Kiteworks

2024

Kiteworks Sensitive Content Communications Privacy and Compliance Report

Communication Tool Proliferation, Data Exchanges With Third Parties, and Lack of Governance Increase Risk

Table of Contents

3 Foreword

4 Executive Summary

5 Introduction
- 5 Security Risks
- 6 AI Cyber Risks
- 6 Compliance Risks
- 6 Human Risks
- 8 Methodology for This Study

9 Insights on Privacy and Compliance of Sensitive Content Communications

9 Cyberattacks and Data Breaches
- 9 Insight: Sensitive Content Communications Are Breached Too Frequently
- 11 Litigation Cost of Data Breaches

13 Data Types and Classification
- 13 Insight: Unable to Track and Control All Their Data Exchanges
- 15 Assessing the Risks of Data Types

18 Compliance and Risk Management
- 18 Insight: Compliance and Risk Management Is a Pressing Priority
- 20 Areas of Focus for Regulations
- 21 Areas of Focus for Validations and Certifications
- 24 Challenges With Compliance Reporting

26 Cybersecurity and Risk Management
- 26 Insight: Protecting Sensitive Content Communications Remains a Big Challenge
- 28 Progress Toward Zero Trust
- 29 Advancing Security to Protect Sensitive Content
- 30 Tracking, Classifying, and Controlling Sensitive Content Access
- 32 Using Security Tools for Sensitive Content

33 Operational Processes
- 33 Insight: It Takes a "Village"—and a Lot of Time—to Manage Data Security and Compliance
- 33 Third-party Multiplication and Risk
- 35 Proliferation of Communication Tools and Risk
- 37 Log Reconciliation That Adds Up
- 38 File Size Limits and Risk
- 39 Biggest Drivers to Address Sensitive Content Communications Risk

40 Conclusion

41 Survey Findings

83 References

Foreword

We are pleased to present the 2024 Kiteworks Sensitive Content Communications Privacy and Compliance Report. This comprehensive report provides invaluable insights into the current state of sensitive content protection and the challenges organizations face in safeguarding their critical information assets.

Today, the protection of sensitive content has become more critical than ever. As organizations increasingly rely on digital communication and collaboration and their third-party ecosystems grow, the risks associated with data breaches continue to escalate. Our report highlights the trends and challenges that organizations must navigate to ensure the security and compliance of their sensitive content.

Malicious events from the past year ratcheted up risks associated with third parties and the software supply chain (e.g., the MOVEit and GoAnywhere managed file transfer data breaches). Accordingly, Verizon, in its 2024 Data Breach Investigations Report (DBIR), highlighted a staggering 68% increase in data breaches connected to third parties, which now account for 15% of all incidents. At the same time, personal data is the target of most cyberattacks, leading government and industry bodies to double-down on instituting additional data privacy regulations—all which makes data security and compliance increasingly more complex and difficult to achieve.

On that note, as cross-analysis of our survey data shows, proliferation of communication tools used to send and share sensitive content, as well as a continued broad universe of third parties with which sensitive content is exchanged, remain critical risk factors. Failure to vet communication tools to ensure they employ advanced security capabilities is also a salient takeaway in the survey findings. Ultimately, the proof is in the survey "pudding": Data breach rates and litigation costs are significantly higher for organizations that rely on higher numbers of communication tools, exchange sensitive content with larger numbers of third parties, and fail to employ advanced security technologies.

While we are certainly a bit biased, we believe the Kiteworks Private Content Network can help organizations overcome these challenges—safeguarding email and file data communications while enabling organizations to demonstrate compliance with various data privacy and cybersecurity compliance mandates. We hope you find the data insights and takeaways in this year's report informative and actionable. And as always, we welcome your comments and suggestions.

Sincerely,

Patrick Spencer

Patrick Spencer, Ph.D.
VP of Corporate Marketing and Research
Kiteworks

Executive Summary

Our Sensitive Content Communications Privacy and Compliance Report provides IT, cybersecurity, and risk and compliance leaders with data insights from their peers. The objective is to help you ensure the sensitive content you send and share through various communication channels, such as email, file sharing, managed file transfer, secure file transfer protocol (SFTP), and web forms, is protected. At the same time, this helps ensure your sensitive data shares and sends remain compliant with various data privacy regulations and moreover your communication systems adhere with stringent security standards and validations.

This year's survey was conducted by Centiment during the February–March 2024 time frame, which consisted of 33 questions on a variety of different topics related to data security, privacy, and compliance. Some of the questions are "blasts from the past"—repeats from the surveys conducted in one or both of the previous two years—while others were added to capture details on new trends. A total of 572 survey responses were received from IT, cybersecurity, and risk and compliance leaders in North America, Europe, Middle East, and Africa (EMEA), and the Asia-Pacific regions.

Some of the questions we asked to pinpoint trends and facilitate insights included:

- How the number of communication tools affect risk management
- The ongoing impact of data breaches on litigation costs
- What data types pose the greatest risk and why
- How regulatory compliance and security standards are driving better data protection by creating baseline security standards and more comprehensive data privacy regulations
- How advanced security capabilities in communication tools translate into lower risk
- Why and how legacy and inadequate approaches to sensitive content communications create inefficiencies and incur greater privacy and compliance risks

57%

Cannot Track, Control, and Report on External Content Sends and Shares

57% of respondents said they cannot track, control, and report on external content sends and shares. This is a *substantial governance risk gap*.

Two-thirds

of Organizations Exchange Sensitive Content With 1,000+ Third Parties

66% of respondents indicated they exchange sensitive content with *over 1,000 third parties*. Once data leaves an organization, the ability to track and control access becomes much more important.

3.55x

Greater Likelihood of 10+ Data Breaches When Using 7+ Communication Tools

The more communication tools an organization employs, the greater the risk. Respondents with *over seven* communication tools experienced *10-plus data breaches*—3.55x higher than the aggregate (those experiencing between one to 10-plus data breaches).

$5M

In Annual Data Breach Litigation Costs Felt by Half of Organizations

Half of respondents exchanging sensitive content with *5,000 or more third parties* spent over $5M in *annual litigation* costs last year.

89%

Admit They Must Improve Sensitive Content Communications Compliance

Only *11%* of respondents said they require no improvement when it comes to measuring and managing sensitive content communications compliance.

62%

Expend 1,500+ Staff Hours to Complete Compliance Reporting

62% of organizations spend over 1,500 staff hours annually compiling and reconciling communication tool logs for compliance reporting.

Introduction

Welcome to the third annual Kiteworks Sensitive Content Communications Report! This is where we conduct an in-depth survey on how well organizations are doing in protecting the privacy and security of their sensitive content and complying with data privacy regulations and security standards.

We use the term "sensitive content" to refer to a wide variety of content types that are targets of malicious actors—and pose significant risk to a legitimate organization if these bad actors get their hands on them. It is what is compromised when all-too-frequent news headlines contain the term "data breach." Sensitive content contains the data of customers and employees—personally identifiable information (PII), protected health information (PHI), and payment card industry (PCI) data. It also includes an organization's intellectual property (IP), legal communications and documents, financials, mergers and acquisitions data, and other types of private and confidential information.

Security Risks

From a security perspective, the problem with sensitive content is that it does not stay in one place. During daily operations, it is shared among employees but also between employees and partners, suppliers, contractors, legal counsel, accountants, auditors, and more. For organizations to move forward, this information must move in a frictionless way between the organization and thousands of third parties. And as we will see, this occurs over multiple communication channels.

As a result, organizations must protect their content—not only where it is stored but also as it travels through various communication channels to third parties. Unfortunately, in recent years, cybercriminals discovered that vulnerabilities in the software supply chain give them access to hundreds or even thousands of organizations and millions of sensitive data files. This year's Data Breach Investigations Report (DBIR) by Verizon corroborates this trend, revealing a year-over-year 180% increase in software vulnerability exploits and revelation that software supply chain data breaches jumped 68% year over year—comprising 15% of all data breaches.[1] Last year's Clop ransomware attacks on Progress Software's MOVEit[2] and Forta's GoAnywhere[3] managed file transfer (MFT) solutions demonstrate the risk.

AI Cyber Risks

In addition to protecting content communication channels, enterprises and government entities have another increasingly urgent priority that has grown over the past 18 months. As artificial intelligence (AI) explodes in both technical advancement and popular use, it is critical that they keep their sensitive content out of large public language models (LLMs) that may now be routinely used by their employees and partners.

According to Gartner, the *top three risk-related concerns* about the usage of GenAI LLMs include access to sensitive data by third parties (nearly half of cybersecurity leaders), GenAI application and data breaches (40% of respondents), and erroneous decision-making (over one-third respondents).[4] The risks associated with employees placing sensitive data into GenAI tools is real. Nearly one-third of employees in a survey completed late last year admitted to placing sensitive data into public GenAI tools. Unsurprisingly, 39% of respondents in the same study cited the potential leak of sensitive data as a top risk to their organization's use of public GenAI tools.[5]

At the same time, lower barriers to entry that have brought AI use to the masses have also opened doors to less sophisticated cybercriminals to launch increasingly complex attacks.[6] It adds to the sense that nation-state threat actors and cybercriminals are in an escalating "arms race" with legitimate organizations—with what could be existential implications.

Compliance Risks

Unless your company does business in a single jurisdiction, the difficult thing about regulatory data privacy compliance is the patchwork of requirements from place to place—which adds to the complexity and cost of being compliant—and documenting that compliance. The rise in new regulations and evolution in existing ones prompted 93% of organizations to rethink their cybersecurity strategy in the past year.[7] The European Union's General Data Protection Regulation (GDPR), implemented in 2018, unified its 27 member states under a single data privacy standard.

For the rest of the world, things are not that simple. United Nations data shows that 137 out of the world's 194 countries now have data privacy laws—but they naturally vary greatly.[8] In the United States, the most stringent federal legislation is the Health Insurance Portability and Accountability Act (HIPAA)—which covers PHI but not PII. With Congress unable to pass a national standard, individual states have stepped into the fray—starting with the passage of the California Consumer Privacy Act (CCPA) in 2018. Since then, an additional 17 states have enacted comprehensive data privacy laws—with legislation moving through the process in an additional 10.[9] While it is good that more U.S. citizens and residents are being protected by such laws, it exacerbates the patchwork for those who need to comply.

The different bodies managing these data privacy regulations continue to apply pressure on organizations to comply. Fines and penalties for GDPR noncompliance in 2023 hit $2.269 billion (€2.1 billion)—exceeding the fines and penalties issued in 2019, 2020, and 2021 combined.[10] The amount per fine and penalty is spiraling upwards as well; $4.75 million (€4.4 million) per violation last year compared to $540,000 (€500,000) per violation in 2019. Fines and penalties behind HIPAA are just as daunting, hitting $4.176 billion last year.[11]

In addition to data privacy regulations, cybersecurity standards and rules have been a key focus area for governmental and oversight bodies. Some of the major new cybersecurity regulations introduced in the past year include the SEC's Cybersecurity Risk Management and Incident Disclosure rules for public companies, Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), the Cyber Resilience Act (CRA) and Digital Operational Resilience Act (DORA) in Europe, and the National Institute of Standards & Technology (NIST) Cybersecurity Framework (CSF) 2.0, among others.

Human Risks

The human risk element in data security and compliance remains a serious problem and the root cause behind many sensitive data breaches. The DBIR found that end-users account for 68% of errors leading to breaches.[12] This occurs in various ways, including employees and third parties sending sensitive information to the wrong recipients, failing to properly secure data, or falling victim to social engineering attacks like business email compromise and phishing. Lack of visibility and governance around sensitive content communications is a leading factor, in addition to deficient security infrastructure and controls.

Nearly half of cybersecurity leaders cite access to sensitive data by third parties as their top risk-related concern this year.

"2024 Gartner Technology Adoption Roadmap for Larger Enterprises Survey," Gartner, February 2024

Methodology for This Study

This year's Kiteworks Sensitive Content Communications Report is based on a comprehensive survey of 572 professionals working in IT, cybersecurity, and risk and compliance management at organizations with more than 1,000 employees. Our analysis reports on respondent feedback for the overall cohort, compares it with our survey results from 2023 and 2022, and cross-analyzes it according to various demographic details.

Diverse Pool of Respondents

Respondents come from eight countries globally, with representation from North America (34%), Asia-Pacific (18%), and Europe-Middle East-Africa regions (48%) (Figures 1 and 2). They represent a broad range of enterprise-level company sizes, with 54% having between 1,000 and 10,000 employees and 46% having more than that (Figure 3).

The cohort comes from a wide range of industries, with security and defense (15%), manufacturing (12%), healthcare (12%), and financial services (12%) organizations seeing the highest representation (Figure 4). More than two in 10 participants (22%) work in government or education, while one-quarter work in financial, legal, and professional fields and 10% work in the energy industry.

In terms of job function, the survey pool includes professionals at different levels in their organizations, with 31% in executive positions and 69% in mid-level management roles (Figure 5). And they are split between the risk and compliance (27%), IT (42%), and security (31%) functions.

75%

of the world's population will have their personal data regulated by modern privacy laws by the end of 2024.

"Gartner Identifies Top Five Trends in Privacy Through 2024," Gartner Press Release, May 31, 2022

Insights on Privacy and Compliance of Sensitive Content Communications

Now that we introduced our respondents, we want to share what we have gleaned from the survey results they provided. This year, we uncovered insights on the topics of measuring and managing the risks of cyberattacks and data breaches, data types and classification, cybersecurity, compliance, and operational processes.

CYBERATTACKS AND DATA BREACHES

Insight: Sensitive Content Communications Are Breached Too Frequently

Malicious cyberattacks remain a serious risk to sensitive content across every industry sector. Accordingly, the Identify Theft Resource Center reported 3,205 publicly reported data compromises that impacted over an estimated 353 million individuals last year—a *78% increase* over 2022.[13] The good news is that things are slightly better for our 2024 respondents than for our 2023 cohort. The bad news is that organizations are still frequently suffering dangerous breaches. Nearly *one-third* of respondents (32%) reported suffering *seven or more* external malicious hacks of sensitive content in the past year, compared with 36% last year (Figure 6). And while more companies (36%) reported three or fewer breaches than last year, even those numbers are higher than ideal.

There was a lot of variation by industry in the number of hacks suffered (Figure 7). Higher education, security and defense, and oil and gas saw even more breaches, with 68% or more reporting four or more breaches, compared with 55% for the full cohort. The *federal government sector* also revealed concerning data, with 17% indicating they had 10 or more and another 10% reporting between seven to nine. Even more alarming, 42% of *security and defense organizations,* which exchange some of the most sensitive content of any industry segment, admitted to seven or more data breaches. On the upside, pharmaceutical and life sciences companies are doing much better, with just 28% of respondents reporting four or more breaches.

Organizations in the Asia-Pacific region also suffered disproportionately from breaches, with 72% of respondents reporting four or more incidents (Figure 8). With Asia-Pacific organizations having a higher number of third parties with which they exchange sensitive content (see below), additional sleuthing is likely to evince a connection between the two. Finally, companies with 20,001 to 30,000 employees fared much worse than the others, with 75% or more reporting four or more breaches—while both smaller and larger company size groups kept that figure well below 60% (Figure 9).

42%

of security and defense firms admitted to seven-plus data breaches last year.

68%

of Asia-Pacific companies indicated they experienced four-plus data breaches last year.

32%

of organizations experienced *seven-plus* external malicious hacks of sensitive content last year.

Litigation Cost of Data Breaches

When it comes to data breaches, the cost can be far-reaching—encompassing regulatory noncompliance fines and penalties, operational downtime, diminished productivity, and lost revenue. Last year's annual Cost of a Data Breach Report by IBM and Ponemon Institute pegged the cost of a data breach at *US$4.45 million*, a number that continues to increase year over year.[14] And that number may be too low, as legal costs associated with data breaches are often missed or underestimated. With that in mind, we added the litigation cost question to our survey this year, which elicited actionable intelligence.

On that note, *six in 10* respondents reported spending *more than $2 million* every year to deal with the legal costs of both internal and external data loss incidents, while 45% spent over $3 million and one-quarter spent *more than $5 million* (Figure 10). We also found the larger an organization, the higher the litigation cost, with 16% (17% experienced seven to nine and 22% experienced over 10) of organizations with over 30,001 employees indicating their cost of legal fees was over $7 million and well over half with more than 15,001 employees spending over $3 million (Figure 11). *Higher education* was the most affected industry sector, with 49% reporting they paid over $5 million last year (Figure 12). Geographically, *North America* topped the list with 27% indicating they paid out over $5 million. One troubling gap in the report was the 14% of *EMEA* respondents who do not know the litigation cost of their data breaches (Figure 13).

24%

of organizations with over 30,001 employees reported data breach litigation costs over $7M annually.

45%

of respondents indicated litigation costs exceeded $3M annually, with one-quarter spending over $5M.

DATA TYPES AND CLASSIFICATION

Insight: Unable to Track and Control All Their Data Exchanges

An already exponential growth in data accelerated further over the past 18 months with the adoption of generation AI (GenAI) large language models (LLMs). When content leaves an application such as email, file sharing, SFTP, managed file transfer, or web forms, it is important that organizations can track and control access to that content.

Organizations need to understand their data types, where it resides, and where it is being sent and shared. To identify which unstructured data should be controlled, it is necessary for a classification system to be in place. When asked how much of their unstructured data is tagged or classified, *less than half* of respondents (48%) claim that this is the case for *75% or more* of their data (Figure 14). Among industries, 65% have achieved this level in healthcare, 56% in financial services, and 55% in legal (Figure 15).

Notwithstanding, organizations indicated not all unstructured data needs to be tagged and classified. *40% of organizations said 60% or more* of unstructured data needs to be tagged and classified. And the larger an organization, the more unstructured data needs to be tagged and classified. For example, those with more than 30,001 employees expressed such: 15% indicated all data needs to be tagged and classified, and another 20% said over 80% needs to be tagged and classified (Figure 16). Regionally, more North American respondents said it must be tagged and classified; 10% said all unstructured data must be tagged and classified and another 16% noted 80% or more (Figure 17). Federal government respondents said all data must be tagged and classified in the highest number (24%), with 17% more saying 80% or more must be tagged and classified (Figure 18).

40%

of organizations said 60%-plus of unstructured data needs to be tagged and classified.

Only 49% of organizations said more than 75% of their unstructured data needs to be tagged and classified.

Assessing the Risks of Data Types

As delineated above, sensitive content exists in different forms across organizations. Each does not pose the same level of data breach risk. Per IBM's annual cost of a data breach study, *PII* is the costliest and most common record compromised. PII was also the most breached record type in 2023, comprising 52% of all data breaches, a spot it also claimed the prior two years.[15] IBM's findings align with those in the latest DBIR, where 50% of all data breaches were tied back to PII.

When this is overlaid against our respondent rankings, there are variances. For example, based on the research data from IBM and Verizon, one would assume respondents would cite PII as their top content type concern. But that was not the case. Instead, they named *financial documents (55%)*, *intellectual property (44%)*, and *legal communications (44%)* as their top three concerns (Figure 19).

41% of federal government respondents said 80% or more of their unstructured data needs to be tagged and classified.

Some corroboration of the IBM and Verizon data was found in our cross-analysis of *PHI*, where those who pinpointed it as one of their three data type concerns experienced a higher rate of malicious data breaches than those who ranked other data types. For example, *43%* of those who ranked PHI in their top three data type concerns said they experienced *over seven* data breaches (in contrast with the 32% across all respondents who reported seven or more breaches) (Figure 20). The second data type with the highest rate of data breaches was *IP* (35% said they experienced seven-plus data breaches).

Strikingly, half of all North American respondents named GenAI LLMs as a top-three concern, only ranking behind financial documents (Figure 21). By industry, LLMs are an especially big concern in oil and gas (62%), pharmaceuticals (61%), federal (61%) and state government (58%), and law firms (58%).

There is substantial variance across data types and industries as to which one is considered the highest risk:

GenAI LLMs were selected most often by energy and utilities firms and security and defense sector firms at 50%.

PII was cited most often by higher education firms at 50%.

PHI was cited most often by healthcare at 58%.

CUI and FCI were cited most frequently by manufacturers at 79%.

Legal communications were cited most often by oil and gas companies (62%) and federal government agencies (61%).

Merger and acquisition details were identified most often by pharmaceutical and life sciences firms (40%).

Respondents who listed **PHI** as one of their **top three data type concerns** experienced a higher rate of **malicious data breaches** than those who ranked other data types.

COMPLIANCE AND RISK MANAGEMENT

Insight: Compliance and Risk Management Is a Pressing Priority

These days, it seems that cybersecurity risk accounts for a bigger share of an organization's overall risk portfolio every year. CrowdStrike, in its annual threat report, pinpointed a *76% year-over-year increase* in victims named on eCrime dedicated leak sites.[16] In its latest DBIR, Verizon analyzed over 30,000 real-world security incidents and confirmed that around one-third (10,626) were data breaches.[17]

With sensitive data at the center of most data breaches, government agencies and industry bodies have responded with a series of new regulations and standards and tightening of existing ones. All of this results in a geographic patchwork that adds complexity for incident response and compliance audits and reporting, particularly for global businesses.

As in previous years of our survey, 2024 respondents reported continued struggles around compliance and risk management. This was made clear in the answers respondents gave to a basic question about how well their organizations are doing in managing compliance risk around sensitive content communication tools (Figure 22). *Only 11%* claimed that no improvement was needed in this area—much lower than with the 2022 and 2023 cohorts. The good news is that *fewer respondents* (32%) report that *significant* improvement is needed.

Regional variations on this question are small, but company size is a factor. Specifically, larger companies are more likely to say significant improvement is needed (Figure 23), with *one-third or more* of companies in every grouping above 15,001 employees giving that answer. Notwithstanding, there is some variance in confidence when it comes to regulatory compliance. 29% of French respondents said *no improvement* is needed at a much higher rate than other country respondents—for example, 5% for Germany, 10% for the United Kingdom, and 13% for Saudi Arabia and the UAE (Figure 24). Interestingly and perhaps alarmingly, *41% of federal government respondents* cited significant improvement is needed in managing and measuring sensitive content communications compliance, higher than any other industry sector (next highest was professional services at 36%) (Figure 25).

Only

11%

of organizations said **no improvement is needed** in their measurement and management of sensitive content communications compliance.

Areas of Focus for Regulations

For global businesses, there are a lot of data privacy regulations and security standards to address. To date, over 160 privacy laws have been enacted internationally, and more continue to be passed. Noncompliance results in brand degradation, lost revenue, fines and penalties, and ongoing litigation costs. As a result, 37% of respondents in this year's ISACA privacy report said they are only somewhat confident—and another 13% said they are either not so confident or not confident at all—when it comes to their ability to ensure data privacy and achieve compliance with new privacy laws and regulations.[18]

When respondents were asked to name their top two areas of data privacy and compliance focus, two of the choices dominated—the EU's General Data Protection Regulation (GDPR) and the data privacy laws being passed by individual U.S. states, such as the California Consumer Privacy Act (CCPA). Both were cited by 41% of all respondents (Figure 26).

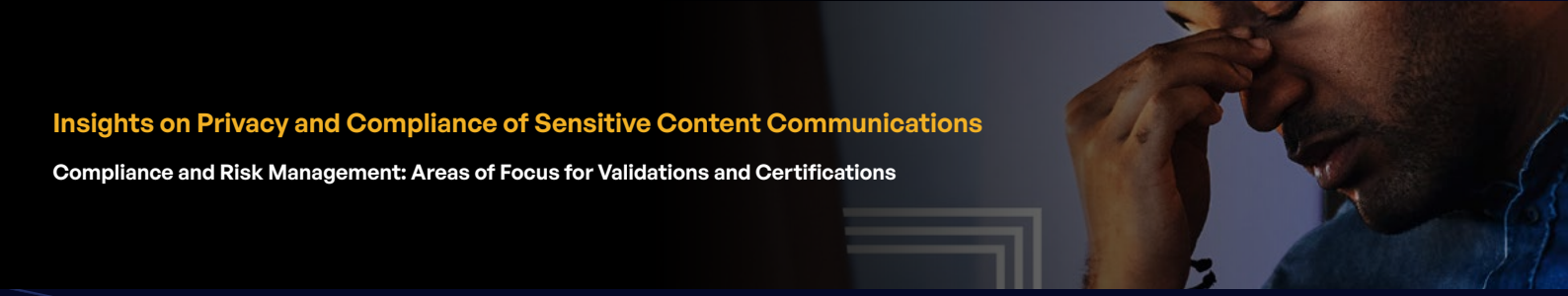
Not surprisingly, GDPR was much more commonly cited in EMEA (57%), while U.S. state laws were cited by 63% of North American respondents (Figure 27). Of the different job roles, risk and compliance leaders (52%) place a greater emphasis on GDPR than IT (38%) and cybersecurity (33%) leaders (Figure 28). IT leaders place the greatest emphasis on U.S. state data privacy laws (52%) versus risk and compliance (25%) and cybersecurity (40%) leaders. At the same time, cybersecurity leaders (35%) afford greater focus on CMMC 2.0 than IT (22%) and risk and management (18%) counterparts. The HIPAA—a law specific to the U.S.—was cited by 38% of North American respondents, though ironically by a higher percentage (43%) of respondents in the Asia-Pacific region.

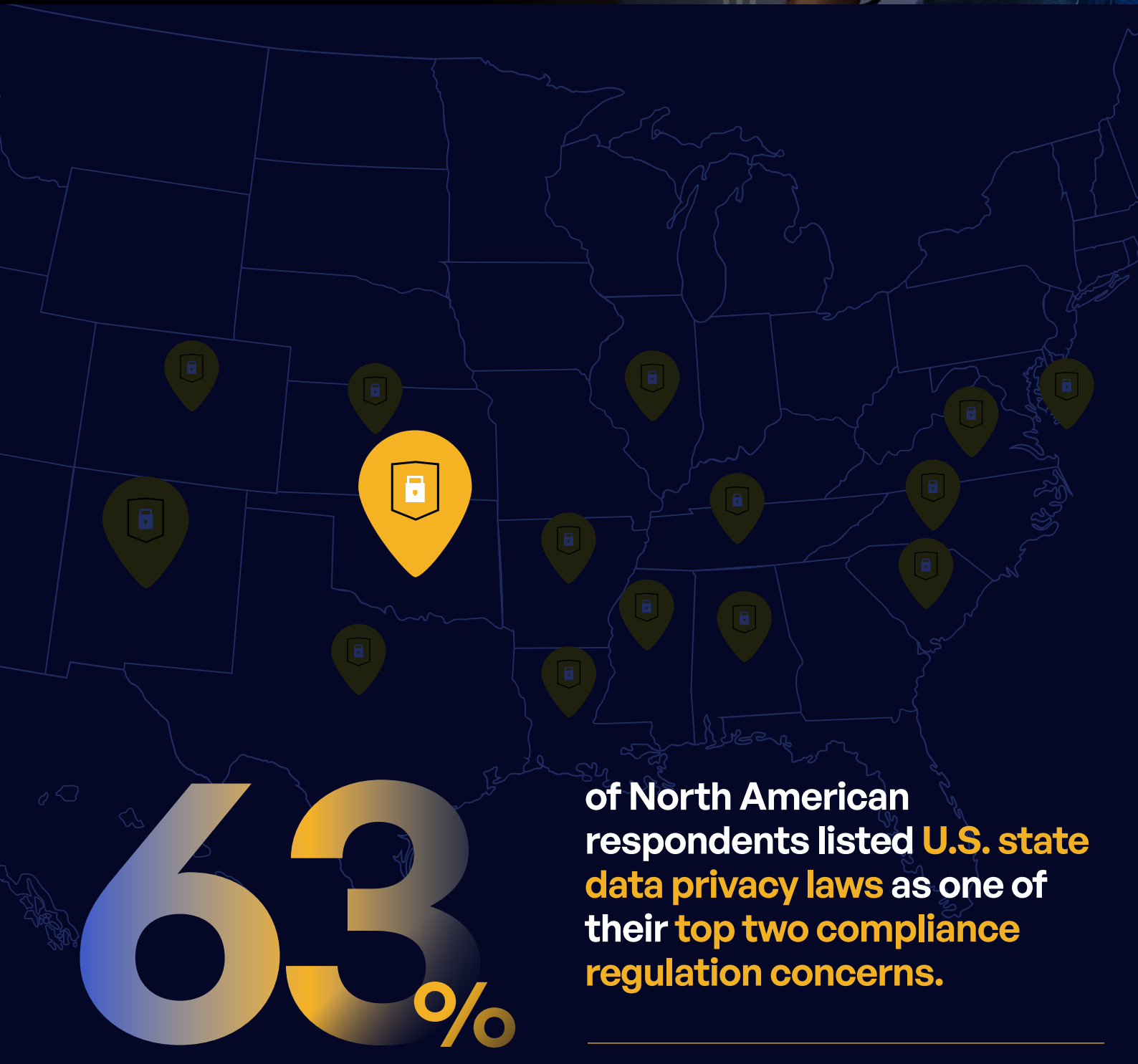
There are a few concerning risk gaps when regulatory compliance is examined from an industry response standpoint. For example, only 38% of security and defense contractors listed CMMC compliance as one of their top two priorities. With a phased implementation of CMMC 2.0 underway now, this appears to be a serious risk—namely, security and defense contractors and subcontractors that aren't compliant will lose DoD business.

Areas of Focus for Validations and Certifications

When it comes to validations and certifications as opposed to regulations, two standards were most cited as among respondents' top two priorities (Figure 29)—standards published by the International Organization for Standardization (ISO; 53%) and the National Institute of Standards and Technology (NIST 800-171; 42%). As the 110 controls in NIST 800-171 are the same as the ones in CMMC 2.0 Level 2, this high level of prioritization is promising, especially with the phased implementation of CMMC 2.0 currently underway. ISO 27001, 27017, and 27018 standards were most cited across all geographies and most industries; the latter include 59% in EMEA, 67% in the pharmaceutical industry, and 69% in local government (Figures 30 and 31).

59% of EMEA respondents listed **ISO 27001, 27017, and 27018** as one of their **top 2 security validations and certifications** (19% higher than Asia-Pacific and 22% higher than North America).





63%

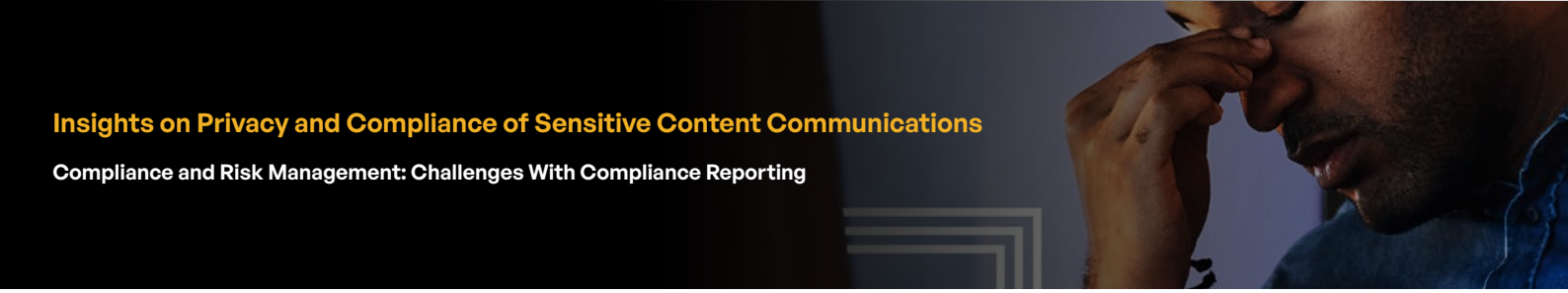
of North American respondents listed U.S. state data privacy laws as one of their top two compliance regulation concerns.

Only 38% of security and defense contractors listed CMMC 2.0 as one of their top two compliance regulation concerns.

With a sizable percentage of Asia-Pacific respondents from Australia, it makes a lot of sense that the Information Security Registered Assessors Program (IRAP) was selected by more Asia-Pacific organizations than the other two regions (45%). Interestingly, NIS 2 Directive was selected as one or two by only 20% of EMEA organizations (though higher than North America at 8% and Asia-Pacific at 4%). One would assume NIS 2 compliance would be a higher priority with the deadline for the directive going into national laws on October 17, 2024. Across our three main job responsibilities, NIS 2 received the least attention from risk and compliance leaders (19%) compared to IT (31%) and cybersecurity (33%) counterparts. North American organizations selected SOC 2 Type II compliance more often than the other regions (41%).

In terms of industry sectors, SOC 2 Type II was selected most by professional services firms (47%). ISO 27001, 27017, and 27018 was selected by pharmaceutical and life sciences firms more often (67%). Security and defense firms topped the list for FedRAMP Moderate at 44%. Legal firms topped the list for IRAP (50%).

ISO 27001, 27017, and 27018 standards were cited most frequently by respondents as the most important cybersecurity standard.



Challenges With Compliance Reporting

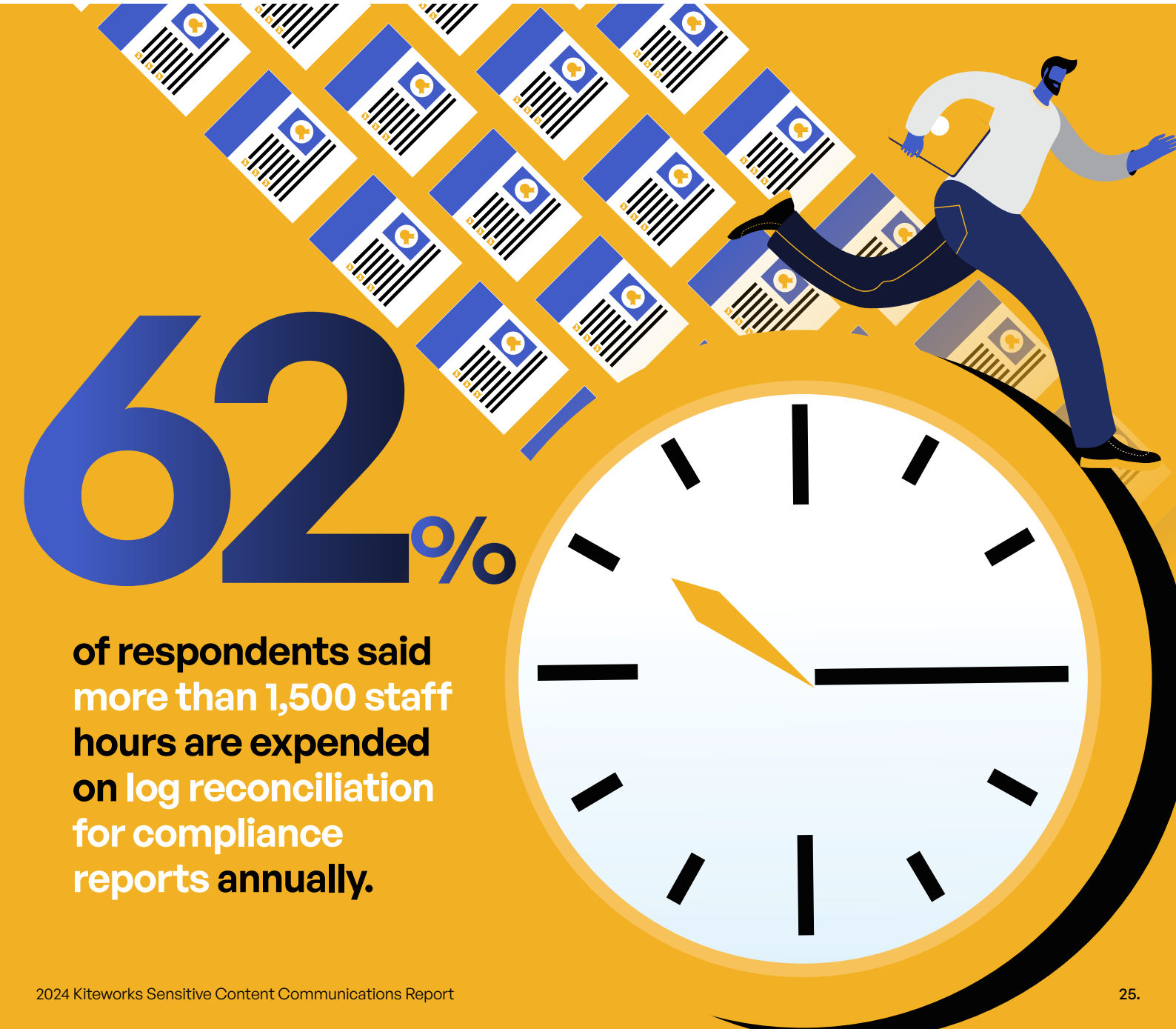
Regardless of the specific regulations, validations, and certifications a company must adhere to, documenting compliance remains a big challenge. Organizations struggle with external sends and shares of sensitive data, with *57%* indicating they cannot track, control, and report on those exchanges (Figure 32). One cause is the patchwork of requirements facing companies that create complexities and incur significant staff resources and time. When asked how often they must generate detailed audit logs for compliance reporting, *72%* of respondents reported that they must do so five or more times per year (Figure 33). For more than one-third (34%), that number is eight or more times.

89%

of organizations must generate detailed compliance reports eight or more times annually.

Regional and company size variations on this question were not great (Figures 34 and 35). North American companies, as well as smaller companies, tend to have slightly fewer log requirements. Organizations with over 30,001 employees have more audit logs (19% have 9x) than other organization sizes. Industry sectors with the highest number of audit logs per year are professional services, security and defense, and federal government, with 78%, 77%, and 72%, respectively. Legal/law firms have the lowest number with 15% or fewer having five or more (Figure 36).

Compliance reporting requires a lot of staff time due to the number of times detailed logs must be pulled into reports. Among all respondents, *63%* reported *more than 1,500 hours* of staff time per year is required for this task (Figure 37). For companies with more than 15,001 employees, the number of hours spike substantially with one-third of 30,001-plus employee organizations reporting they spend over 2,500 hours (Figure 38). Half of oil and gas respondents and nearly half of higher education respondents spend over 2,000 hours annually—by far the highest industry segments (Figure 39).



62%

of respondents said more than 1,500 staff hours are expended on log reconciliation for compliance reports annually.

