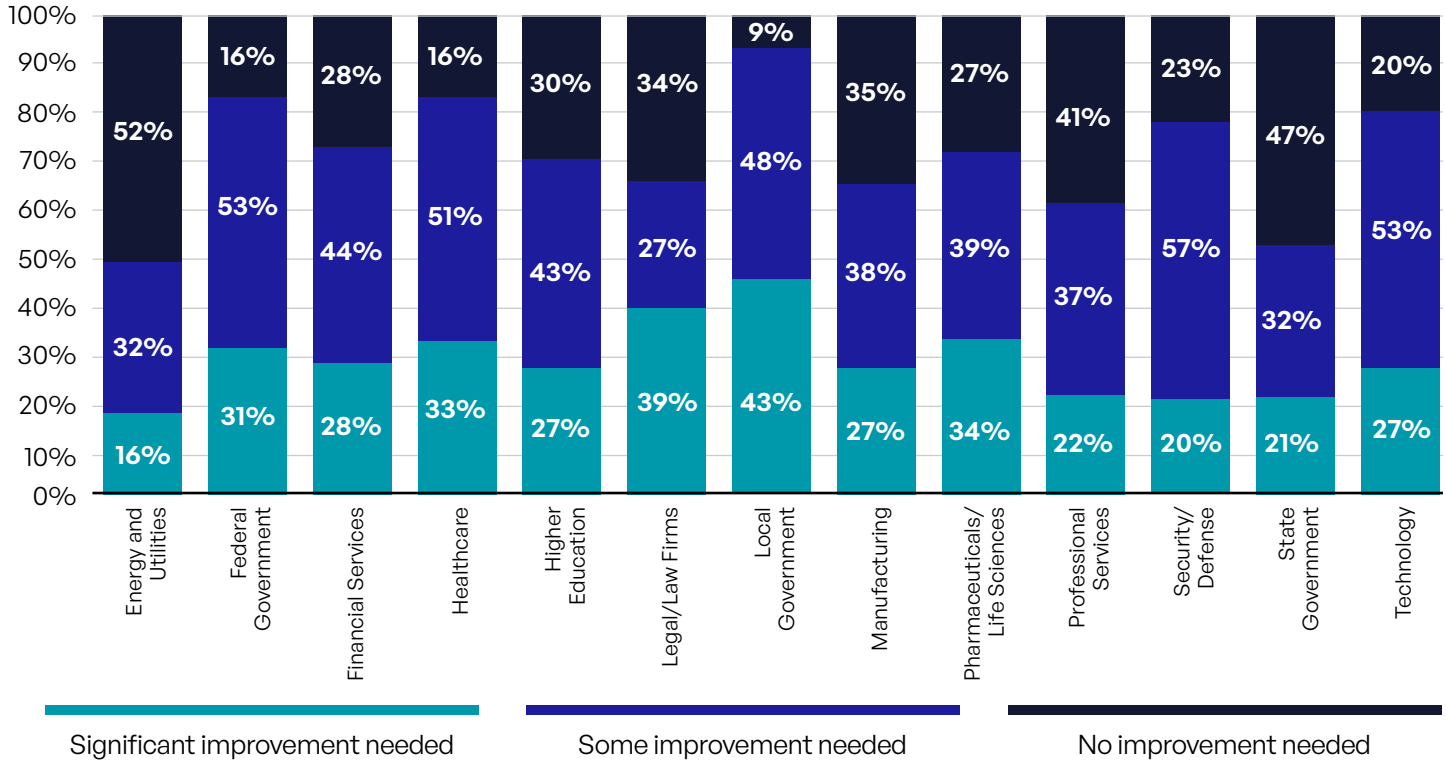


Figure 11: Measurement of security risk for sensitive content communications.

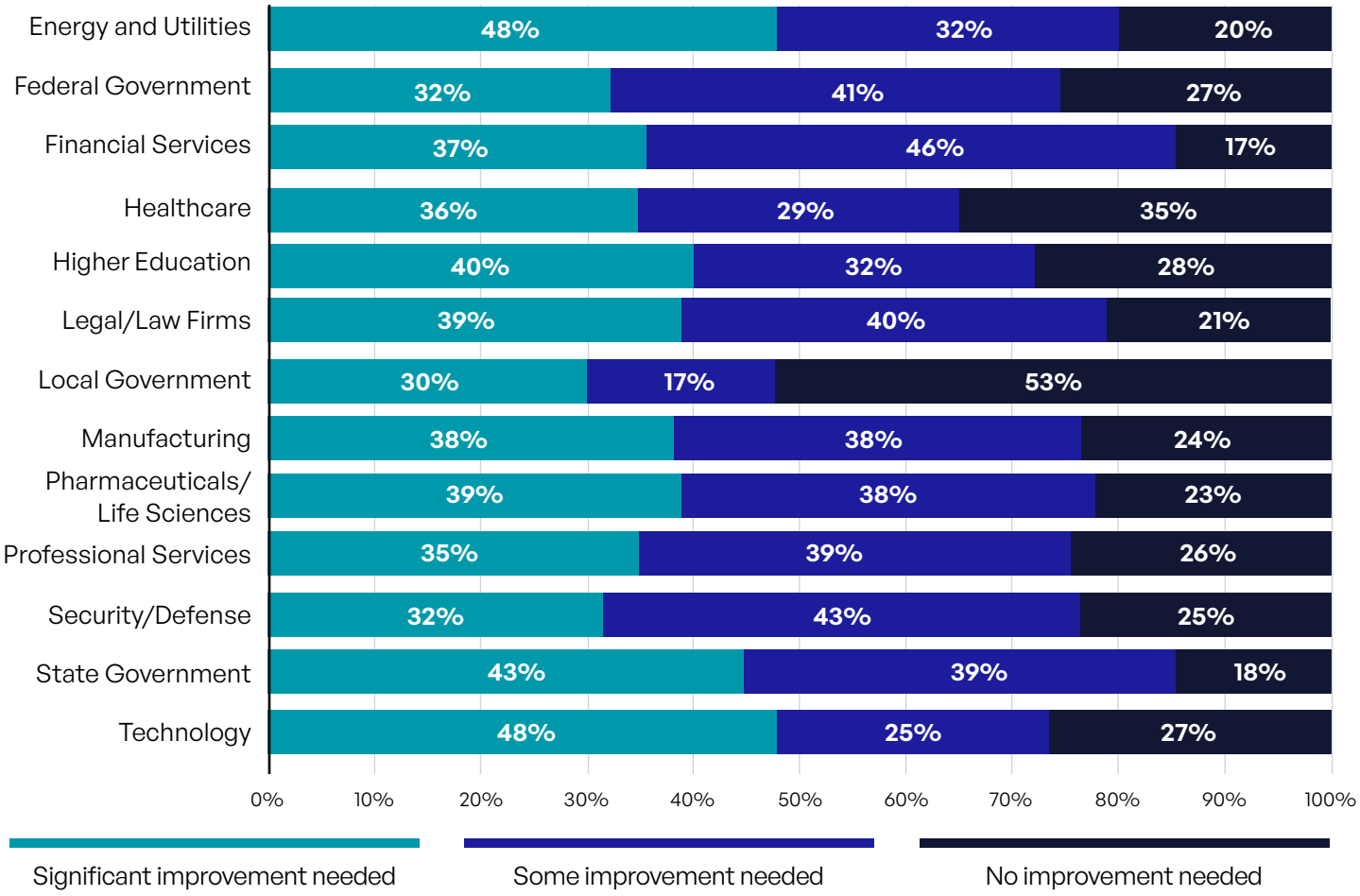


Figure 12: Management of security risk for sensitive content communications.

Every Channel Brings More Risk!

We are sure that everyone will be shocked to learn that email is the clear leader in risk perception over other content communication channels, with one in five ranking it number 1 and two-thirds ranking it in the top four (Figure 13). Even so, email ranks less risky in 2023 than in 2022, when all respondents ranked it in the top four and 30% ranked it as number 1. File sharing and file transfer and automation tools were seen as much more risky last year as well, with well over 95% of respondents ranking these in the top four in 2022 compared with 58% and 46%, respectively, in 2023.

Since this is a ranking question, part of the reason these longstanding risks rank somewhat lower is because of the rise in the risk profile for emerging content communications channels like application programming interfaces (APIs), text messaging, and mobile applications—all of which grew exponentially in their perceived risk from last year. The sharing of content by chat was added to the survey this year, and it debuts with 37% ranking it among the top four risks.

File sharing services are seen as an especially big risk in energy and utilities companies (32% ranked it number 1), while web forms (25%) are higher in financial services. Email is seen as an even bigger risk in technology and security and defense companies, with 32% in both industries ranking it as number 1.

Regardless the ranking that specific respondents assign to different channels, organizations cannot let up their guard. For example, a recent spate of hacks targeted at managed file transfer (MFT) tools in the news and resulted in theft of sensitive data.[9]

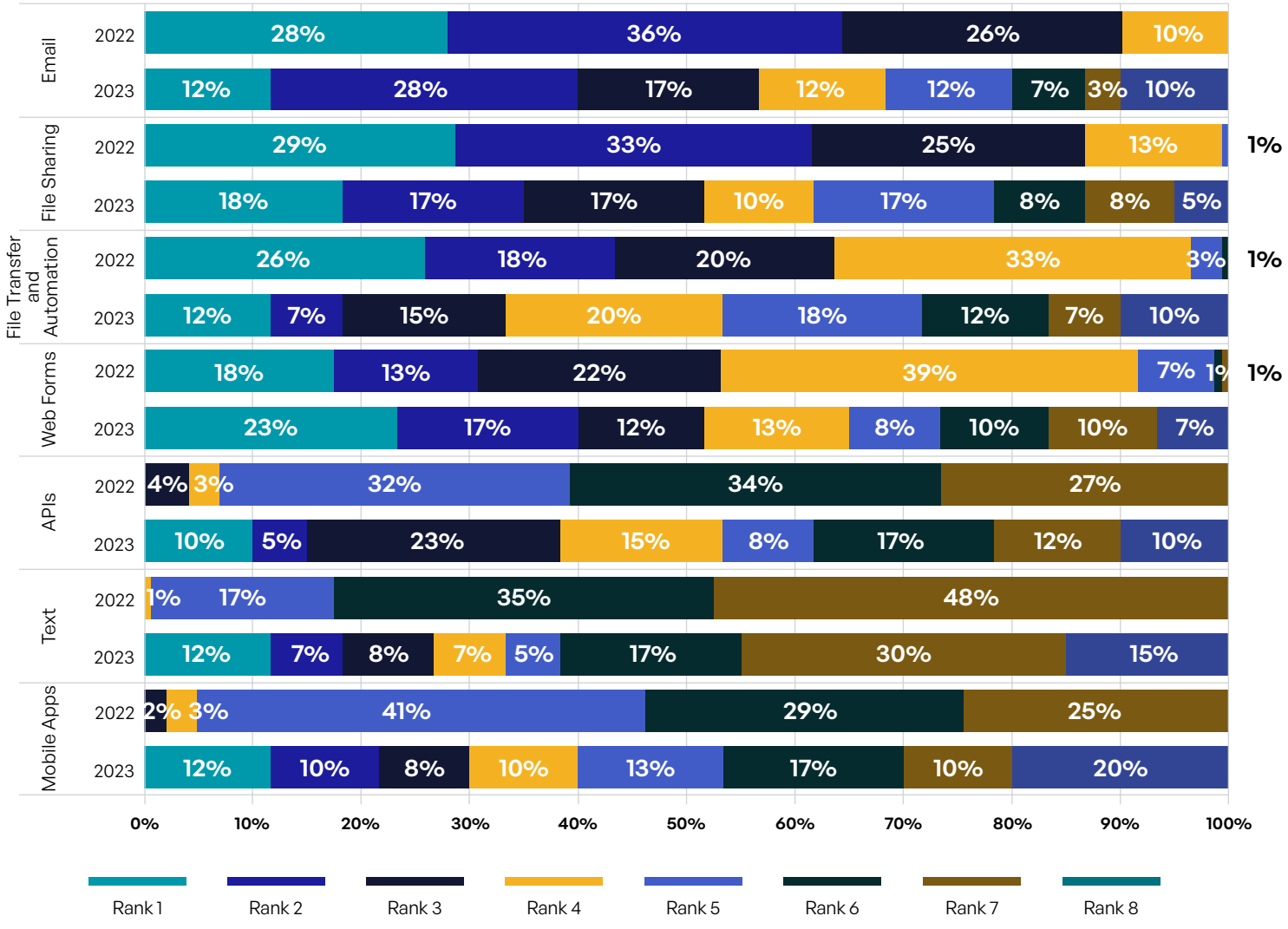


Figure 13: Communication channels that pose the highest risk.

Losing Sleep Over Too Many Attack Methods

When asked to identify their top three concerns among a list 13 possible attack vectors and tactics, it is telling that every item on the list is ranked first, second, or third by at least 9% of respondents. But when we weighted the responses to give more weight to higher rankings, password or credential theft comes out far ahead of other tactics (Figure 14) and is by far the most-cited tactic, ranked in the top three by 34% of respondents. That said, rootkits and URL manipulation got more number 1 rankings than anything else on the list.

It is notable that the two top concerns are human-oriented. Whether respondents are concerned about attackers gaining access by impersonating an internal user or a customer account, the attack methods are the same—and all revolve around human error.

Some methods to obtain user credentials involve actively manipulating an unsuspecting user with a social engineering attack, and most common among those types of attacks is URL manipulation: making users believe they are browsing a certain legitimate website by presenting them with a URL that is very similar to the real one, but not quite the same.

Other attack vectors are less direct, but are rather based on human predictability. Users tend to use the same or very similar passwords across multiple systems. If adversaries know one password, there's a good chance they can guess the others. This is why enforcement of a proper password policy, alongside proper and consistent user awareness training, are considered some of the best tools against common attacks.

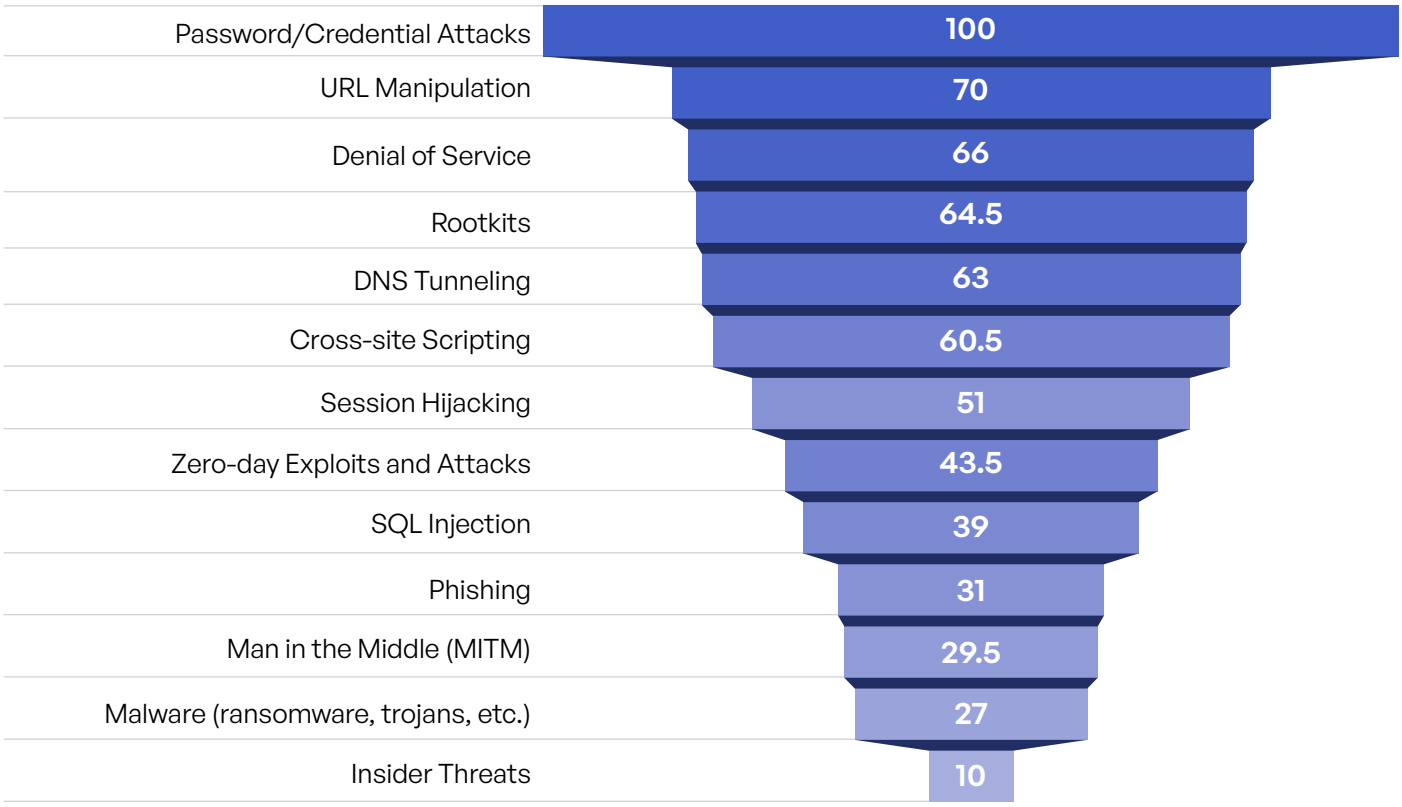


Figure 14: Weighted scores: Top attack vector concerns for sensitive content communications.