CYBERSECURITY AND RISK MANAGEMENT

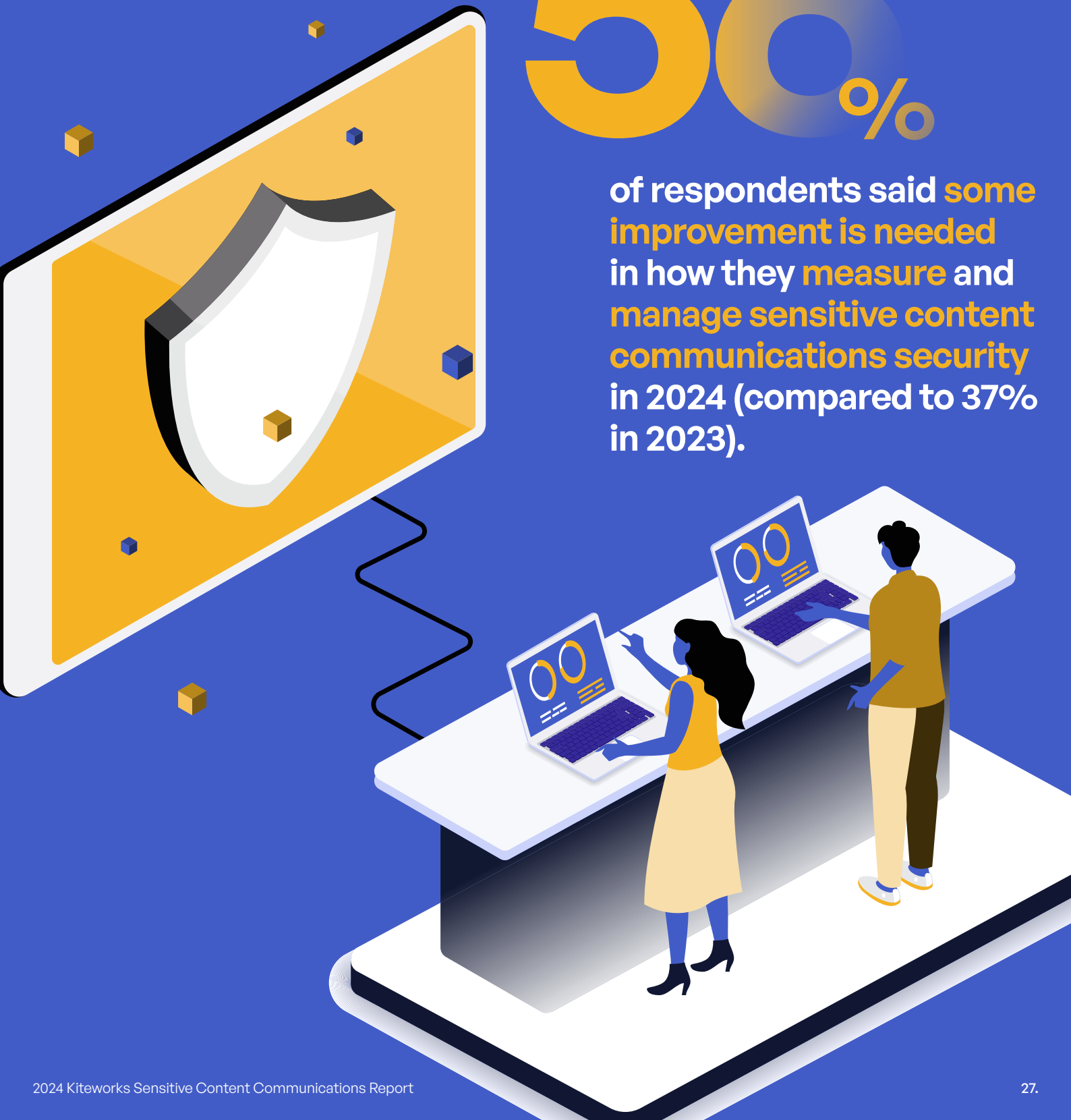
Insight: Protecting Sensitive Content Communications Remains a Big Challenge

For the security team, sensitive content is at the center of what they need to protect in their corporate IT systems. And the 2024 respondents to our survey are much less likely to claim that no improvement is needed in their management of content security than their 2023 counterparts (Figure 40). Only *11%* made that claim this year, but the percentage that said significant improvement is needed also declined. This leaves *more than half* (56%) who say that *some improvement* is needed. We can perhaps take heart that organizations are making some progress—while being more realistic about the need for further improvement.

But these percentages were not uniform across the different groups. 30% or more respondents in Saudi Arabia, the United Arab Emirates, North America, and Asia-Pacific indicated significant improvements are needed (Figure 41). The same is true for professional services (47%), financial services (43%), oil and gas (42%), federal government (41%), manufacturing (36%), and healthcare (34%) (Figures 42 and 43).

56%

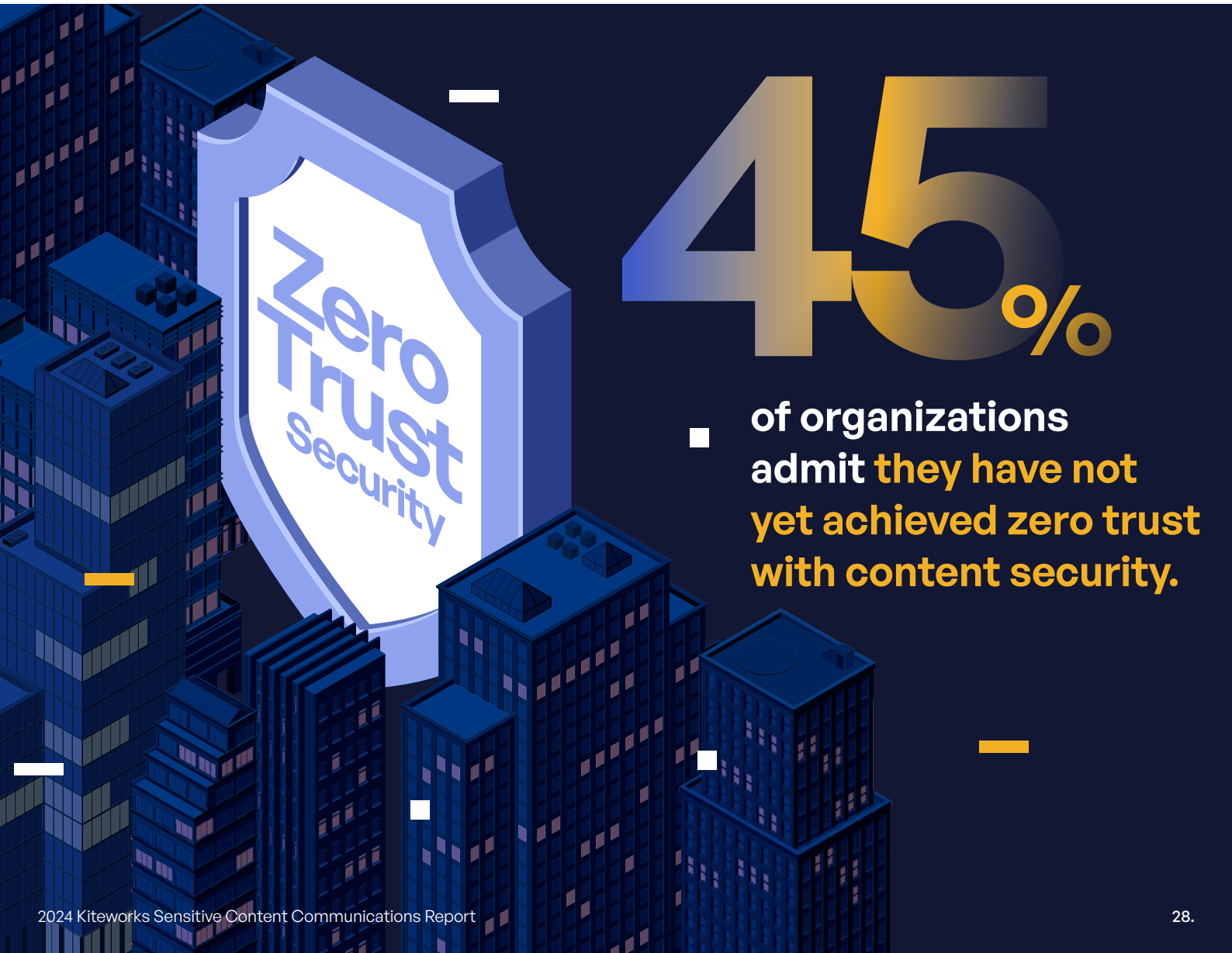
of respondents said some improvement is needed in how they measure and manage sensitive content communications security in 2024 (compared to 37% in 2023).



Progress Toward Zero Trust

Zero trust in organizations reflects a significant adoption and integration across various security layers. Zero-trust principles at the network layer are being enforced through microsegmentation and strict access controls to minimize the lateral movement of threats. Endpoint security under zero trust involves deploying advanced threat protection and endpoint detection and response (EDR) solutions to ensure all devices accessing the network are continuously authenticated and monitored. For identity and access management, multi-factor authentication (MFA) and privileged access management (PAM) are critical components, ensuring that user access is tightly controlled and continuously verified. At the content layer, organizations are implementing data encryption and real-time monitoring to secure sensitive information. Despite organizations prioritizing zero trust, nearly half (48%) report difficulties integrating zero trust across both on-premises and cloud environments.[19]

Our interest for this report obviously focuses on the content security layer (Figure 44). Our first observation is the regrettable 45% of companies that have *not* yet achieved zero trust with content security. Second, there are some demographic areas where performance was even worse. Only 35% of U.K. respondents met this benchmark and 39% in both the Middle East and Asia-Pacific (Figure 45). By industry, state government (21%), oil and gas (33%), and pharmaceuticals and life sciences (39%) are lagging on zero trust protection for content (Figure 46).



Advancing Security to Protect Sensitive Content

For organizations that admitted they do not use advanced security capabilities for sensitive content communications, a much higher percentage (36%) indicated they do not know how many data breaches affected their organizations—compared to those who said they employ advanced security for some content communications or all content communications (8% respectively for both) (Figure 47). This reveals a serious risk gap. Across industry segments, findings highlight the biggest challenges in legal (55% use them for some or none), local government (50%), federal government (48%), and healthcare (44%). These contrast with the 41% from the global cohort that do so. Strongest industry performers include professional services (71% use them for all), state government (71%), and higher education (65%) (Figure 48).

Tracking, Classifying, and Controlling Sensitive Content Access

When content leaves an application such as email, file sharing, SFTP, managed file transfer, or web forms, it is important that organizations can track and control access to that content. While only 16% of respondents can do this every time, *45%* indicated they can do so around three-quarters of the time (Figure 49). This percentage is better for certain segments—70% for North America, 79% for manufacturing, and 73% in healthcare (Figures 50 and 51). On the flip side, higher education (31%) and oil and gas (34%) fared worse.

To identify which unstructured data should be controlled, it is necessary for a classification system to be in place. When asked how much of their unstructured data is tagged or classified, *less than half* of respondents (48%) claim that this is the case for 75% or more of their data (Figure 14). Things are slightly better in North America, where 56% have achieved this (Figure 52). Among industries, 65% have achieved this level in healthcare, 56% in financial services, and 55% in legal (Figure 53).

Only 16%

of organizations can track and control access to *all* content when it leaves an application.

65%

of healthcare respondents said they tag and classify over 75% of their unstructured data (highest of all industries).

Using Security Tools for Sensitive Content

All enterprises have multiple security tools that they use across their networks, endpoints, and cloud applications. Whether these are used to protect internal and external sensitive content communications is another question.

When asked whether they use capabilities like multi-factor authentication, encryption, and governance tracking and controls for such communications, results are mixed (Figure 54). Nearly six in 10 (59%) say these protections are always in place for external sensitive content communications. Almost everyone else says that they are in place some of the time. North American respondents have the highest security posture, with 67% reporting they do so all the time versus 57% for Asia-Pacific and 53% for EMEA respondents.

Maturity of measuring and managing sensitive content communications security remains a key focus area for organizations: only 11% indicated no improvement is needed compared to 26% in last year's survey (Figure 55). A *higher percentage* of organizations this year noted *some improvement* is needed (56% to 37% in last year's survey).

While the numbers were the same for the whole cohort, there were interesting differences when the question is analyzed by different groups. For internal communications, 71% of state government and professional services both said they always use these tools (Figure 56). Two-thirds (67%) of North American respondents said the same, while only 53% did so in EMEA (but 63% in the U.K.) (Figure 57). Interestingly, law firms (45%) did the worst with internal communications. For external communications, pharmaceuticals and life sciences (78%) and higher education (72%) were high performers, as were North American organizations (69%) (Figure 56).

56%

of organizations said how they measure and manage sensitive content communications security requires some improvement —33% greater than last year's percentage.

OPERATIONAL PROCESSES

Insight: It Takes a "Village" —and a Lot of Time— to Manage Data Security and Compliance

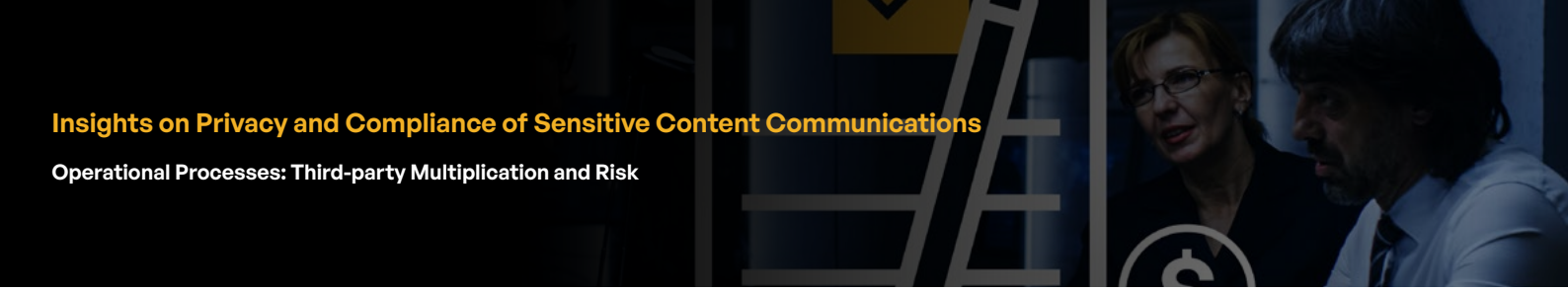
Many of the challenges we describe above—data breaches and compliance and security issues—are exacerbated by the complexity of operational processes at most organizations. Between a proliferation of communication tools and most organizations' inability to get rid of manual processes, it is inevitable that security and compliance problems will slip through the cracks.

Third-party Multiplication and Risk

For most organizations, they exchange large volumes of sensitive data during daily business with hundreds and often thousands of third parties. Third-party risk has never been higher for organizations in all industries, and the necessity of exchanging sensitive content accentuates the threat.

When we asked the 2024 cohort to estimate how many third-party individuals receive sensitive content from their companies, *two-thirds* (66%) estimated *more than 1,000* (Figure 58). Among the largest enterprises with more than 30,001 employees, 33% exchange content with more than 5,000 third parties (Figure 59). 77% of Asia-Pacific organizations exchange sensitive data with 1,000 third parties, 66% for North America, and 63% for EMEA (Figure 60).

The federal government exchanges sensitive content at a significantly higher rate than most other industry sectors (28% send and share data with 5,000-plus third parties) (Figure 61). Also sustaining a high third-party data exchange rate is higher education; 47% of respondents said they do so with 2,500-plus third parties.



Once sensitive content leaves an organization, 39% of organizations indicated they are only able to track and control access to *50% or less*. The EMEA region has the largest challenge here with *46%* admitting they lose the ability to track and control access to *50% or less* of sensitive content once it leaves their organization (Figure 62). Those with the highest risk due to the lack of tracking and controls include local government organizations (54% admit to being unable to track and control sensitive content once it leaves their organization) and pharmaceutical and life sciences companies (50% cannot track and control sensitive content outside their organizations) (Figure 63).

Comparison of data breach occurrence with the number of third parties with which organizations exchange sensitive content shows significantly higher risk (Figure 64). For example, 35% of those reporting they exchange sensitive content with over 5,000 third parties experienced more than 10 data breaches last year. 50% of those exchanging sensitive content with 2,500 to 4,999 third parties experienced over seven data breaches. The same is true in terms of litigation costs (Figure 65). For those exchanging sensitive data with 5,000 or more third parties, half spent over $5 million in litigation costs. 44% of those exchanging sensitive content with 2,500 to 4,999 third parties also spent over $5 million.

35%

of those reporting they exchange sensitive content with over 5,000 third parties experienced more than 10 data breaches last year.

Proliferation of Communication Tools and Risk

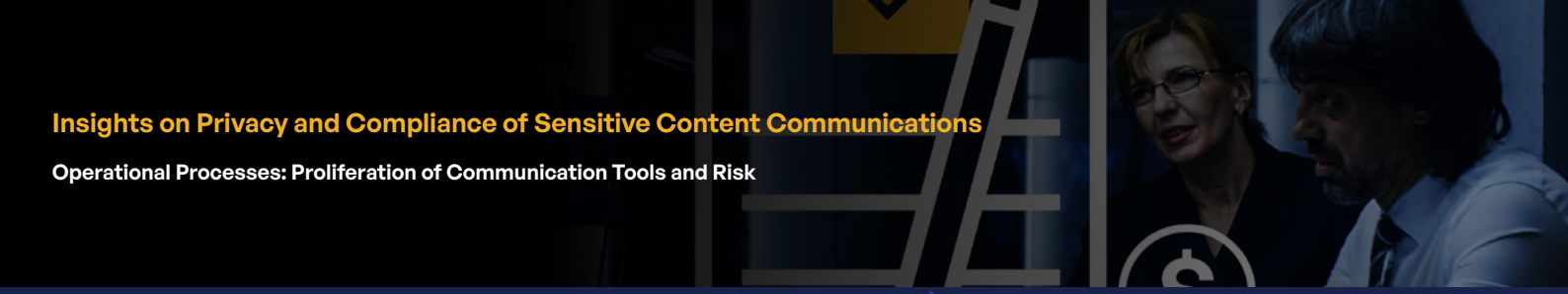
A proliferation of communication tools exists when it comes to sending and sharing sensitive content: email, file sharing, managed file transfer, SFTP, web forms, and the like. Moves to mitigate risks, reduce costs, and improve operational efficiency appear to have resulted in a move to consolidate content communication tools: Half of respondents in 2023 indicated they had six more or more content communication tools compared to 32% this year (Figure 66). *North America* has the highest tool proliferation with 59% using five or more versus 50% for EMEA and 52% for Asia-Pacific (Figure 67). An astounding *77% in North America* employs four or more tools, and that figure is 80% or more in financial services, legal, professional services, and oil and gas (Figure 68).

Cross-analysis of the above pinpoints that organizations with a *higher rate of data breaches* have *more communication tools* (Figure 69). For example, 32% of organizations with 10 or more data breaches have more than seven communication tools, and 42% of those with six communication tools experienced seven to nine data breaches. These numbers are dramatically higher than the average number of data breaches across all respondents: only 9% reported 10 data breaches (compared to the 32% with seven-plus communication tools) and only 23% reported seven to nine data breaches (Figure 6). This equates to a rate of 3.55x more for those with 10 or more communication tools and 2x higher rate for those with seven to nine communication tools. The same is true when it comes to the amount organizations pay in data breach litigation costs: *26%* of those that reported paying *over $7 million* last year have over seven communication tools (3.25x higher than the norm of 8%) (Figure 70).

32%

of respondents that experienced over 10 data breaches have more than seven communication tools.

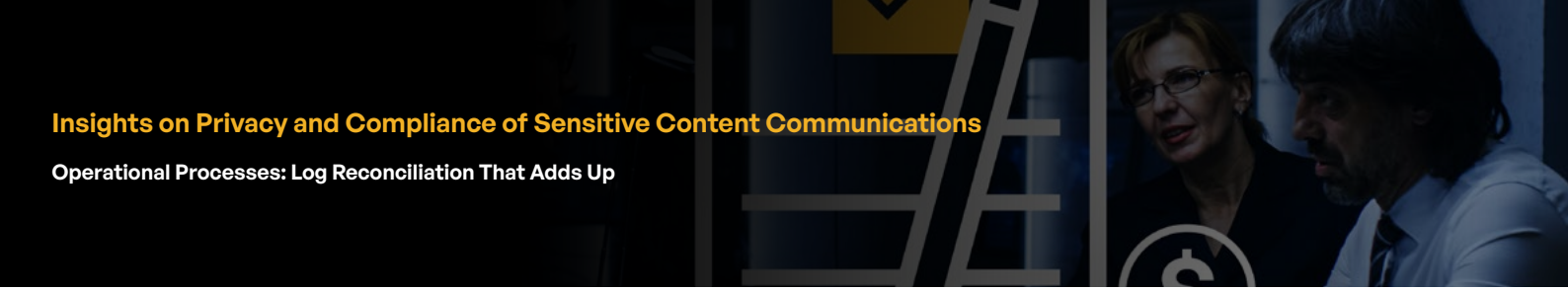
The more communication tools an organization has in place, the more data breaches it experiences and the higher its litigation costs.



38%

of North American respondents said they use six-plus communication tools (higher than other regions).

Two-thirds of organizations exchange sensitive content with 1,000-plus third parties.



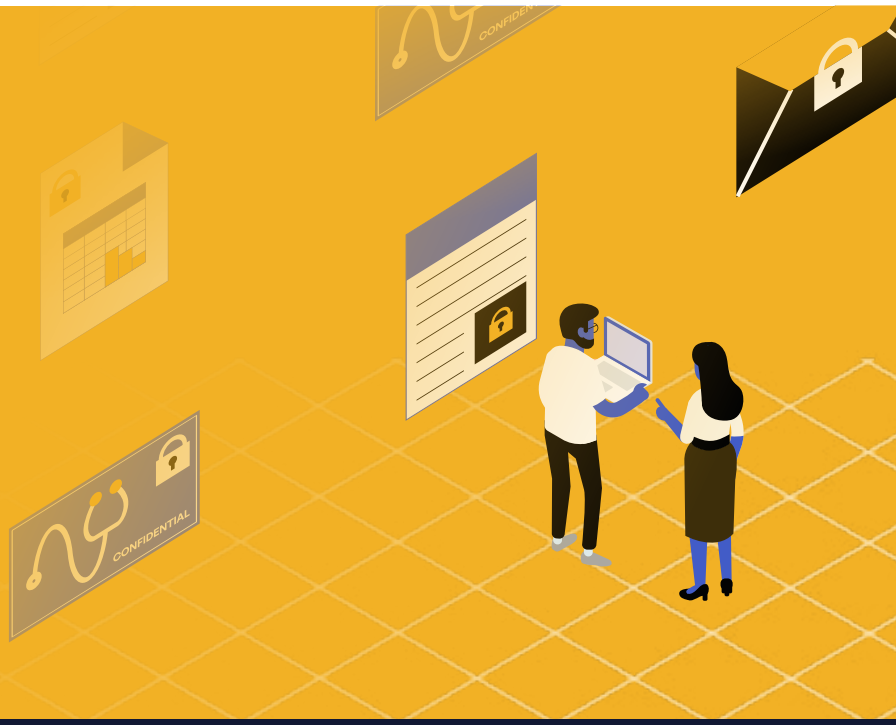
Log Reconciliation That Adds Up

Reconciliation of sensitive content communication logs for audit reports is a time-consuming task for many respondents; *48%* said they must consolidate *over 11 logs*, with 14% needing to consolidate over 20 logs. Not knowing what logs need to be reconciled is a risk in itself; 8% said they do not know how many they have (Figure 71).

Larger organizations indicated they must consolidate higher numbers of audit logs; for example, 34% of those with over 30,001 employees consolidate over 20 (compared to 14% for organizations with 20,001 to 25,000 employees and 11% for those with 25,001 to 30,000 employees) (Figure 72).

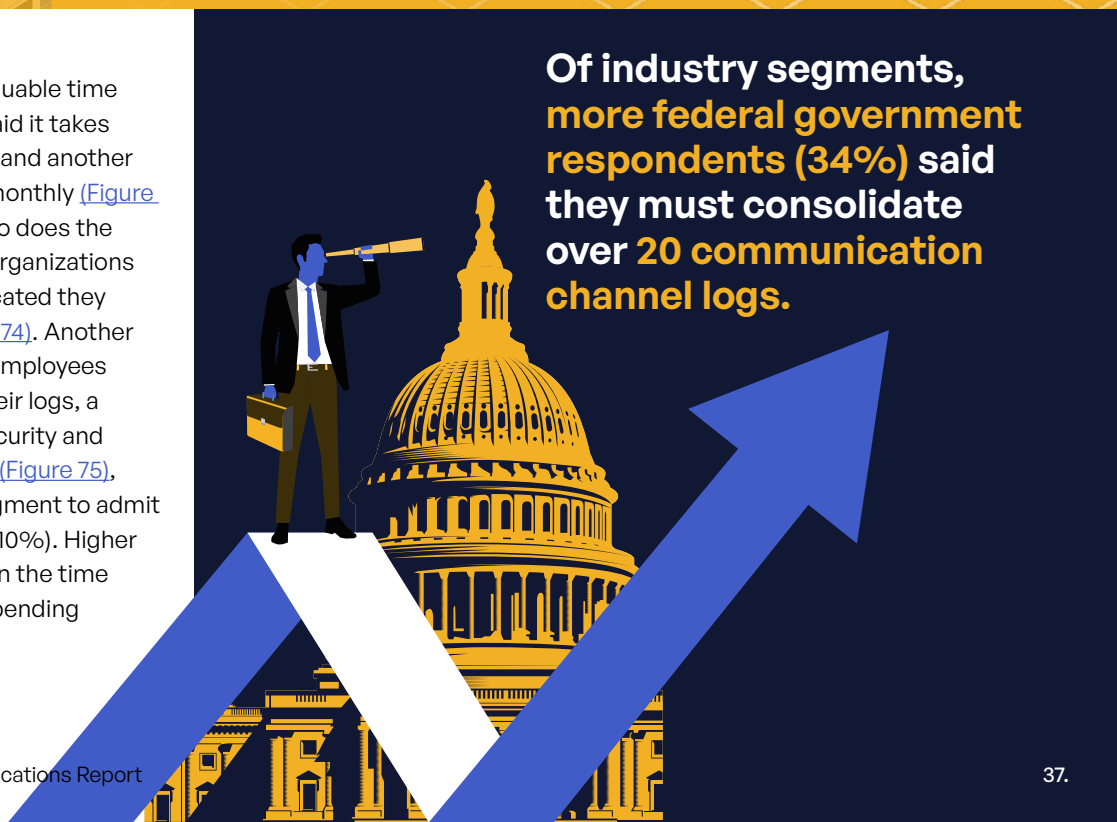
34%

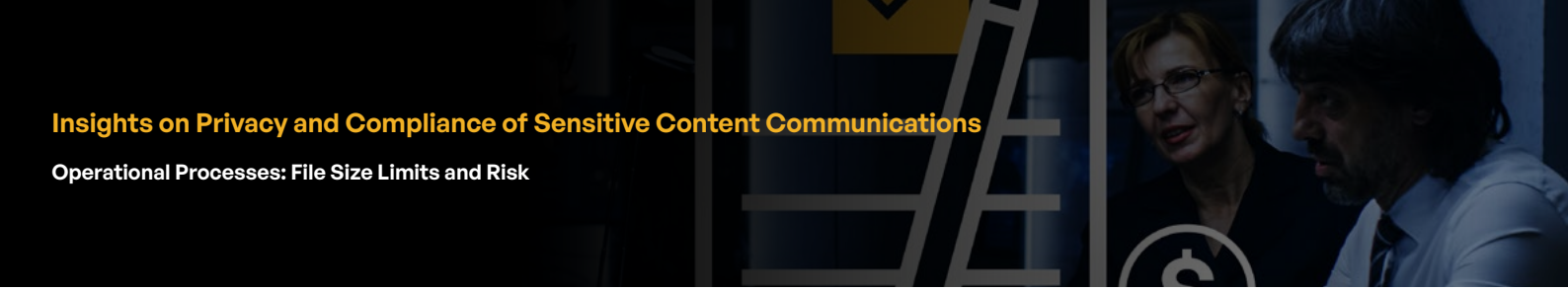
with 30,001 employees indicated they must reconcile 20-plus communication tool logs.



All this log reconciliation consumes valuable time and resources; 20% of respondents said it takes over 40 hours of staff time per month, and another 40% said it takes over 25 staff hours monthly (Figure 73). As organizational size increases, so does the difficulty in aggregating logs; 24% of organizations with more than 30,001 employees indicated they spend *over 40 hours* per month (Figure 74). Another 9% of organizations with 30,001-plus employees noted it is not feasible to aggregate their logs, a revelation that there is a significant security and compliance risk. On the industry front (Figure 75), legal firms are the highest industry segment to admit it is impossible to reconcile their logs (10%). Higher education institutions lead industries in the time spent consolidating logs—with 30% spending 40 or more hours each month.

Of industry segments, more federal government respondents (34%) said they must consolidate over 20 communication channel logs.





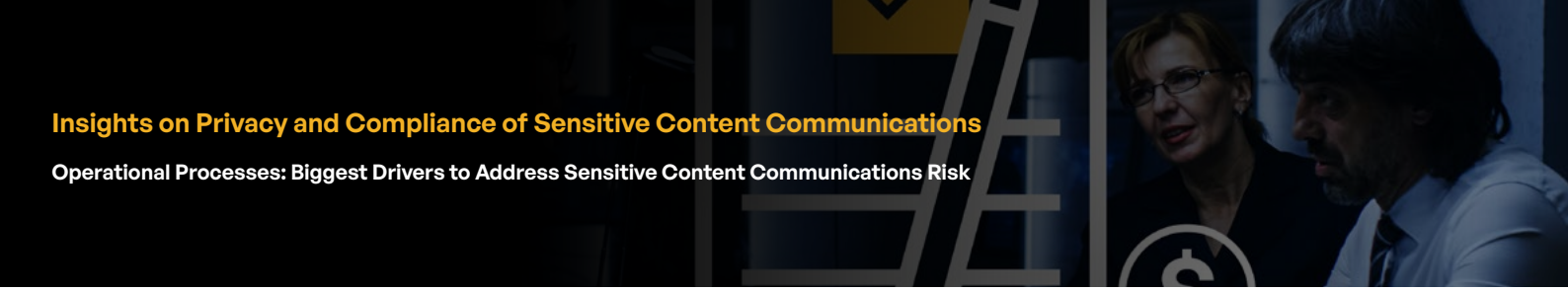
File Size Limits and Risk

File size limits is a challenge faced by many content communication tools. Frustration by employees who are simply trying to do their jobs can sometimes lead to the unauthorized use of consumer-grade file sharing services to bypass the limitations. But even for those users who follow the rules, the resulting workarounds can trigger significant expenditure of staff time.

Except for SFTP (at 27%), over *three in 10* organizations need to implement workarounds due to file size limits for email, file sharing, and managed file transfer over 50 times per month (Figure 76). Around 10% said they must do so over *100 times per month* (10% for email, 11% for file sharing, 8% for SFTP, and 11% for managed file transfer). More than half do so more than *25 times per month* across these four communication channels. In terms of regions, the frequency rate is higher in North America than EMEA and Asia-Pacific; those needing to do so over 100 times per month are *more than twice as much* across each of the communication channels (Figure 77).

30+%

organizations must implement file size workarounds 50x per month for email, file sharing, managed file transfer, and SFTP.



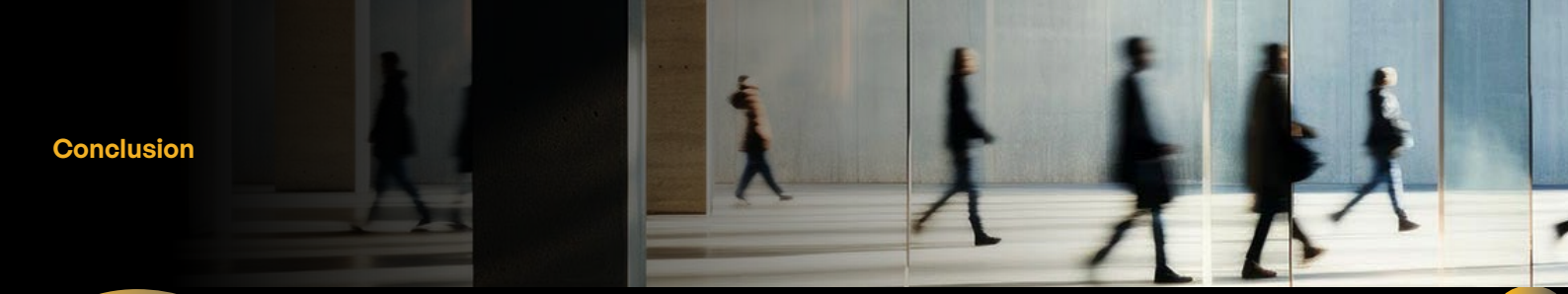
Biggest Drivers to Address Sensitive Content Communications Risk

By now, readers are probably seeing some of the problems posed by having many sensitive content communication tools—the risks and challenges of security and compliance, the lack of transparent visibility across data types, and inefficient manual processes. To gauge how survey participants are dealing with this complexity, we asked them to choose their top two drivers for unifying and securing their sensitive content communications (Figure 78). The most-cited response (56%) was to *protect intellectual property and corporate secrets*. Close behind were *mitigating litigation* (51%) and *avoiding regulatory violations* (48%).

There were interesting differences in the prominence of litigation according to job role (Figure 79). It was cited by 79% of IT professionals and 61% of security team members—but only 39% of risk and compliance employees. Respondents in the legal (75%), oil and gas (75%), and federal government (69%) sectors were especially concerned about leakage of IP (Figure 80).

Regionally, there were interesting variances as well (Figure 81). By far, *Asia-Pacific* respondents marked avoidance of detrimental brand impact as a top driver (79%) followed by mitigation of lengthy and expensive litigation (61%). For *EMEA*, the highest driver was preventing leakage of confidential IP and corporate secrets (62%) followed by mitigation of lengthy and expensive litigation (51%). *North American* respondents cited avoidance of operational outages and lost revenue at the top of their list (57%) followed by preventing leakage of confidential IP and corporate secrets (51%).

The biggest drivers behind the drive to unify and secure sensitive content communications were protection of IP and corporate secrets (56%), mitigation of litigation (51%), and avoidance of regulatory violations (48%).



Conclusion

Findings from this year's Sensitive Content Communications Privacy and Compliance Report underscore the critical need for organizations to take *proactive measures* in safeguarding their sensitive content. One key takeaway is to *consolidate communication tools* onto a single platform. By reducing the number of disparate tools used for content communication, organizations can significantly lower the risk of data breaches and improve operational efficiency. Specifically, organizations with fewer communication tools experience fewer breaches, indicating a correlation between tool consolidation and enhanced security.

The report also emphasizes the substantial risks associated with *untagged and unclassified data*. Organizations that fail to implement robust data tagging and classification systems are at a higher risk of data breaches, as they lack the necessary visibility and control over their sensitive content. The exponential growth of data, further accelerated by the adoption of GenAI, makes it imperative for organizations to prioritize data classification to mitigate these risks effectively.

Implementing *zero-trust principles and advanced security capabilities* are critical for enhancing sensitive content communications security. Report findings highlight significant security gaps and the need for strict content-defined zero trust that includes attribute-based access controls, comprehensive encryption, real-time monitoring, and data loss prevention. As our findings show, certain industry segments and regions and countries have larger gaps than others.

The data also highlights *significant risks* associated with sensitive content exchanges with *third parties*: the more third parties with which respondents send and share sensitive content, the more data breaches and higher litigation costs they experience. As a result, organizations must ensure they have comprehensive governance tracking and controls as well as advanced security capabilities in place to mitigate third-party risks.

On that note, a final comment is worth including on the *cost of data breaches*, particularly that connected with *litigation*. This year's survey revealed that many organizations incur significant legal costs that are often not accounted for in traditional breach cost estimations. Damaged brand reputation, lost revenue, and disrupted operations are only one aspect resulting from data breaches. Compliance fines and penalties as well as extended litigation costs often have a long-tail effect felt over extended time frames. This underscores the importance of vetting and selecting sensitive content communication tools that adhere to security standards like FedRAMP, ISO 27001, SOC 2 Type II, NIST CSF 2.0, and others.

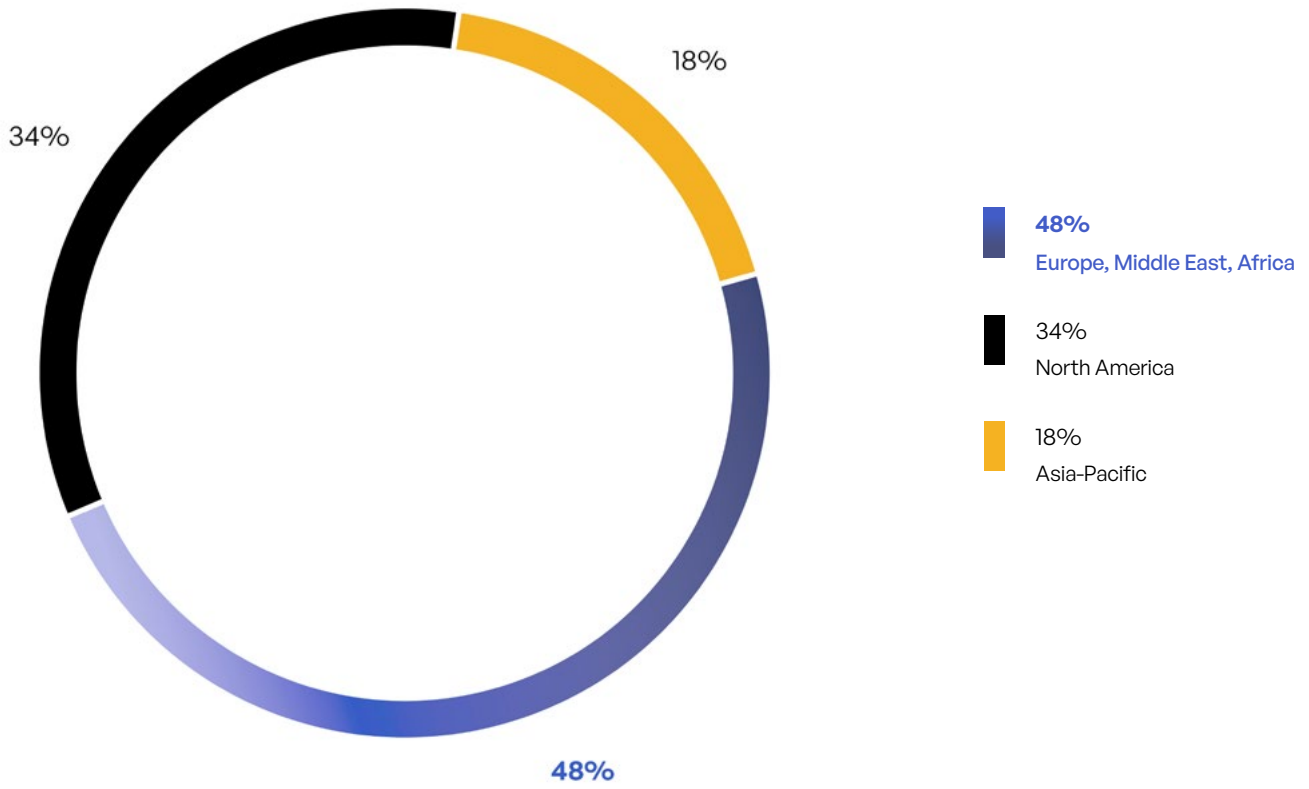


Figure 1: Regional Distribution.

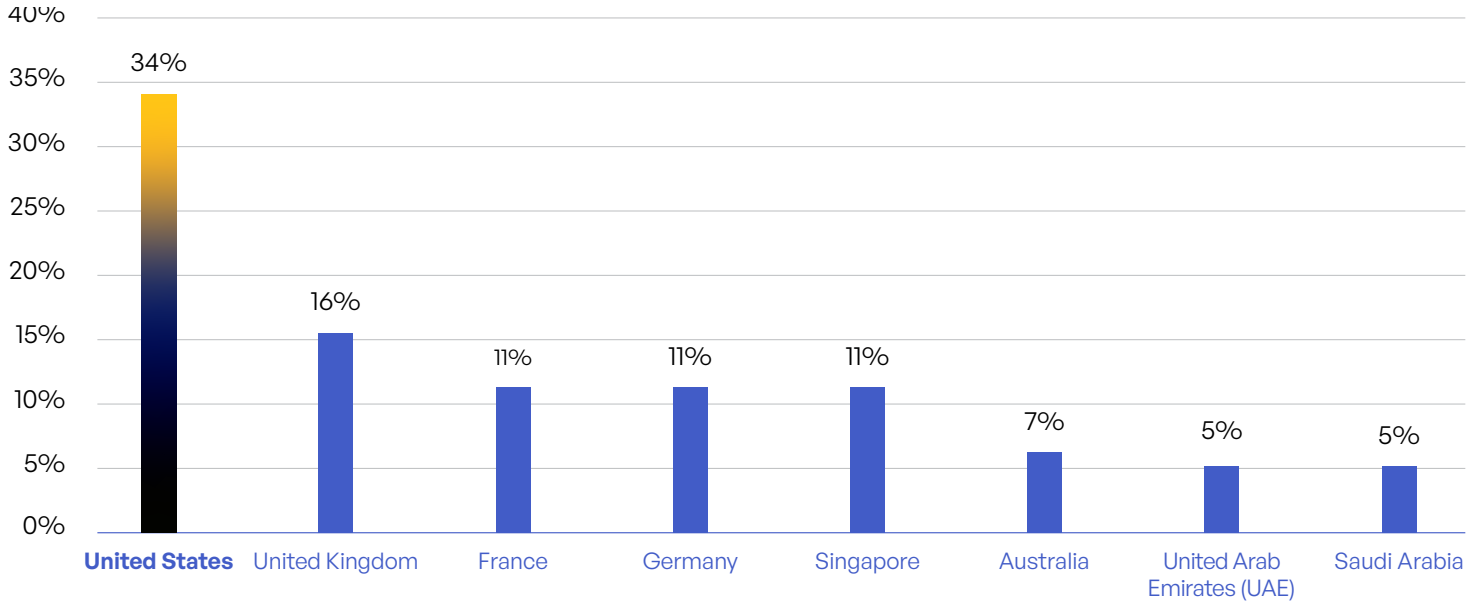


Figure 2: Country Distribution.

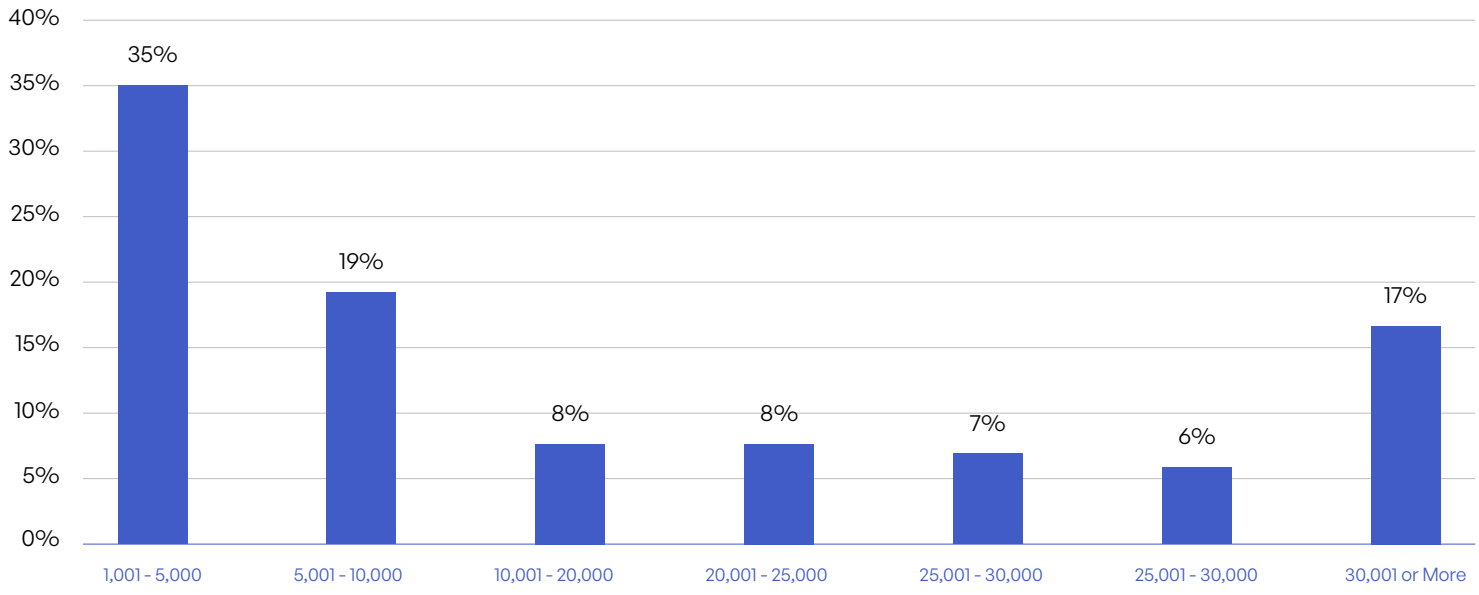


Figure 3: Organization Size.

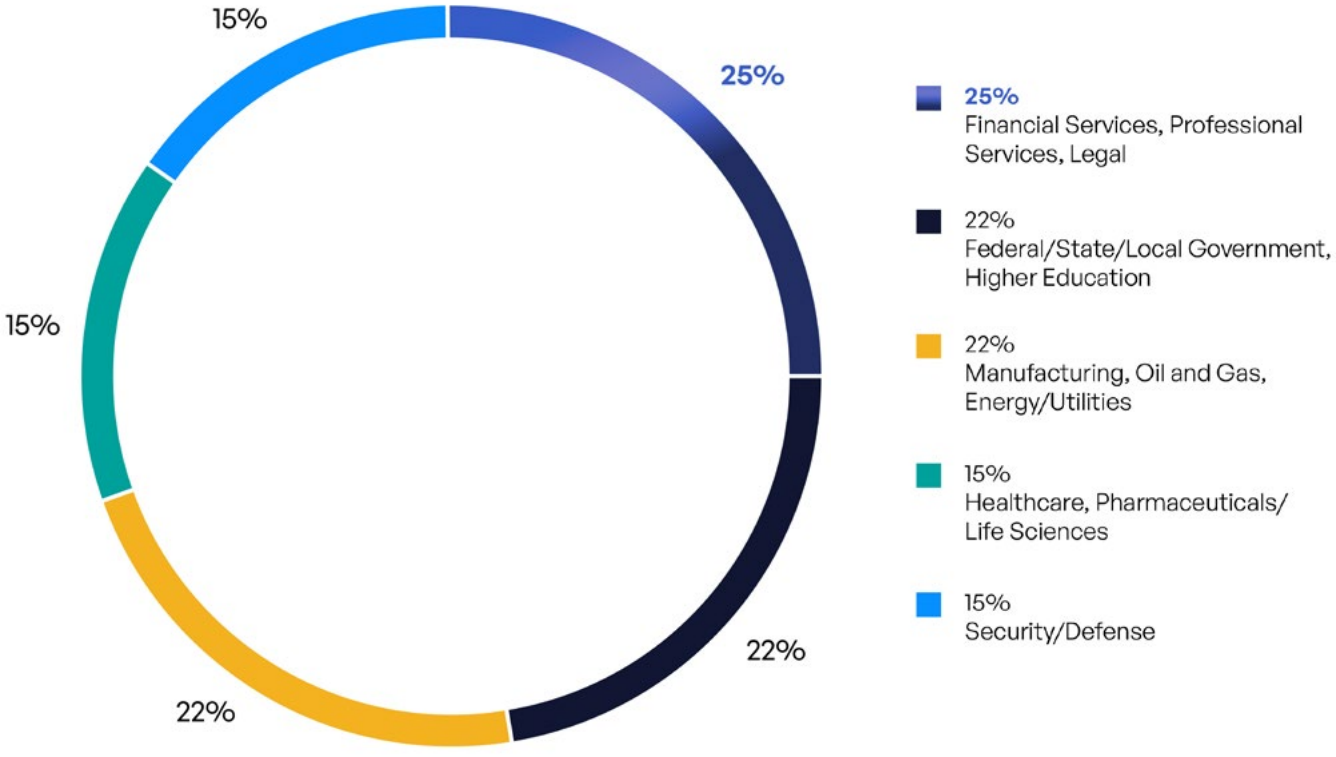


Figure 4: Industry Distribution.

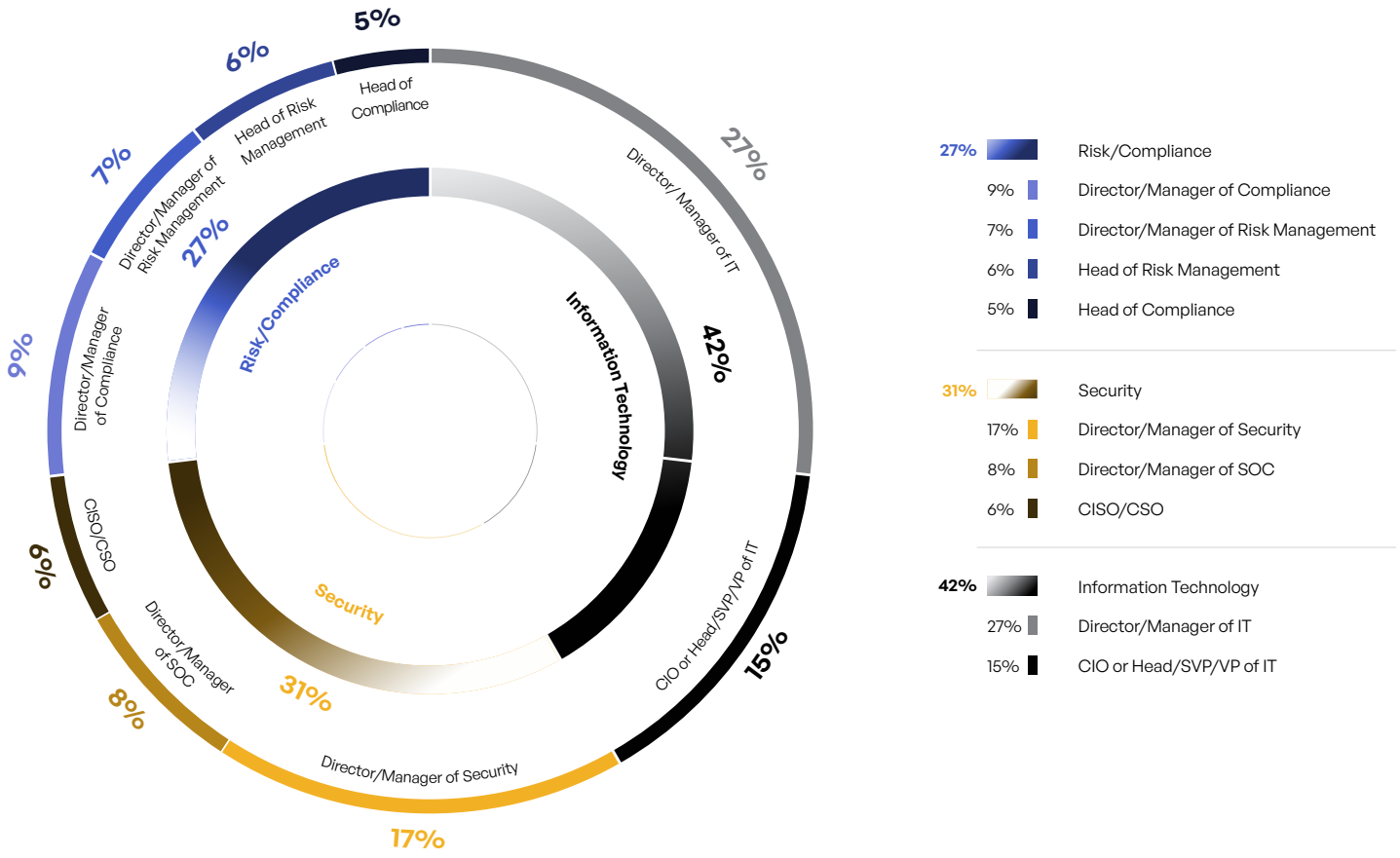


Figure 5: Job Roles/Responsibilities.

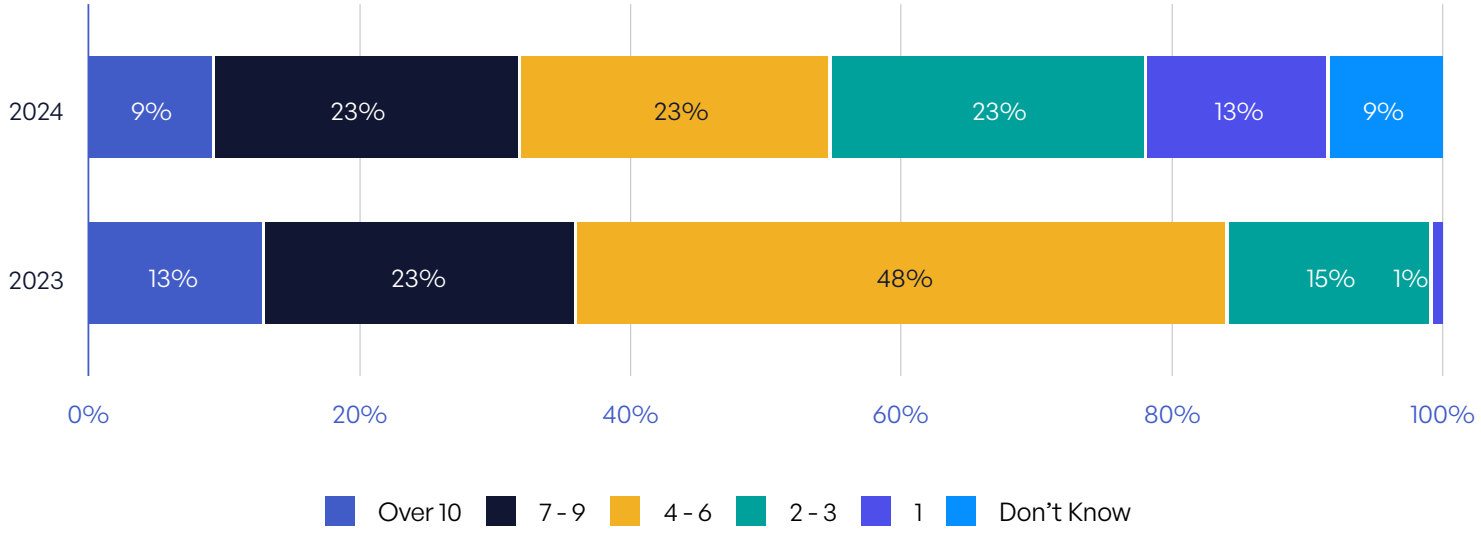


Figure 6: External Malicious Hacks of Sensitive Content in Past Year.

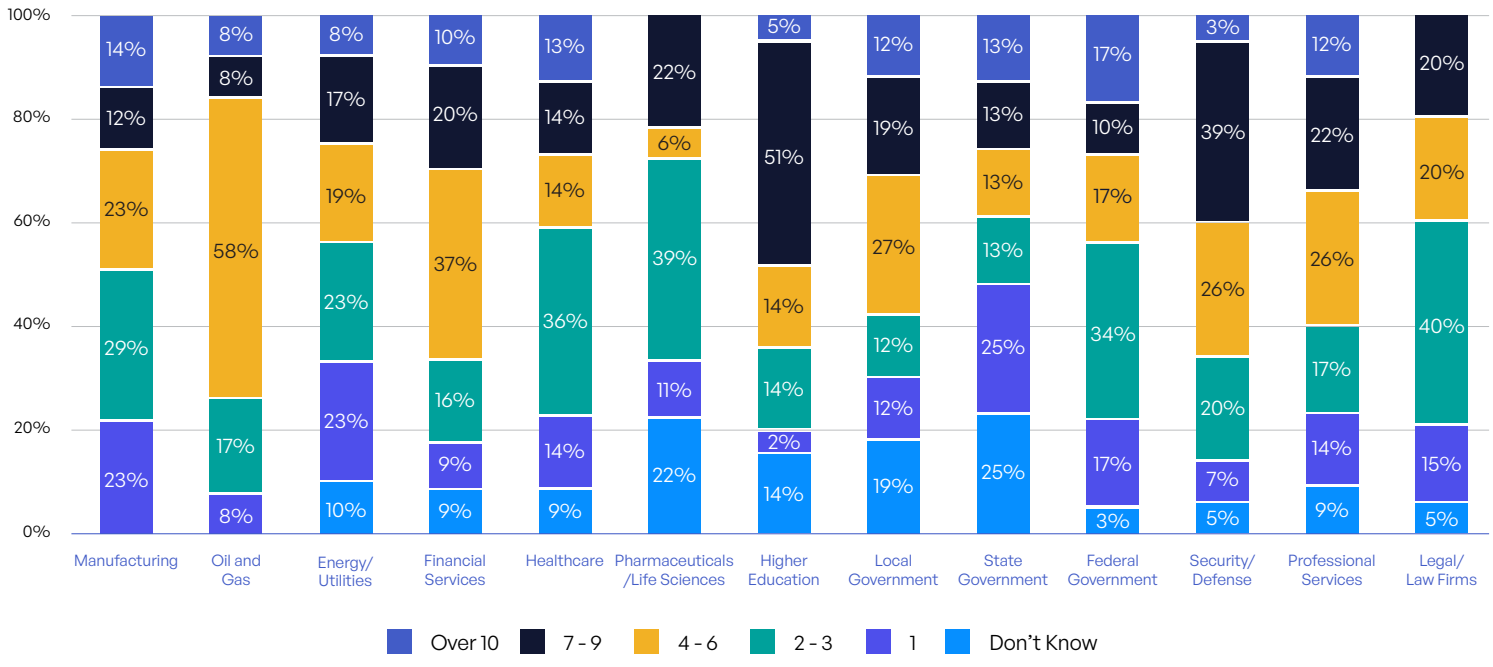


Figure 7: External Malicious Hacks by Industry.

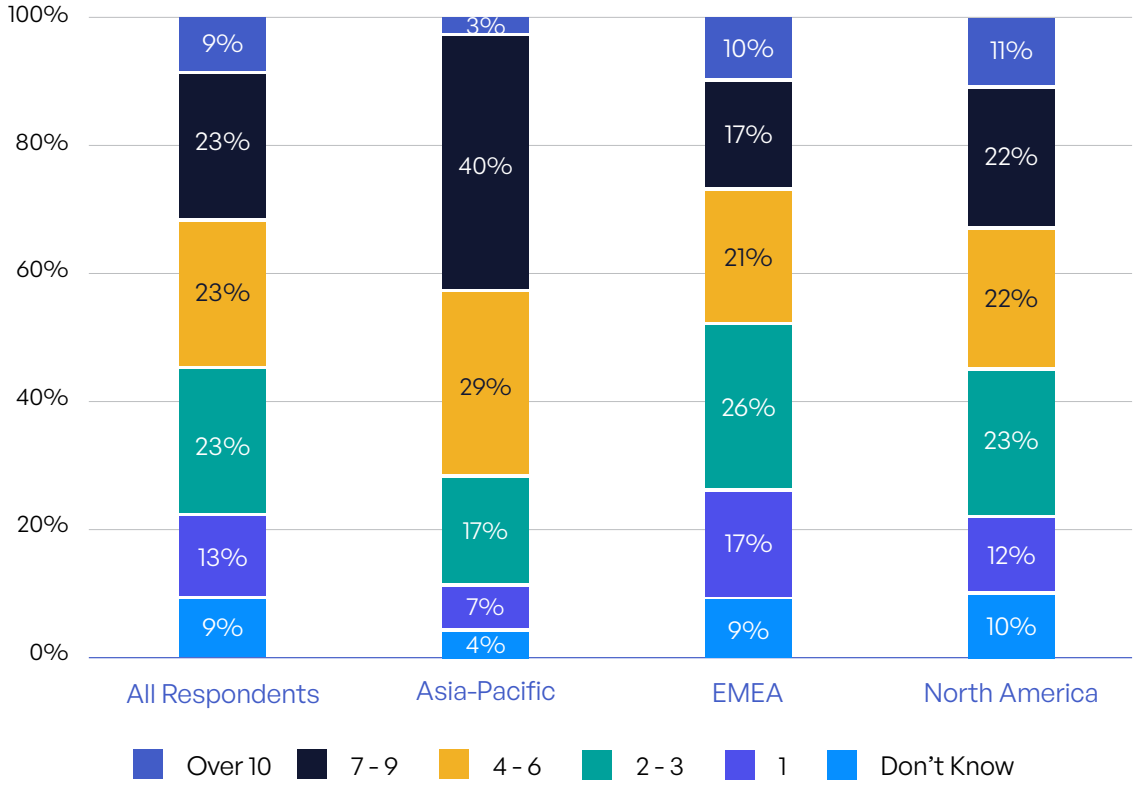


Figure 8: External Malicious Hacks by Region.

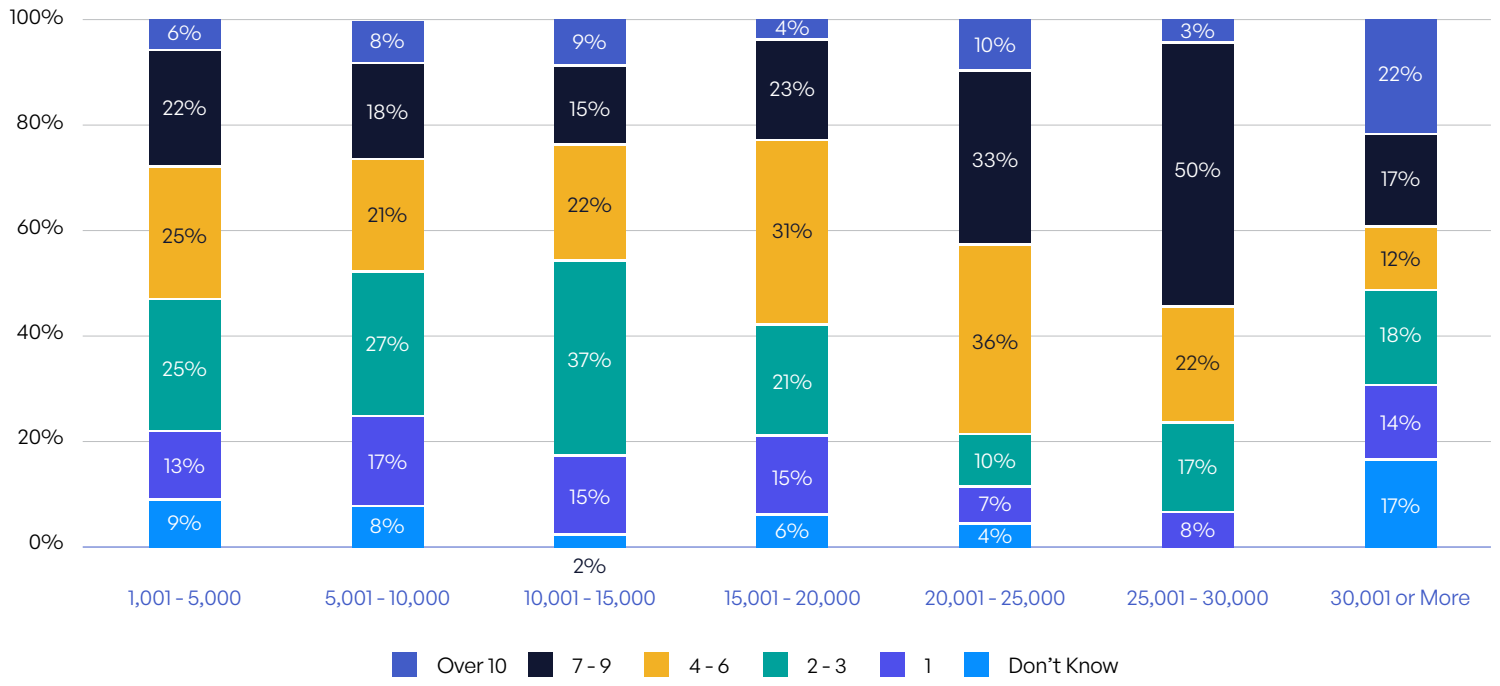


Figure 9: External Malicious Hacks by Company Size.

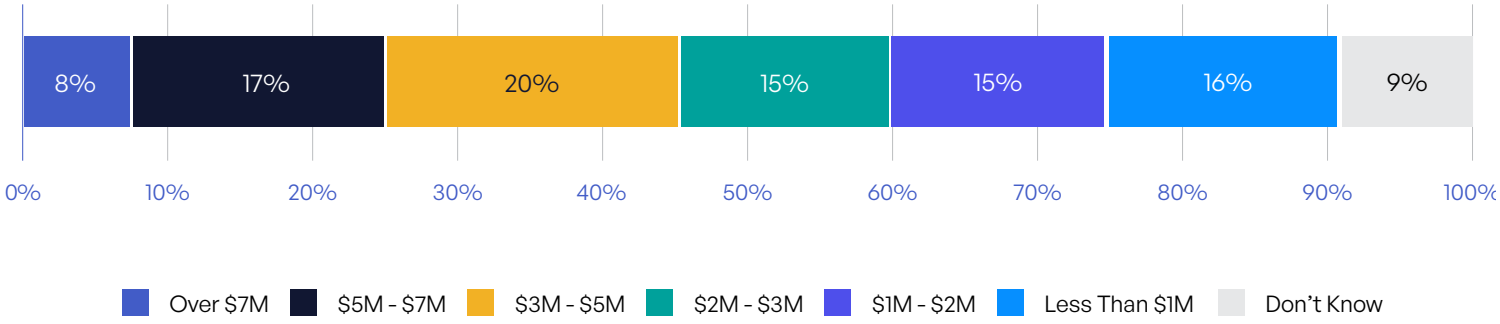


Figure 10: Annual Litigation Cost of Dealing With Data Breaches.

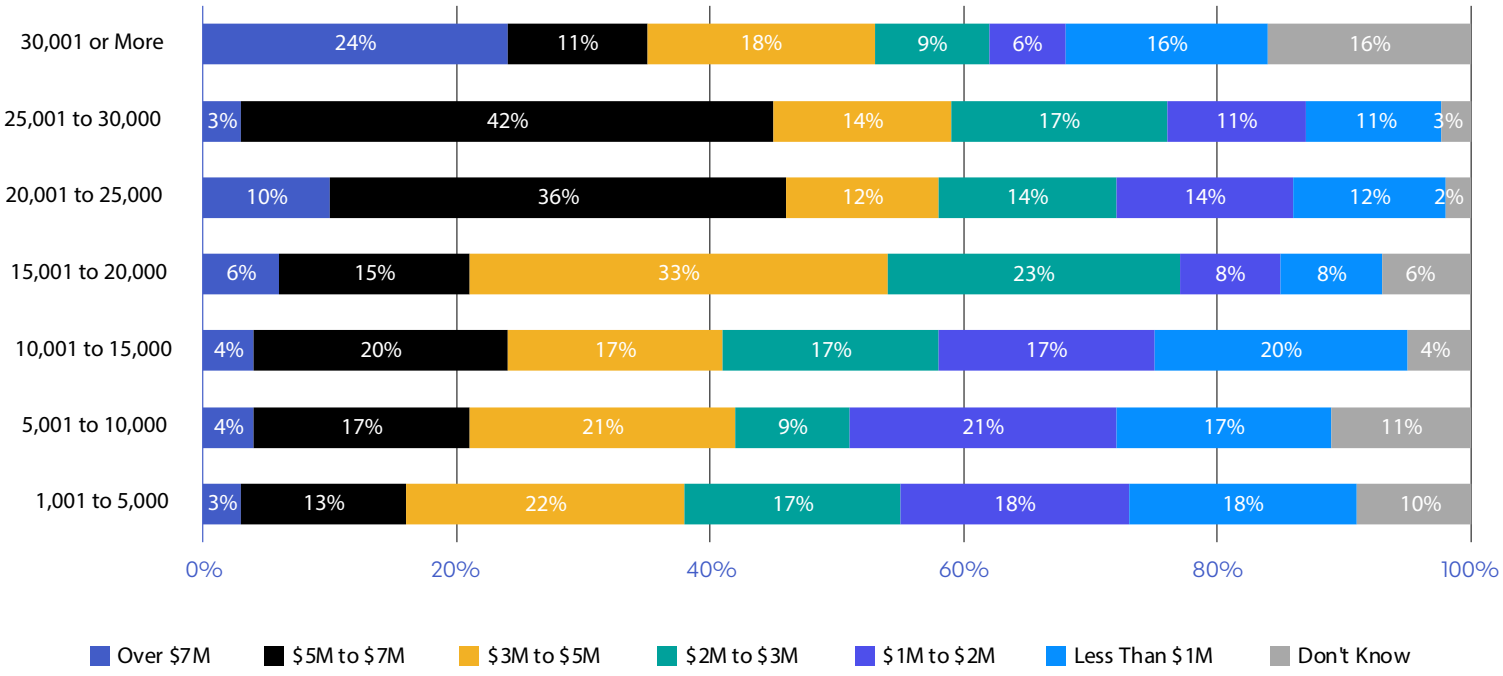


Figure 11: Annual Litigation Cost of Data Breaches per Organization Size.

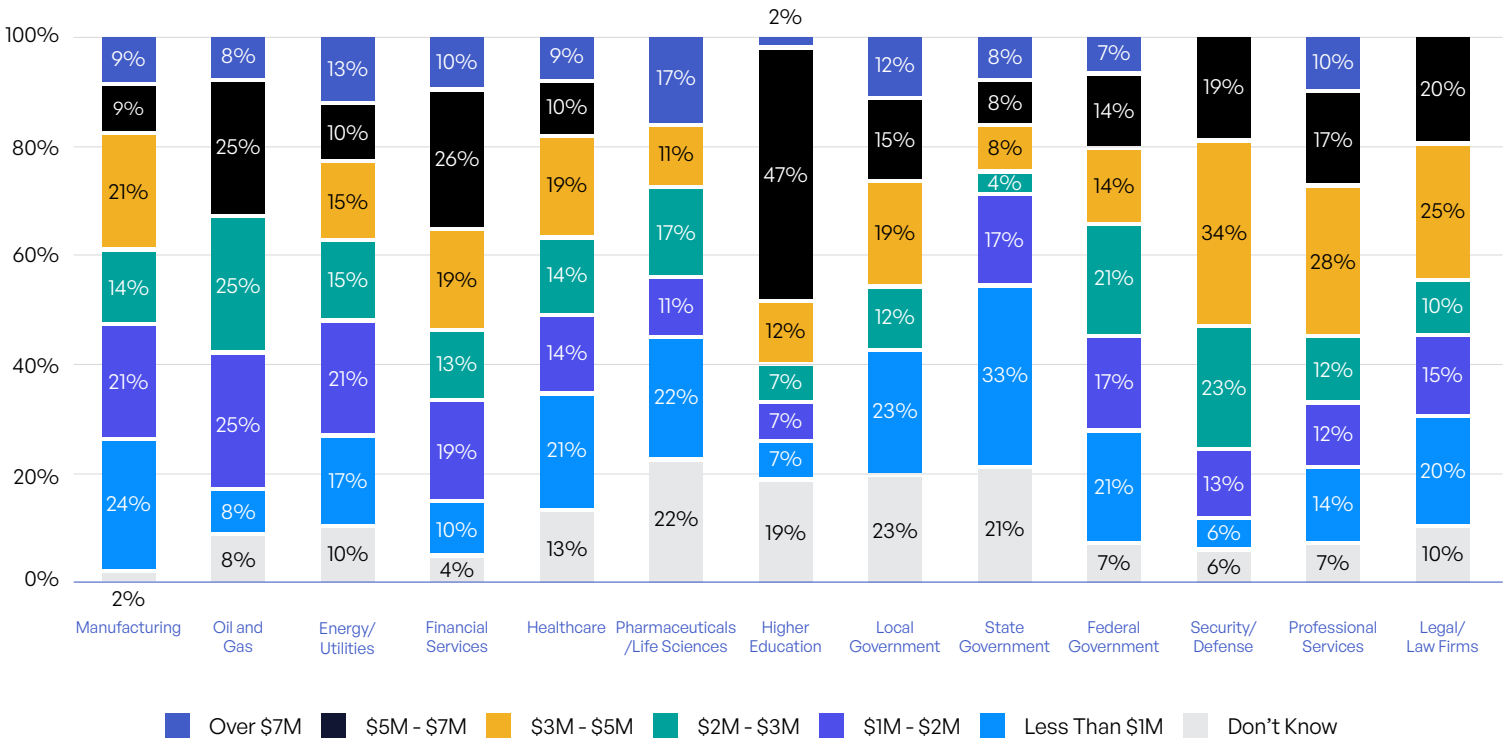


Figure 12: Cost of Dealing With Breaches by Industry.

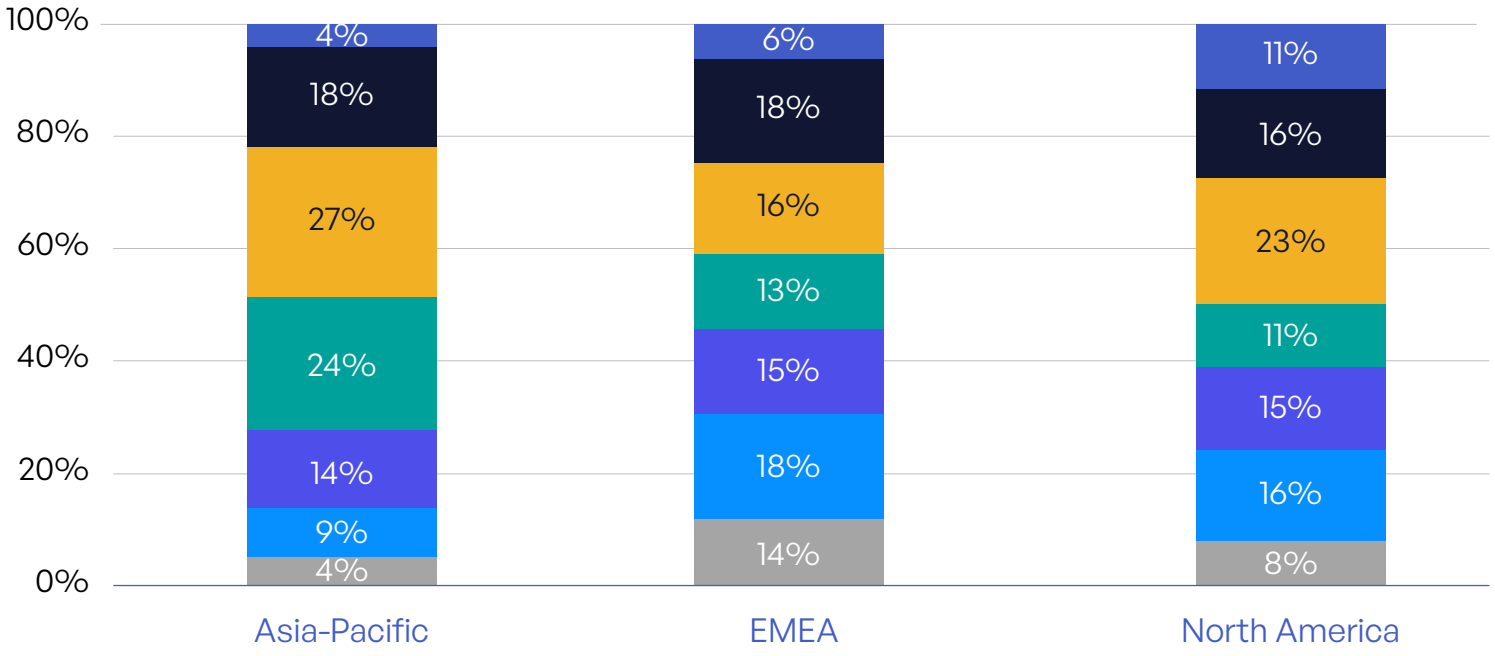


Figure 13: Litigation Cost Across Regions.

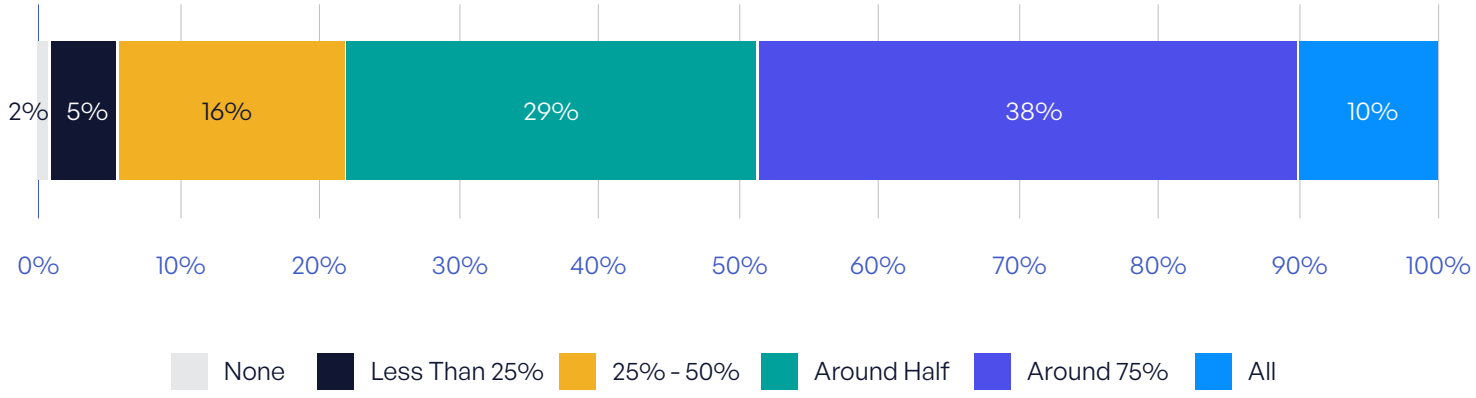


Figure 14: Unstructured Data That Is Tagged/Classified.