More Data Types, More Risk!

In ranking six different types of sensitive content by the risk they pose to the organization, answers vary. More than half of respondents rank PII, PHI, and legal documents in the top three (Figure 15). Regional variations are not shocking by any means: There is more emphasis on PII in Europe and Asia Pacific, home of GDPR and similar laws in Asia and Oceania. And North Americans are more concerned with PHI, where HIPAA is a major compliance requirement. Interestingly, IP is a much bigger perceived risk in the Middle East, with 60% placing it in the top three.

Most of the variation by industry is also unsurprising—or at least understandable:

- More concern about legal documents in financial services, higher education, and healthcare
- More emphasis on M&A in law firms, professional services, and pharmaceutical/life sciences companies
- More citation of financial documents in local government
- More emphasis on PHI in energy and utilities companies and federal government agencies—but not in healthcare, where they presumably have more of a handle on protecting it

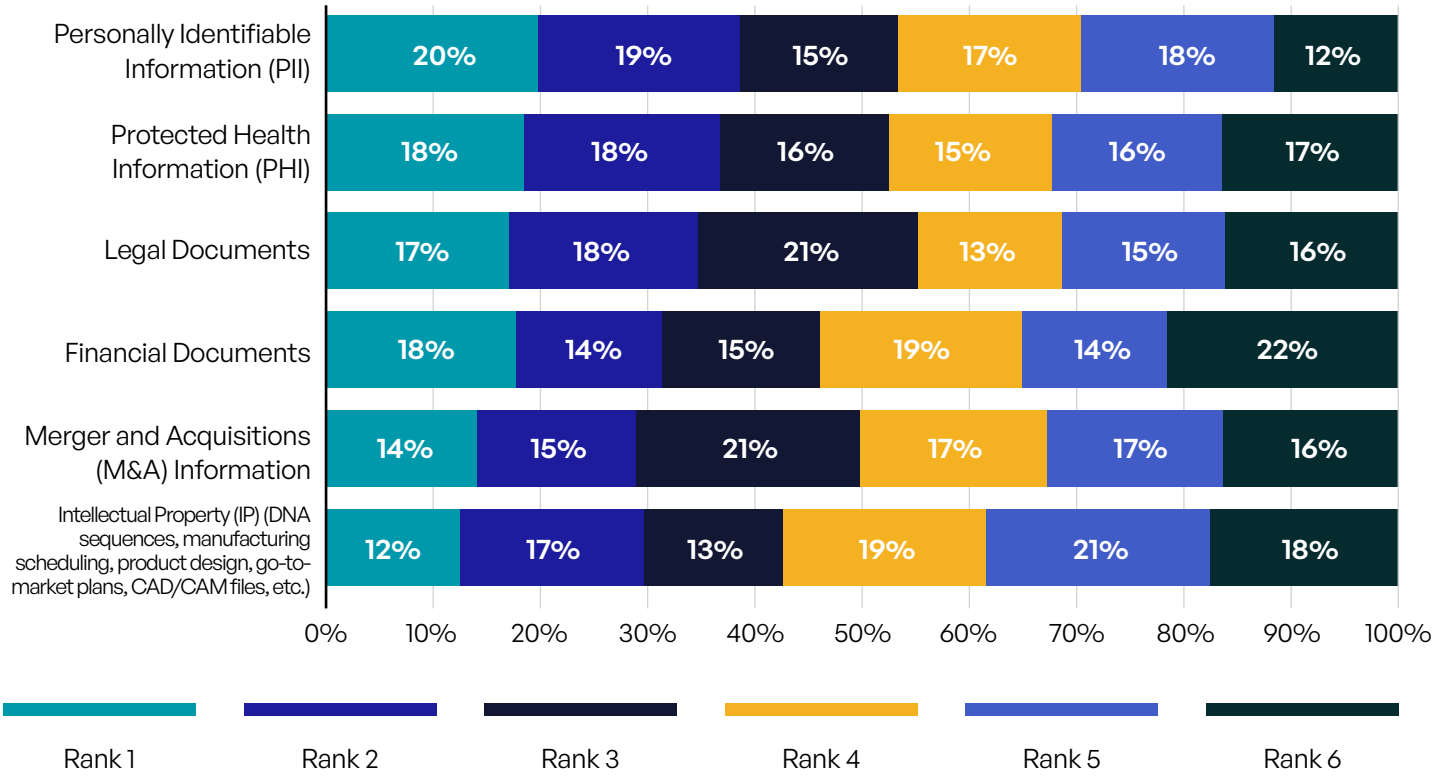


Figure 15: Security and compliance risks per sensitive data type.

Multitenant Hosting Infrastructure Makes It Even Harder

Multitenant hosting solutions are a less costly way to access cloud-based services and are quite popular. Under the model, multiple organizations share the same virtual machine(s) when they access a specific application or infrastructure from a cloud services provider. Of course, segmentation theoretically means organizations do not have access to each other's data—but there is a risk that something will go wrong if there is an intrusion. This risk is not unnoticed by our highly prescient respondents, 99% of whom cite multitenancy risk as a concern (Figure 16).

Significant numbers of respondents select each of the three provided reasons why multitenant hosting solutions present a risk, but the most-cited concern is that bad actors can move laterally once they have intruded on one tenant's infrastructure. Asia Pacific respondents are somewhat more concerned that a bad actor could acquire a cloud instance of an application, set up a sandbox, and identify vulnerabilities that can be exploited (36% versus 32% for the full cohort).

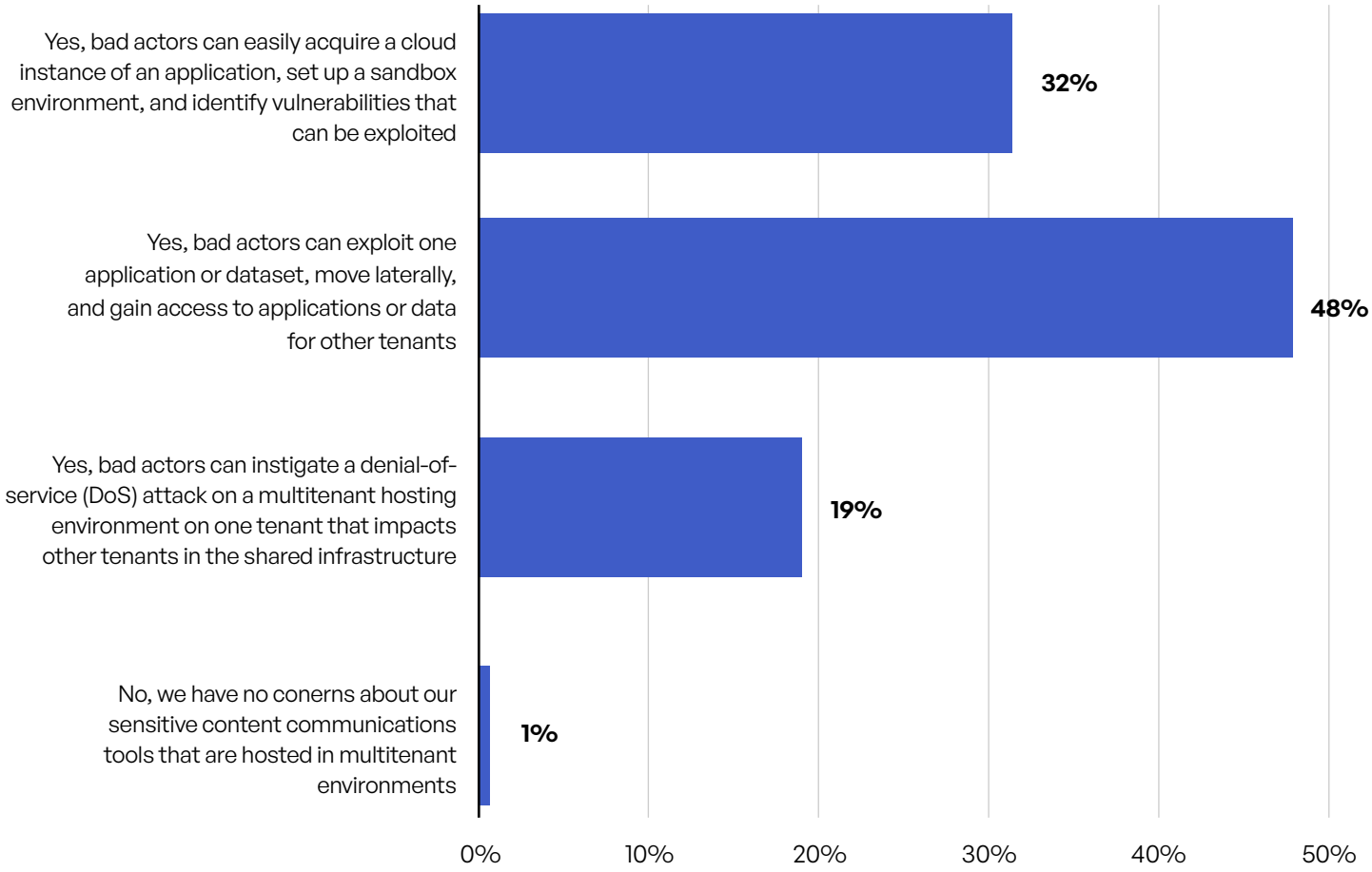


Figure 16: Security concerns involving multitenant hosting of communication tools.

Getting Off the "Hamster Wheel" to Talk Strategy

Now that we've interacted with a number of specific questions about security risk, we want to turn the focus from the tactical to the strategic. One priority for improving an organization's security posture in any given area is to ensure that these efforts are aligned with the company's overall risk management strategy—including both measurement and management. When asked about the status of that alignment, 28% of respondents report their alignment is already complete, while 47% say that it is in progress and expected to be completed in the next 12 months (Figure 17). Another 22% see the alignment effort as a priority for the coming year.

Some industries are further along than others. State government (57%), law firms (52%), and energy and utilities (44%) are more likely to report that the alignment is complete, while—ouch—pharmaceutical/life sciences (13%), financial services (16%), and higher education (21%) are less likely.

When asked about their overall level of satisfaction with their organizations' risk management for third-party communications, it is important to note that 84% said that at least some improvement is needed (Figure 18). More than 4 in 10 say that significant improvement is needed—or even throwing the baby out with the bath water and starting all over again.

It is perhaps heartening to see that a lower percentage of respondents cited the need for a whole new approach in 2023 compared with 2022. While more still say significant improvements are needed, this may represent incremental progress. Unfortunately, in three industries—higher education, law firms, and technology—more than half of respondents cite the need for major improvements. More than half of European respondents make the same assessment.

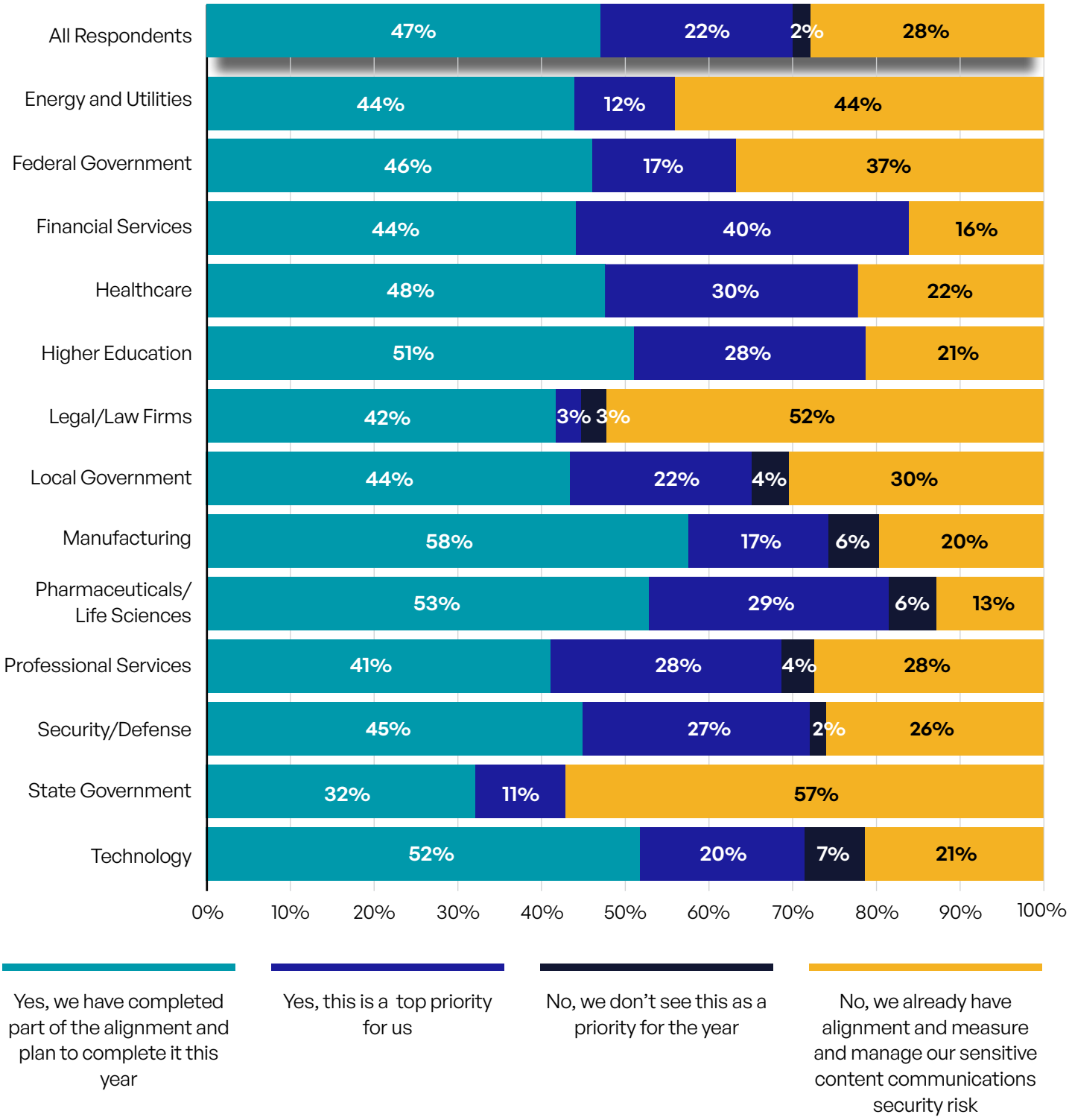


Figure 17:Alignment of risk management strategy with measurement and management of sensitive content communications a priority in 2023.

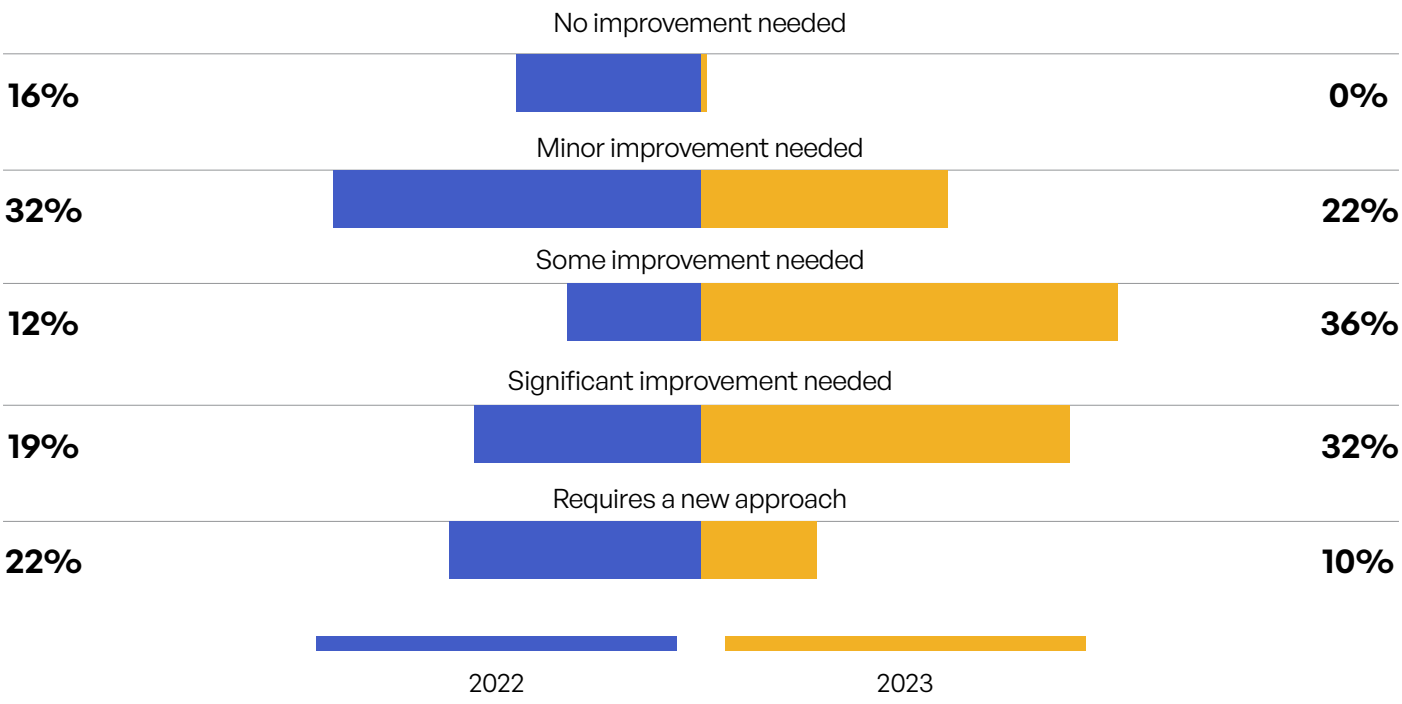


Figure 18: Level of satisfaction with risk management of third-party communications.