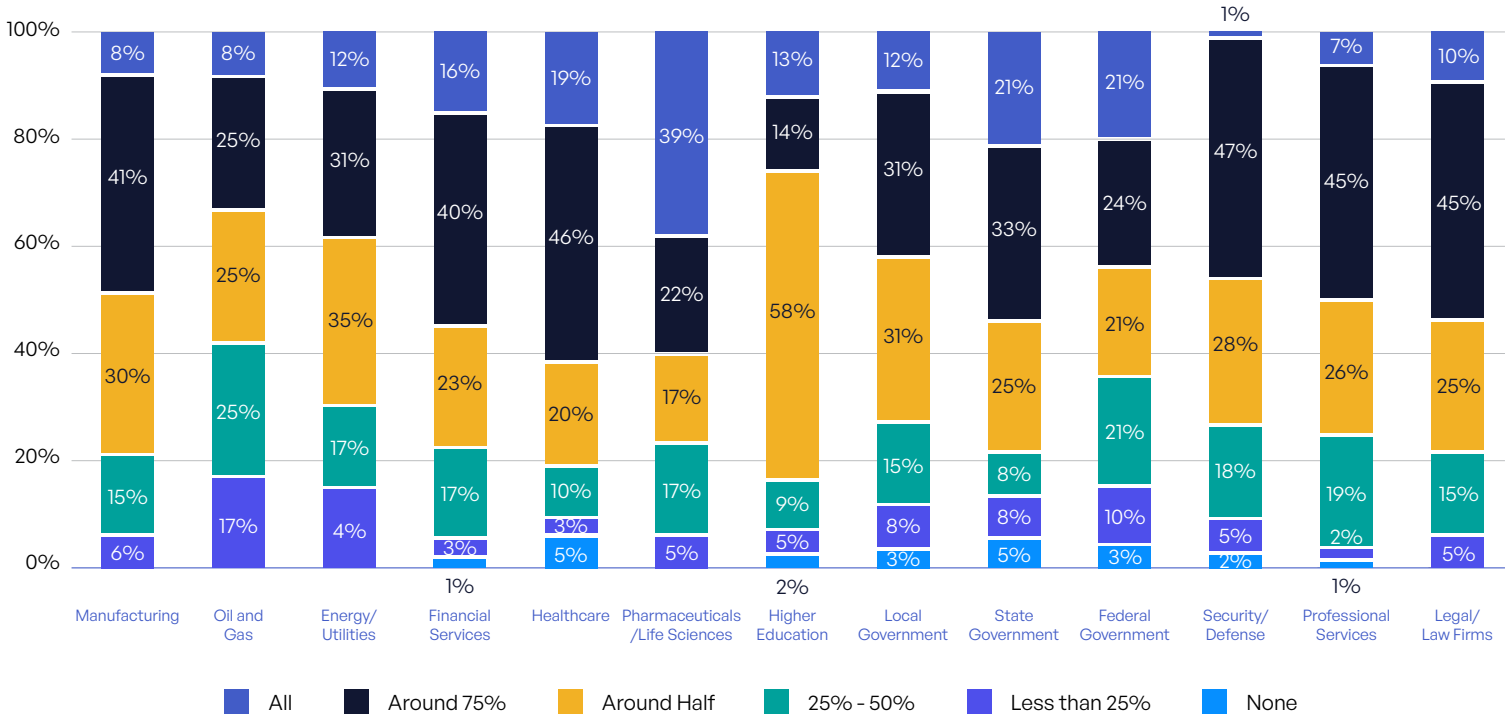


Figure 15: Unstructured Data Classification and Tagging Across Industries.

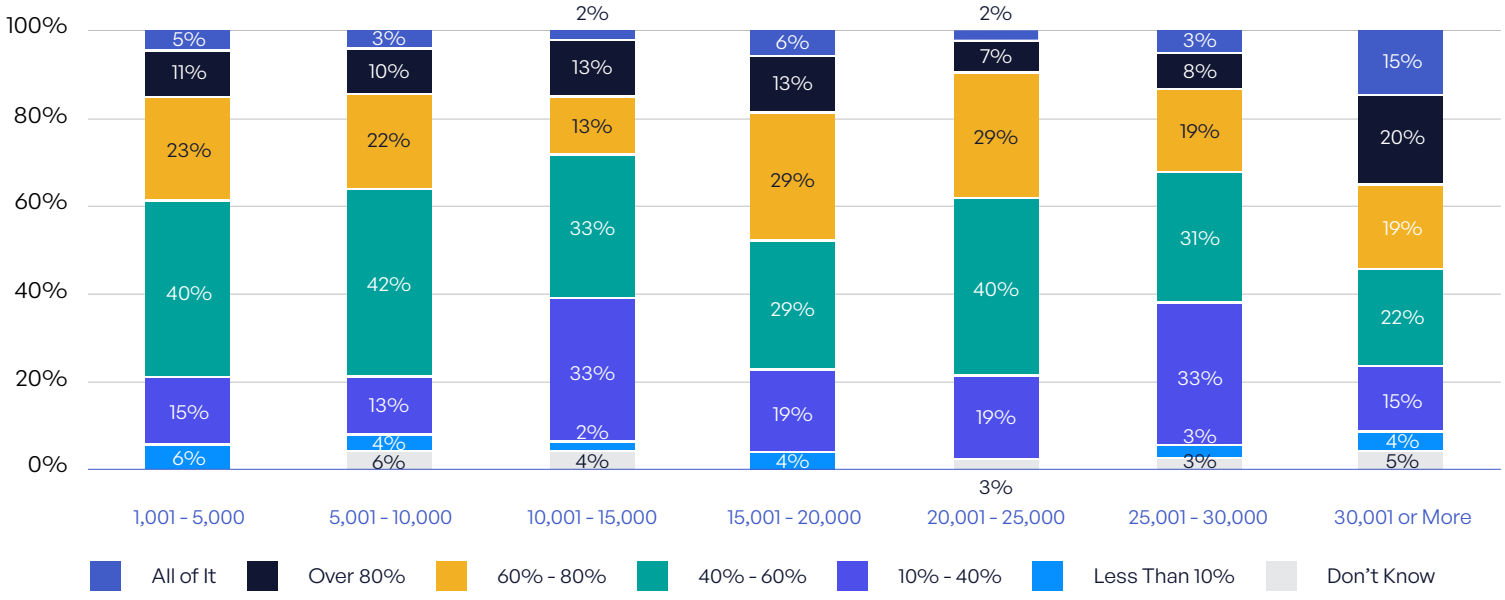


Figure 16: Unstructured Data That Is Tagged and Classified per Organization Size.

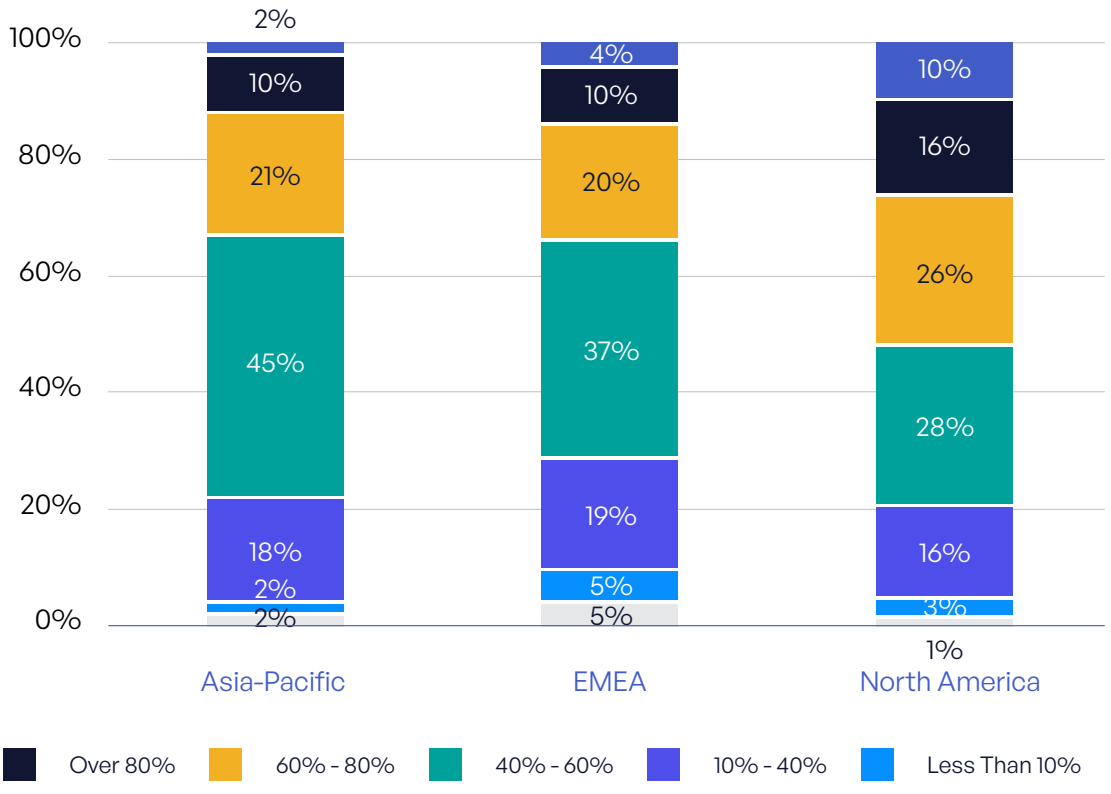


Figure 17: Unstructured Data That Is Tagged and Classified per Region.

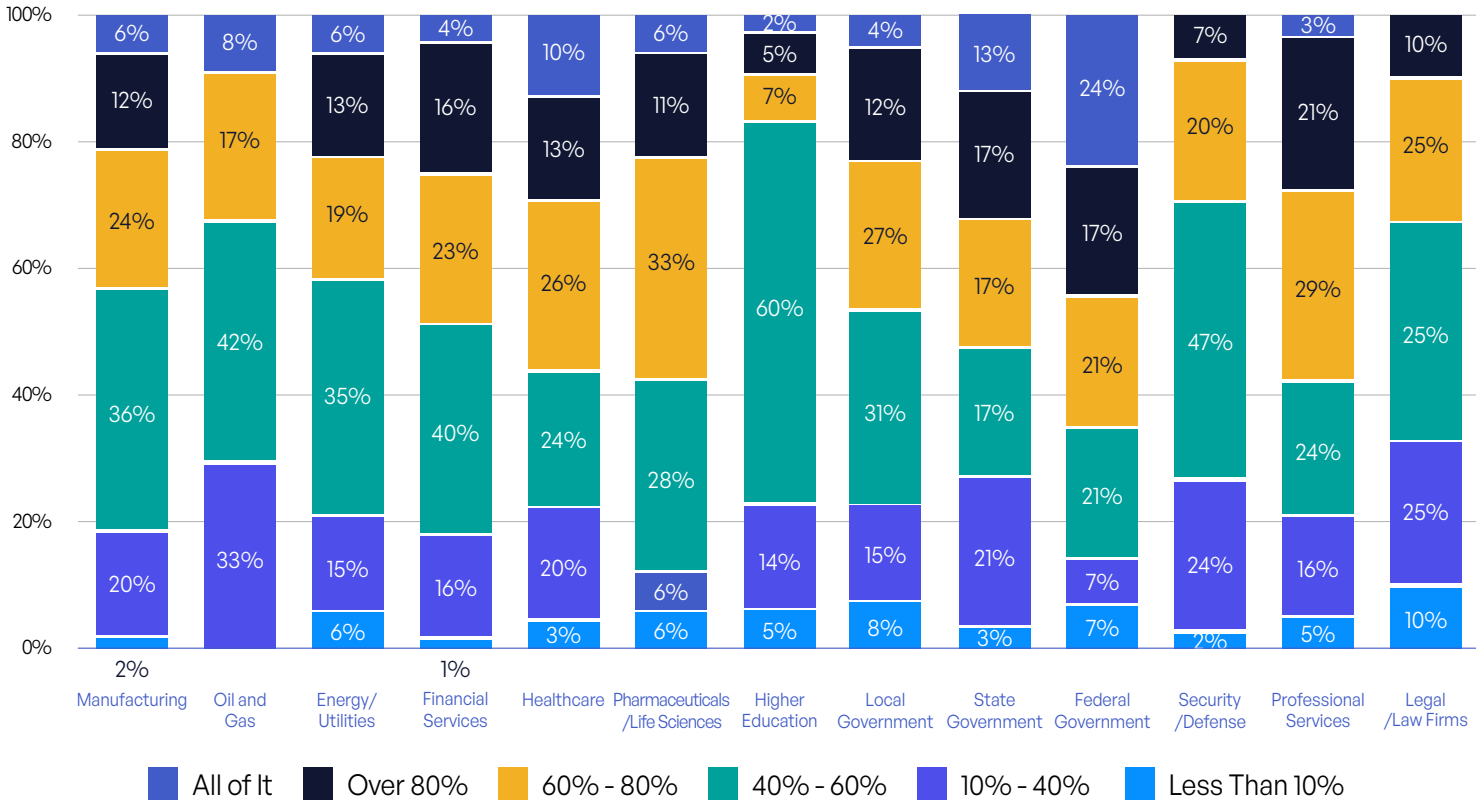


Figure 18: Unstructured Data That Is Tagged and Classified Across Industries.

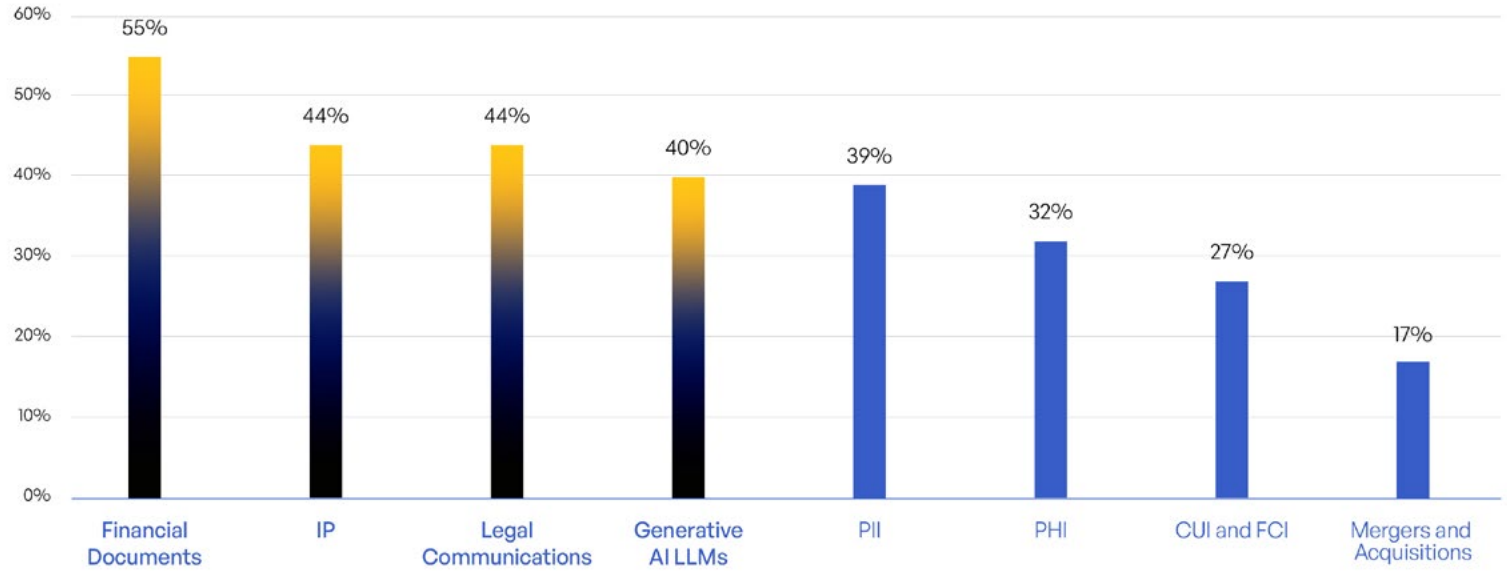


Figure 19: Top 3 Data Types and Concerns.

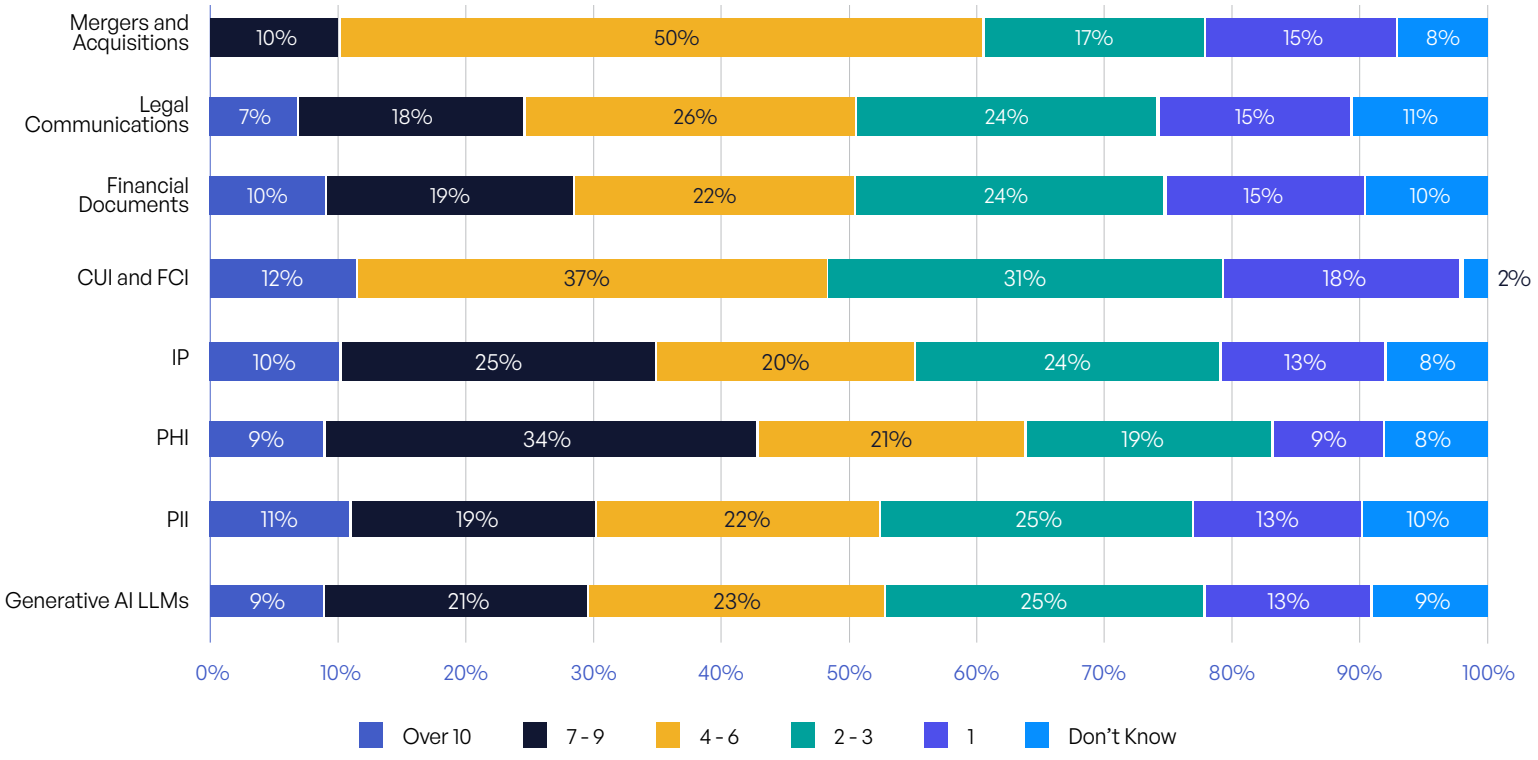


Figure 20: Data Types and Data Breaches.

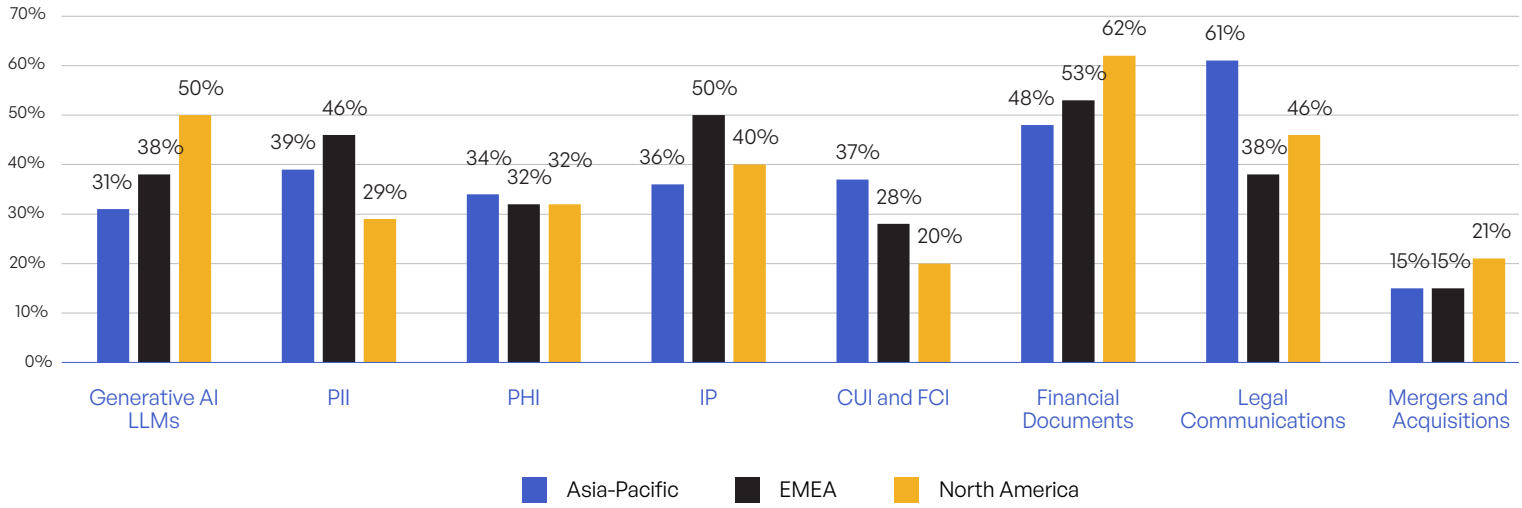


Figure 21: Top Data Type Concerns Across Regions.

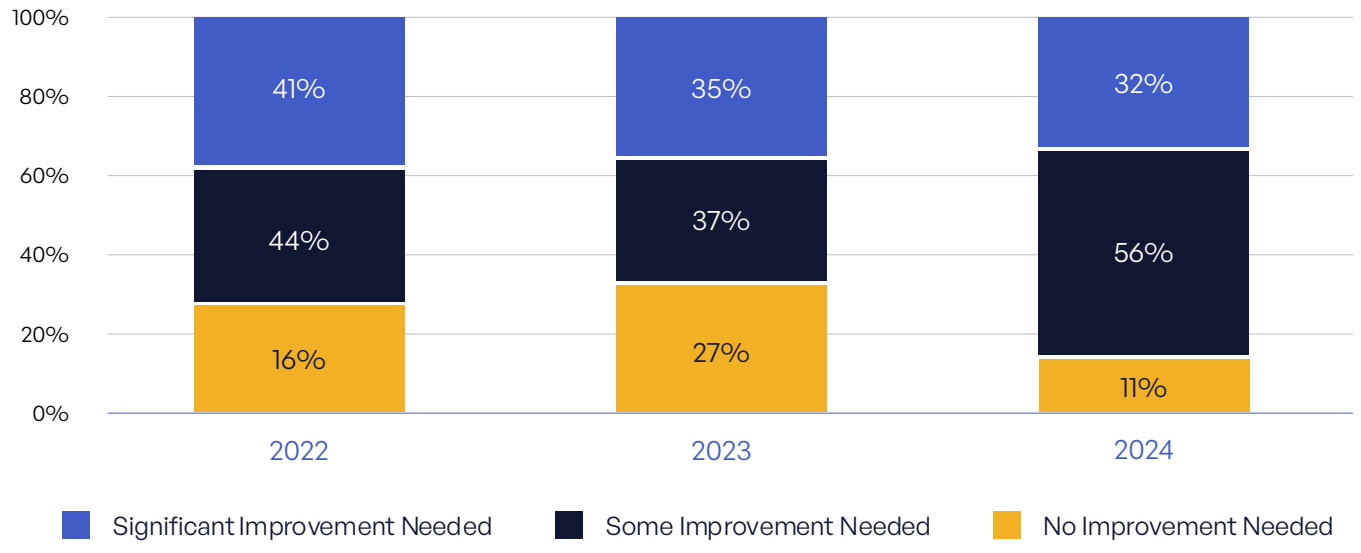


Figure 22: Improvement Needed in Measuring and Managing Content Communications Compliance Risk.

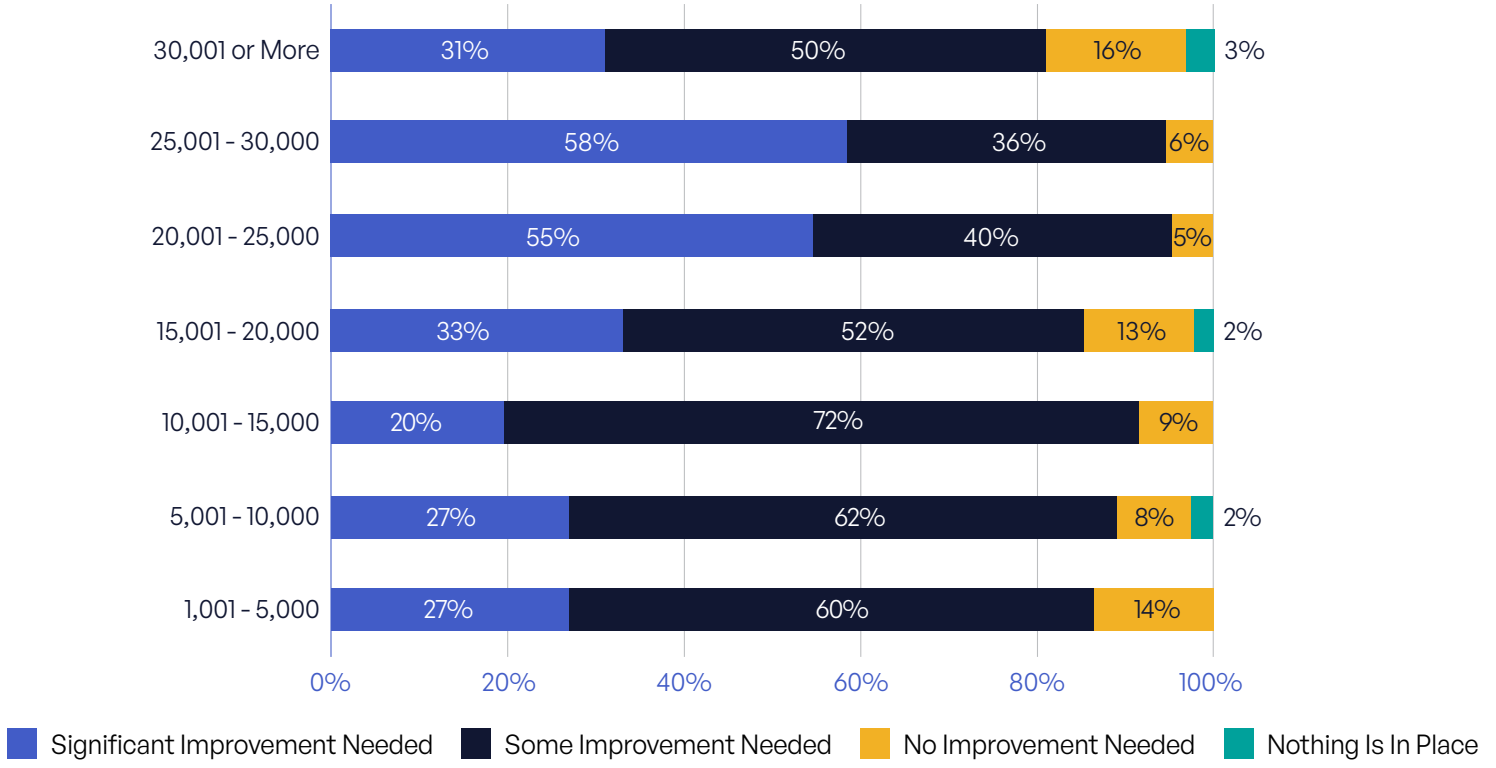


Figure 23: Improvement Needed in Measuring and Managing Content Communication Risk per Organization Size.

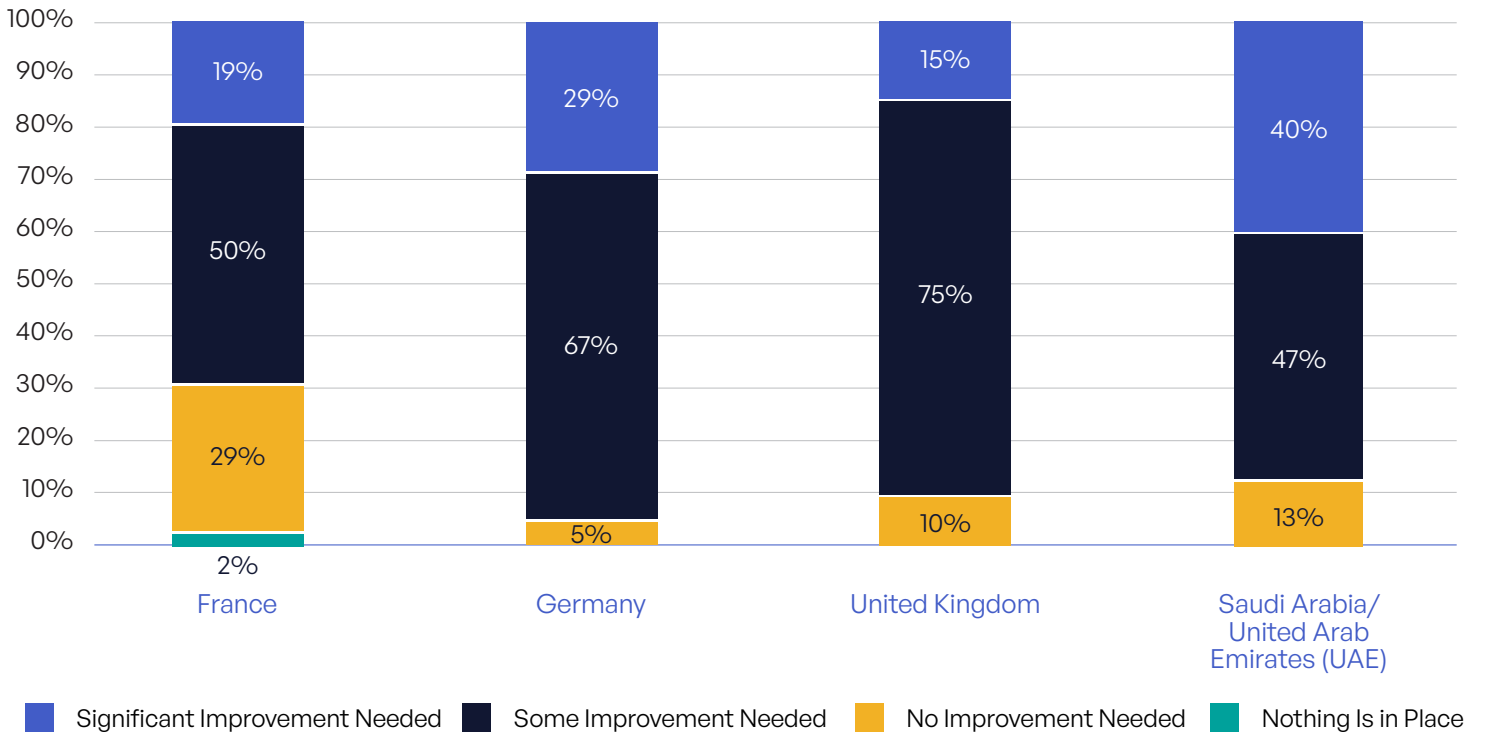


Figure 24: Improvement Needed in Managing Content Communication Compliance Risk Across Countries.

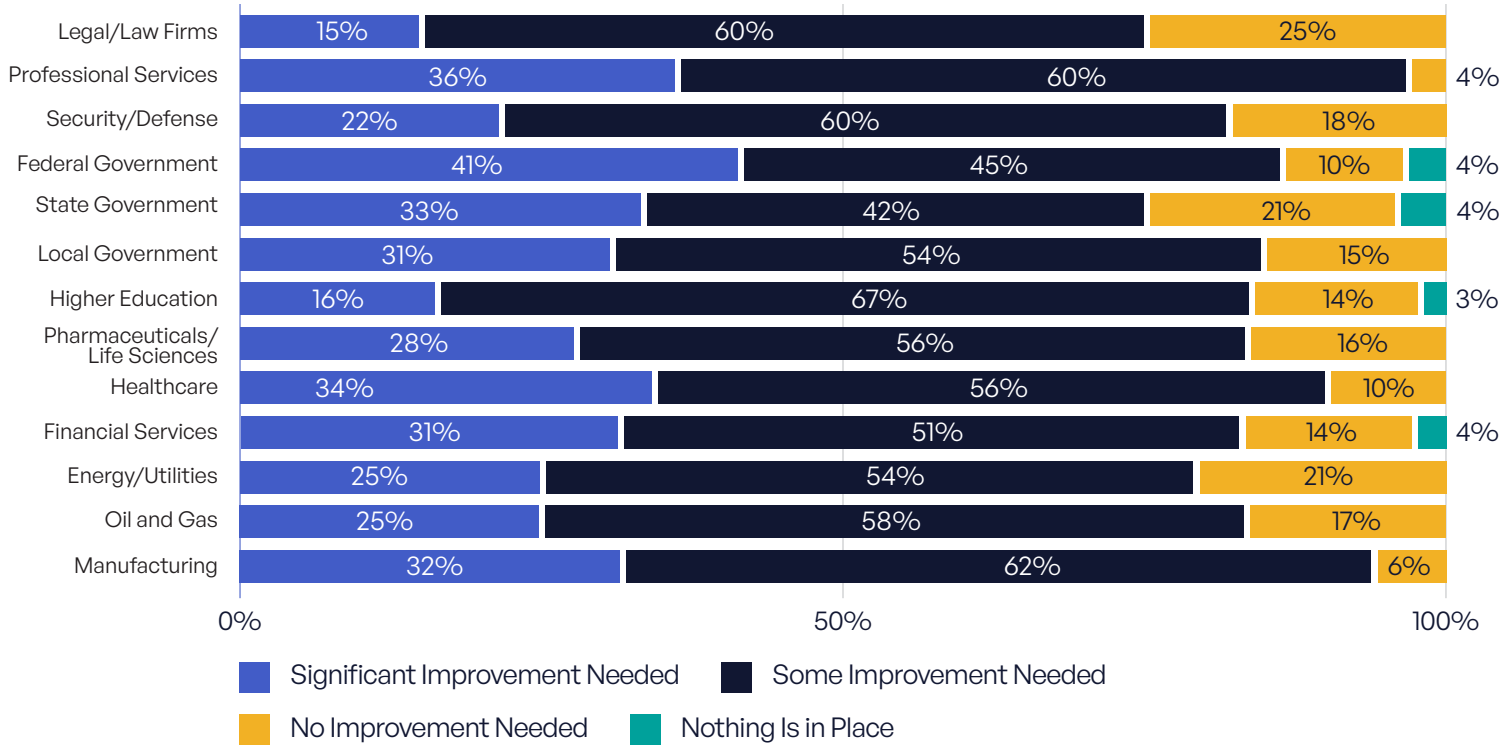


Figure 25: Improvement Needed in Managing Content Communication Compliance Risk Across Industries.

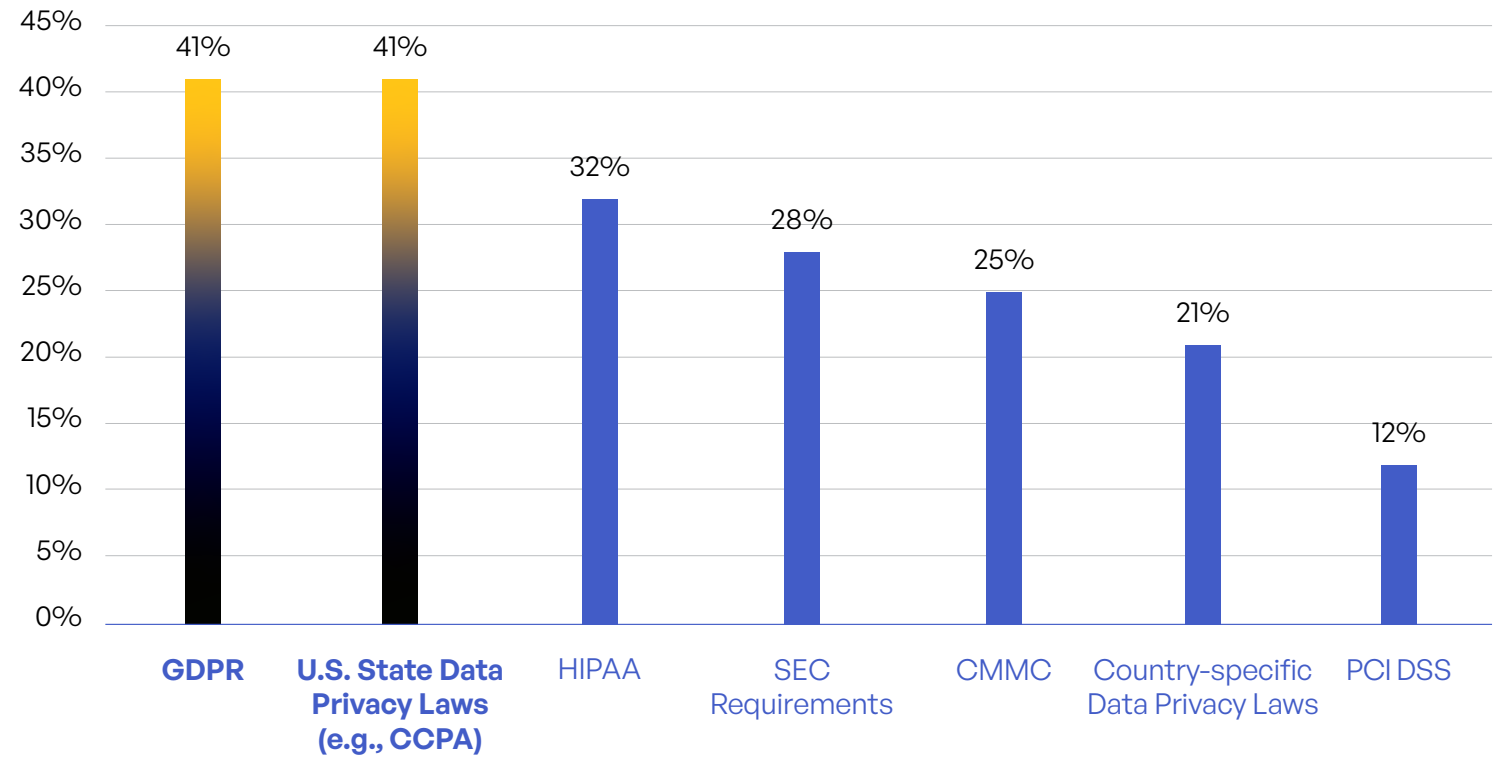


Figure 26: Biggest Areas of Focus for Privacy and Compliance.