Compliance Risk

Insight: As Compliance Requirements Multiply, Organizations Must Forge Ahead

The other area of risk around sensitive content communication revolves around compliance—a word that many associate with government regulation. And there certainly are plenty of those—especially for global companies that do business in many jurisdictions.

However, laws and regulations are not the only compliance requirements that most companies must adhere to. To cite the most obvious example, any entity that processes payment card transactions must comply with PCI DSS, a framework designed and maintained by the industry itself. And standards like NIST CSF are voluntary but help organizations operate within some industries, conduct business with some government entities, or secure cyber insurance at affordable terms.

Whatever the compliance requirement, preparing for audits is likely a privilege that occurs at least several times a year for the risk management or IT security teams. Audits may also take place in the aftermath of a cyber incident. Either way, the risks to the business from a failed audit can be significant.

Flunking Measurement and Management of Compliance

Our survey respondents answered similar questions about compliance as those we reported about security in the last section—the current state of measuring and management (Figure 19). As with security, barely one-quarter of overall respondents claim that no improvement is needed for either measurement or management of compliance risk. The result is even worse in North America when it comes to measurement, where 79% say that improvement is needed. In the Middle East, on the other hand, 35% report that no improvement is needed for measurement.

Looking at this question by industry, energy and utility companies are especially pessimistic about compliance measurement, with only 8% reporting no improvement needed. Ironically, the same industry finds 36% needing no improvement in compliance management. Local government is somewhat the opposite, with 39% seeing no need for improvement in measurement, but only 21% for management.

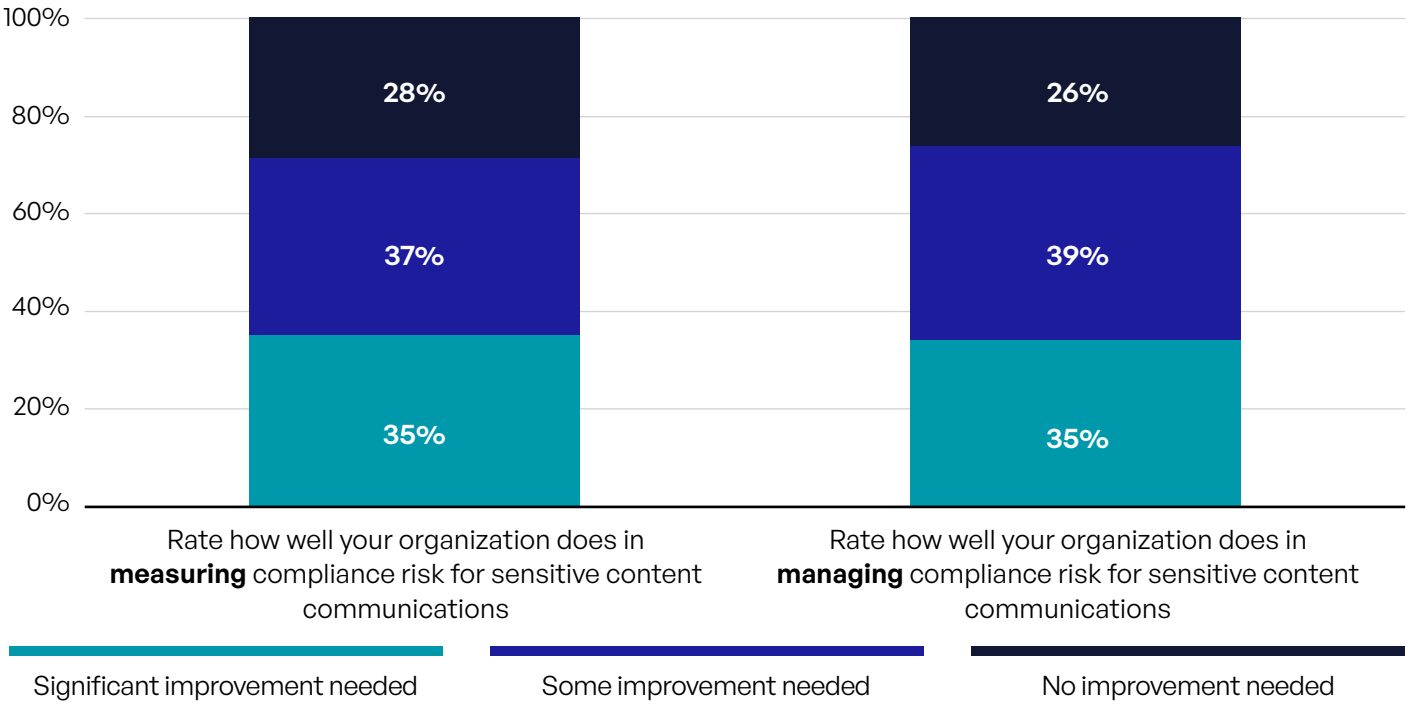


Figure 19: Maturity level of organizations measuring and managing compliance risk.

Audits for Myriad Regulations and Standards

Asked what compliance regulations and standards they must adhere to, PCI DSS (40%) is the most common response—not surprising since it is a global standard (Figure 20). GDPR is second with 37% of overall respondents—including 96% of Europeans (Figure 20). And HIPAA is a requirement for 34% of respondents, including 92% in the United States. Beyond HIPAA, North American respondents are subject to a wide variety of regulations with acronyms like HIPAA, GLBA, SOX, FINRA, and FISMA—as well as the aforementioned state-level regulations. Respondents in other countries often must adhere to country-specific requirements.

Security frameworks in common use include ISO 27001, 27017, and 27018—the most cited by our respondents (Figure 21). U.S. organizations doing business with the Department of Defense now must comply with CMMC 2.0, and those working with other agencies are subject to FedRAMP. And different standards by NIST, even though it is a U.S. agency, are becoming more global in adoption.

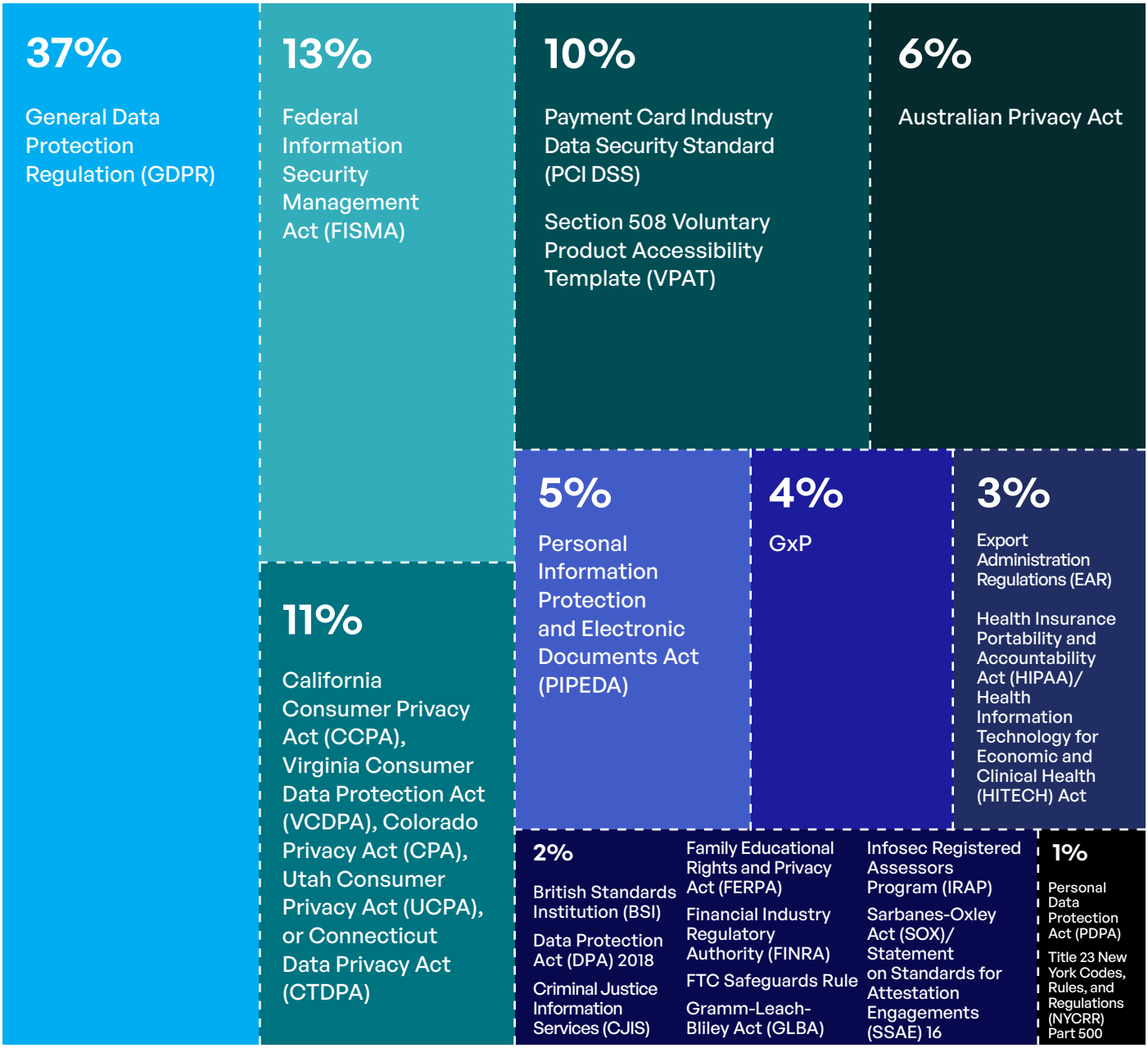


Figure 20: Data privacy regulations that apply.

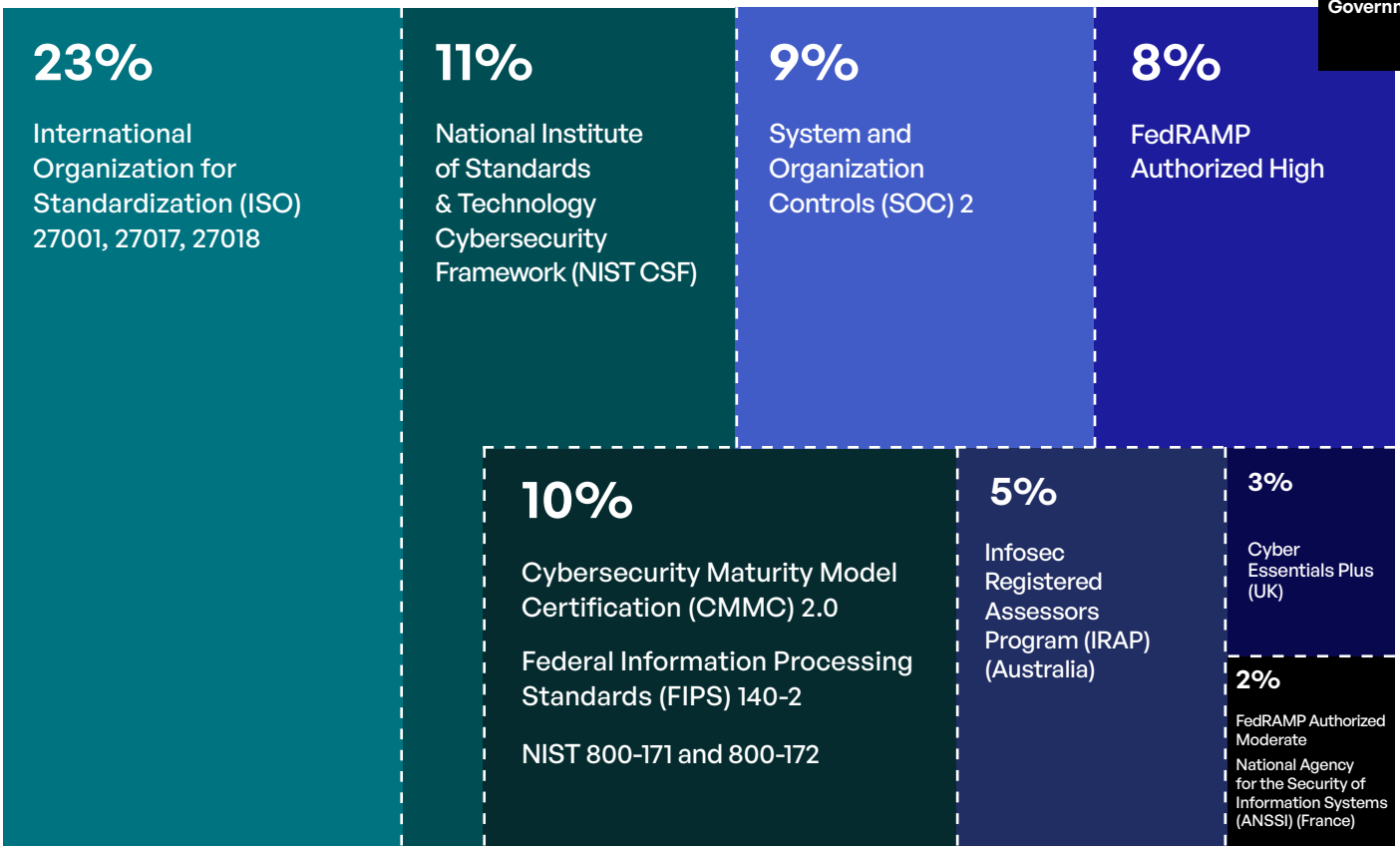
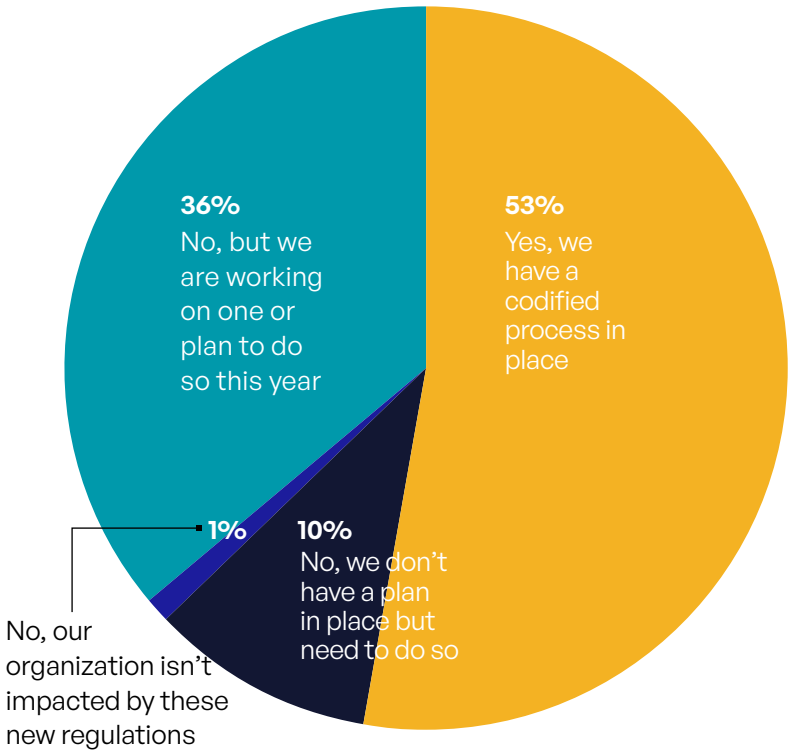


Figure 21: Data privacy standards that apply.

While the California Consumer Privacy Act (CCPA) got some publicity when it was passed in 2018, the new state-level regulations passed in Virginia, Colorado, Utah, and Connecticut over the past year have gotten less attention in the general news media. Most survey respondents who will be impacted, however, understand they will need to comply in the next few months if they do business in these states (Figure 22). Among U.S. respondents, more than half (53%) say they already have a codified process in place, and 36% say they are working on one.

While much of our discussion of government contracts thus far has related to the U.S. government, almost all respondents globally report doing business with government agencies, and almost all are subject to audits (Figure 23). A big majority in every region undergoes audits once a year, but a slightly higher percentage in Asia (25%) is audited more frequently.



U.S. respondents only.

Figure 22: Does your organization have a strategy in place to deal with new data privacy regulations from four states that will go into effect this year (UT, VA, CT, CO)?