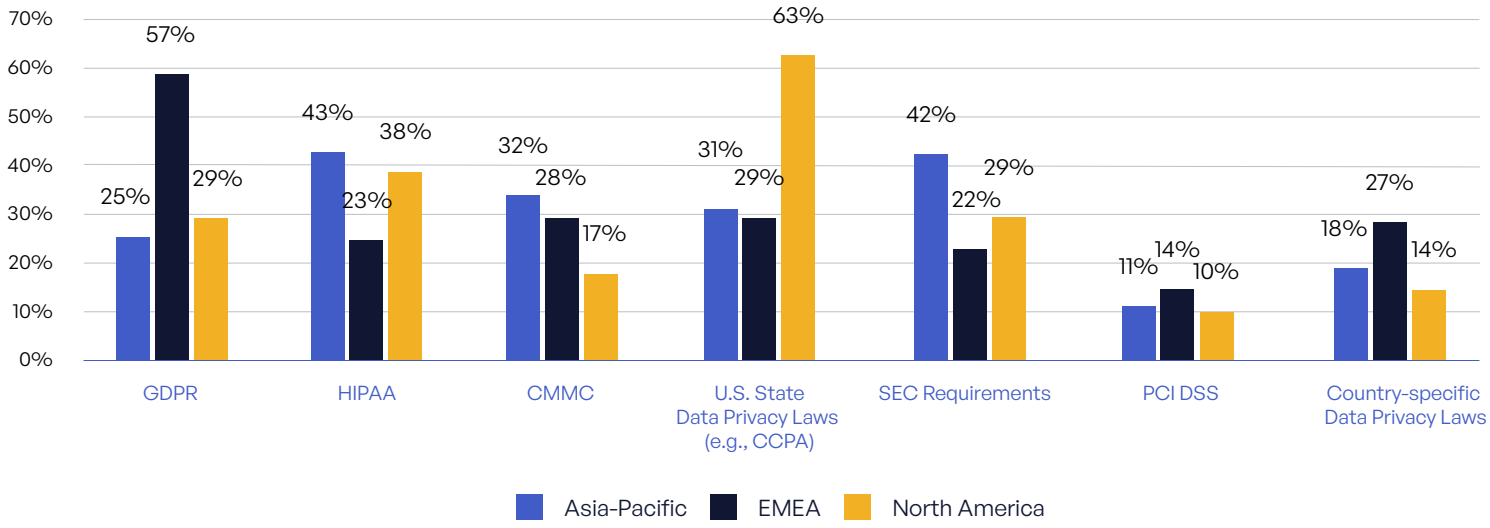


Figure 27: Biggest Data Privacy and Compliance Regulation Priorities per Region.

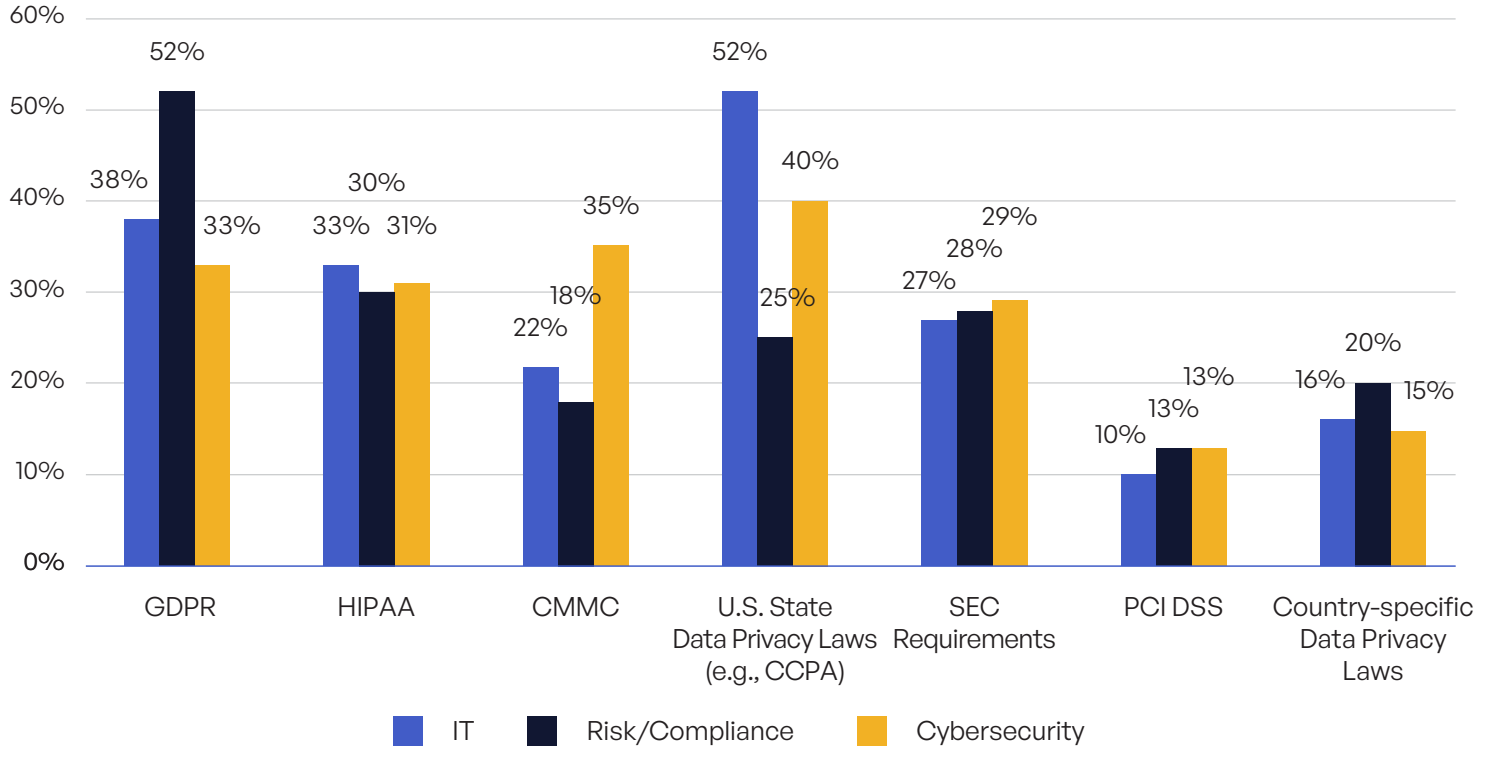


Figure 28: Biggest Data Privacy and Compliance Regulation Priorities per Job Function.

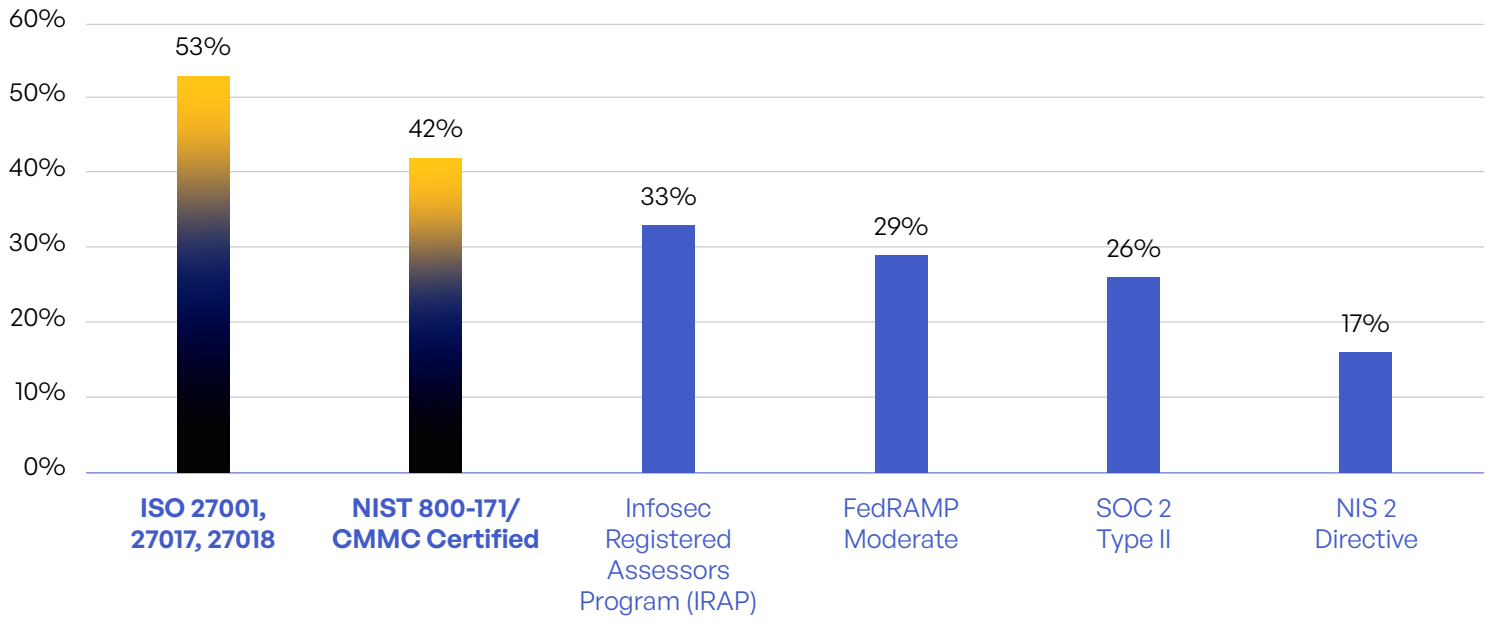


Figure 29: Most Important Security Certifications and Validations (Top 2 Priorities).

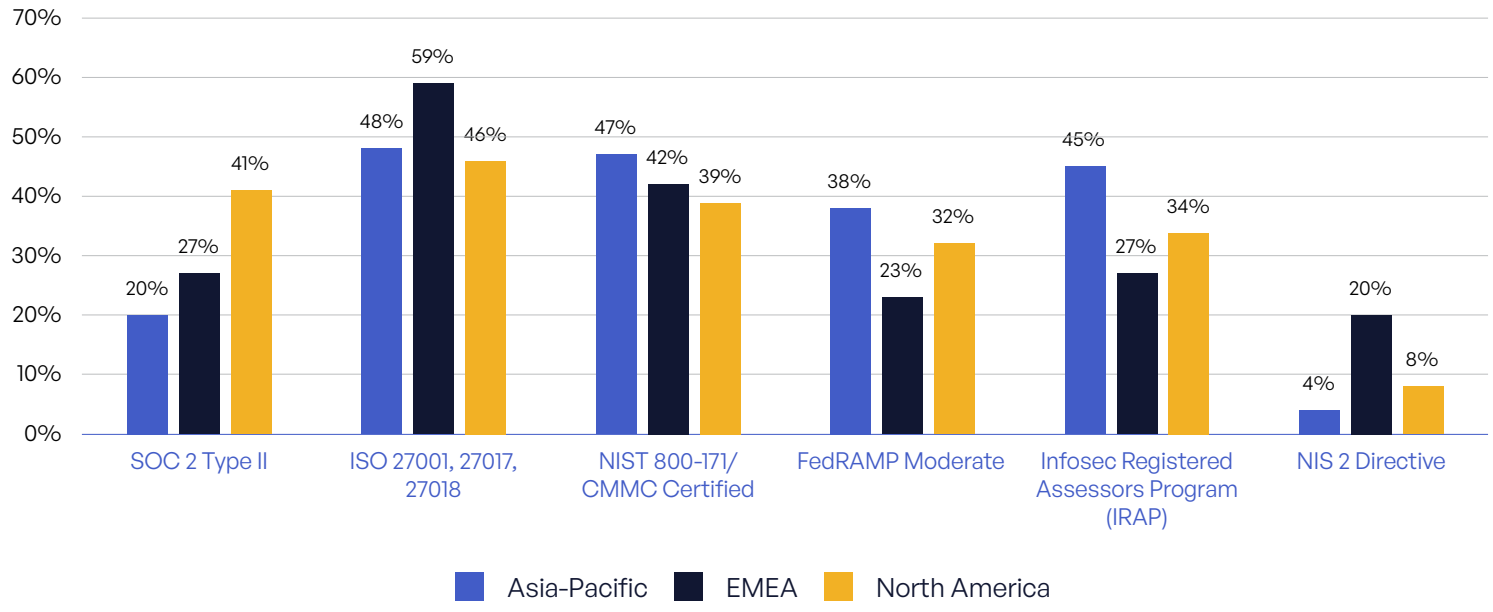


Figure 30: Biggest Security Standard Priorities per Region.

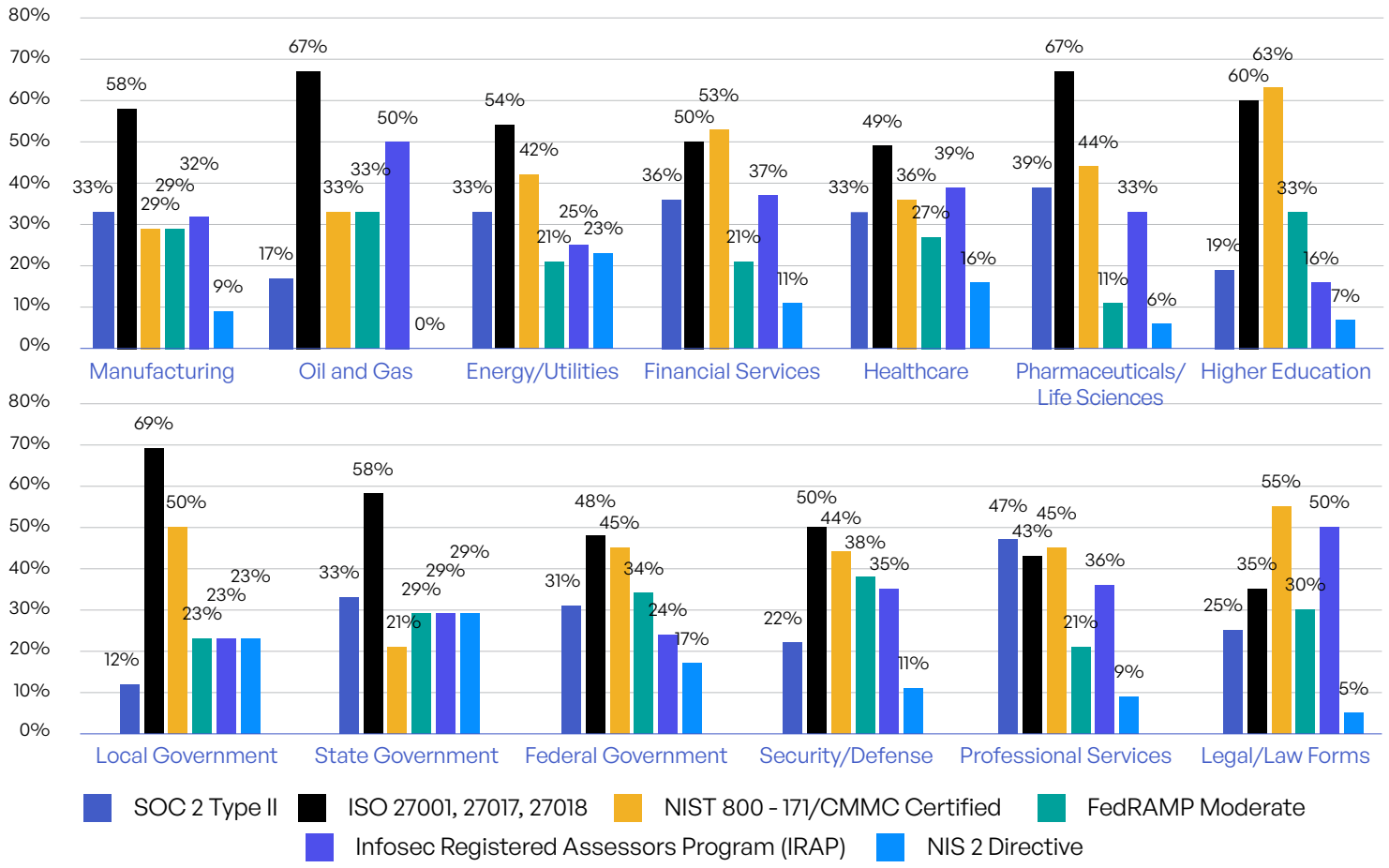


Figure 31: Biggest Security Standard Priorities per Industry.

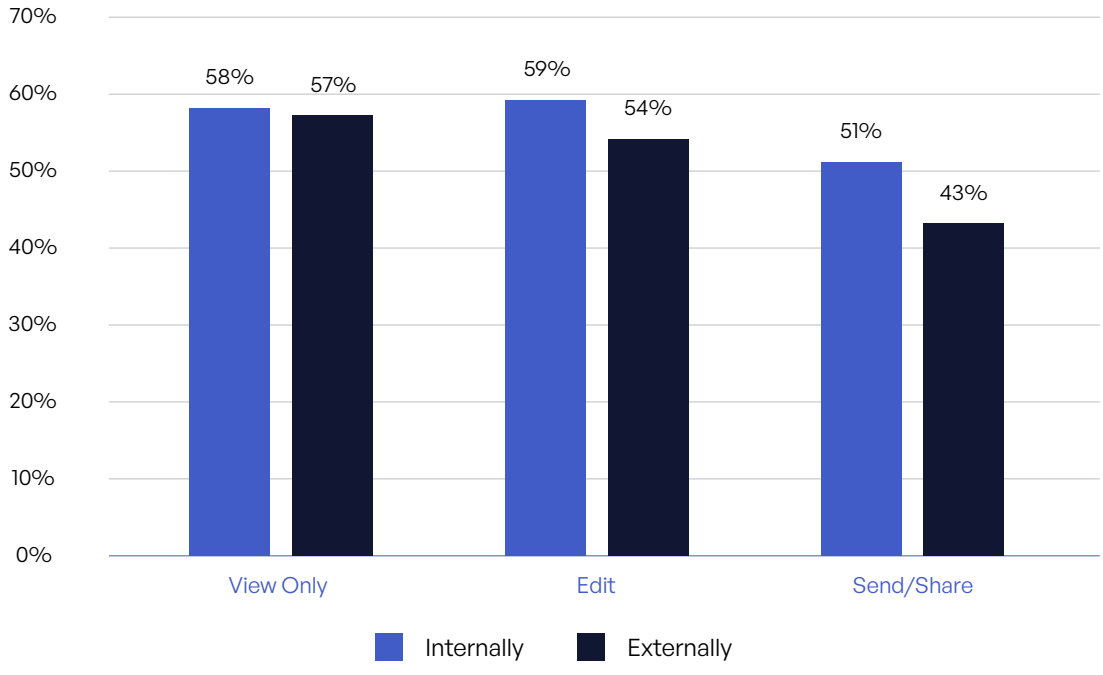


Figure 32: Ability to Track, Control, and Report Sensitive Content Shares and Sends.

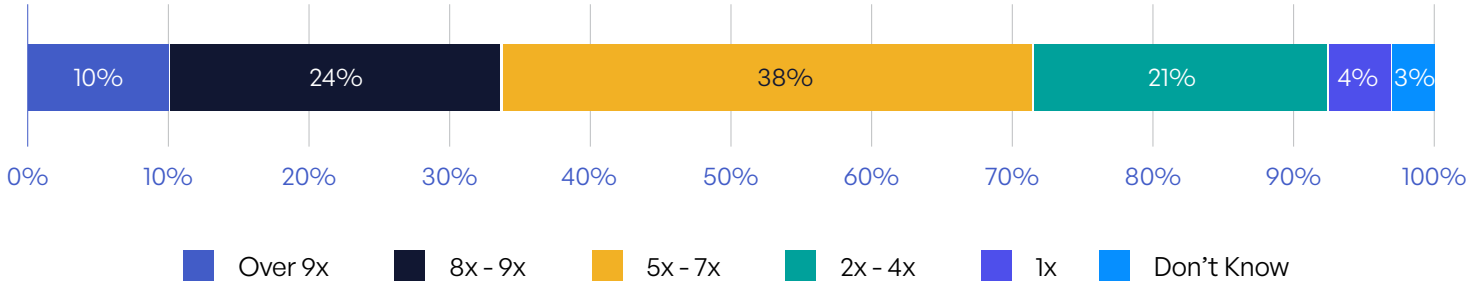


Figure 33: Annual Need for Audit Logs for Compliance.

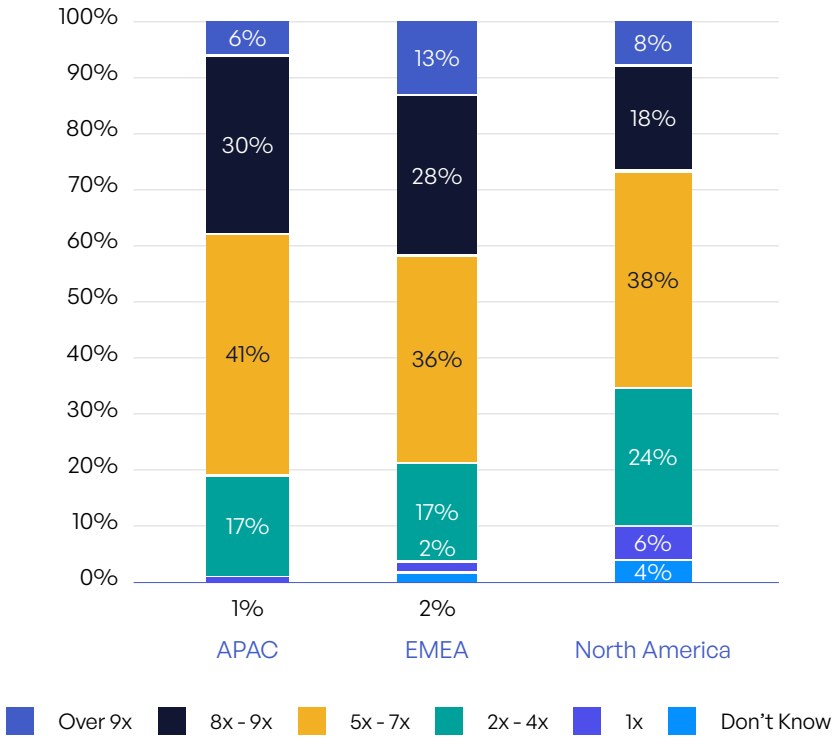


Figure 34: Annual Need for Audit Logs by Region.

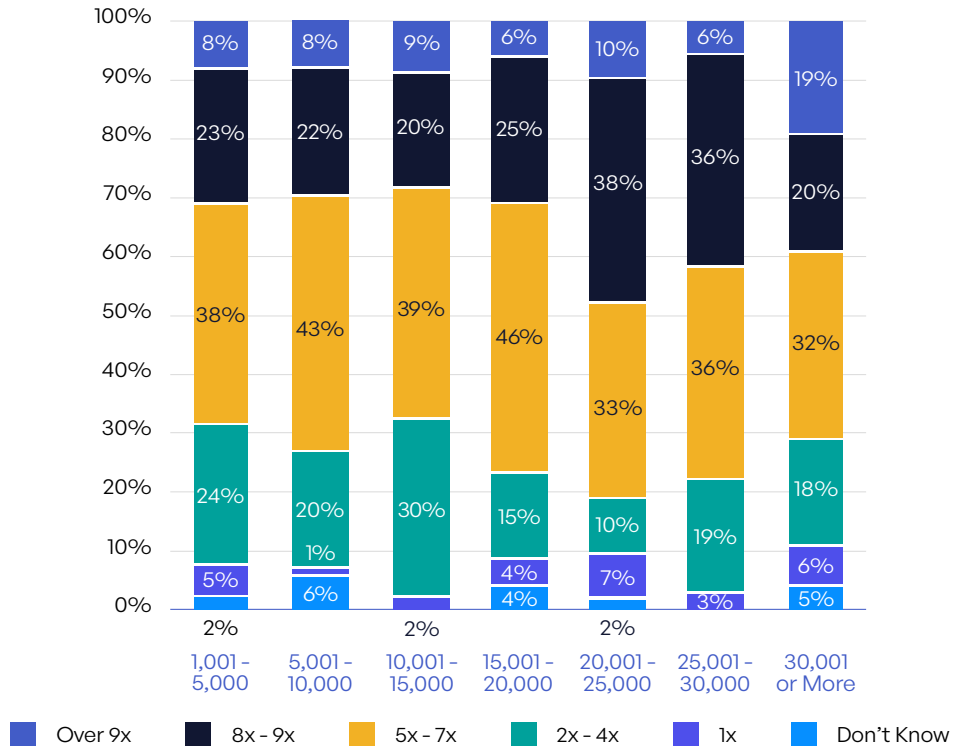


Figure 35: Annual Need for Audit Logs for Compliance by Organization Size.

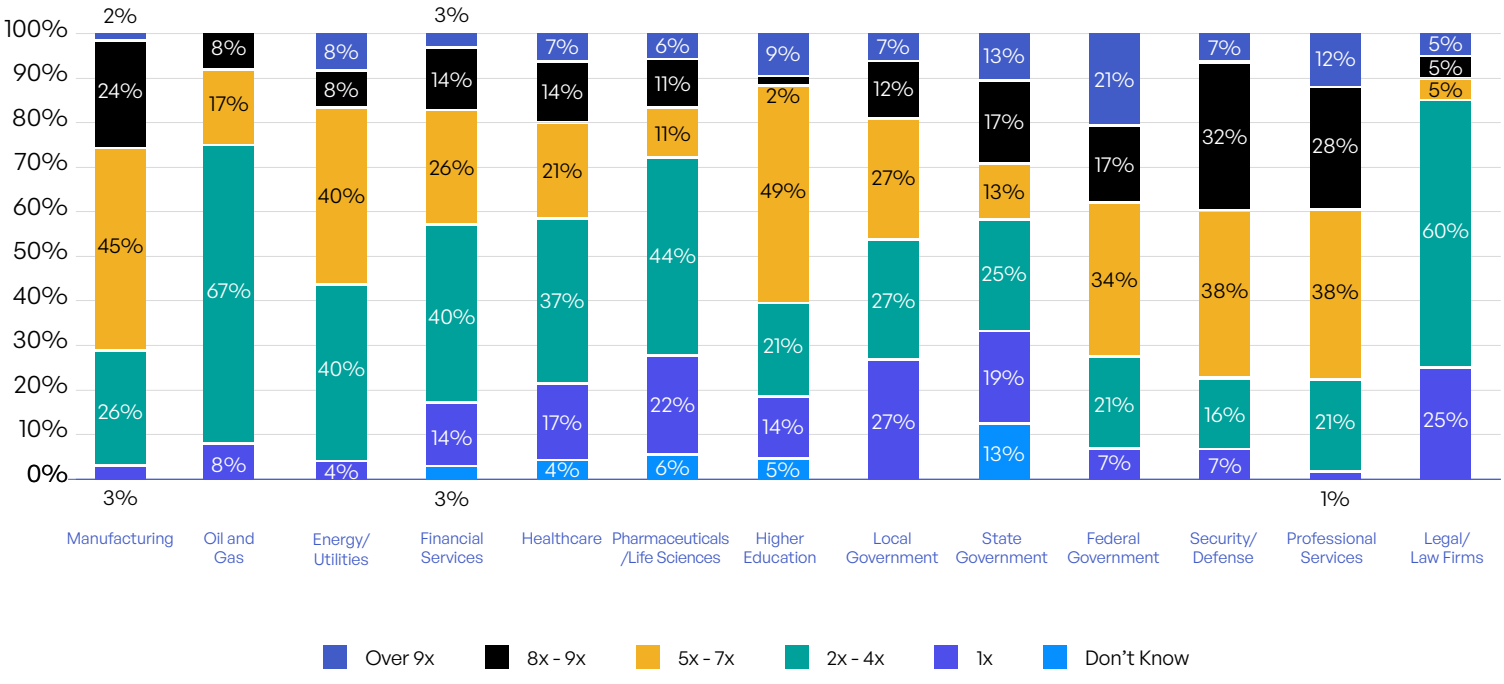


Figure 36: Annual Need for Audit Logs for Compliance by Industry.

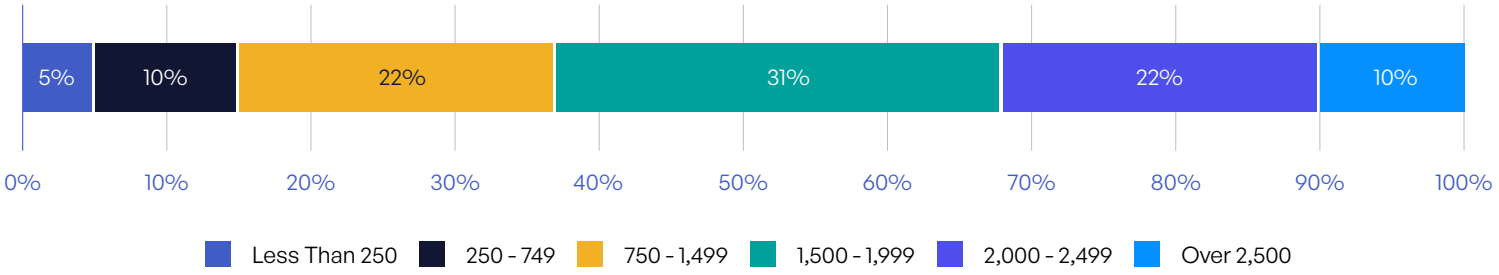


Figure 37: Annual Staff Hours for Compliance Audit Reports.

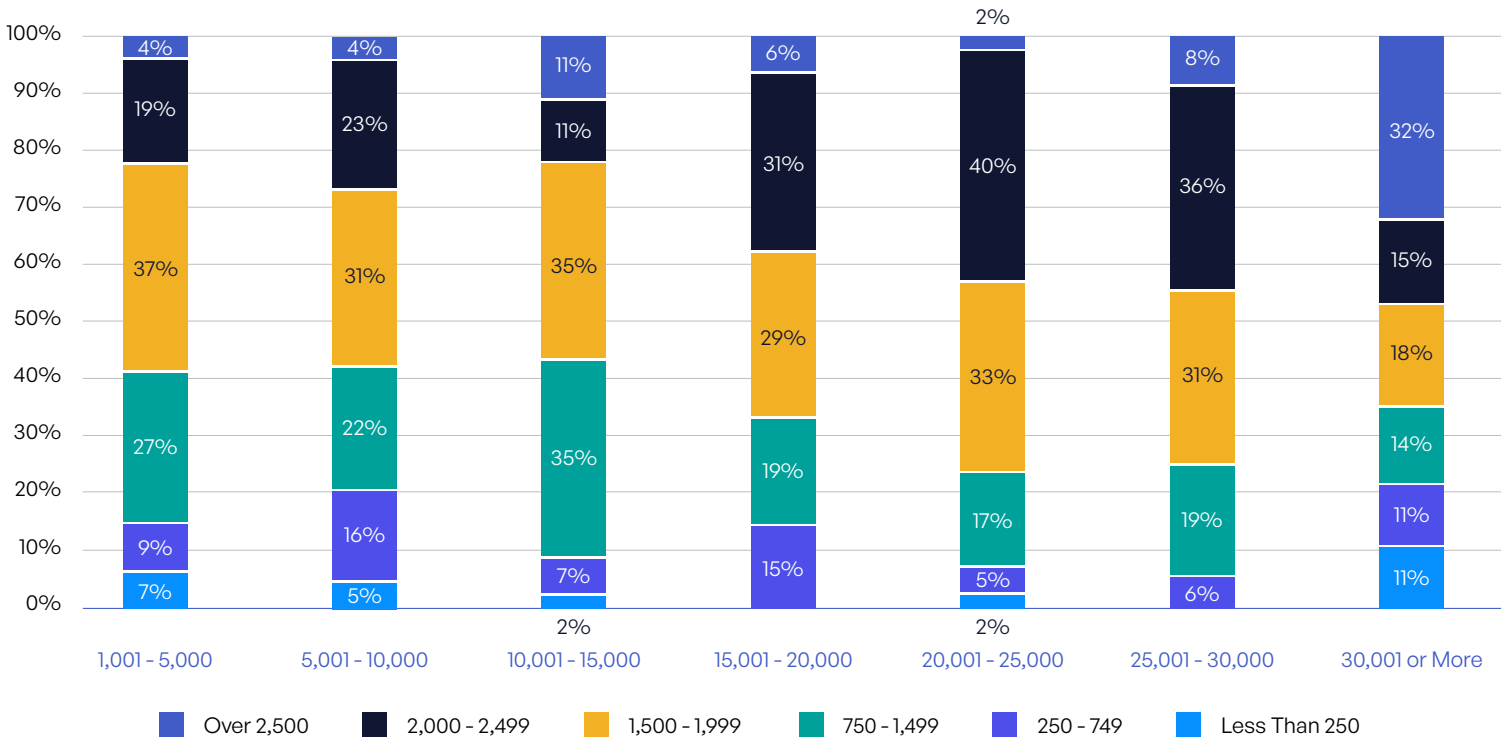


Figure 38: Time Spent Annually Compiling Compliance Audit Reports per Organization Size.

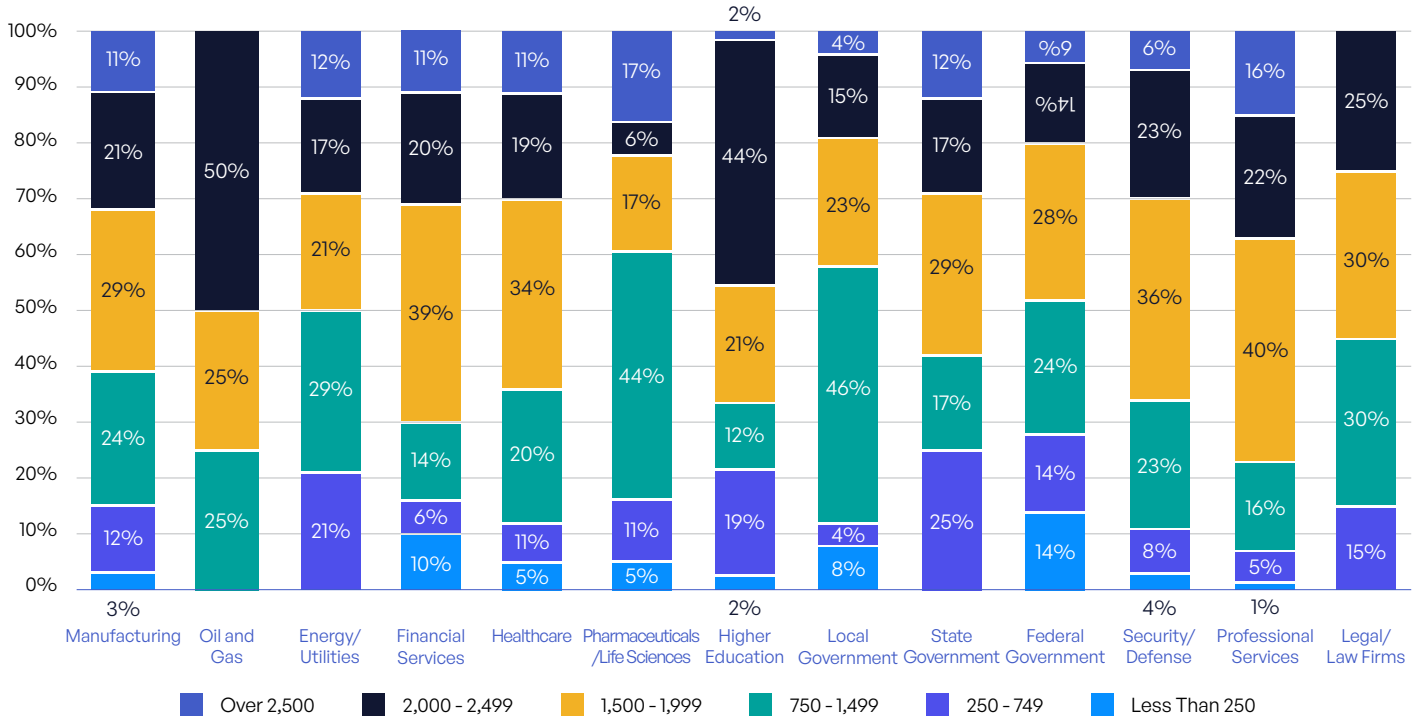


Figure 39: Time Spent Annually Compiling Compliance Audit Reports Across Industries.

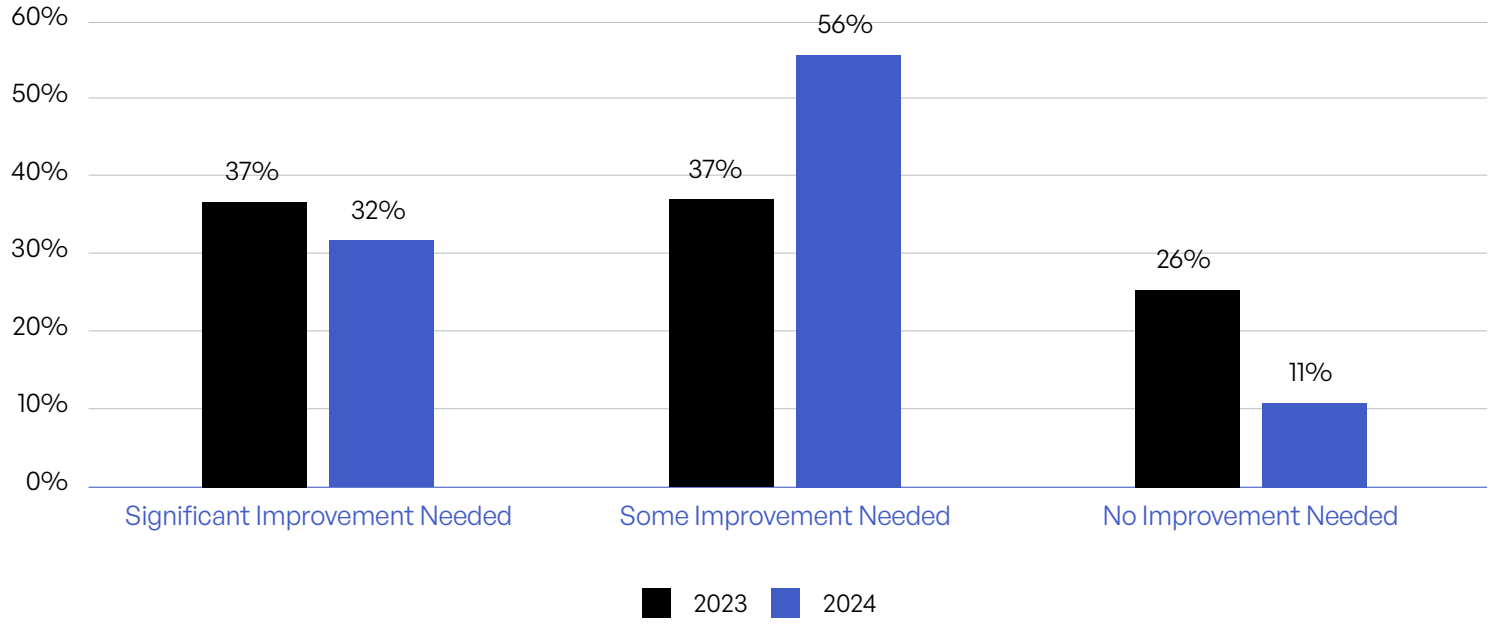


Figure 40: Improvement Needed in Managing Content Security.