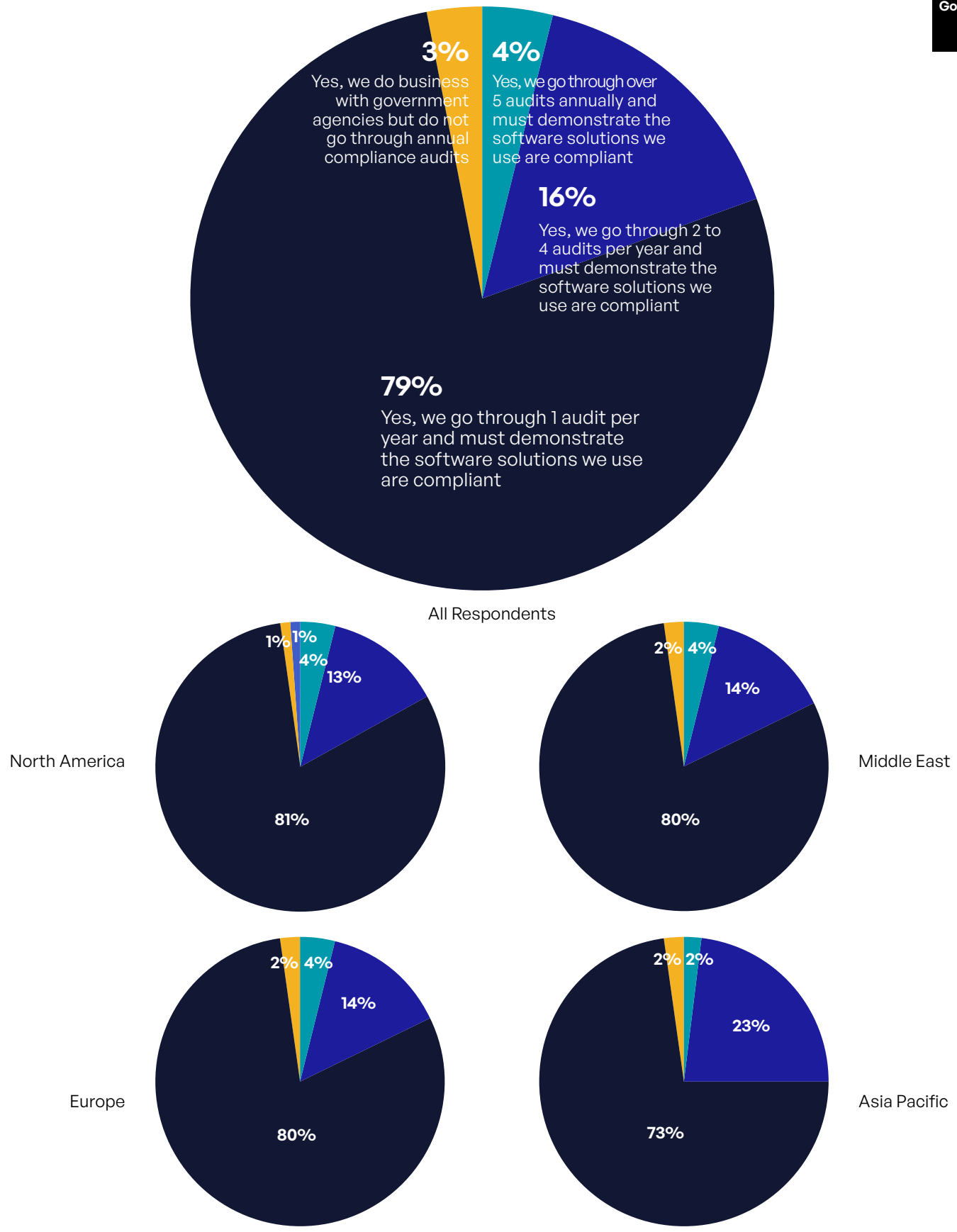


Figure 23: Conduct business with government agencies that require software tools we use are compliant with cybersecurity frameworks.

Insurance Coverage: Another Incentive for Compliance

Another reason organizations are motivated to comply with regulations and standards is to get better terms on cyber insurance coverage—or to be able to purchase such coverage at all. Overall, 88% of respondents report that their insurance providers consider compliance risk management practices in their underwriting process (Figure 24). This percentage is even higher in North America, with 93% of respondents affirming a connection between compliance and insurance coverage.

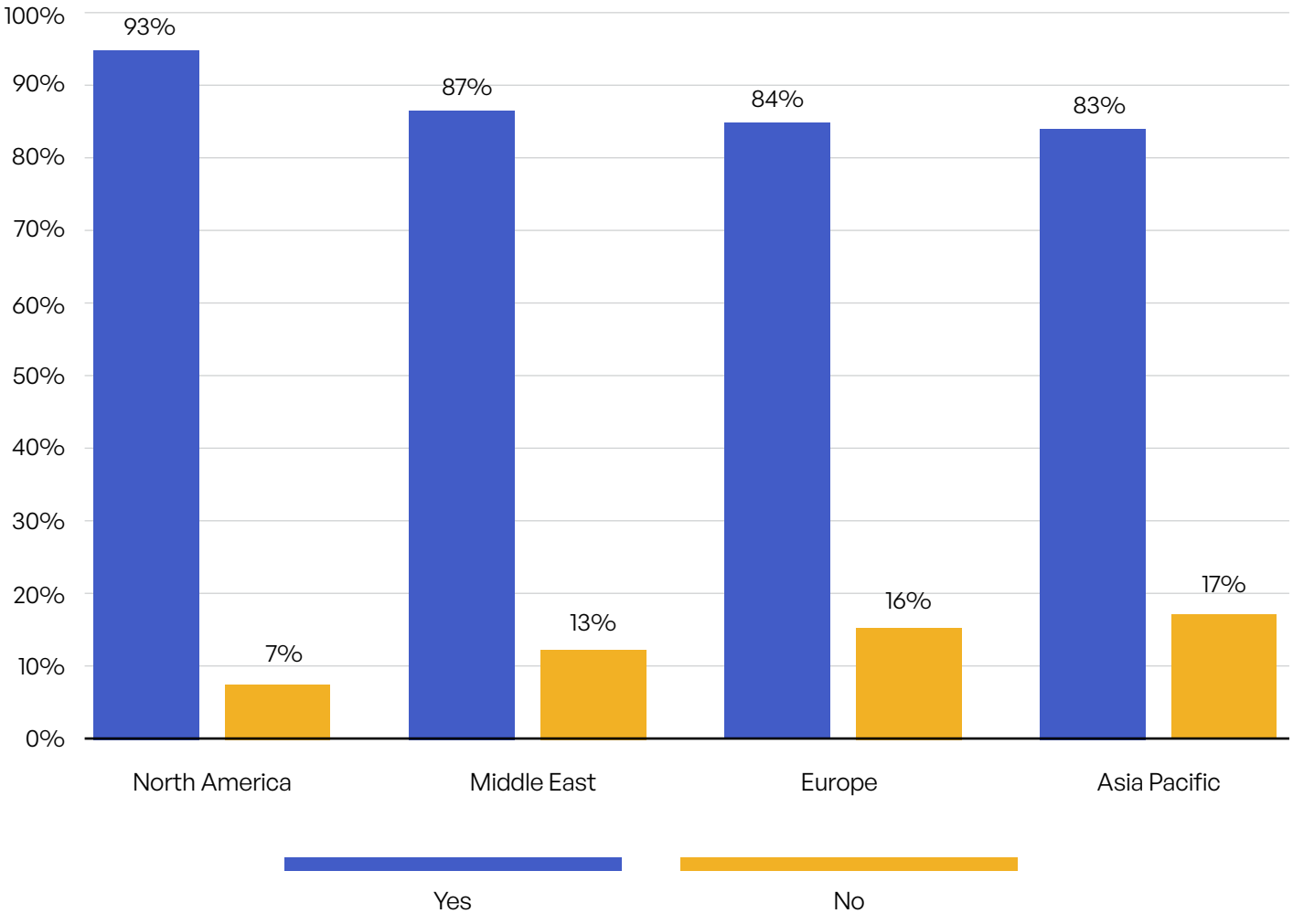


Figure 24: Cyber insurance providers consider data privacy and compliance risk management for rate coverage.

Getting Strategic About Compliance

The amount of time, money, and energy organizations expend on compliance is by no means trivial. Among all respondents, 69% report that their compliance efforts for sensitive content communications require more than 300 staff hours per year for both tracking and reporting. Well over one-third (36%) say that figure is above 500 hours (Figure 25). Several industries—financial services, healthcare, higher education, and pharmaceutical/life sciences—saw more than 80% of their respondents report 300 or more hours spent on sensitive content communications compliance.

When asked about the number of headcount dedicated to compliance for sensitive content communications, nearly half of respondents (49%) reported a single full-time equivalent (FTE; Figure 26)—but 42% reported that two or more FTEs are devoted to compliance. Industries like financial services, healthcare, higher education, and pharmaceutical/life sciences saw more than half of respondents in our cohort report more than a single headcount required to manage compliance.

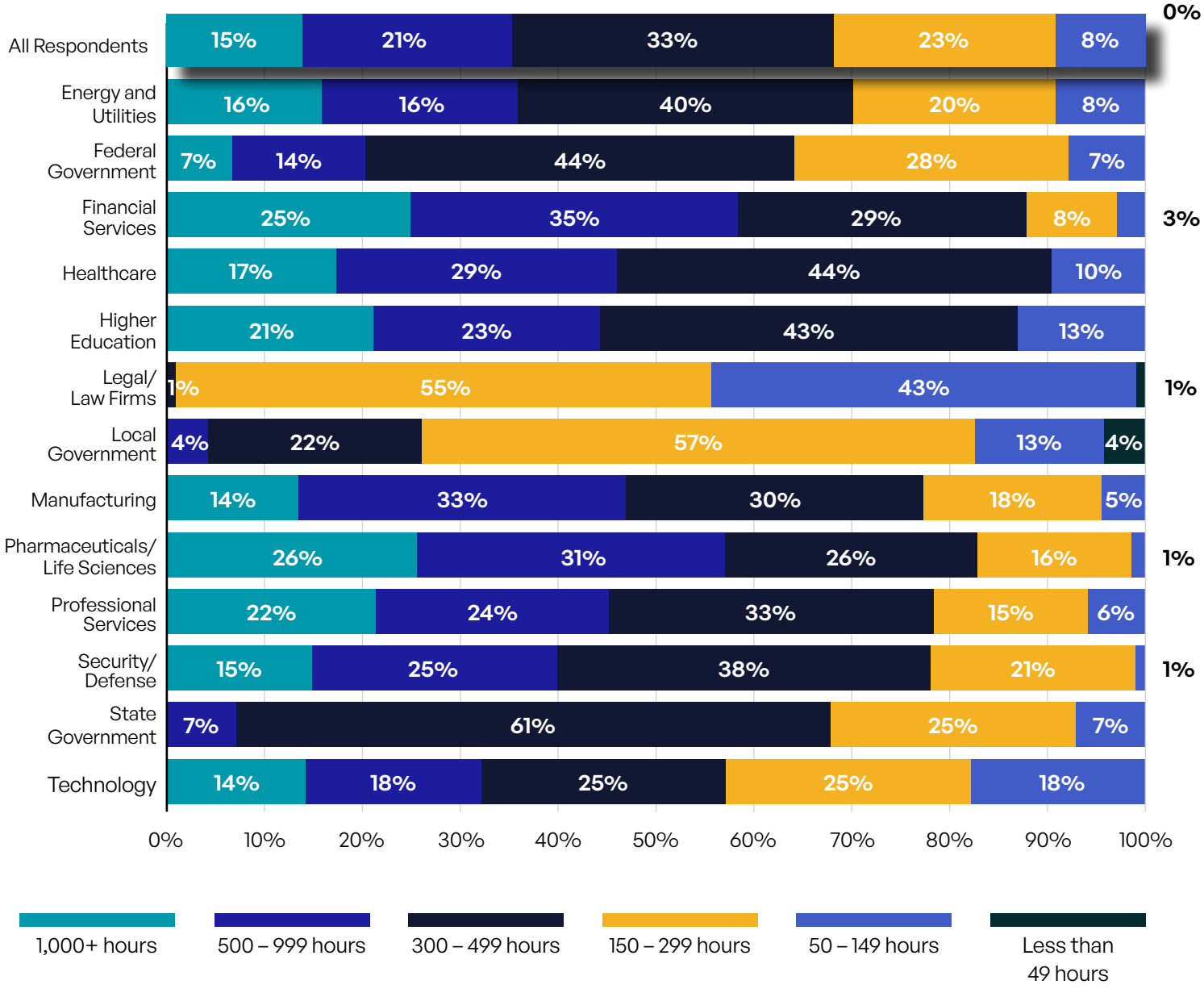


Figure 25: Time spent annually tracking and reporting regulatory compliance of sensitive content communications.

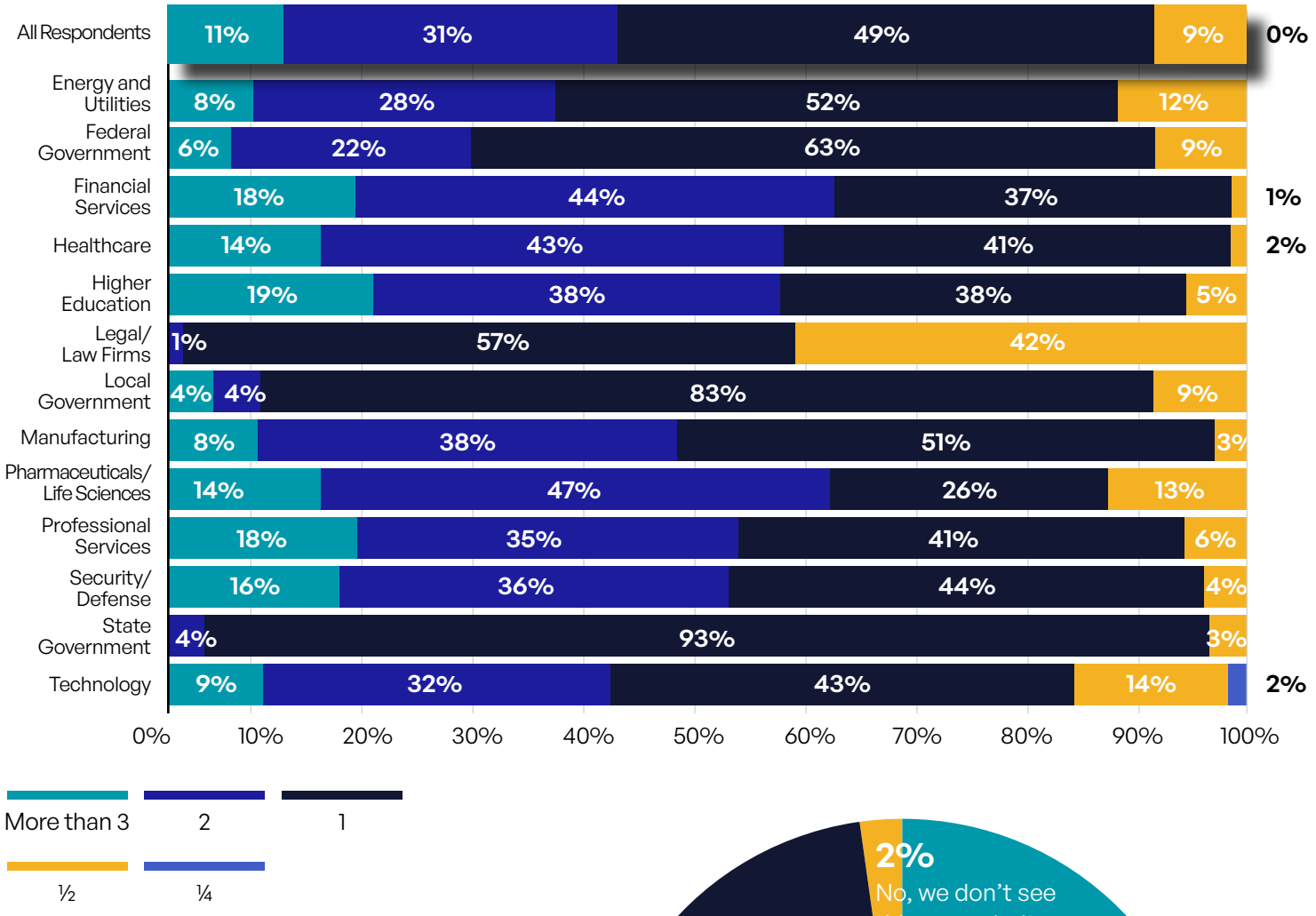


Figure 26: Headcount allocation for tracking and reporting regulatory compliance of sensitive content communications.

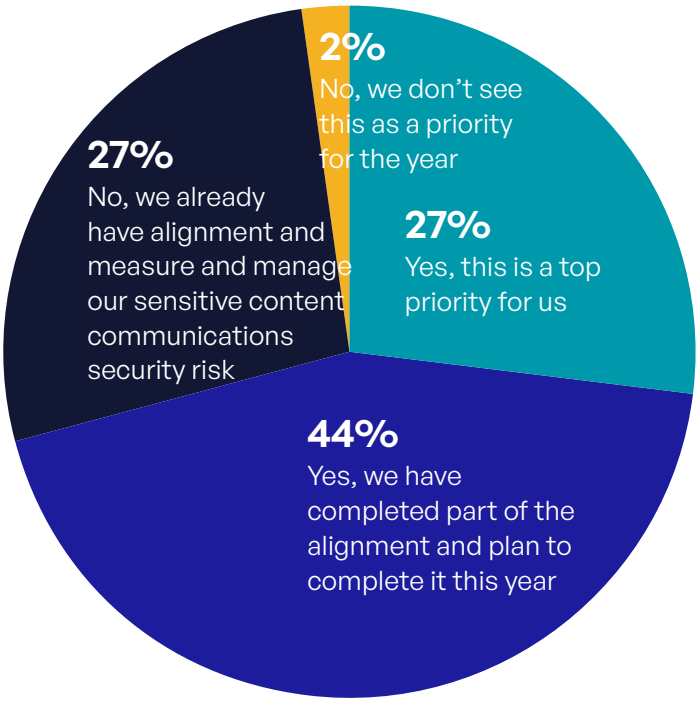


Figure 27: Alignment of risk management strategy and measurement and management of sensitive content communications compliance risk.