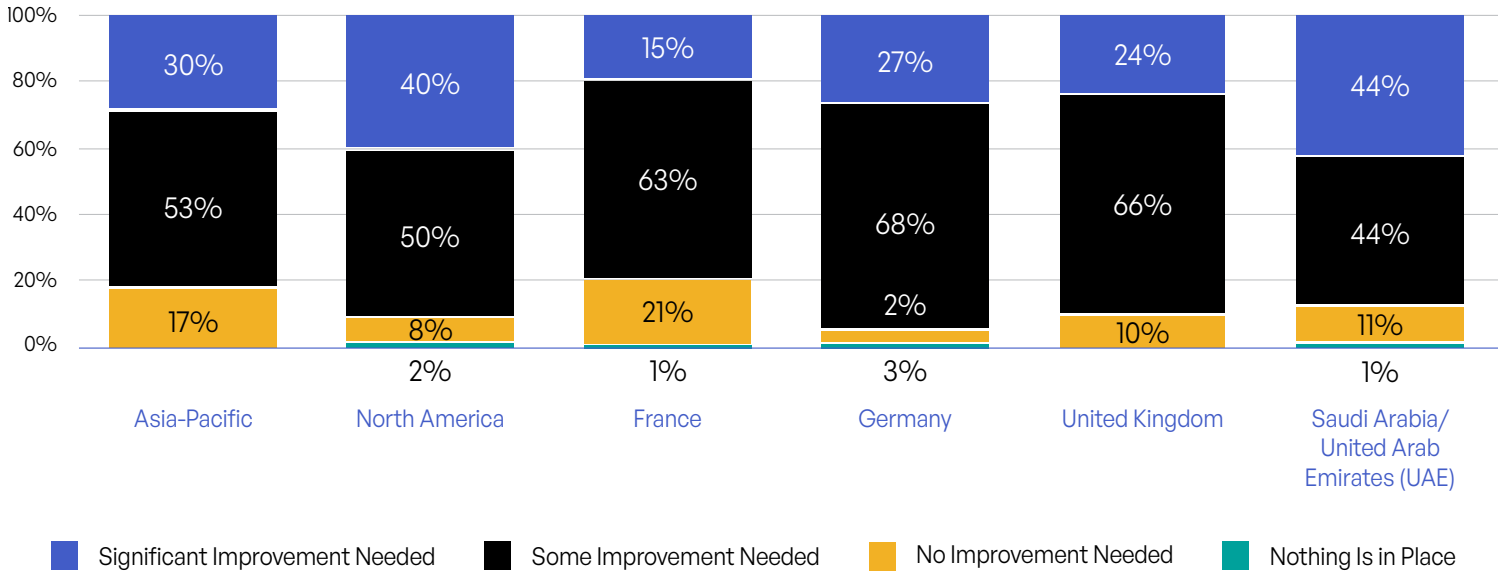


Figure 41: Improvement Needed in Managing Sensitive Content Security Across Regions and EMEA Countries.

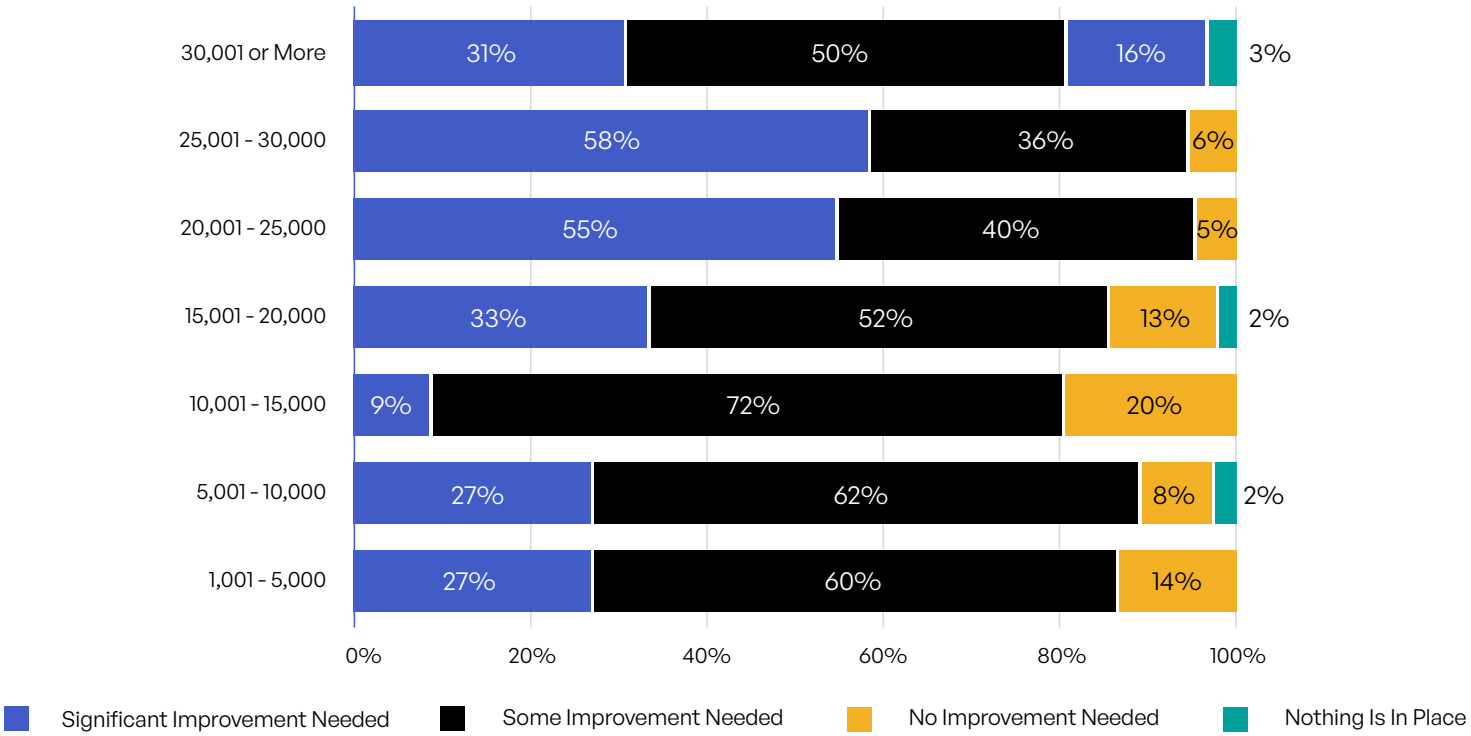


Figure 42: Improvement Needed in Sensitive Content Security per Organization Size.

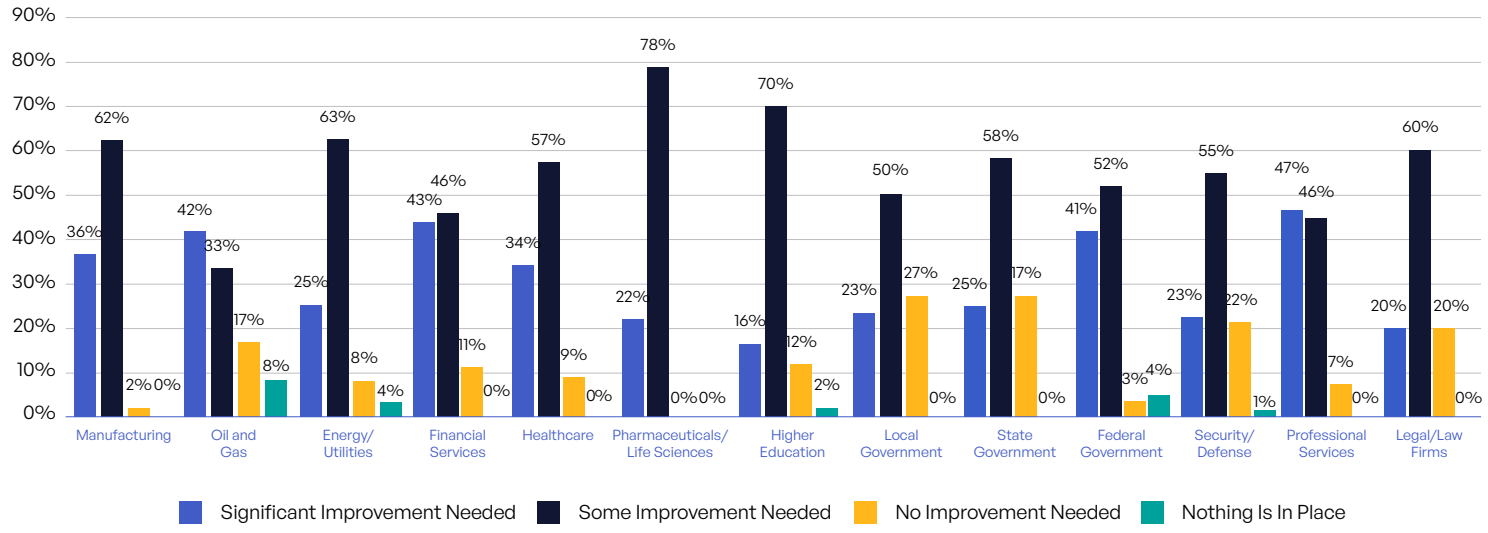


Figure 43: Improvement Needed in Managing Sensitive Content Security Across Industries.

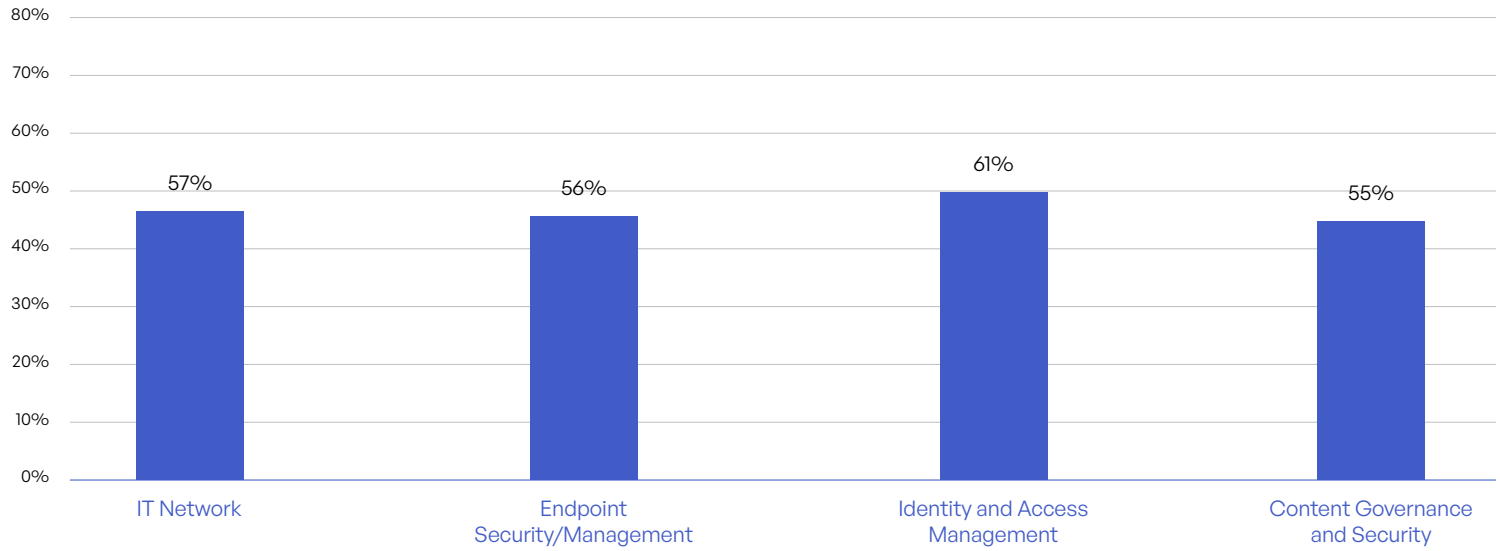


Figure 44: Areas Where Zero Trust Has Been Achieved.

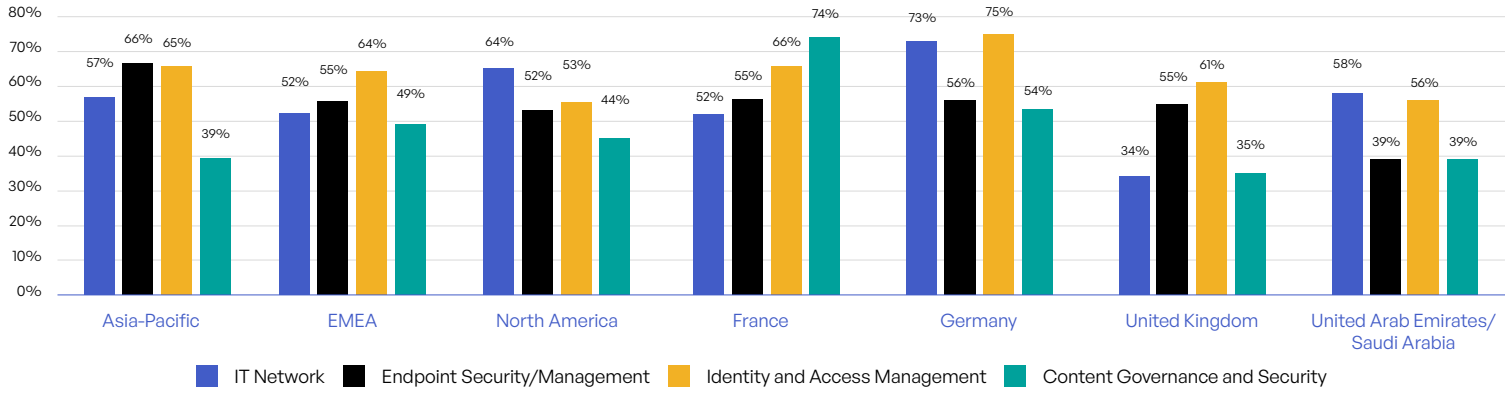


Figure 45: Zero Trust per Region and EMEA Countries.

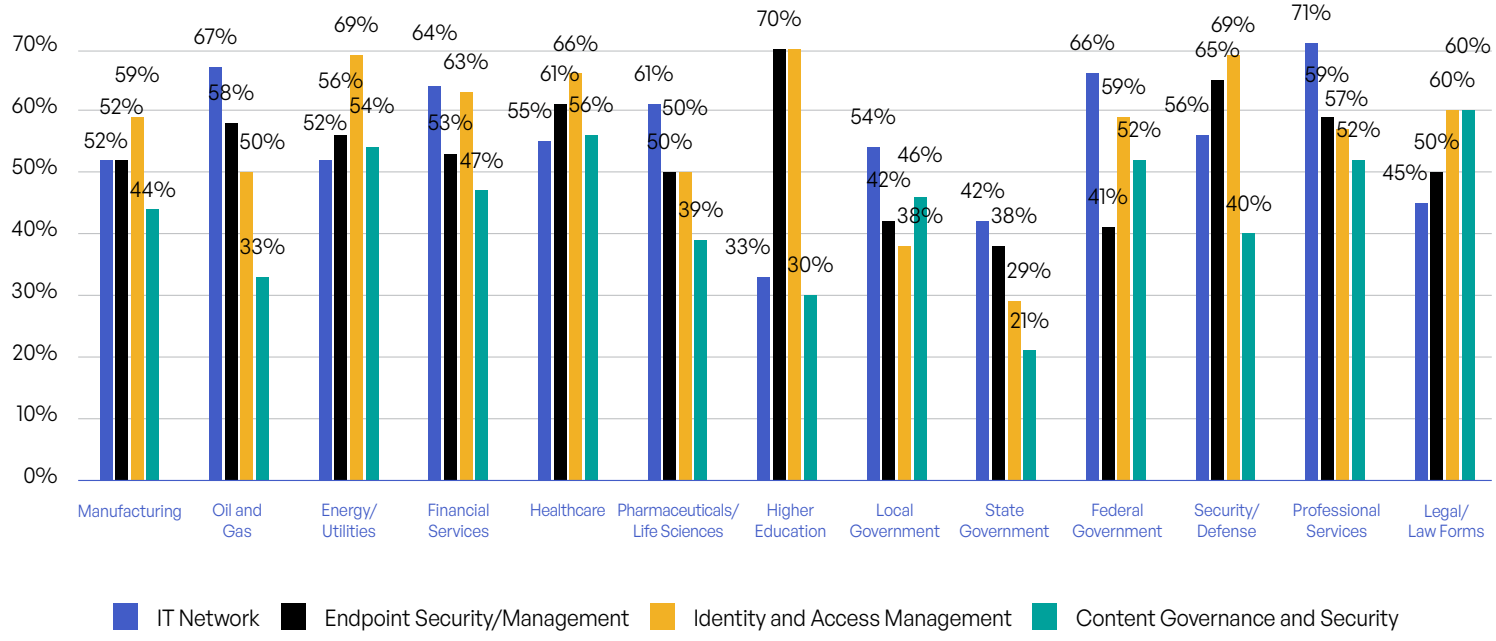


Figure 46: Areas Where Zero Trust Has Been Achieved Across Industries.

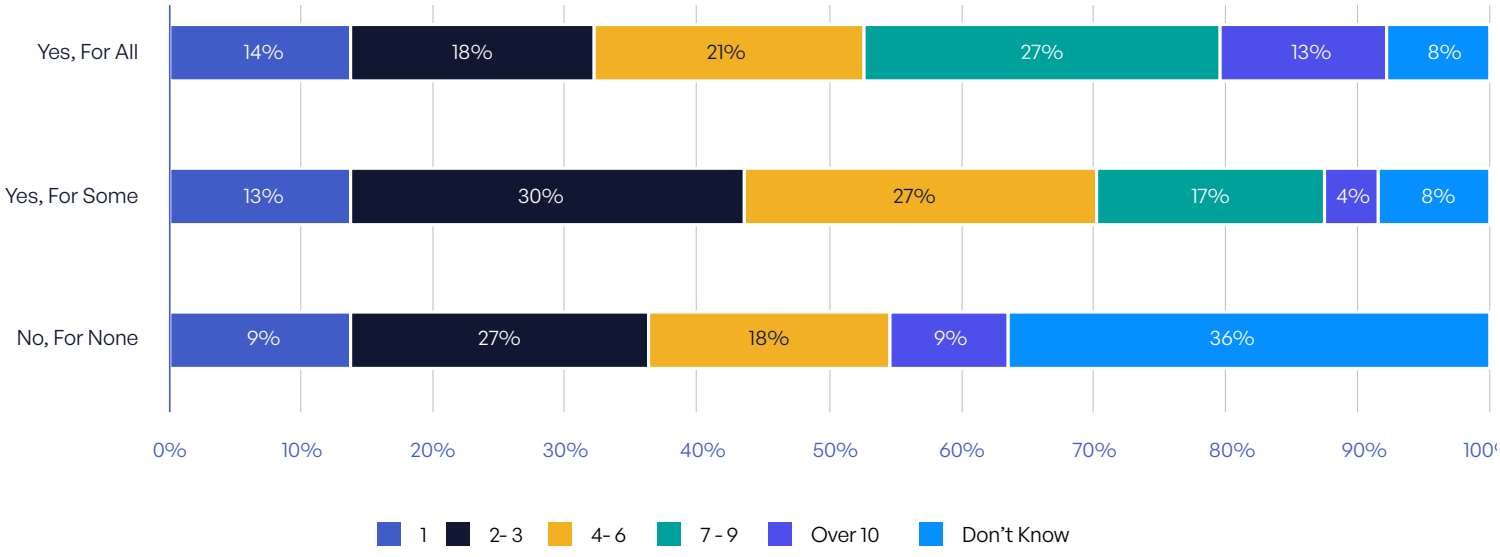


Figure 47: Advanced Security Used for Sensitive Content Communications and Data Breaches.

	Manufacturing	Oil and Gas	Energy/Utilities	Financial Services	Healthcare	Pharmaceuticals/ Life Sciences	Higher Education	Local Government	State Government	Federal Government	Security/ Defense	Professional Services	Legal/ Law Firms
Yes, for All	58%	58%	58%	60%	56%	61%	65%	50%	71%	52%	55%	71%	45%
Yes, for Some	42%	42%	40%	36%	44%	39%	28%	50%	25%	45%	45%	28%	50%
No, for None	0%	0%	2%	4%	0%	0%	7%	0%	4%	3%	0%	2%	5%

Figure 48: Use of Advanced Security Content Communications Across Industries.

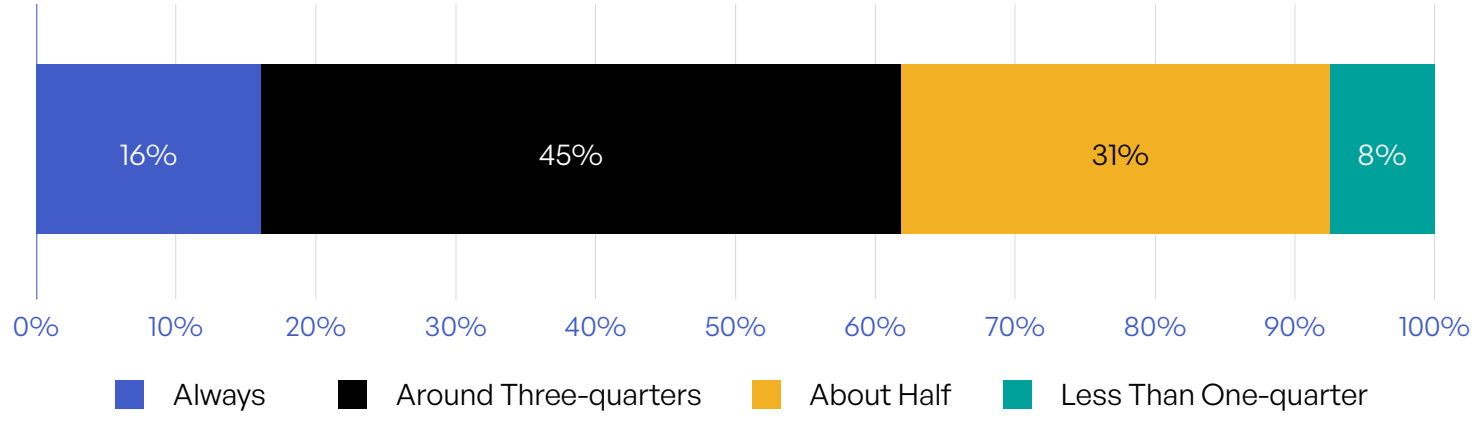


Figure 49: Ability to Track and Control Sensitive Content Once It Leaves an Application.

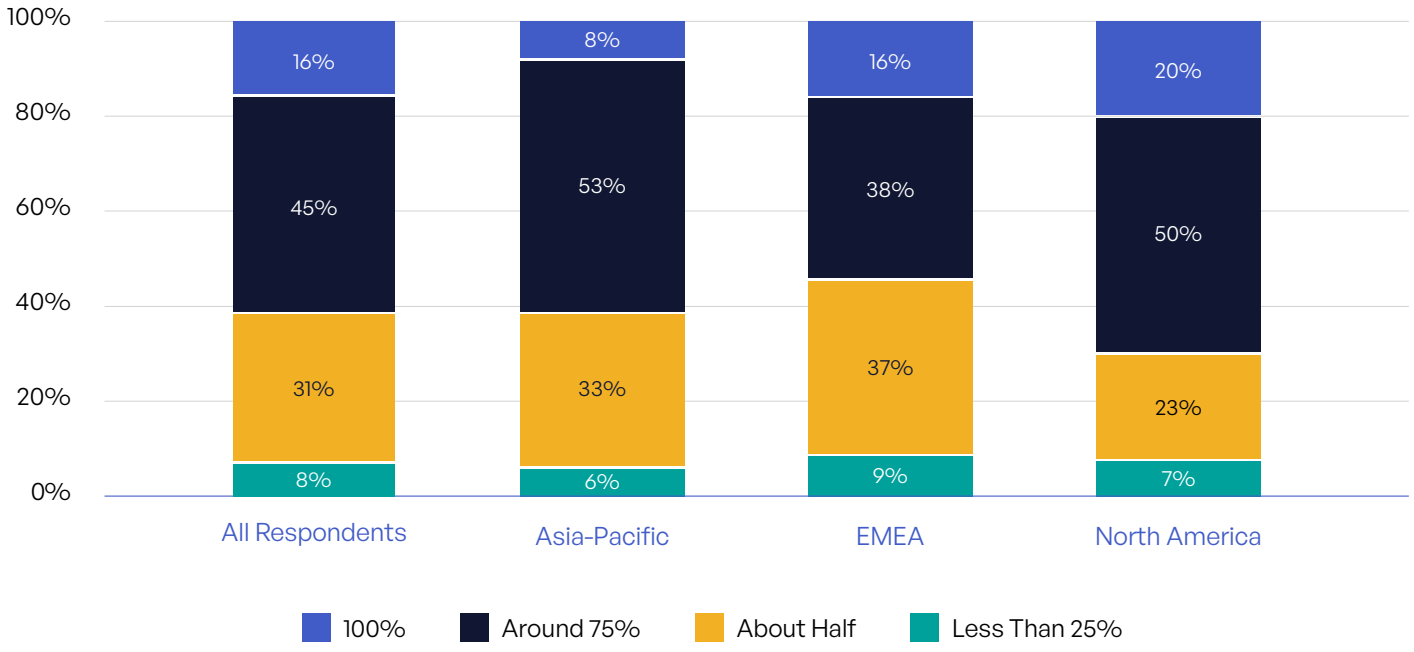


Figure 50: How Often Organizations Can Track and Control Access to Sensitive Content Communications Across Regions.

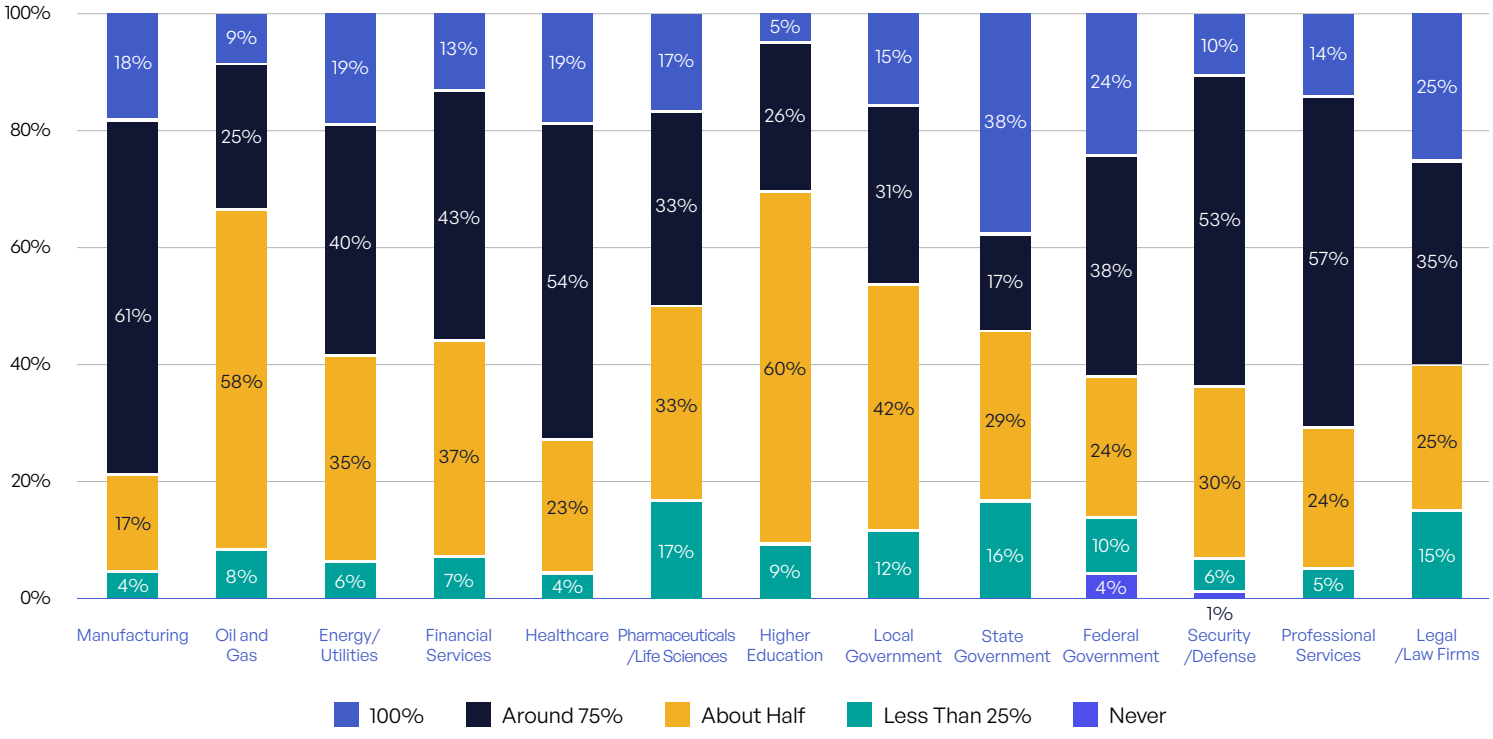


Figure 51: How Often Organizations Can Track and Control Access to Sensitive Content Communications Across Industries.

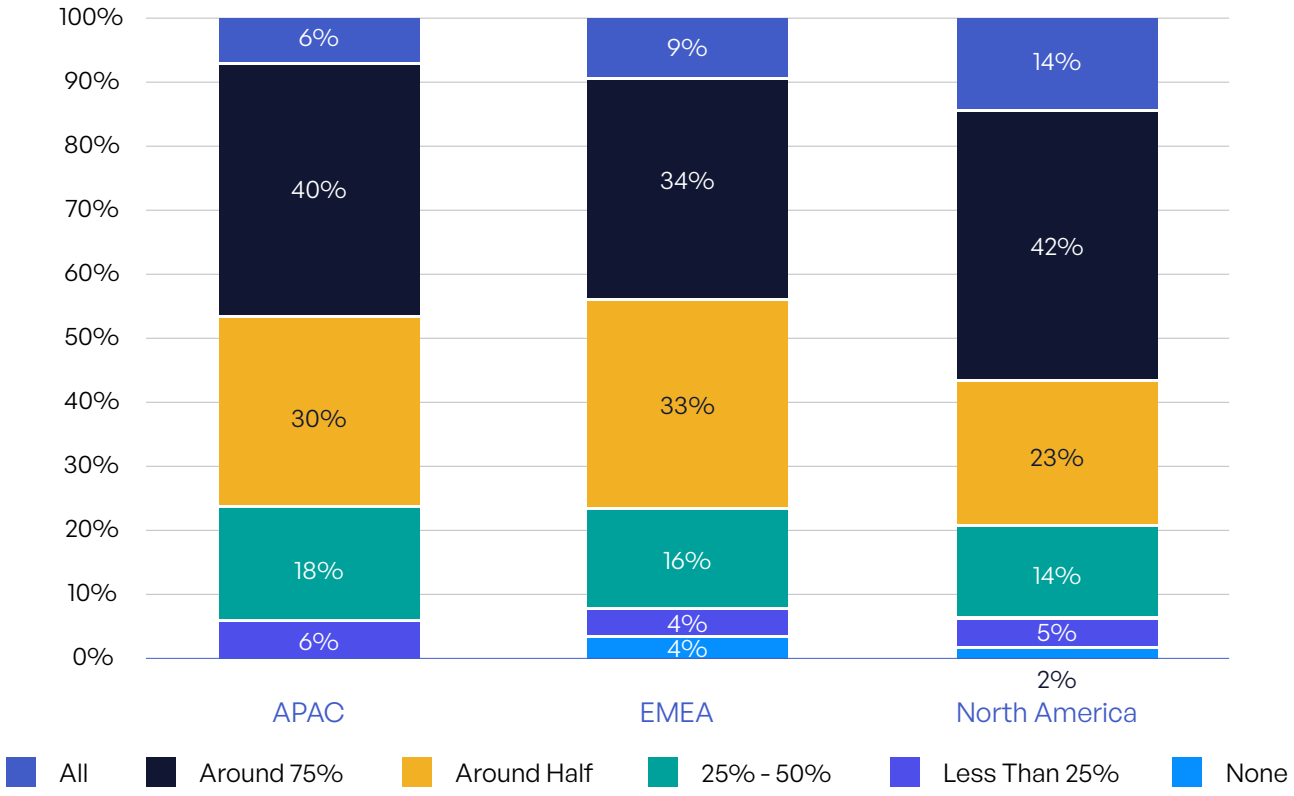


Figure 52: Unstructured Data That Is Tagged and Classified Across Regions.

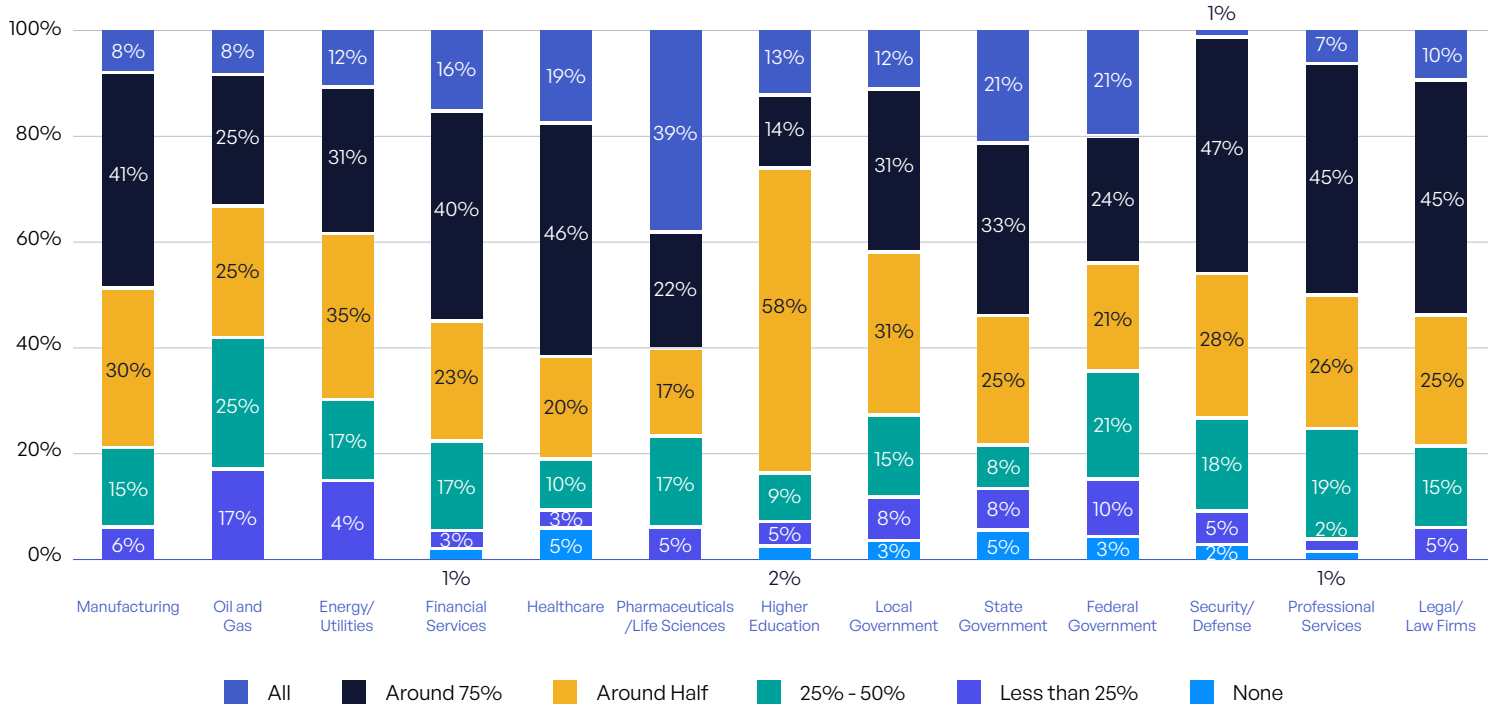


Figure 53: Unstructured Data That Is Tagged and Classified Across Industries.

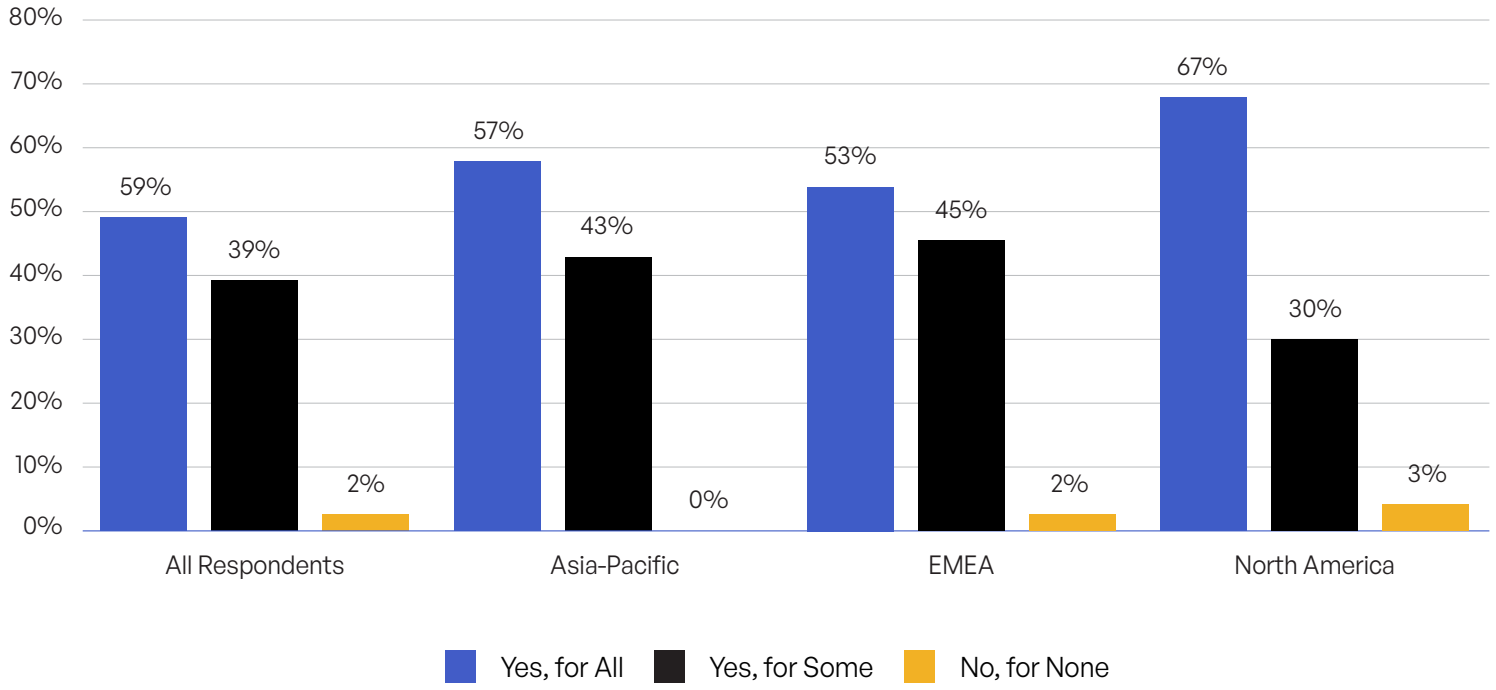


Figure 54: Advanced Security Used for Sensitive Content Communications Across Regions.

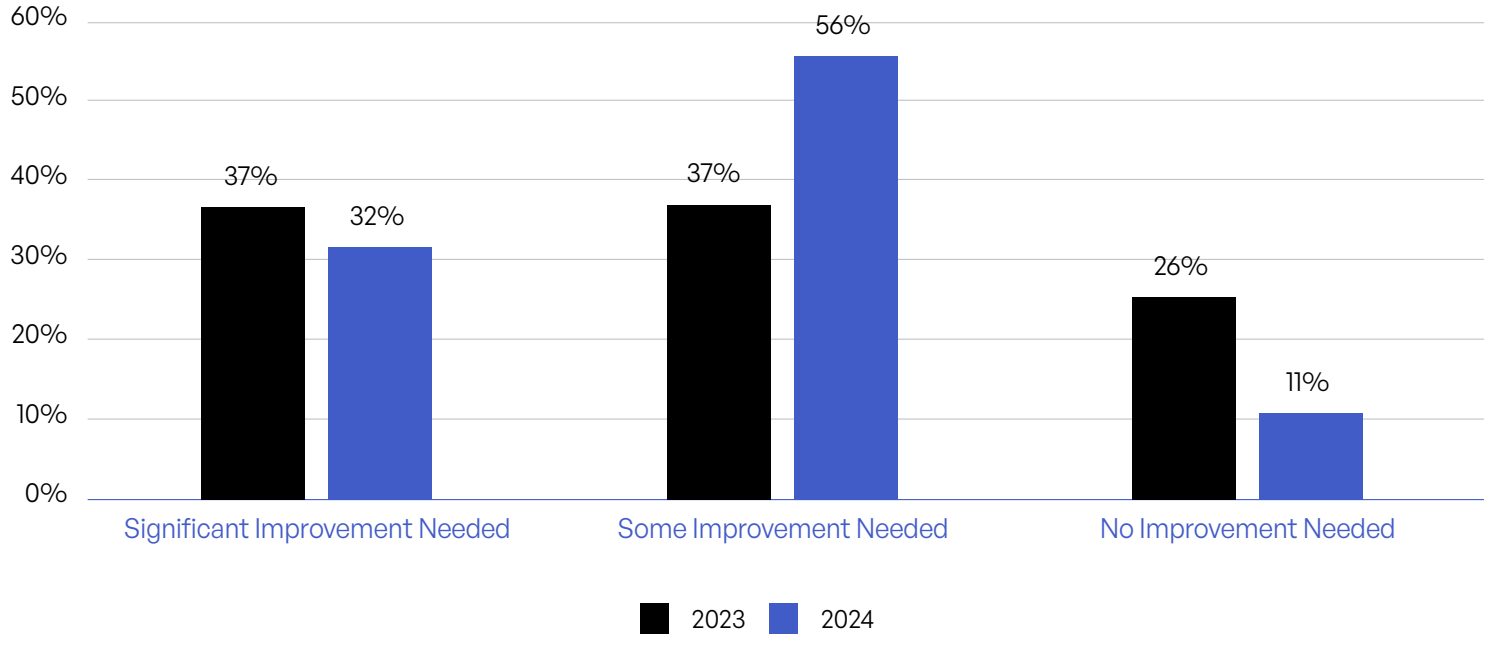


Figure 55: Improvement Needed in Managing Content Communication Risk.

Ability to Track, Control, and Report Sensitive Content Sharing, Internally and Externally

		All Respondents	Manufacturing	Oil and Gas	Energy/Utilities	Financial Services	Healthcare	Pharmaceuticals/ Life Sciences	Higher Education
Internal	Yes, for All	59%	58%	58%	58%	60%	56%	61%	65%
	Yes, for Some	39%	42%	42%	40%	36%	44%	39%	28%
	No, for None	2%	0%	0%	2%	4%	0%	0%	7%
External	Yes, for All	59%	62%	58%	44%	70%	56%	78%	72%
	Yes, for Some	38%	38%	42%	52%	27%	44%	22%	21%
	No, for None	3%	0%	0%	4%	3%	0%	0%	7%

		Local Government	State Government	Federal Government	Security/ Defense	Professional Services	Legal/ Law Firms
Internal	Yes, for All	50%	71%	52%	55%	71%	45%
	Yes, for Some	50%	25%	45%	45%	28%	50%
	No, for None	0%	4%	3%	0%	2%	5%
External	Yes, for All	50%	67%	48%	51%	60%	50%
	Yes, for Some	38%	29%	45%	48%	40%	45%
	No, for None	12%	4%	7%	1%	0%	5%

Figure 56: Advanced Security Used for Sensitive Content Communications Across Industries.

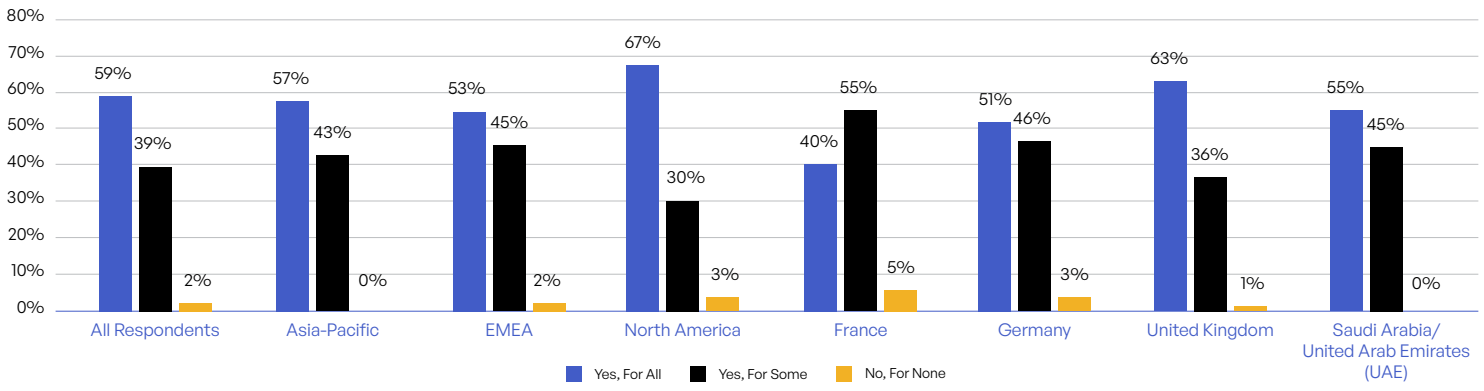


Figure 57: Advanced Security Used for Sensitive Content Communications Across Regions.

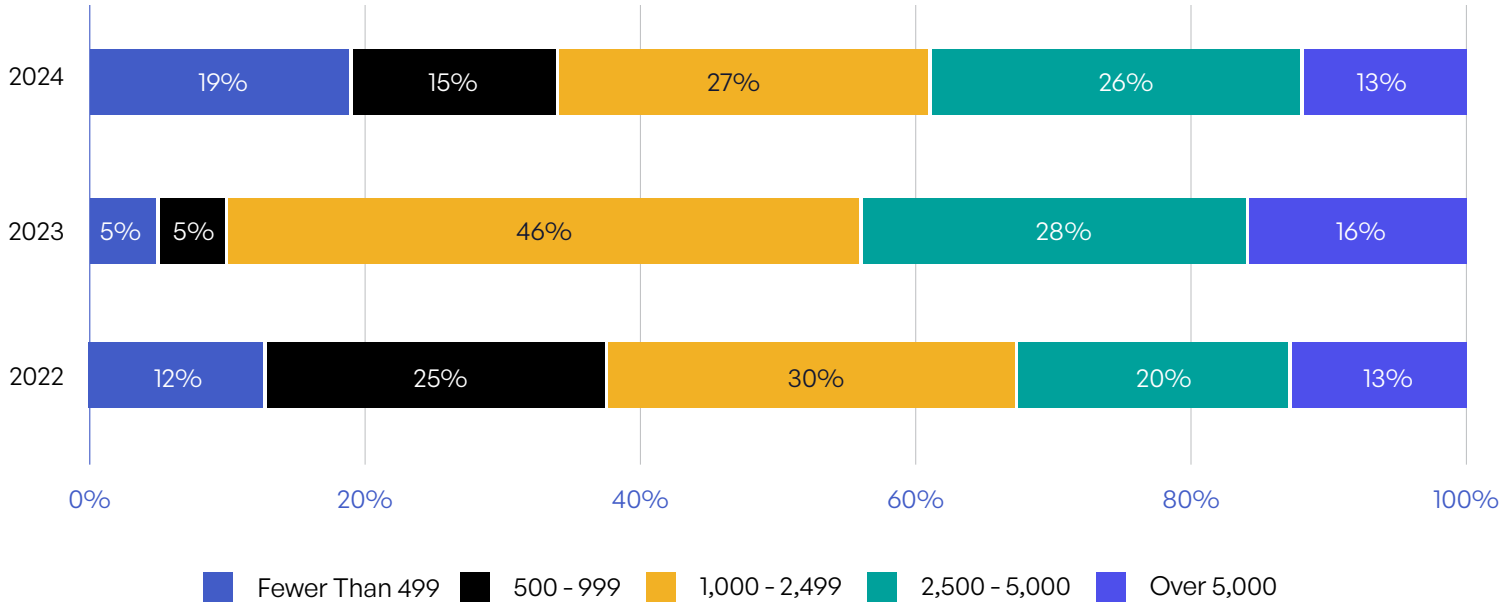


Figure 58: Number of Third Parties With Which Respondents Exchange Sensitive Content.

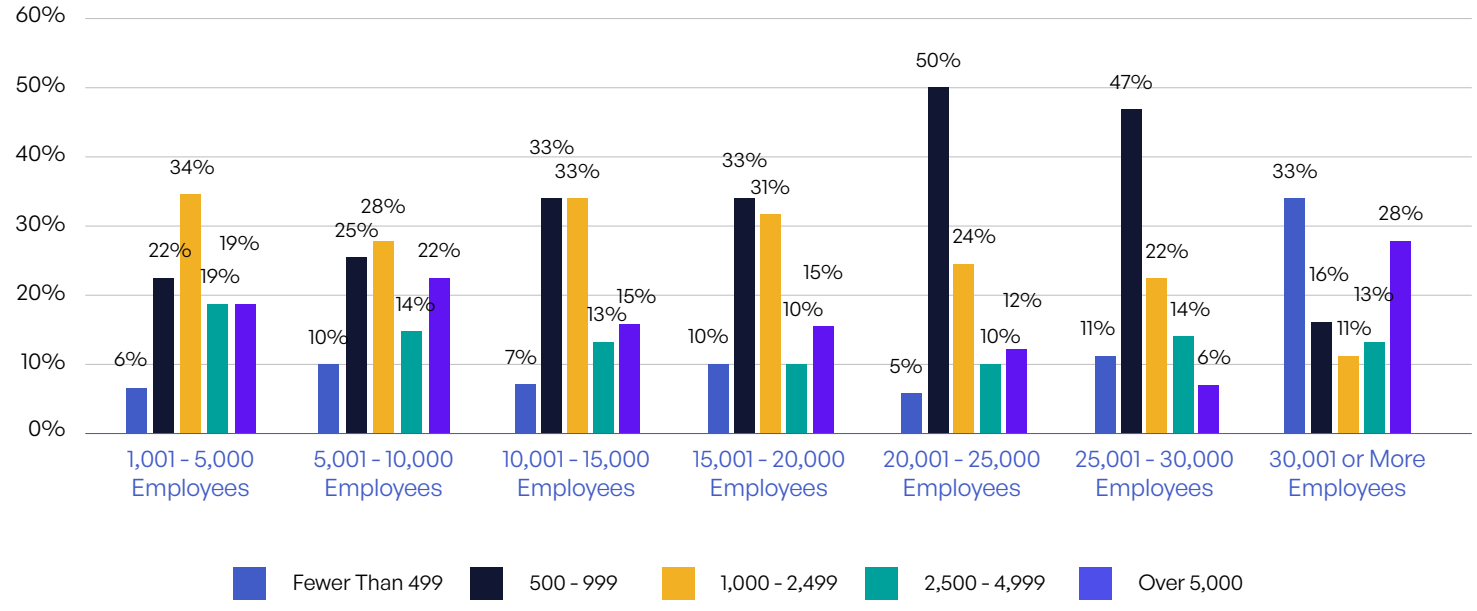


Figure 59: Sensitive Content Communications With Third Parties per Organization Size.

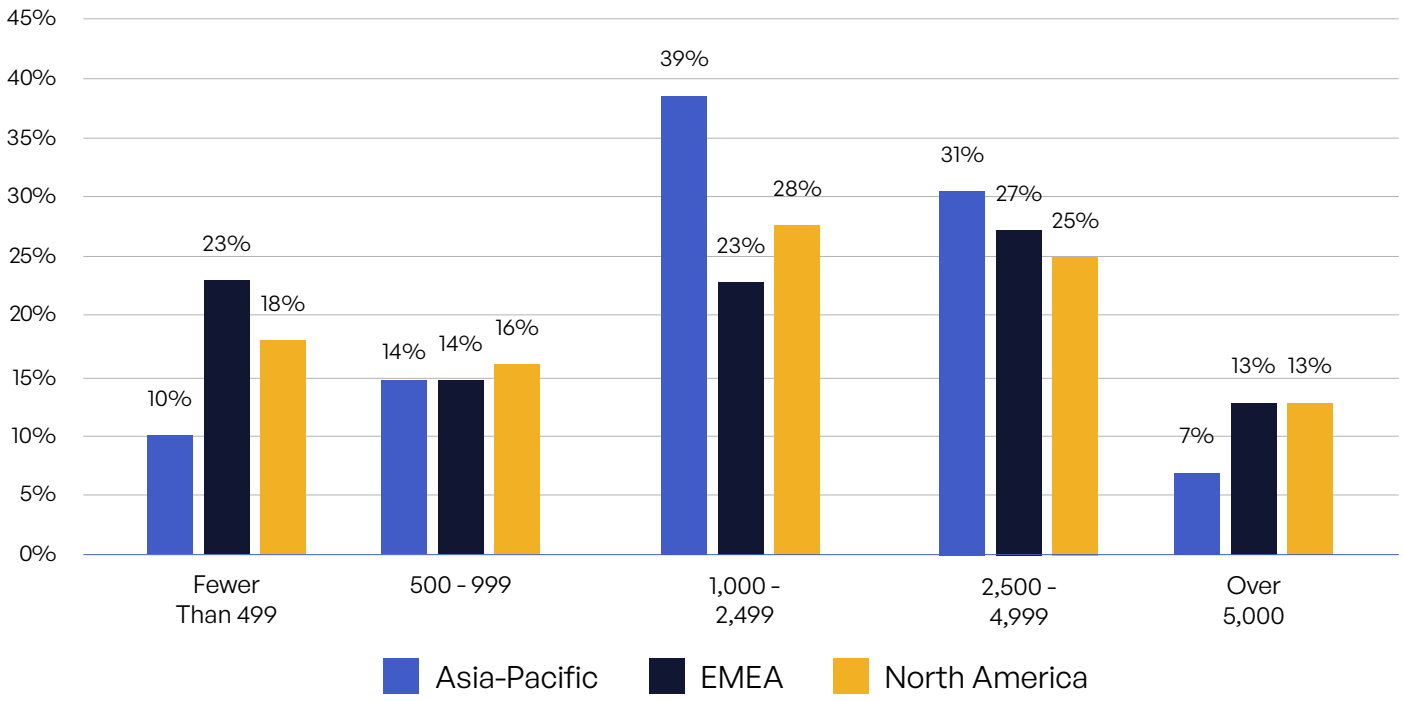


Figure 60: Number of Third Parties With Which Organizations Exchange Sensitive Data Across Regions.

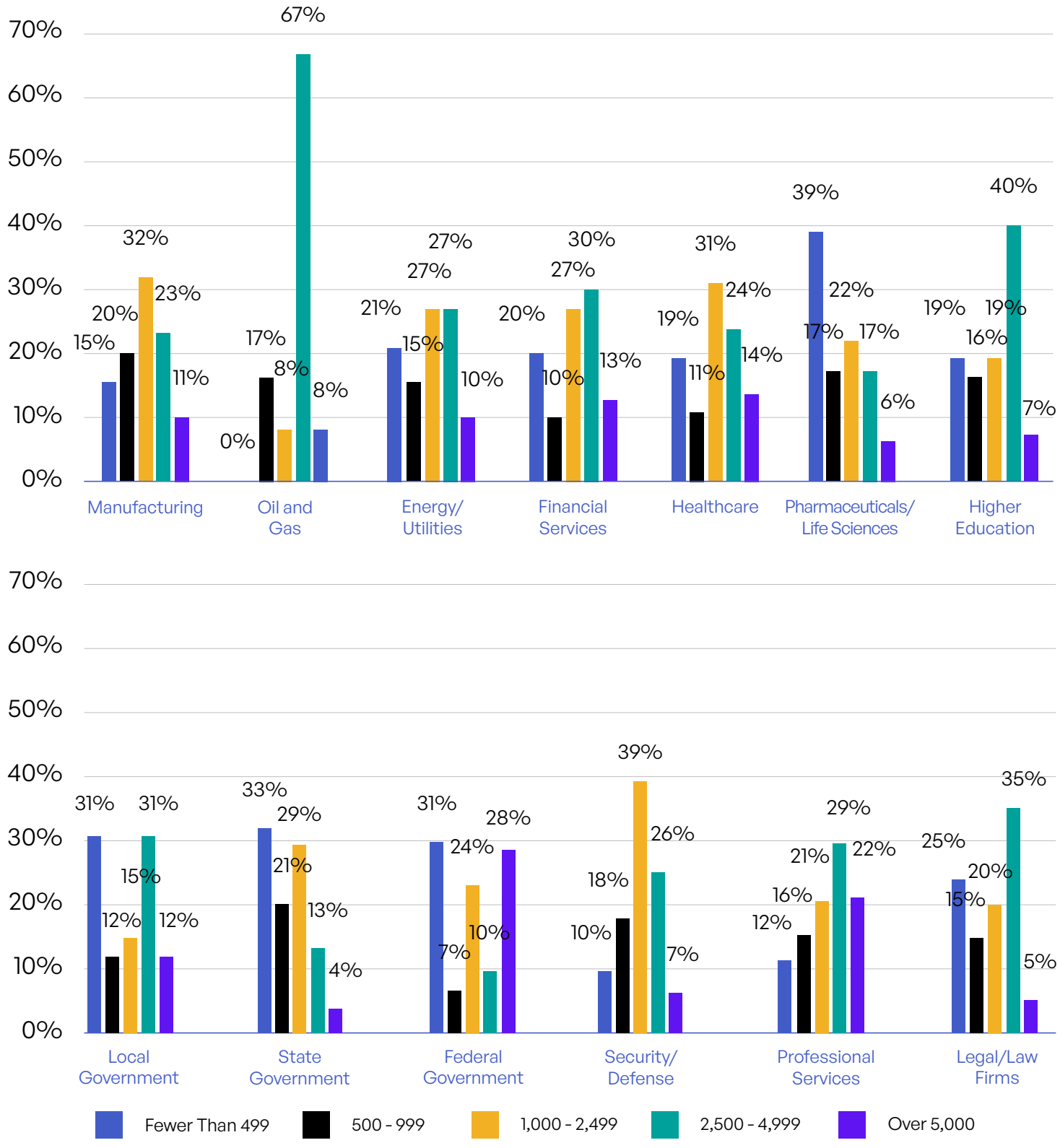


Figure 61: Sensitive Content Communications With Third Parties Across Industries.

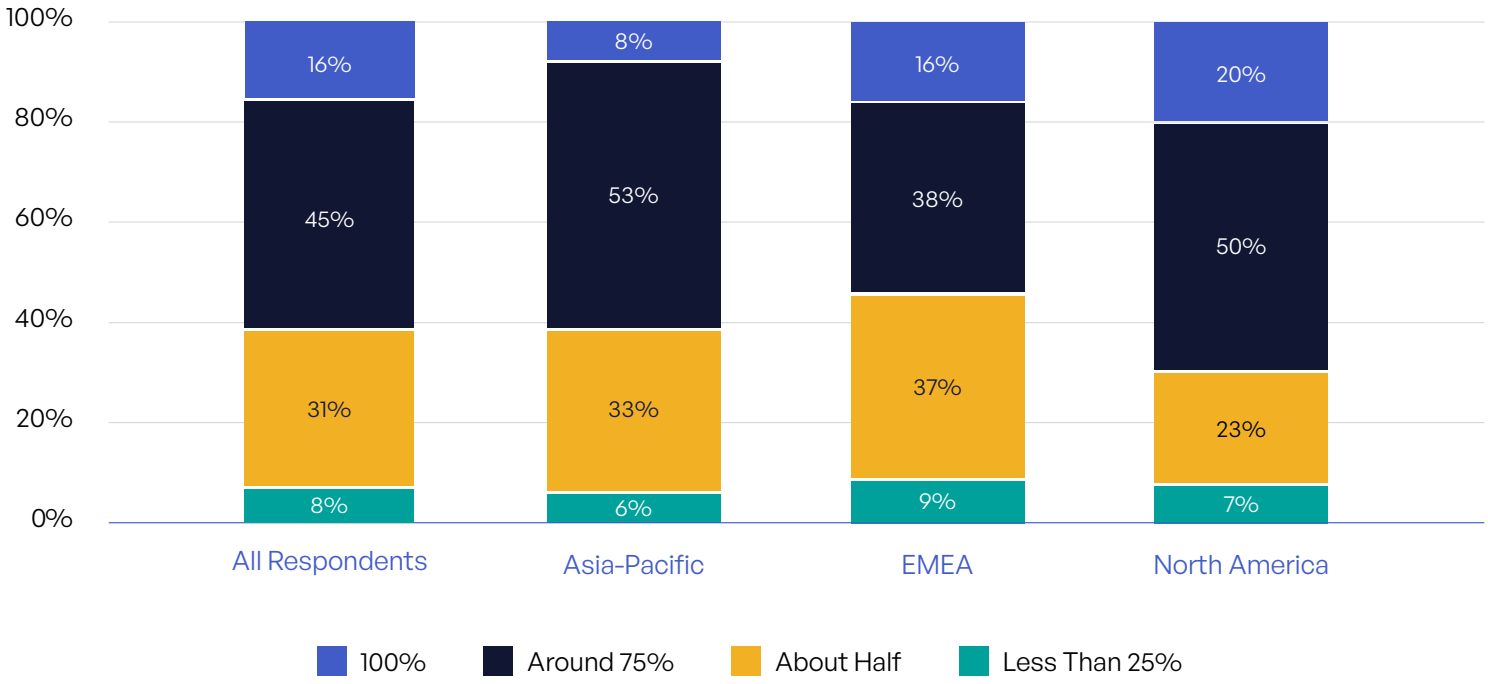


Figure 62: What Percentage of Sensitive Content Communications Are Tracked and Controlled Across Regions.

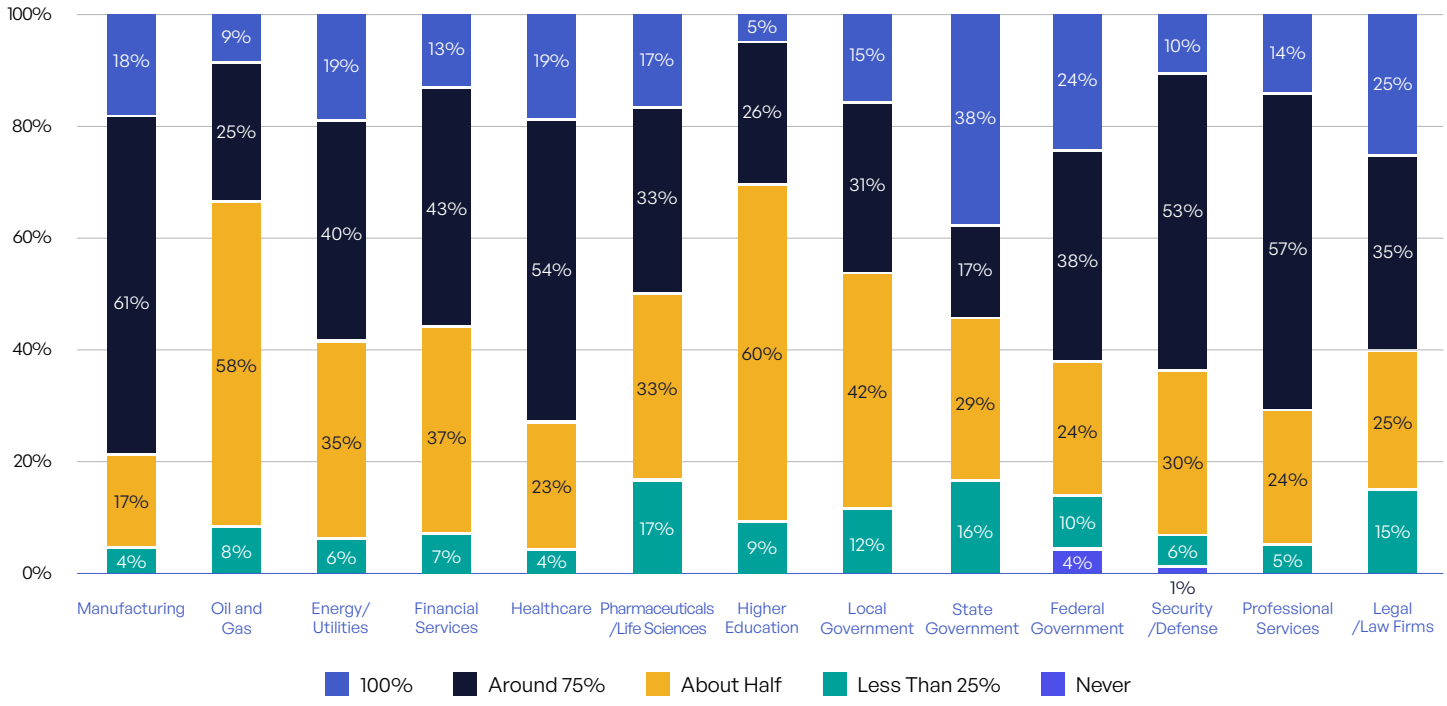


Figure 63: How Often Organizations Can Track and Control Access to Sensitive Content Communications Across Industries.

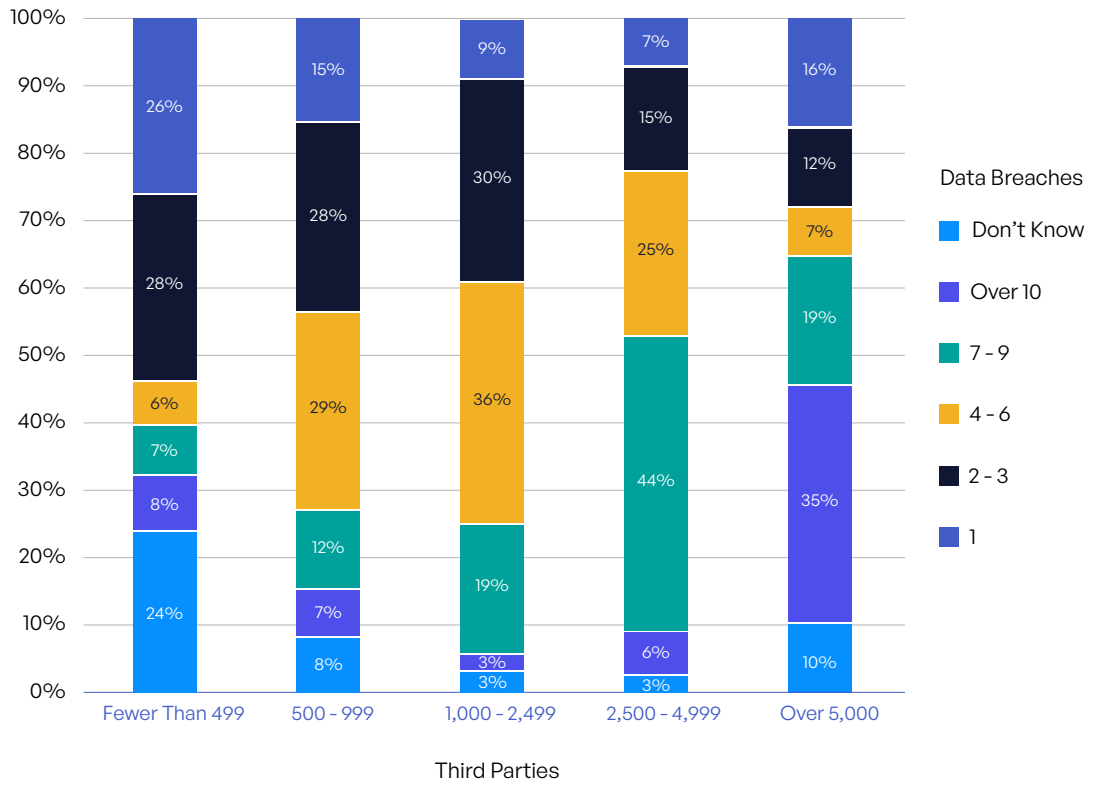


Figure 64: Number of Third Parties and Number of Data Breaches.

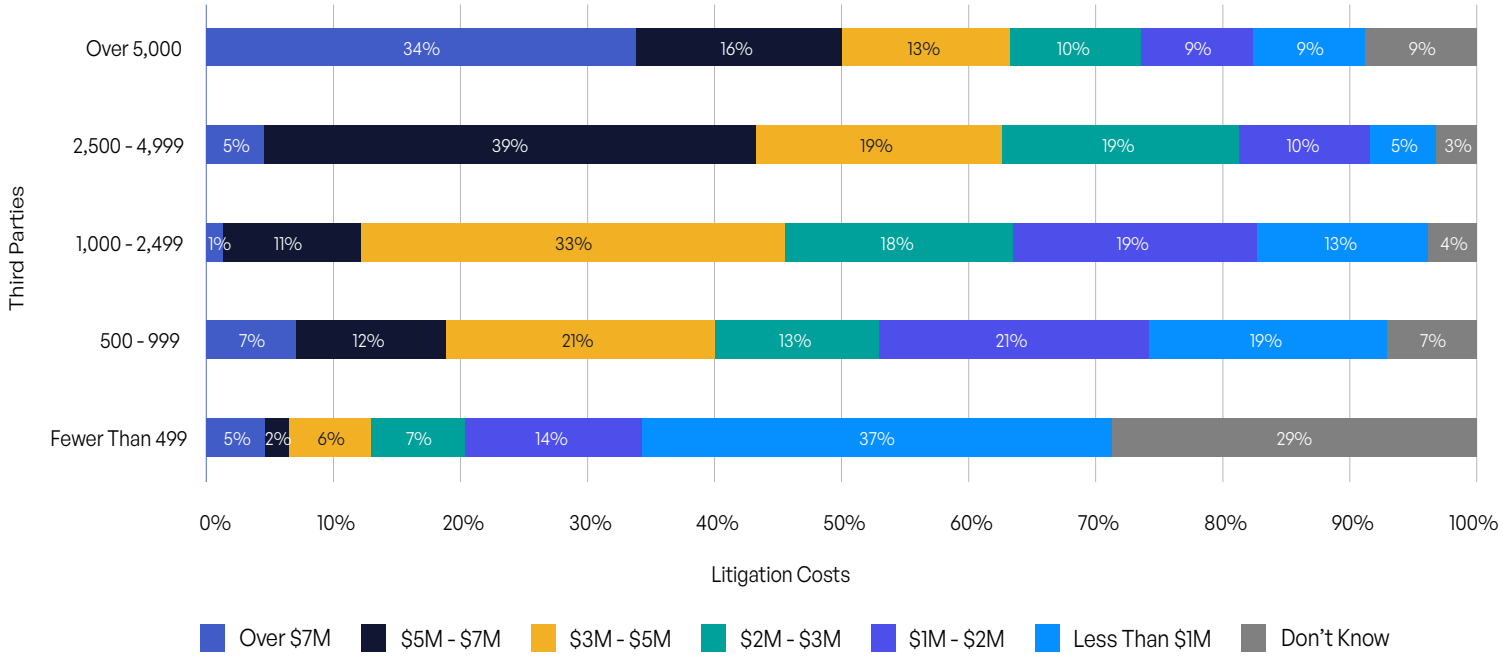


Figure 65: Number of Third Parties and Litigation Costs.

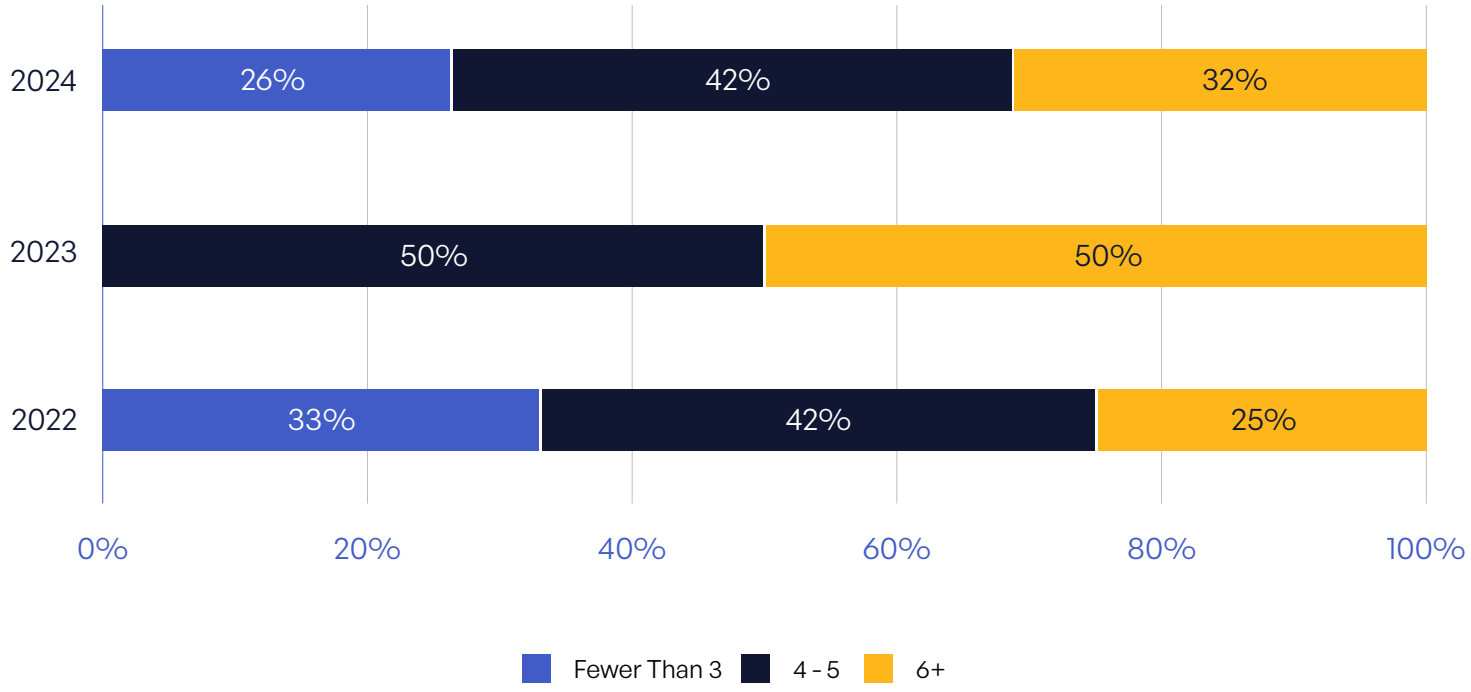


Figure 66: Number of Tools/Systems Used for Sensitive Content Communications.

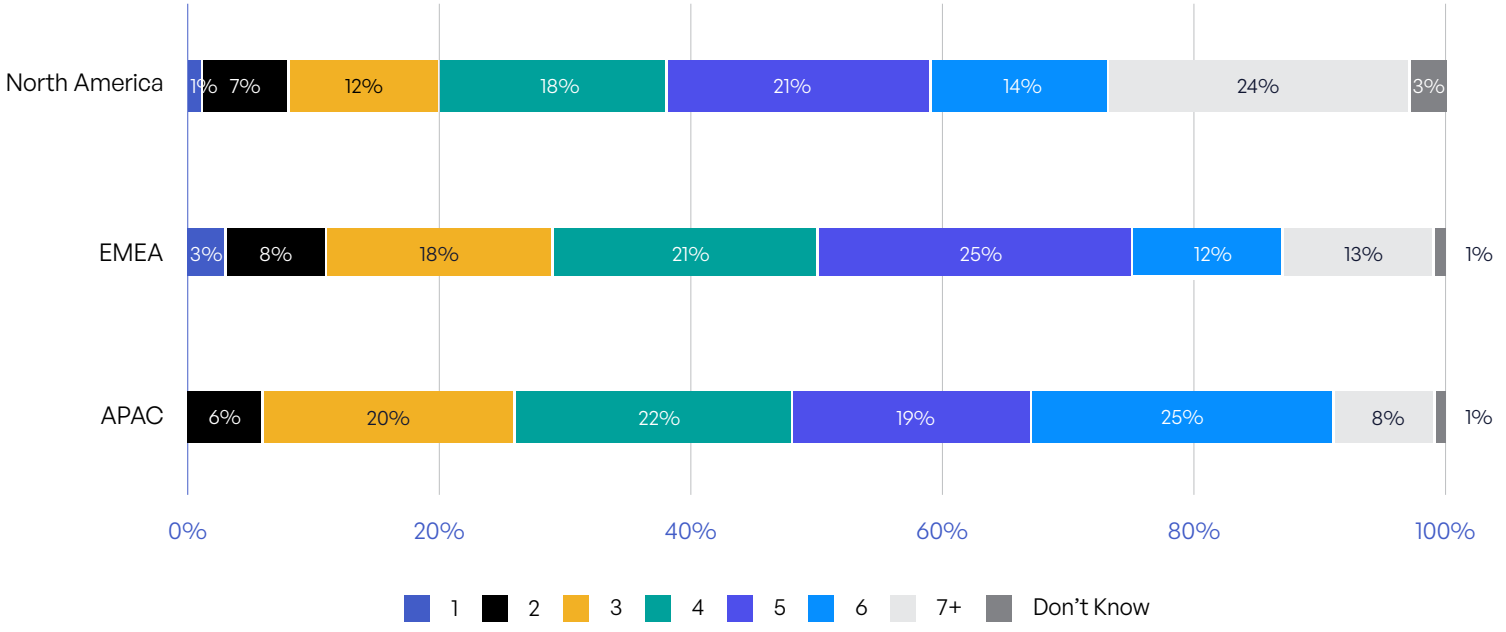


Figure 67: Number of Communication Tools Used Across Regions.