Finally, we asked an identical question about compliance to the one about security that we discussed at the end of the prior section. When it comes to alignment of the corporate risk management strategy with content communications compliance strategy, 27% report that the two are already aligned, 44% say that alignment is in process and slated to be completed this year, and 27% say it is a top priority for the coming year (Figure 27).

FedRAMP and CMMC: Keys to Doing Business With the U.S. Government

The United States government is the largest single purchaser of goods and services in the world, and hundreds of thousands of businesses contract with at least one federal agency. Naturally, the government has a vested interest in making sure that its vast supply chain is compliant with security best practices. After all, some of the world's most sensitive data resides on U.S. government systems.

These concerns have led the government to take a global leadership role in developing cybersecurity standards over the years, most notably through agencies like NIST and the Cybersecurity and Infrastructure Security Agency (CISA). Their work has resulted in frameworks that are well on their way to becoming global standards—such as NIST CSF.

These days, two specific standards are front of mind for federal contractors and those who aspire to work with federal agencies—FedRAMP and CMMC.

FedRAMP: Standardized Requirements for Cloud Services

As cloud adoption grew in the private sector, the Office of Management and Budget (OMB) established the Federal Risk and Authorization Management Program (FedRAMP) to provide a standardized approach to cloud security. Published in 2011, all cloud services providers that provide services for federal agencies must comply with FedRAMP—whether they provide Infrastructure-as-a-Service, Platform-as-a-Service, or Software-as-a-Service.

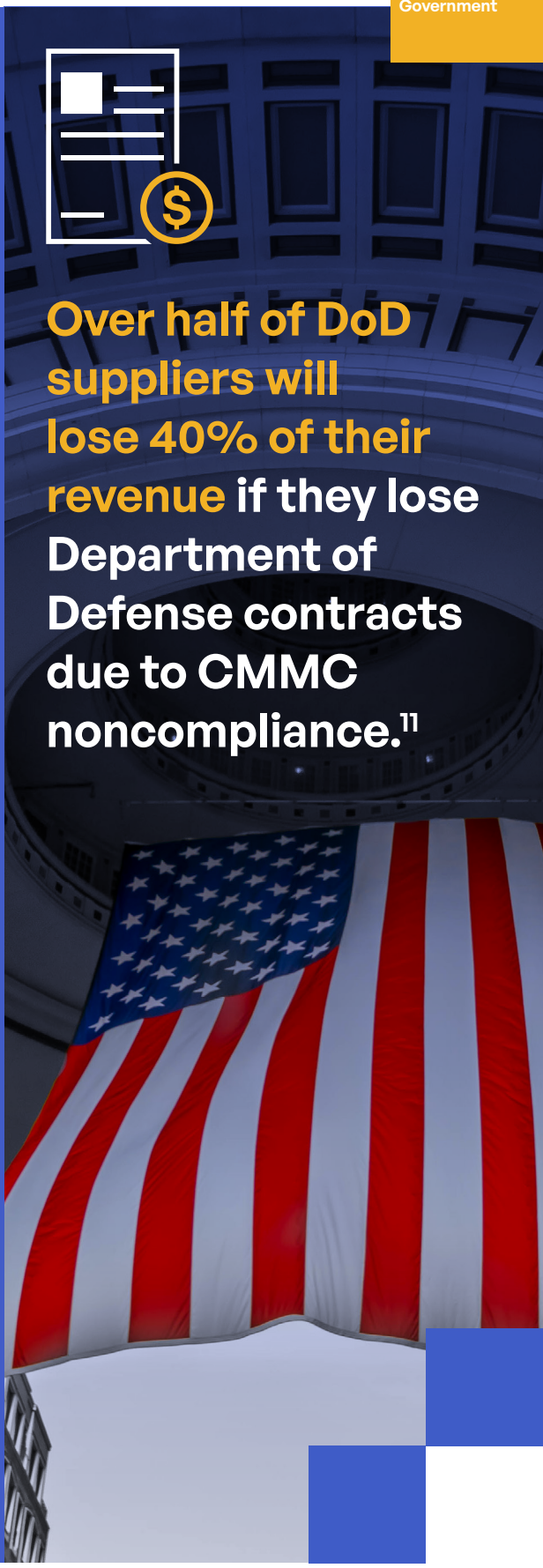
Organizations that hope to secure federal contracts must ensure that all the cloud services they will use in their work for the government are FedRAMP authorized. This includes solutions for sharing sensitive content within an organization and with third parties.

CMMC: Keeping Defense Contractors Secure

Understandably, the Department of Defense (DoD) has reason to put even more stringent requirements on its contractors than other federal agencies. The Cybersecurity Maturity Model Certification (CMMC) is an attempt to do just that. Released in 2020, CMMC 1.0 struggled to get off the ground, mainly because of a shortage of qualified auditors to do the required audits.

To address this problem, CMMC 2.0 was published in May 2023, with a simplified maturity model and less-frequent third-party audits—but the same stringent requirements. CMMC certification is designed to enhance the protection of controlled unclassified information (CUI) and federal contract information (FCI), and the certification applies to all 300,000 DoD contractors.

CMMC 2.0 identifies three maturity levels, and every defense contractor must demonstrate compliance with a specific level according to the level of information they send, share, receive, and store. At every level, controls on the sharing of sensitive content are among the requirements.



Over half of DoD suppliers will lose 40% of their revenue if they lose Department of Defense contracts due to CMMC noncompliance.[11]

Process

Insight: To Put It Nicely, Results Are Mixed on Adherence to Best Practices for Secure Content Communications

No matter to which regulations and frameworks an organization must adhere, being consistent in following established best practices is the best way to protect digital assets. As discussed, this is difficult with sensitive content given the number of third parties it is shared with, the wide array of channels used to transmit it, and the tool soup that organizations deploy to monitor and control it. Our survey includes several questions designed to see how well organizations are faring with the most important controls and procedures.

One question really goes to the heart of the matter. We ask what the typical response is when an encrypted email cannot be decrypted and give respondents three less-than-ideal choices: signing up for a free but unauthorized email service to transmit the content, asking the sender to use an unencrypted but unpublished shared drive link, or asking the sender to send a password-encrypted Zip file.

One would hope that this conundrum would be rare, but it comes up more often than you think since different encryption standards are incompatible with each other. As a result, organizations that do not have automatic decryption in place have few choices beyond these. Among them, the Zip file is at least protected by a password and is likely the best choice.

Among all respondents, half made the best choice and half made a choice that was less good (Figure 28). A higher percentage of respondents in financial services, higher education, law firms, local government, and manufacturing chose the Zip file option.

One piece of good news: When respondents to our 2022 survey answered the same question, only 39% chose the password-encrypted Zip file, while 60% opted for the unencrypted shared drive link. Perhaps this is a sign that respondents are wising up to their bad practices. Regardless, responses reveal that respondents need a different encryption-decryption approach to email to ensure they are not exposed to malicious breaches. Hint: Take a look at Kiteworks' Email Protection Gateway that automates email encryption and makes decryption invisible to users regardless of the encryption protocol supported by the sender and recipient.

Kiteworks Email Protection Gateway

Kiteworks Email Protection Gateway (EPG) makes email encryption invisible to end-users regardless of the encryption standard that is used—S/MIME, OpenPGP, and TLS. Risk and compliance administrators can configure encryption policies centrally and automate key and certificate handling. Kiteworks EPG enables users to work in their normal email clients, encrypting in email clients or gateway rather than via plugins. Private decryption key stays in receiving client with no server-side vendors or attackers able to decrypt it. Security integrations such as DLP, CDR, and antivirus protect bidirectional email privacy and compliance.

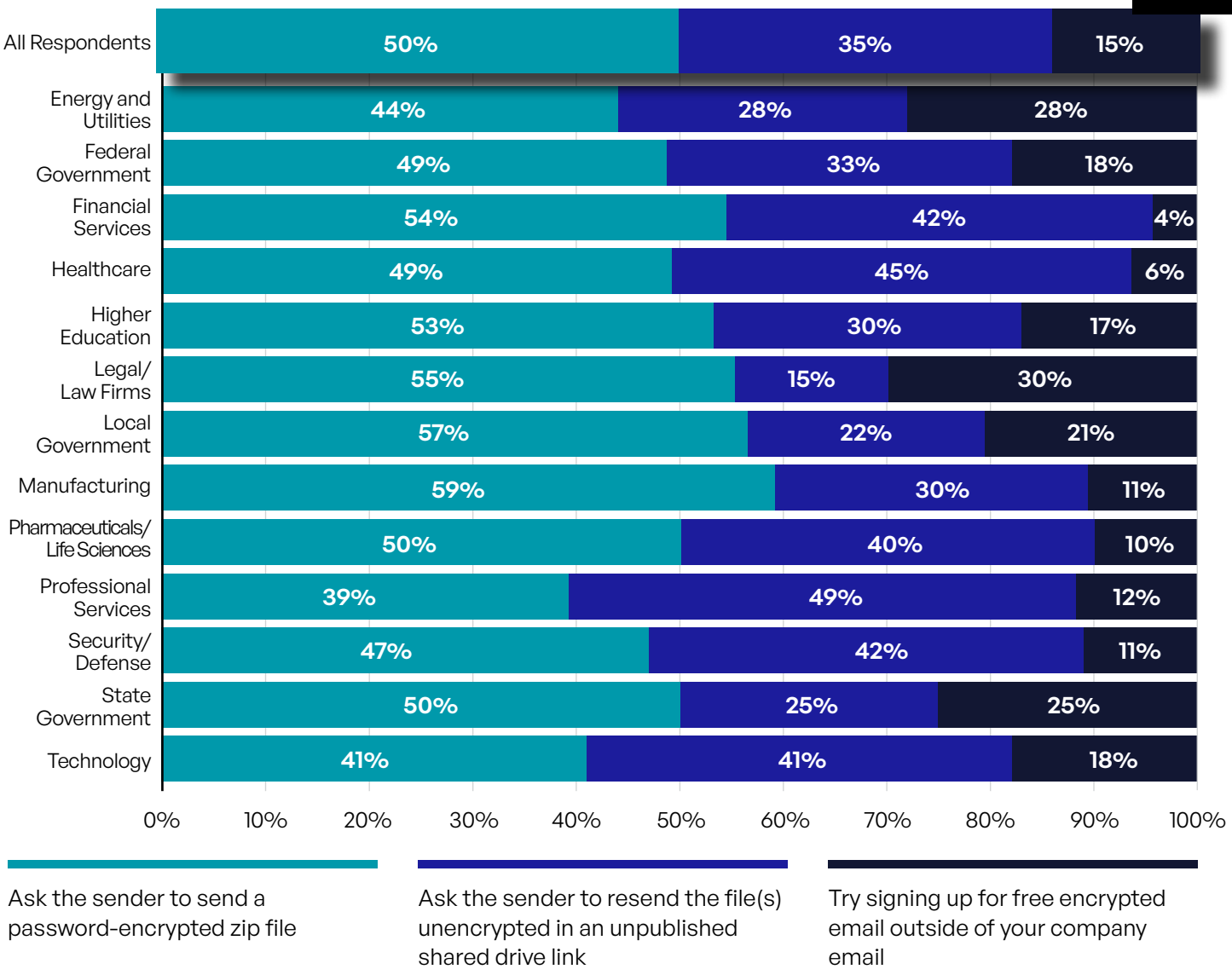


Figure 28: When encrypted email cannot be decrypted.

Zero Trust: A Needed Priority

Our survey moves to several questions about how well respondents are applying a content-defined zero-trust approach to protecting sensitive data. Asked to rank a list of five best zero-trust best practices, all five are seen as important. When we weighted the answers to give more points to higher rankings, least-privilege access comes out on top, followed by tracking and reporting from a compliance perspective (Figure 29).

Least-privilege access ranks even higher among state government (ranked first or second by 64%), legal (58%), and higher education (53%) respondents. Local governments favor configuration audits, with 60% placing that best practice in first or second priority.

Another question involves best practices for ensuring that sensitive content collaboration is secure and unauthorized access does not occur. Again, respondents give similar weight to each of the seven best practices listed (Figure 30). Slightly more respondents favor multi-factor authentication (33% as first or second priority) and an application-level firewall (31%).

However, different industries have different priorities in this regard. Digital rights management (DRM) is a favored best practice in the energy and utilities industry, while data encryption is favored in that industry and in higher education, local government, and state government. Technology and security and defense companies have high regard for monitoring user access and document activity.

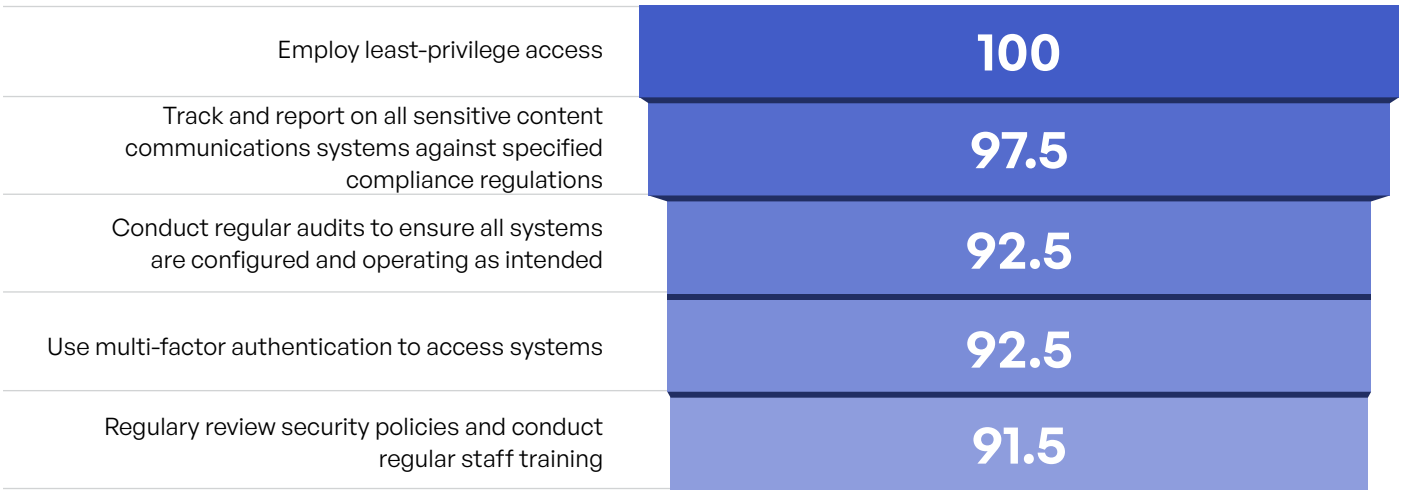


Figure 29: Weighted scoring: Policies and procedures for protecting privacy and compliance of sensitive content communications.

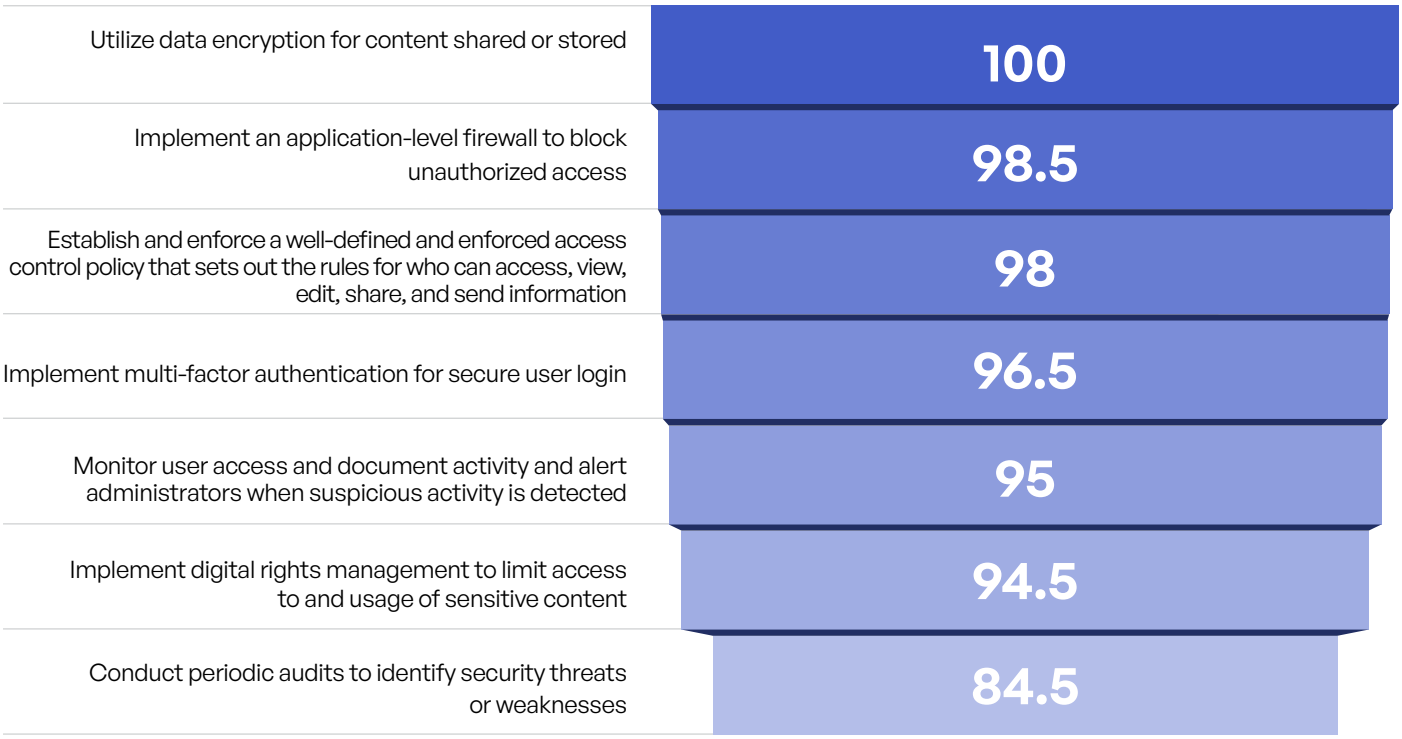


Figure 30: Policies and procedures for ensuring that sensitive content collaboration is secure and unauthorized access of content does not occur.

Tracking, Recording, and Reporting on Governance, Compliance, and Security (Try to Say That Three Times Fast)

When it comes to tracking and recording third-party access to sensitive files and folders, our survey results worsened considerably compared with 2022. This year, just 22% report they do this tracking across all departments (Figure 31). And while 97% of organizations do some tracking, three-quarters do not do it for all departments or content types—or are inconsistent in applying it generally. Our 2022 results showed 49% of respondents having deployed full tracking and reporting. It makes us wonder whether some in last year's cohort were claiming undeserved credit! A few industries—financial services, manufacturing, and pharmaceutical/life sciences—did somewhat better but still had fewer than one-third of organizations with this best practice fully in place.

Another level of tracking and reporting involves communication with executive management and the board of directors. Most respondents (83%) report they have an annual cadence of reporting to the C-suite on security and compliance risk for sensitive content communications (Figure 32). In the healthcare, manufacturing, and professional services industries, more respondents (between 27% and 30%) indicate they do such reporting on a quarterly basis. (Note: For the 2022 report, respondents were allowed to mark more than one answer. 15% marked both Yes, but only for certain departments and Yes, but only for certain content types.)

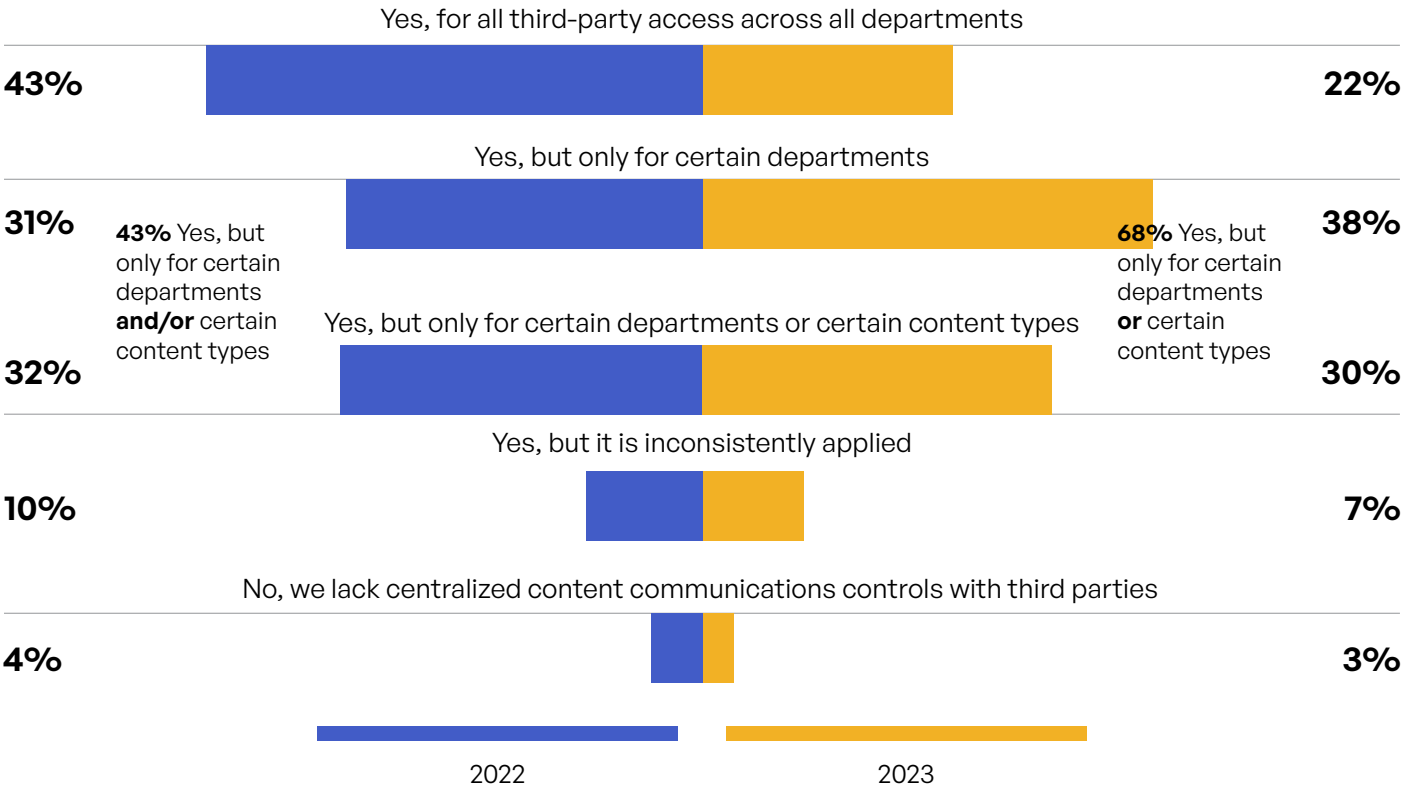


Figure 31: Track and record third-party access to sensitive files and folders.

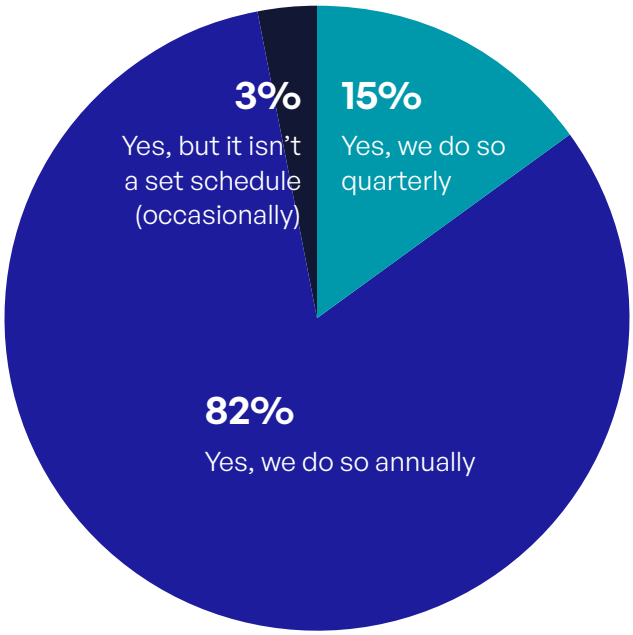


Figure 32: Track and report on security and compliance risk for sensitive content communications to C-suite.

The Door Isn't Fully Locked: Controls That Restrict Access

Unfortunately, as with tracking and recording access to sensitive content, many organizations are inconsistent about controlling such access. When asked whether their organizations manage or restrict third-party access to folders with capabilities such as content permissions, expiration, locking, and versioning, only one-quarter of respondents can claim to do so across all departments and content types (Figure 33). This leaves three-quarters of organizations with gaps in these controls or no controls at all. Talk about leaving the door unlocked to the chicken coop!

Even with the stringent requirements of GDPR, European respondents do only slightly better than the overall cohort, with 29% reporting full protection of sensitive content folders across the organization. The healthcare, pharmaceutical/life sciences, and manufacturing industries do somewhat better, with 36% to 38% of organizations fully covered.

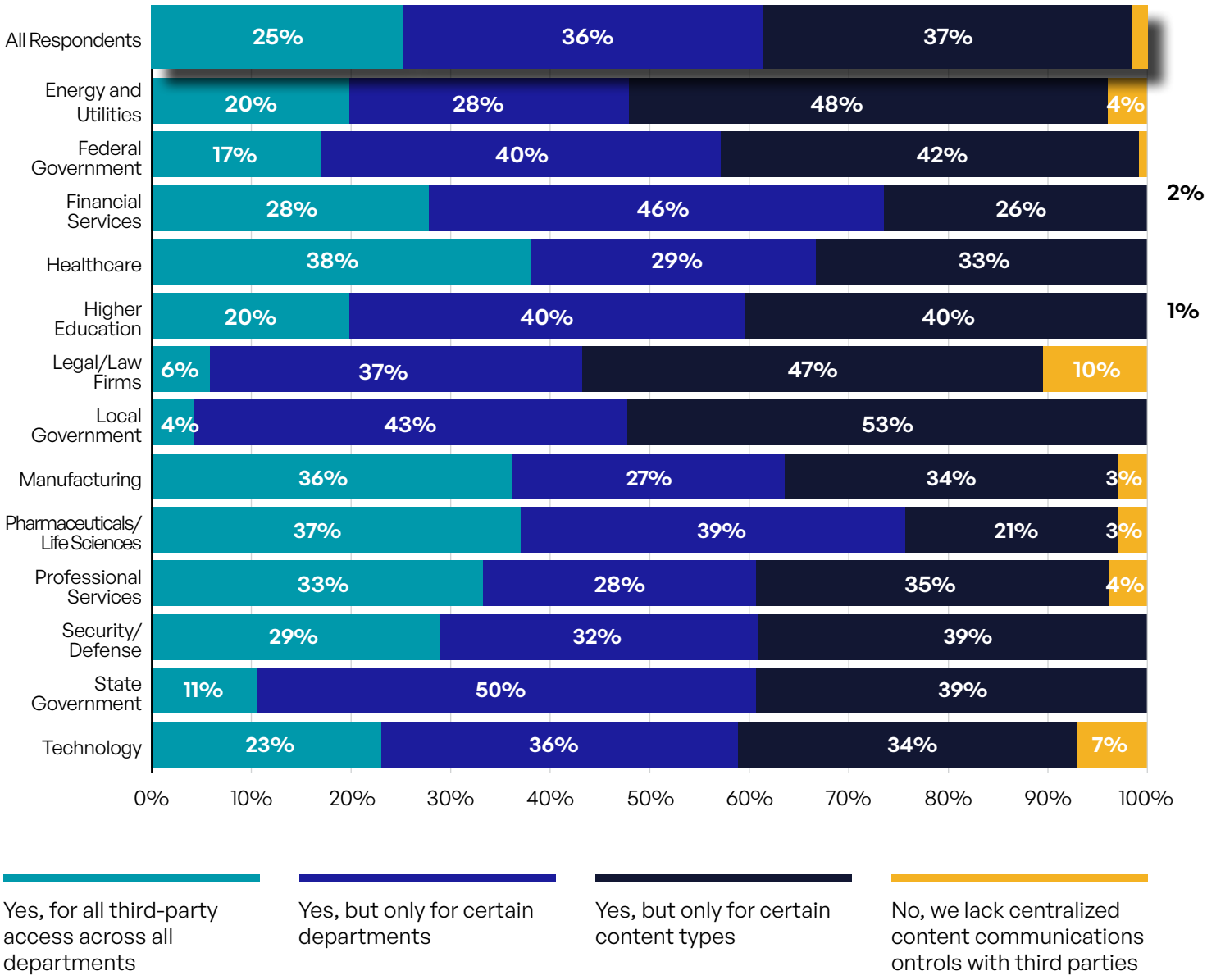
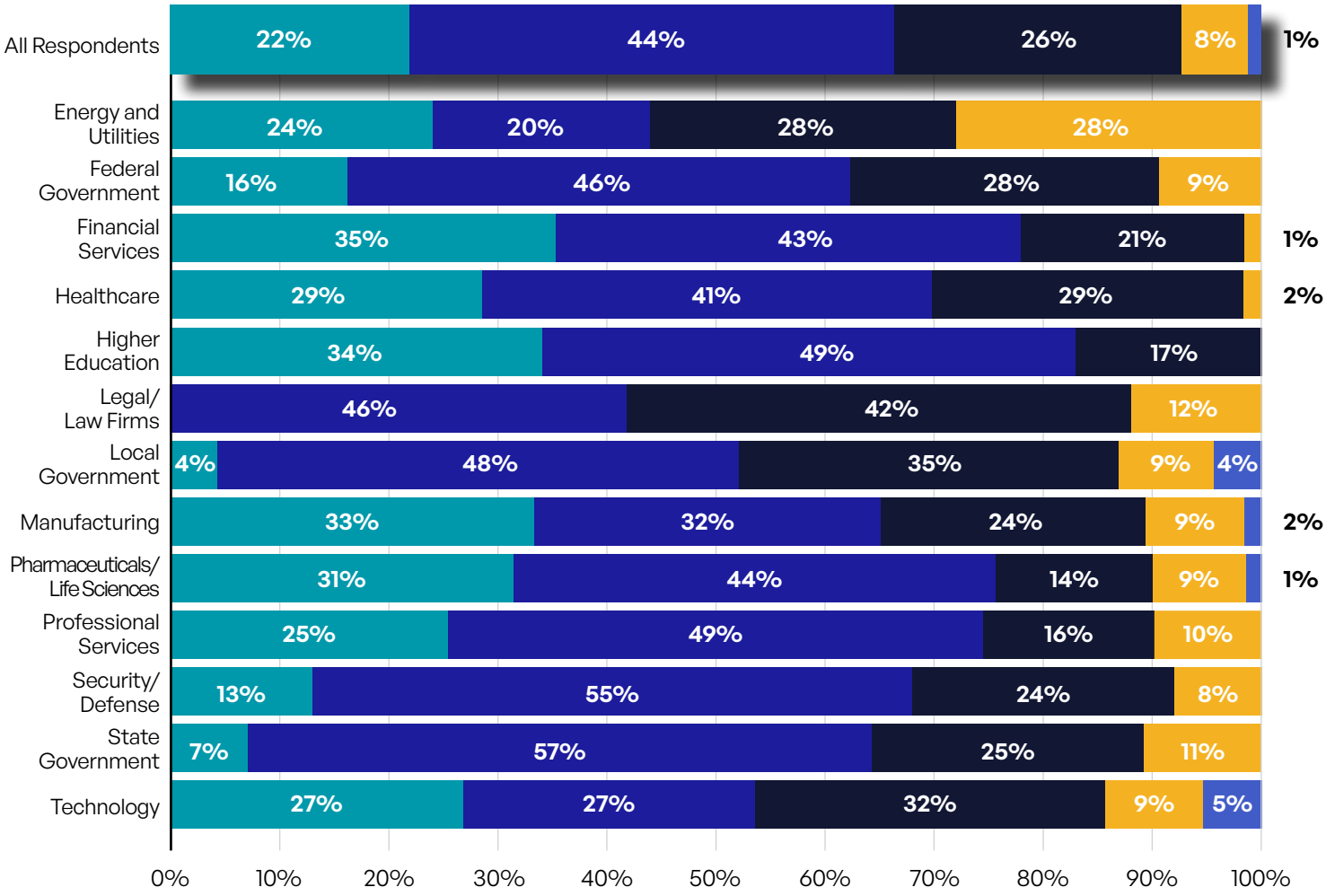


Figure 33: Manage or restrict third-party access to folders (using content permissions, expiration, locking, and versioning, etc.)

Another factor that grows in urgency every year is ensuring that access controls for sensitive content cover both on-premises and cloud-based infrastructure. This year, only 22% of respondents report having these protections in place both on-premises and in the cloud (Figure 34). Some industries do slightly better, with one-third or more reporting controls across the entire infrastructure in financial services, higher education, and manufacturing. On the other hand, government at all levels and security and defense firms all report 16% or lower compliance with this best practice—while none of the law firms we surveyed have achieved this level of protection.



Yes, we have administrative policies for tracking and controlling sensitive content collaboration and communications on-premises and across the cloud

Yes, we have administrative policies for tracking and controlling sensitive content collaboration and communications on-premises but not in the cloud

Yes, we have administrative policies for tracking and controlling sensitive content collaboration and communications in the cloud but not on-premises

Yes, but the policy tracking and controls are at the individual content owner's level and not at an administrator level

No, we do not have the ability to apply policy tracking and controls for sensitive content communications

Figure 34: Policies and systems for tracking and controlling access to sensitive content and to whom it is sent and shared.

Will There Ever Be a U.S. GDPR ... or Even a Global Standard?

Data harvesting has been a lucrative—and legal—business in the United States since the advent of the internet. Personally identifiable information (PII) of just about every kind has been fair game, and it is next to impossible for individuals to have their personal data removed from all such databases.

One longstanding exception to this "Wild West" scenario in the U.S. is protected health information (PHI), which has been regulated since 1996 through the Health Insurance Portability and Accountability Act (HIPAA). At the time of its passage, President Clinton had hoped to enact comprehensive healthcare reform but had to settle for a bill that makes health plans more portable as people move from job to job.[12] Less publicized at the time were the "accountability" provisions in the law, which mandate that the Department of Health and Human Services implement and maintain standards for the use and sharing of healthcare information.

Ever since the European Union passed its General Data Protection Regulation (GDPR) in 2016, advocates have argued for a similar regulation in the U.S. But in today's political climate, it is rarely an unsafe bet to assume that new laws will not be passed, regardless of the topic. There have been efforts in Congress to enact at least some GDPR-like requirements, but these have failed to gain traction.[13]

This is one reason why individual states are taking matters into their own hands. Nine states have passed electronic data privacy laws in the past five years, and 10 additional states have legislation in process.[14] This emerging patchwork of requirements may be enough to inspire Congress and the executive branch to act so that there is a single national standard.

In the meantime, global organizations have been working to find a framework that can bring operational consistency across all geographies while enabling compliance with the regulatory requirements of all jurisdictions. Increasingly, they are settling on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) as a set of best practices that works everywhere.[15] Ironically, while the U.S. government has not managed to enact regulations to protect PII, a framework created by a U.S. government agency is being adopted globally.

Fines assessed under GDPR in 2023 exceed the fines levied in 2019, 2020, and 2021 combined.[16]

Cyber Exploits

Insight: Bad Day at the Office—Many Exploits Are Occurring With Sensitive Content Communications

The ultimate goal of any cybersecurity effort is to minimize the number of successful attacks or exploits by adversaries of all types. When we ask respondents how many exploits they suffered over the past 12 months around sensitive content communications specifically, the results are not encouraging. Overall, 84% of respondents report experiencing four or more exploits over the past year, and 36% report more than seven (Figure 35). When the cost of a successful exploit is factored into consideration, these numbers become even more alarming.

Some industries saw even higher averages: healthcare, financial services, security and defense, manufacturing, and professional services all saw more than 90% of organizations with four or more exploits. And more than half of financial services, healthcare, and higher education organizations saw more than seven security incidents around their sensitive content communications.

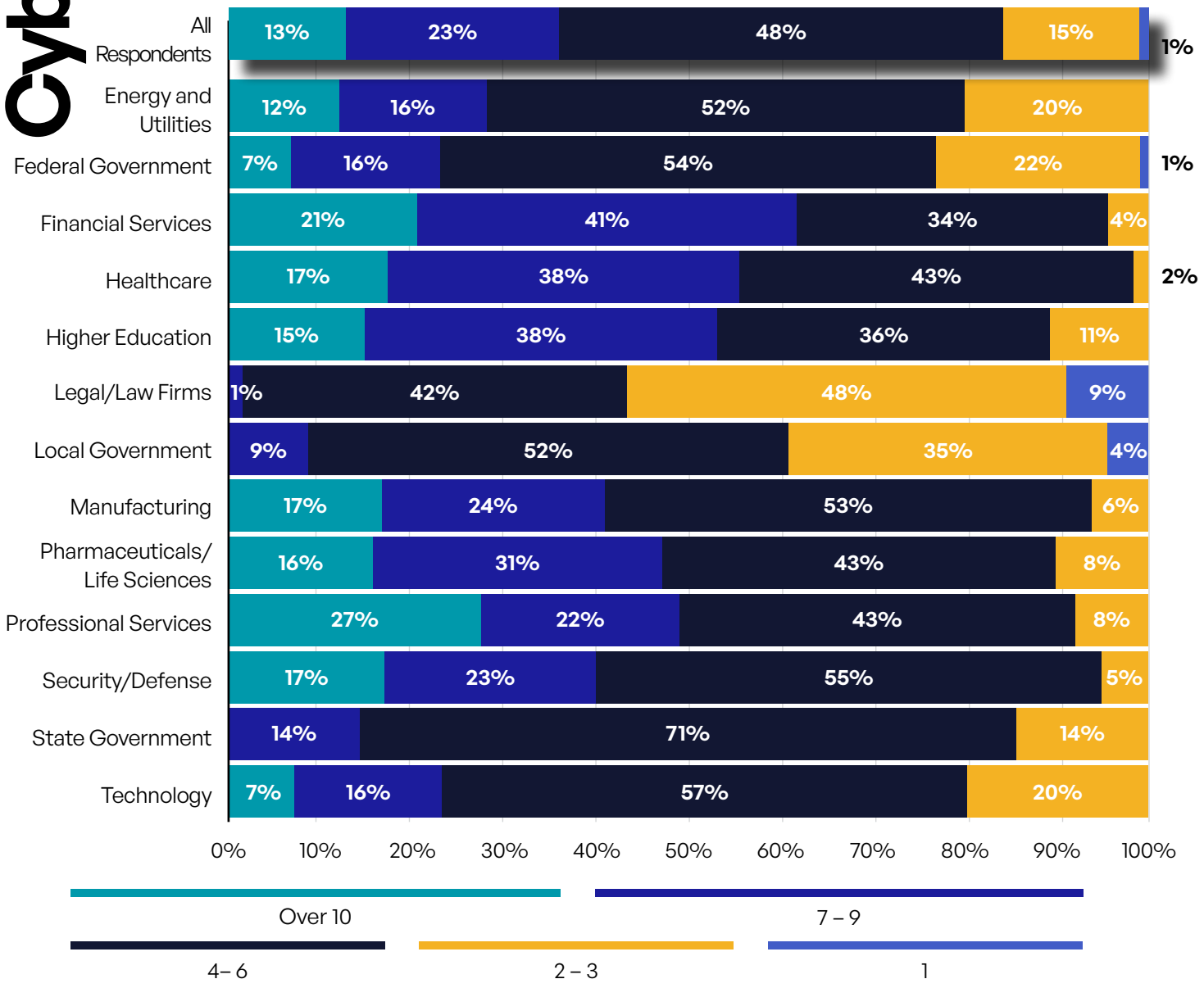


Figure 35: Exploits of sensitive content communications in past year per industry segment.

Impact of Sensitive Content Communications Exploits

The impact of these exploits is not trivial. Among all respondents, 62% report financial implications from at least one of the exploits, while 44% suffered brand impact and 42% were assessed compliance penalties and fines (Figure 36).

Interestingly, more respondents in several verticals saw financial implications—federal and local governments (each 76%), law firms (72%), and technology companies (74%). And brand impact is disproportionately felt by manufacturing (69%), higher education (64%), healthcare (59%), and pharmaceutical/life sciences firms (59%).

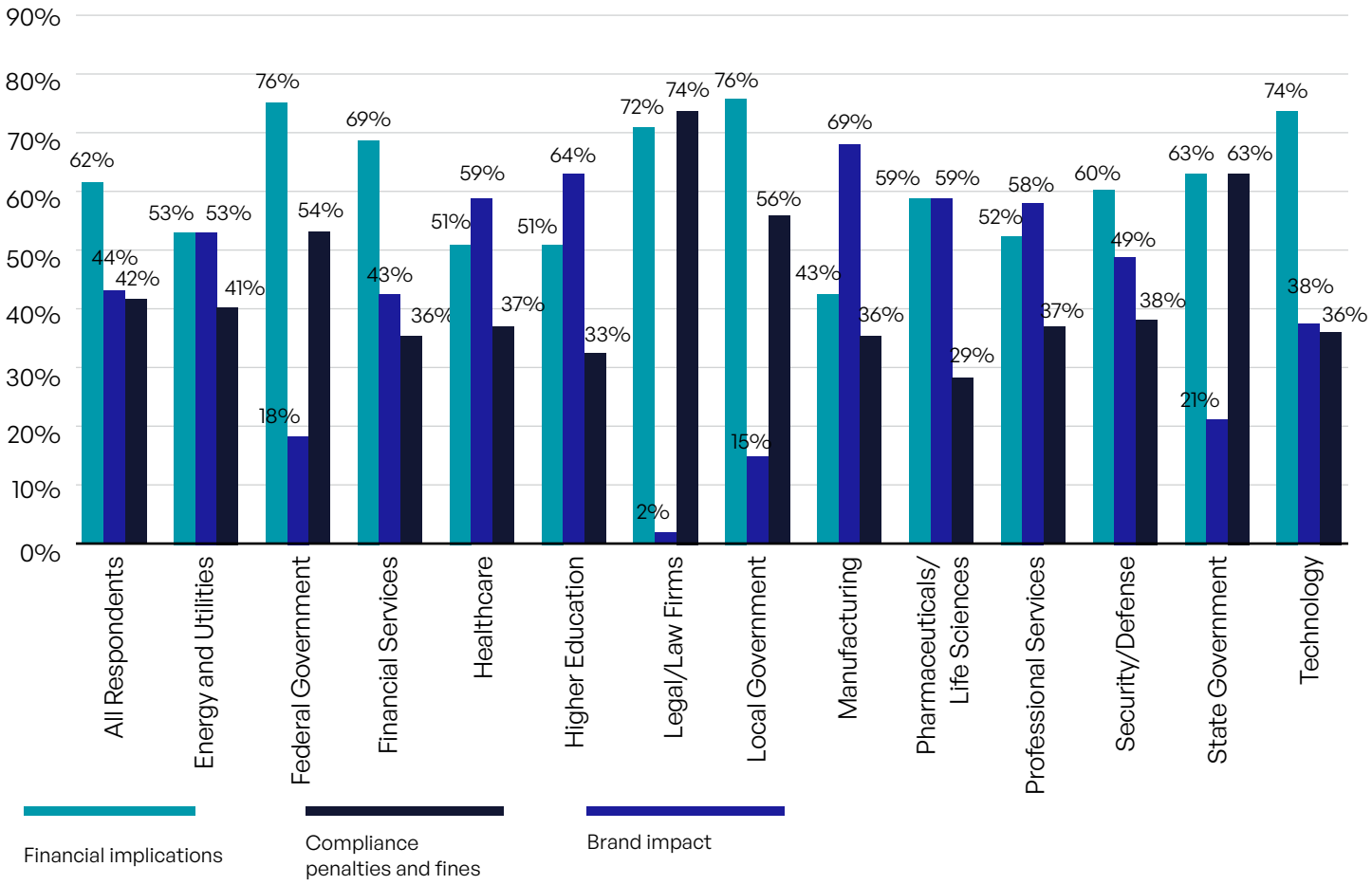


Figure 36: Organizations impacted by sensitive content communications breach in past year by industry segment.

Digital Rights Management

Insight: DRM Is Necessary, But the Journey Is in Its Early Stages

Segmentation is key to protection of sensitive data of every type. If everyone in an organization has access to all data, this increases the risk of accidental or deliberate disclosure of sensitive information. When third parties have access to a company's data, the risk multiplies exponentially. But if digital assets are segmented so that only those who need the data can access it, risk is reduced significantly, and organizations can achieve compliance with different regulations and standards. This is a core component for an approach known as digital rights management (DRM).

For DRM to be successful, comprehensive, detailed data classification is critical. This is because a roles-based approach to access requires definition of what each role requires in terms of access. When we ask respondents the simple question of whether they classify their data, 93% say they do (Figure 37). So, this is good news.

Lots of Business Drivers for Classification

Reported business drivers for data classification are diverse, with seven of the eight drivers listed being ranked number 1 by at least 10% of respondents (Figure 38). Protecting PII seems to be the top priority, with compliance with PII regulations (35%), protecting employee PII (27%), and compliance with third-party PII regulations for customers and partners (26%) most cited among the top two priorities. But the protection of PHI and intellectual property—and compliance with a variety of industry regulations and standards—are common priorities as well.

Another business driver for data classification is which employees need offline access to sensitive content. 98% of respondents have the need to provide offline access to executives, board members, and field workers, while 92% need the same for their sales and customer success teams. Company executives who travel were the most important priority, ranked first by 41% of overall respondents (Figure 39), as well as a strong plurality in all company size categories and most industries.

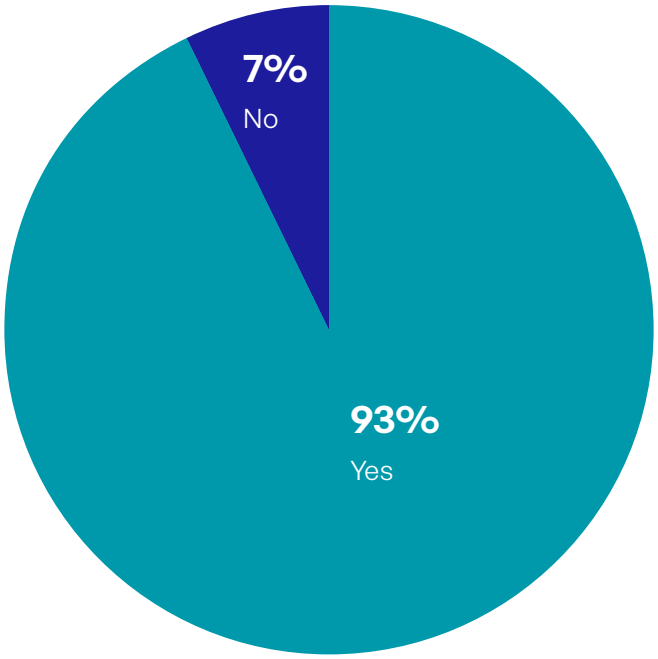


Figure 37: Organizations that classify sensitive content.

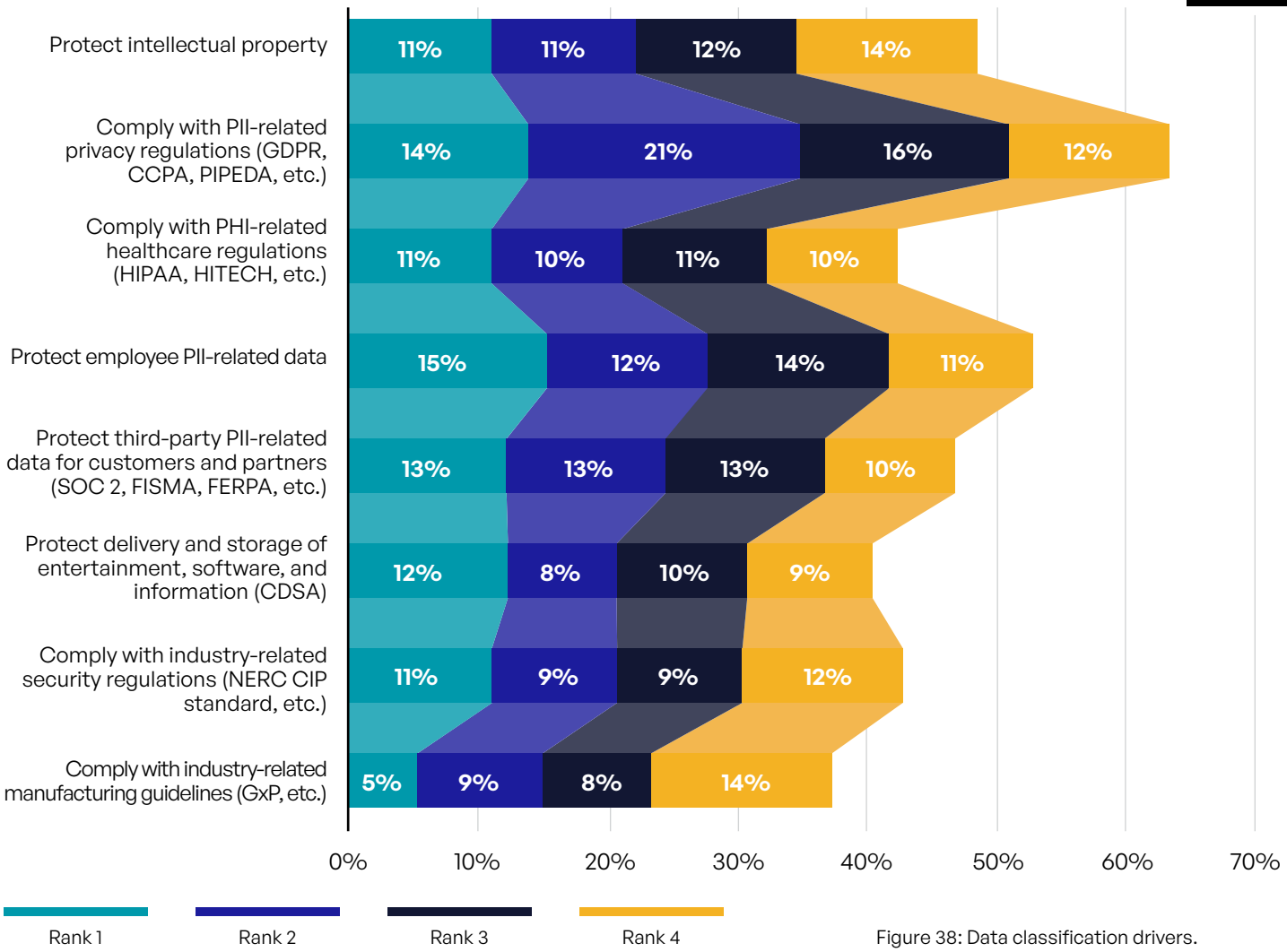


Figure 38: Data classification drivers.

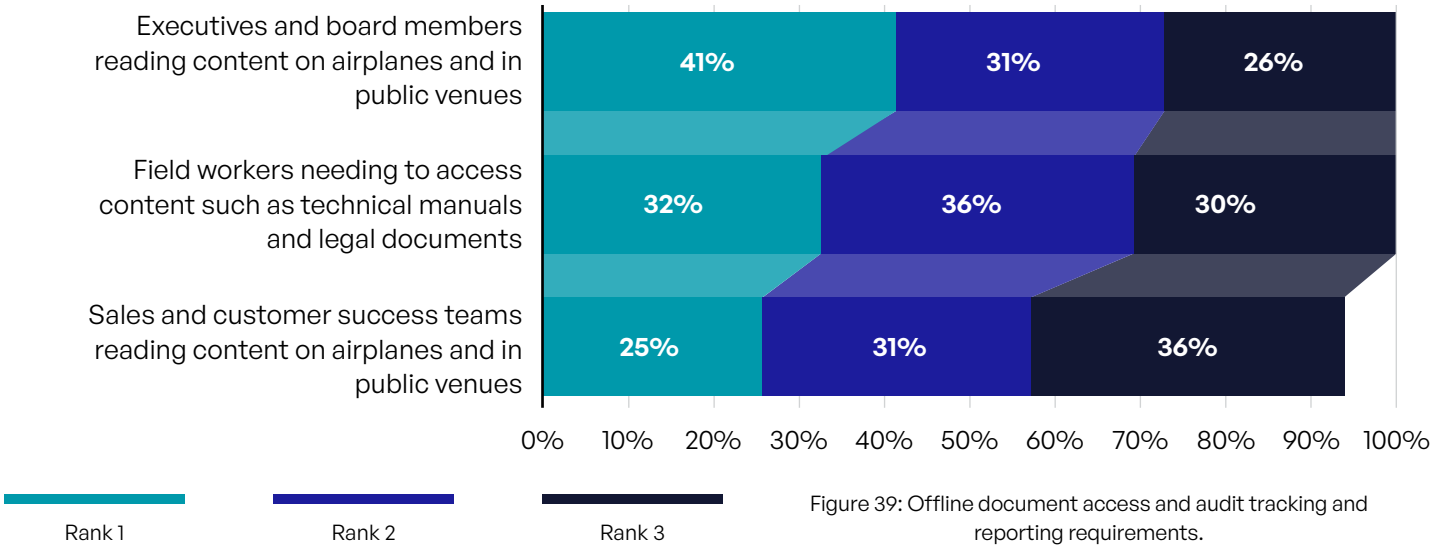


Figure 39: Offline document access and audit tracking and reporting requirements.

Requirements for—and Barriers to—DRM Deployment

Requirements of frameworks like NIST CSF and the need to better protect sensitive content mean that many organizations recognize the need to move beyond simple data classification and controls. To move to the next level, they are beginning to embrace a DRM. DRM tools can be used to protect sensitive content as it is shared with third parties. DRM is not new but dates back decades. Unfortunately, most DRM efforts and projects fail to deliver on their promises. The needed level of governance and security is lacking and protection of the digital assets is insufficient against internal and external threats.

We asked respondents about their biggest requirements for a DRM solution and asked them to rank six possible answers. As with many of our ranking questions, responses were spread out. When they are weighted, ease of use comes out as the winner in a photo finish, followed by protection of the company's "crown jewels" and complete and comprehensive audit log tracking (Figure 40).

When asked about the stumbling blocks experienced in deploying DRM, the choice most cited as a top-two problem (by 55% of respondents) is finding a tool with the ability to align with compliance standards by tying access to users, roles, and content classes (Figure 41). Also widely cited were the need for agents on third-party clients to open unencrypted content (53% in the top two) and the need to be able to view and edit any kind of content (50%).

Holistic compliance features are an even bigger stumbling block for energy and utilities (72% in the top 2), legal (62%), state government (61%), technology (61%), and professional services (60%) organizations. The need for agents is especially burdensome for professional services (70%), local government (69%), and technology (61%) respondents.

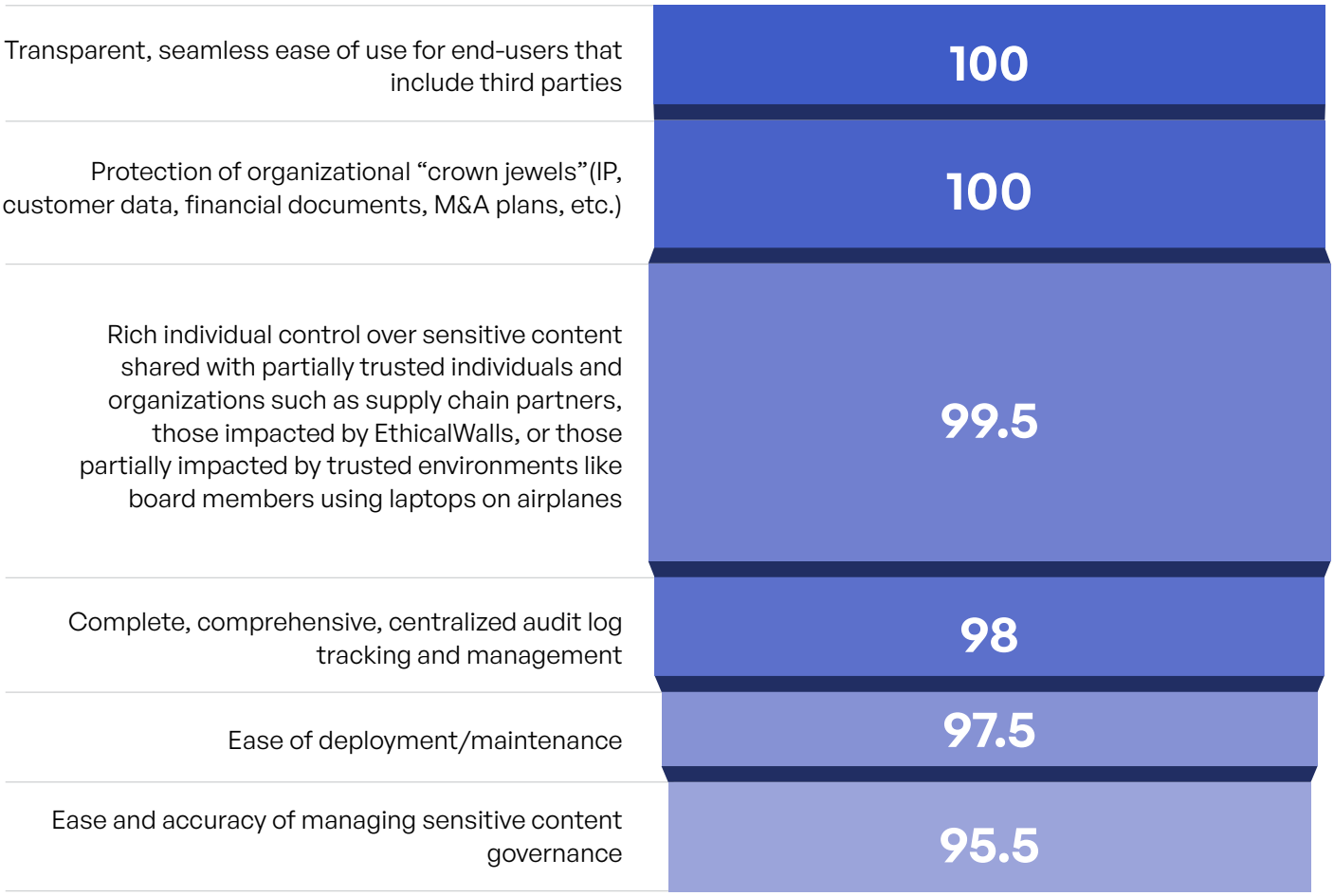


Figure 40: Weighted scores: Biggest DRM challenges for sensitive content communications.

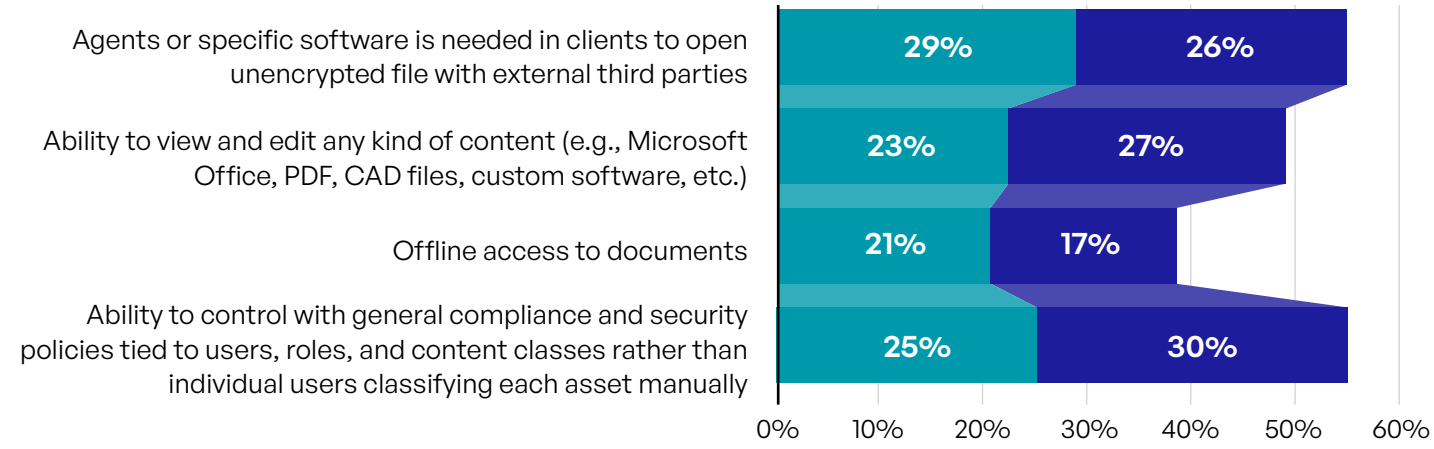


Figure 41: Biggest stumbling blocks with DRM/eDRM.

NIST CSF and DRM: Best Practices for Sensitive Content Communications

As we have made clear, NIST CSF is becoming a de facto global standard—despite the fact that it was developed by the United States government to address cybersecurity at U.S. organizations. As one observer noted, NIST CSF has become the "common language for international cybersecurity."[18]

The existence of a common framework opens up an exciting possibility—the ability to track and control all sensitive file and email data communications in a single platform with policies built around this framework. This can enable a content-defined zero-trust approach that allows administrators to track and control access to specific content classes according to roles—or even individual users—in a way that is compliant with NIST CSF and a wide variety of other requirements.

Such a platform can unlock the next generation of digital rights management (DRM). According to Gartner, DRM has three elements:[19]

- **It has a cryptographic element:** Information is encrypted so that protection travels with data no matter where it moves or rests.
- **It has an identity element:** Users must be authenticated and match policies related to specific user roles and groups before accessing rights-protected data on any system.
- **It has a granular usage control element:** Users are granted specific rights within applications (such as the ability to only view, edit, print, copy/paste, or screen capture sensitive information).

This could enable organizations to take control over the third-party information supply chain—which our data shows has thousands of links at most organizations. They can take control of sensitive content security as it is shared across any and all channels, including email, file sharing, managed file transfer, and web forms.

Putting All the Pieces Together

We're optimists and anticipate seeing incremental improvements in privacy and compliance risk as it relates to sensitive content communications each year when we publish our Sensitive Content Communications Privacy and Compliance Report. While we saw improvement in some areas this year, we witnessed too many data areas that are languishing or even got worse (ouch!). For example, nearly three-quarters of organizations still say they need to make improvements in measuring and managing security and compliance risk. An even higher percentage of respondents—78%—do not yet track and control sensitive content communications both on-premises and in the cloud, nor for all content types in all departments.

This comes at a time when the need for action is urgent. Threat actors are increasingly targeting sensitive content with their exploits, and their tactics are becoming more sophisticated. At the same time, humans demonstrate their humanity all too often—accidentally posting sensitive content publicly or to a set of people with no need to know. In response to this rapidly advancing threat landscape, regulators are developing more stringent requirements and launching all of us—like it or not—into an Era of Compliance.

Unfortunately, financial constraints and the cybersecurity skills shortage mean that it is impossible to throw human resources at the problem—if that would even work. Organizations have no choice but to battle an increasing volume of threats and achieve greatly expanded compliance objectives with the same staffing they've had all along. It is a daunting task for every organization.

There are a few hopeful signs. As we analyzed our survey results, we saw signs that leaders and practitioners recognize problems in the security and compliance of their sensitive content communications—and are prioritizing getting them solved. This is clearly a work in progress, but we believe that next year's report will show that organizations have a better handle on this problem, and are addressing it with both efficiency and effectiveness.

Since the security of sensitive content communications has fallen through the cracks in the past at many organizations, those that take it seriously have the opportunity to make a big contribution in the coming year in improving their overall risk profile. Important areas of focus for 2023 should include:

- **A holistic approach to compliance:** As a patchwork of rules comes online in different jurisdictions—including from state to state in the U.S.—organizations need to shift their focus. In our new Era of Compliance, organizations need to stop focusing on the checkboxes of each individual regulation, and adhere instead to universal best practices that enable compliance with all of them. We believe the best approach is to adopt a universal framework like NIST CSF, and work to deliver full compliance with all of its elements. This leads to DRM.
- **Taking a DRM approach:** It is critical that organizations take a holistic approach to categorizing data in a granular way, and making each category easily available to those who need it to perform their duties according to role—and unavailable to all others.
- **Insider threat protection:** Employees and others with access to internal systems are responsible for nearly one in five of data breaches.[21] By classifying and segmenting data and restricting access to specific data types by role, organizations can protect against malicious, well-intentioned, and accidental data disclosure by insiders.
- **Comprehensive security protections:** Cybercriminals and rogue nation-states recognize the value of sensitive content and are targeting vulnerabilities and gaps in security regimens employed by communication tools used to send and share that information. Understanding and vetting the security capabilities of your communication tools are critical. Reviewing these against top priorities found in this report is a great starting point.

For organizations to operate, they often must share sensitive content with hundreds or thousands of third parties—not to mention enable internal first parties to send, share, collaborate, and store that information. The movement of this data presents tremendous risk, and securing these transfers in the Era of Compliance should be a priority at every organization. Securing sensitive content communications should be a priority alongside network, endpoint, and application security—and the security of data stores where sensitive content is at rest.

At many organizations, this remains one of the biggest security gaps they face. The Kiteworks Private Content Network (PCN) unlocks advanced DRM by helping organizations track and control all sensitive file and email data communications in a single NIST CSF-aligned platform.

References

[1] "M-Trends 2023," Mandiant, May 2023.

[2] "2023 Data Breach Investigations Report," Verizon, June 2023.

[3] Ibid.

[4] Graham Greenleaf, "Now 157 Countries Have Data Privacy Laws," UNSW Law Research, March 15, 2022.

[5] "US State Privacy Legislation Tracker," International Association of Privacy Professionals, updated June 9, 2023.

[6] "2023 Data Breach Investigations Report," Verizon, June 2023.

[7] For our "weighted scores" to several ranking questions in this report, we gave 8 times the weight to #1 rankings compared with #4 rankings. Rankings of #2 and #3 received 4 and 2 times the weight of #4 rankings, respectively. The rankings were calculated on a 100-point scale.

[8] "2023 Data Breach Investigations Report," Verizon, June 2023.

[9] Carly Page, "Hackers Launch Another Wave of Mass-hacks Targeting Company File Transfer Tools," TechCrunch, June 2, 2023; "GoAnywhere MFT Hack Impacts Up to 1 Million Community Health Systems Patients and Growing Gootloader Attacks," Defensorum, February 18, 2023.

[10] "The State of Cloud-Native Security Report 2023," PrismaCloud and Palo Alto Networks, accessed June 15, 2023.

[11] "Defenseless: A Statistical Report on the State of Cybersecurity Maturity Across the Defense Industrial Base (DIB)," Cybersheath Cybersecurity Report 2022, December 2022.

[12] "The History of HIPAA," Accountable, April 7, 2021.

[13] Elizabeth Schultze, "The U.S. Wants to Copy Europe's Strict Data Privacy Law—But Only Some of It," CNBC, May 23, 2019.

[14] "US State Privacy Legislation Tracker," International Association of Privacy Professionals, updated June 9, 2023.

[15] Willem Hendrickx, "NIST's Cybersecurity Framework Has Become the Common Language for International Cybersecurity," SC Media, May 19, 2022.

[16] Martin Armstrong, "Data Protection Fines Reach Record High in 2023," Statista, May 23, 2023.

[17] "M-Trends 2023," Mandiant, May 2023.

[18] Willem Hendrickx, "NIST's Cybersecurity Framework Has Become the Common Language for International Cybersecurity," SC Media, May 19, 2022.

[19] John Girard and Marc-Antoine Meunier, "Succeed With Digital Rights Management, Five Steps at a Time," Gartner, November 21, 2018.

[20] "Global Cybersecurity Outlook 2023," World Economic Forum and Accenture, January 2023.

[21] "2023 Data Breach Investigations Report," Verizon, June 2023.

Kiteworks