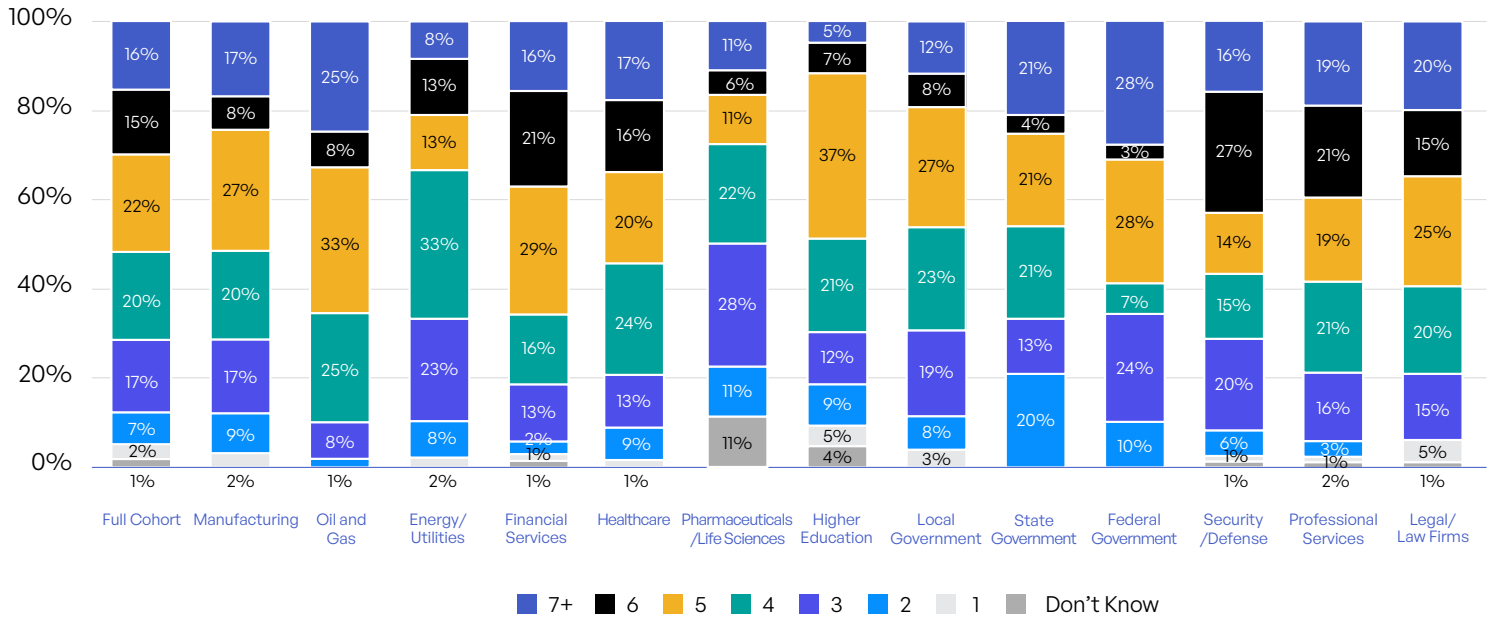


Figure 68: Number of Communication Tools Used Across Industries.

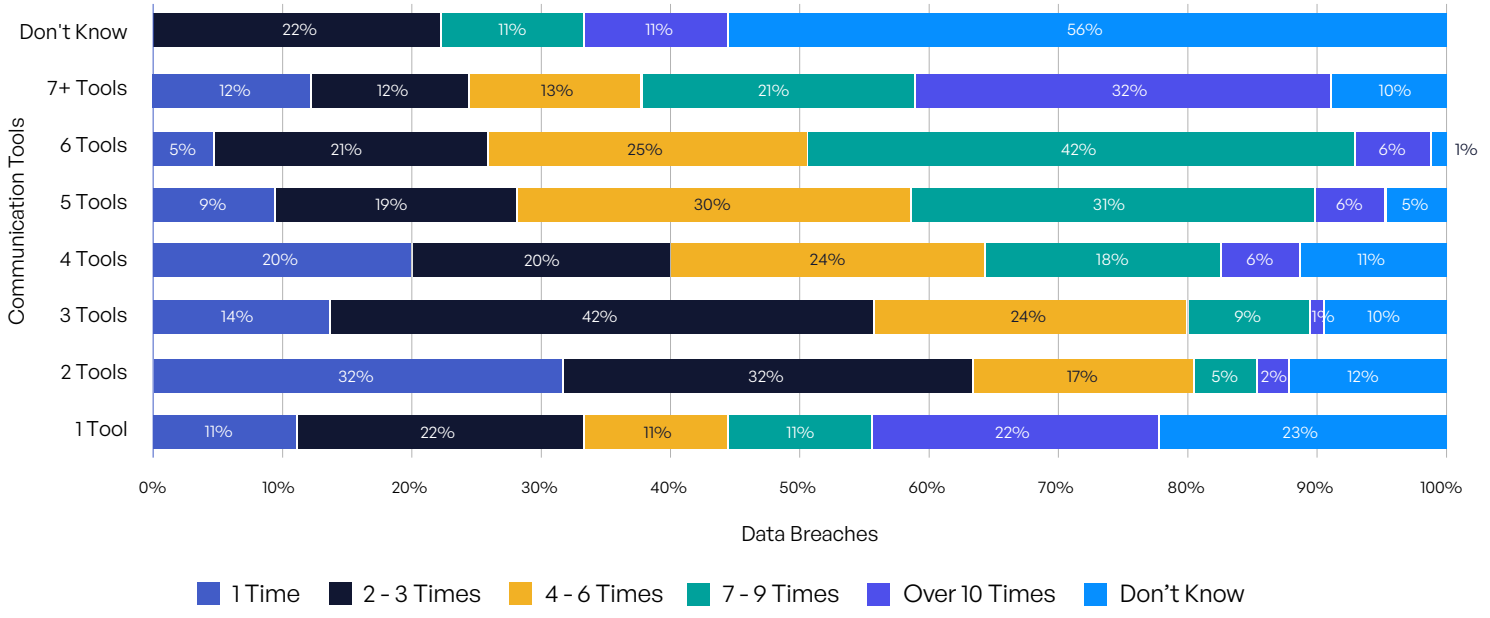


Figure 69: Number of Communication Tools and Data Breaches.

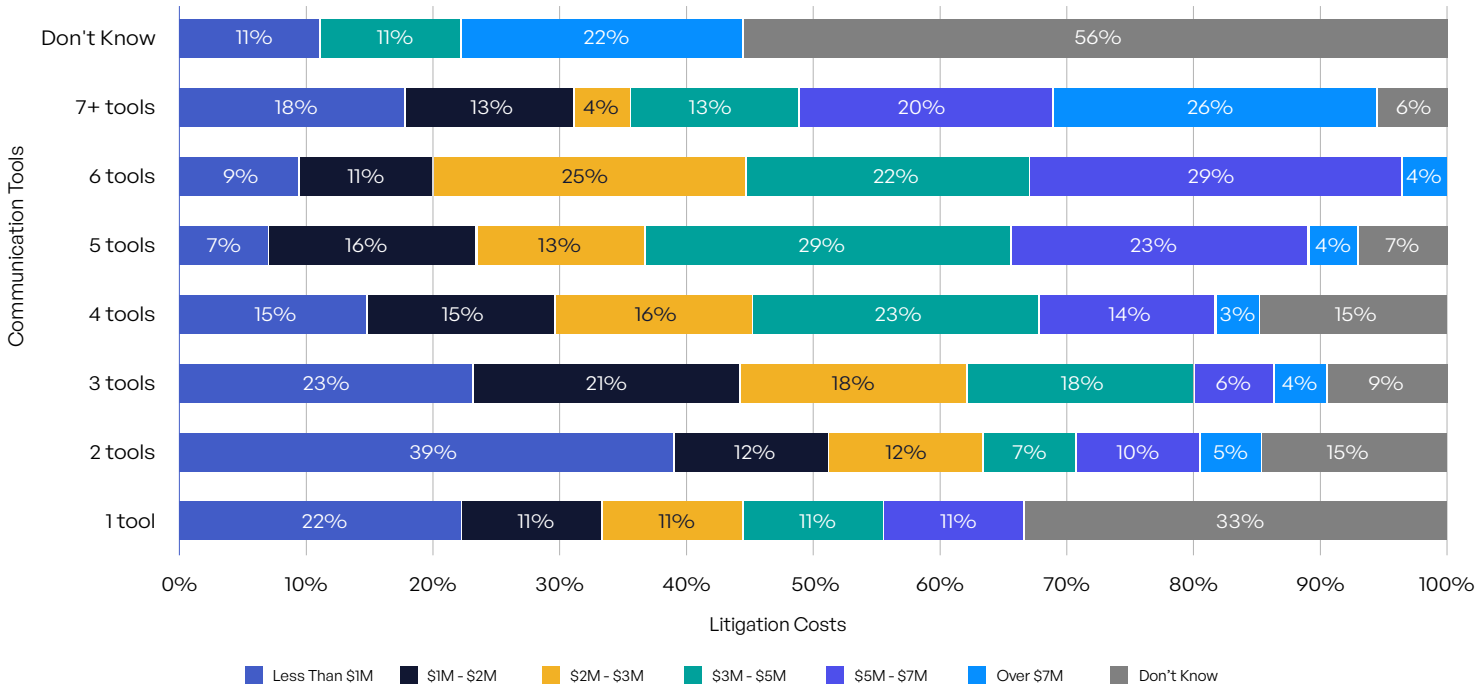


Figure 70: Number of Communication Tools and Data Breach Litigation Costs.

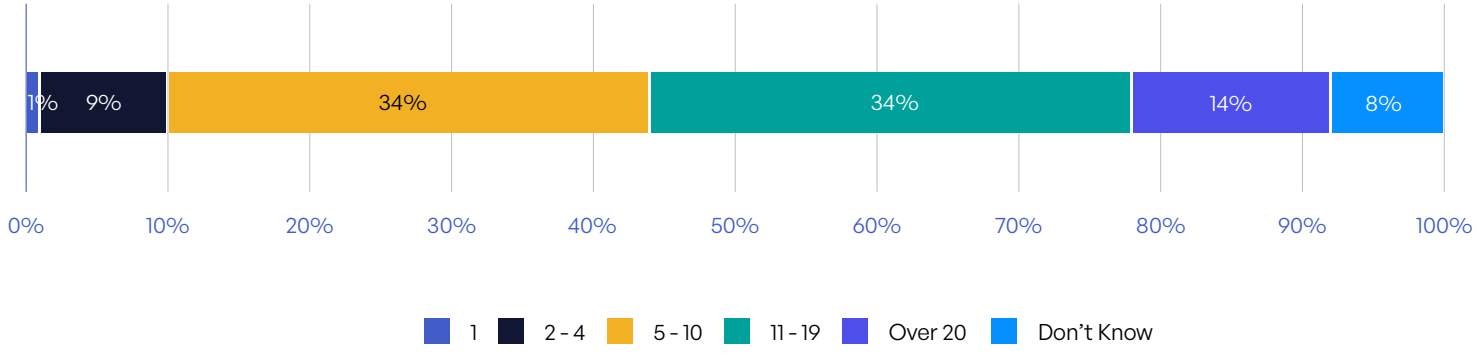


Figure 71: Audits Logs That Must Be Consolidated.

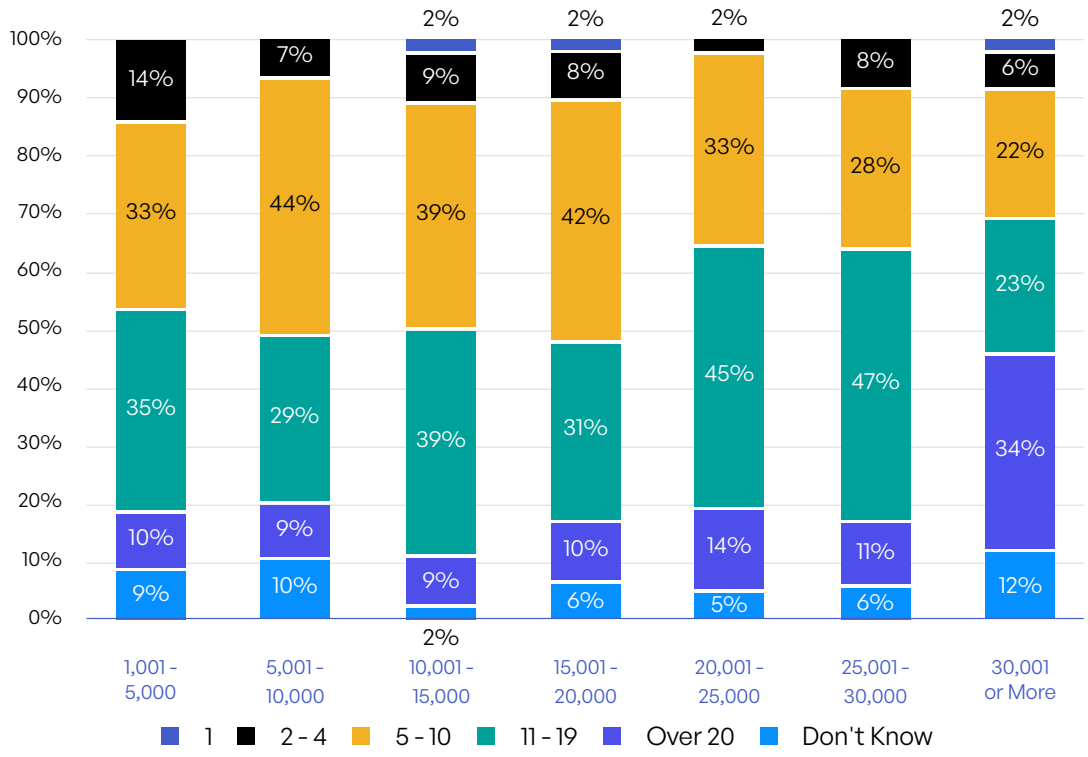


Figure 72: Number of Logs That Must Be Consolidated per Organization Size.

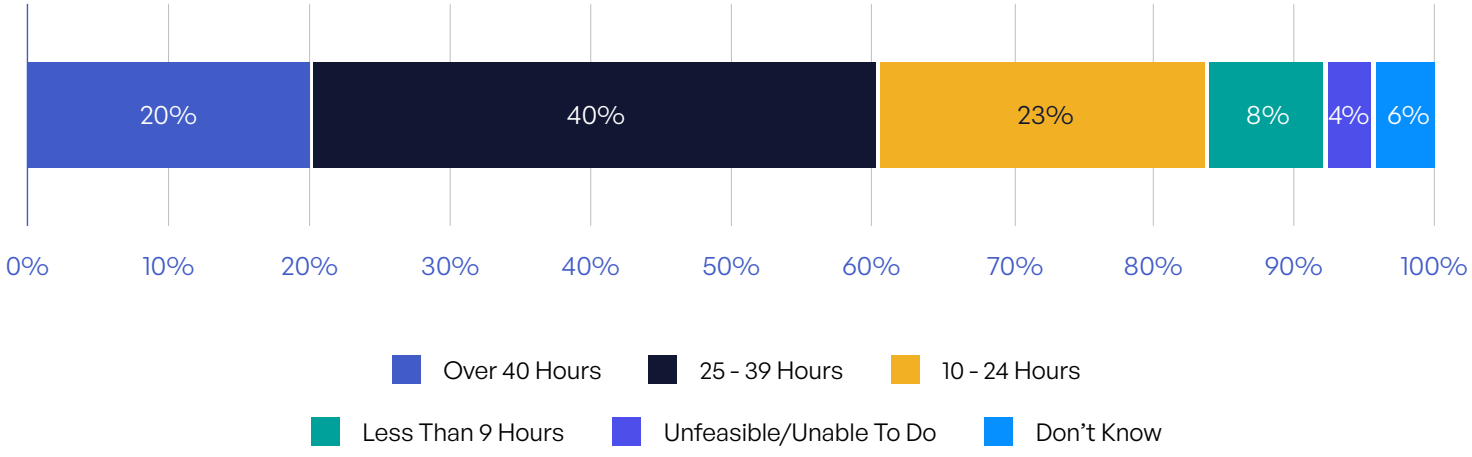


Figure 73: Time Spent Aggregating Audit Logs per Month.

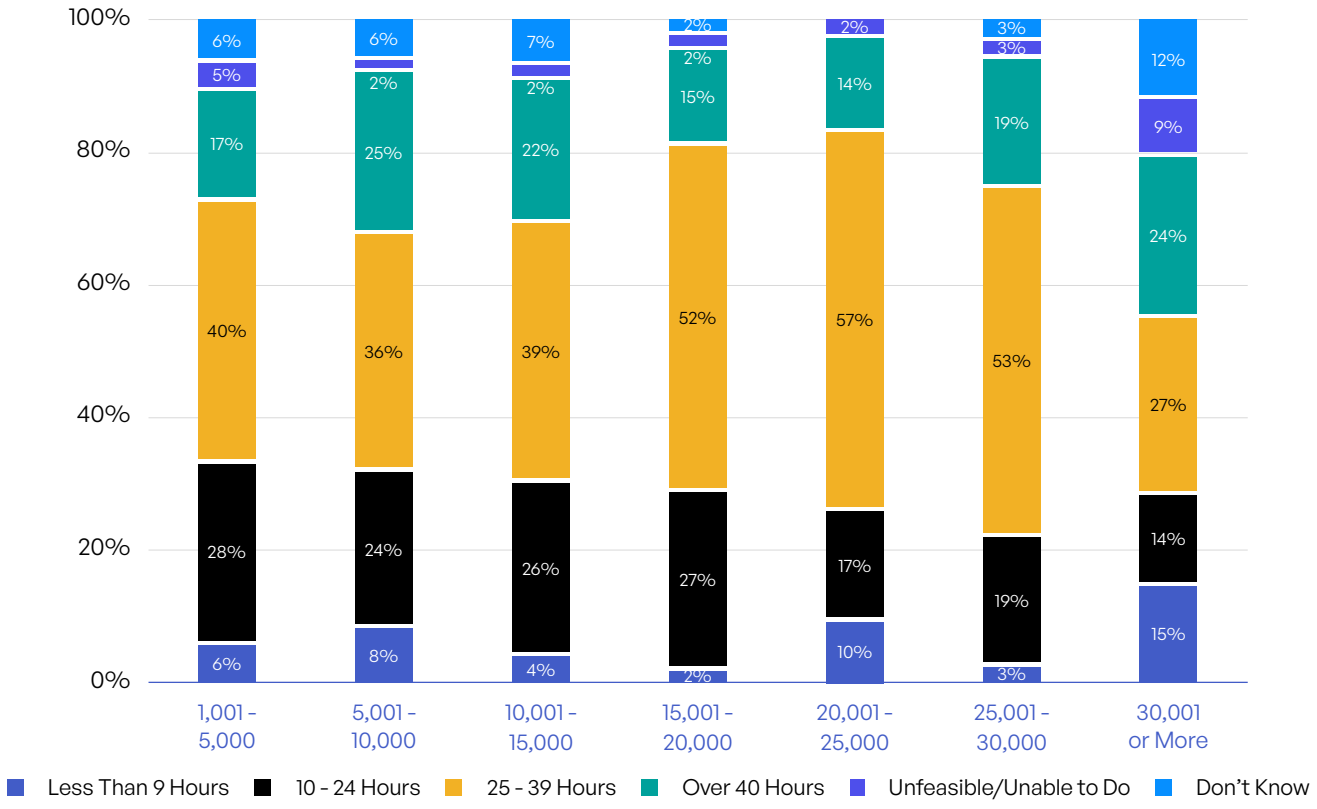


Figure 74: Time Spent Monthly Aggregating Logs for Sensitive Content Communications per Organization Size.

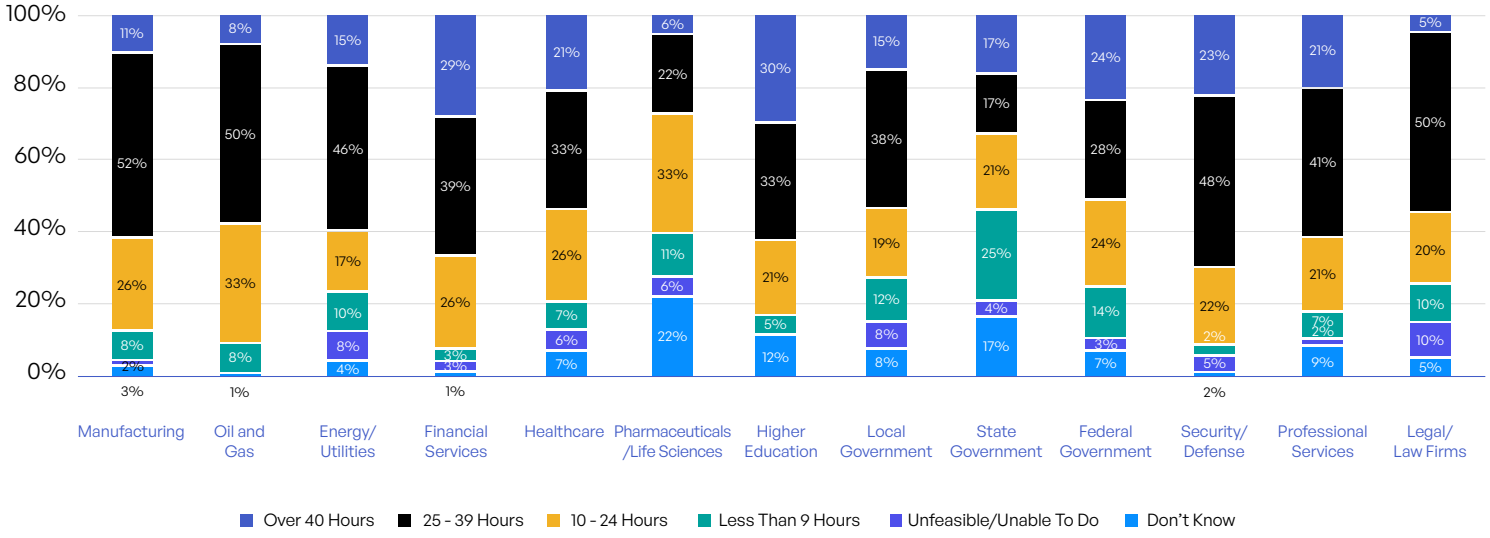


Figure 75: Time Organizations Spend Each Month Manually Aggregating Audit Logs Across Industries.

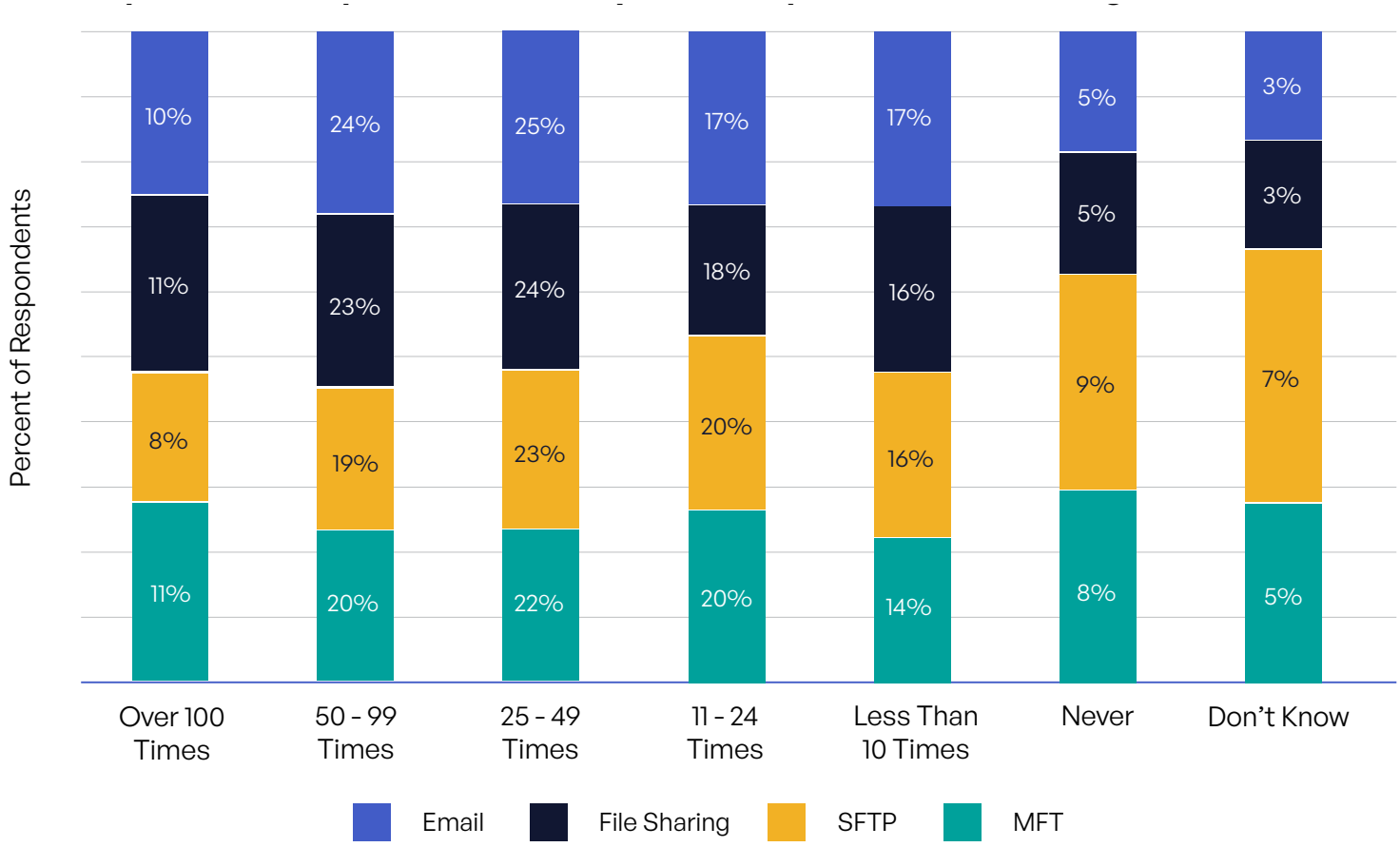


Figure 76: Operational Impact and Security and Compliance Risks of Large File Sizes.

	APAC				NORTH AMERICA				EMEA			
	Email	File Sharing	SFTP	MFT	Email	File Sharing	SFTP	MFT	Email	File Sharing	SFTP	MFT
Never	0%	2%	3%	2%	4%	4%	8%	16%	5%	6%	10%	11%
Less Than 10 Times	9%	14%	9%	9%	14%	13%	14%	10%	21%	17%	18%	17%
10 to 24 Times	27%	17%	27%	27%	11%	18%	18%	17%	14%	17%	17%	18%
25 to 49 Times	32%	24%	24%	25%	20%	23%	22%	21%	24%	24%	21%	20%
50 to 99 Times	17%	26%	18%	19%	30%	24%	21%	25%	22%	21%	18%	17%
Over 100 Times	6%	8%	6%	9%	15%	14%	11%	15%	7%	8%	5%	9%
Don't Know	3%	3%	7%	3%	1%	1%	3%	3%	2%	3%	8%	5%

Figure 77: Workarounds Required Each Month Due to File Size Limits Across Regions.

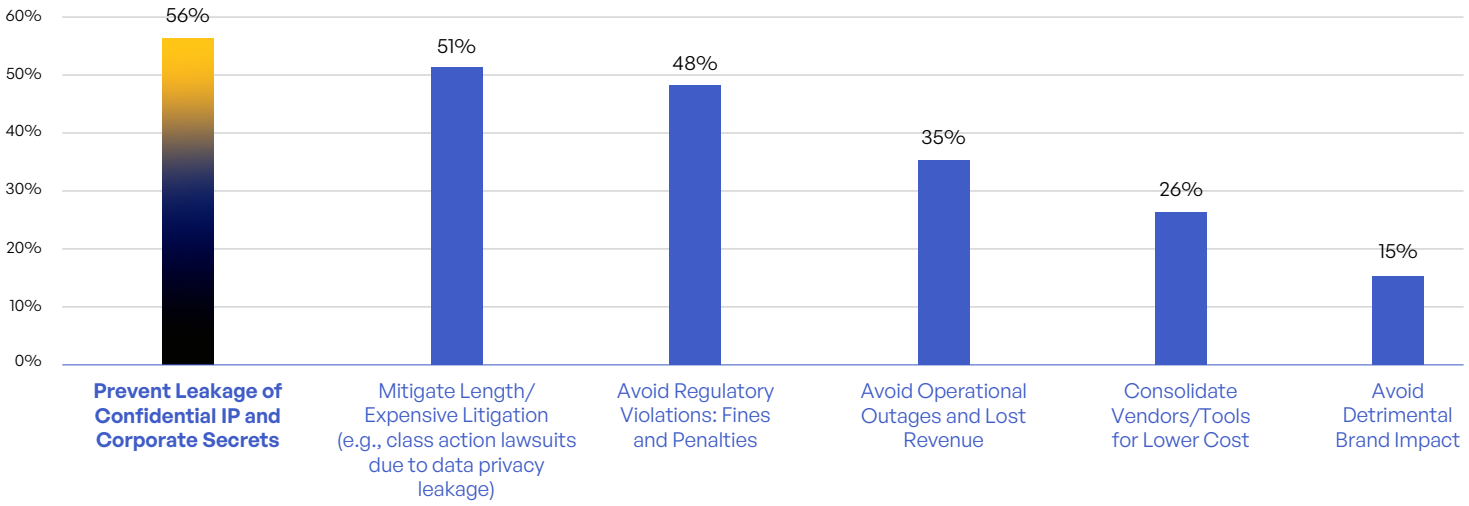


Figure 78: Biggest Drivers Related to Unifying and Securing Sensitive Content Communications.

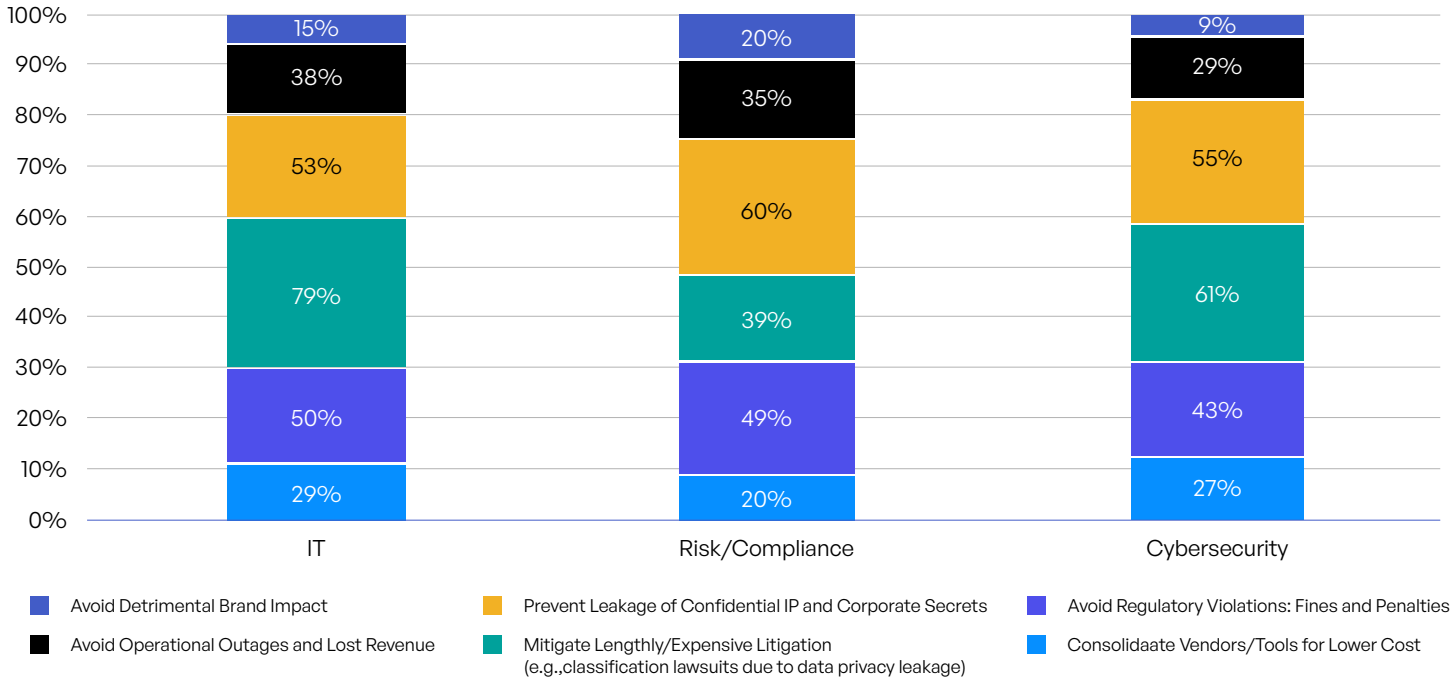


Figure 79: Job Responsibilities and Biggest Sensitive Content Communications Risk Drivers.

Drivers for Unifying and Securing Sensitive Content Communications per Industry

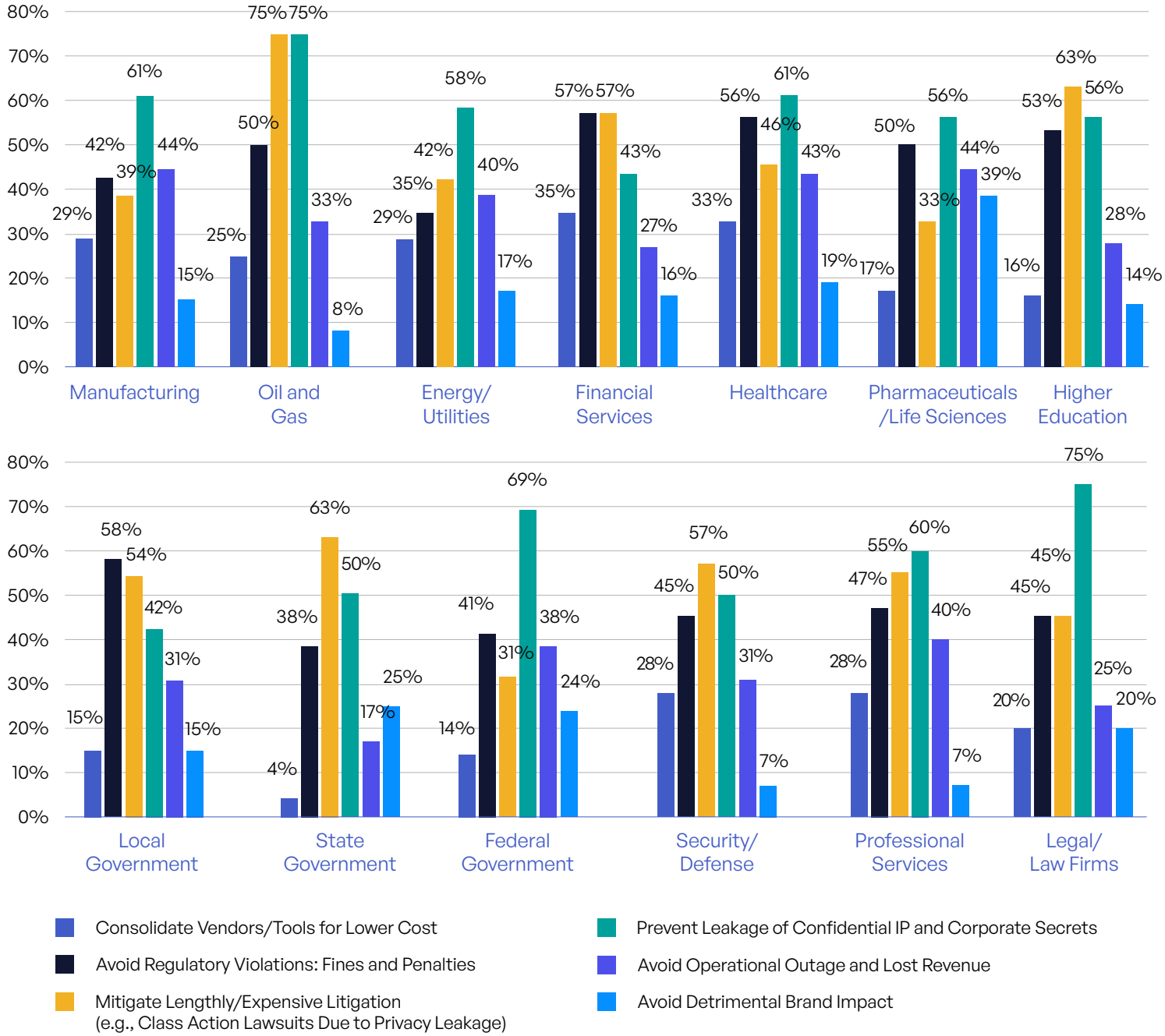


Figure 80: Drivers for Unifying and Securing Sensitive Content Communications per Industry.

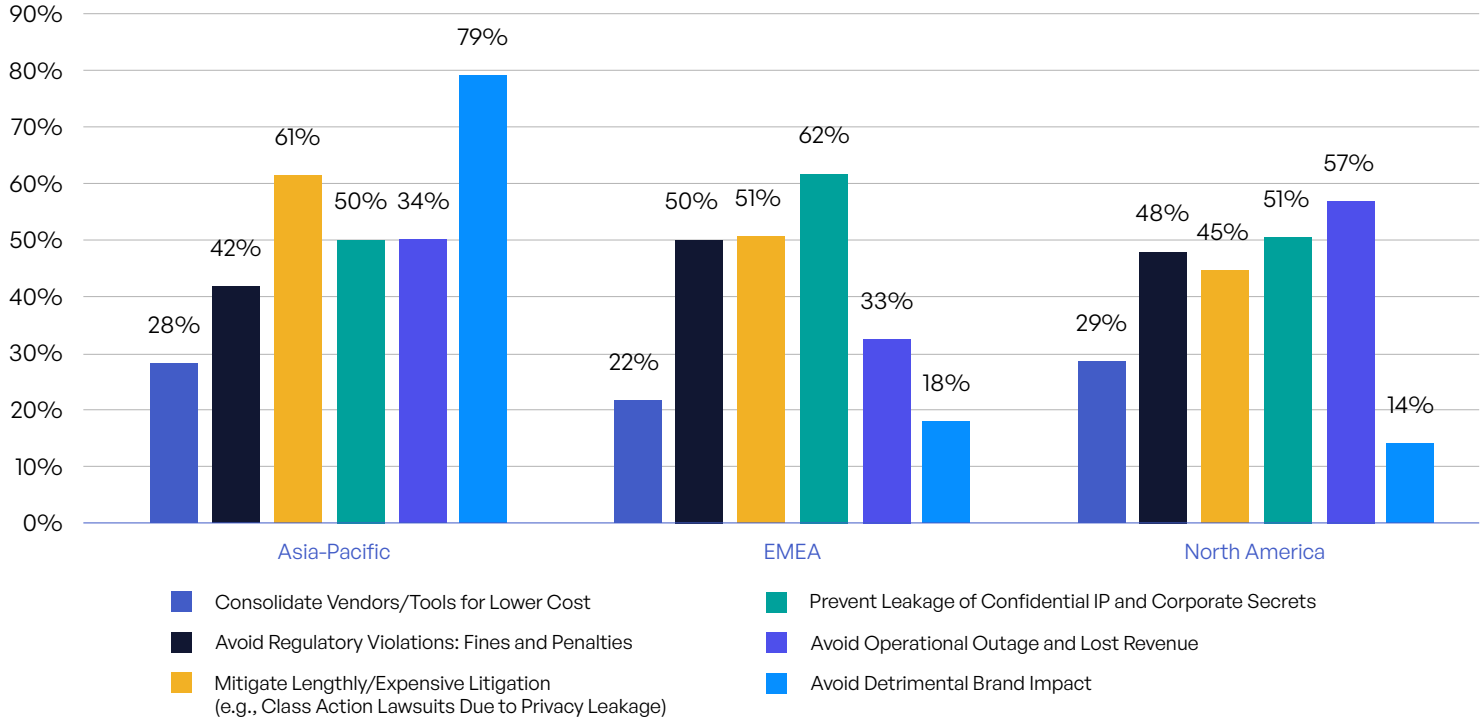


Figure 81: Drivers for Unifying and Securing Sensitive Content Communications Across Regions.

References

1. “2024 Data Breach Investigations Report,” Verizon, April 2024.
2. Matt Kapko, “Progress Software’s MOVEit meltdown: uncovering the fallout,” Cybersecurity Dive, January 16, 2024.
3. Bill Toulas, “Fortra shares findings on GoAnywhere MFT zero-day attacks,” BleepingComputer, April 1, 2023.
4. “2024 Gartner Technology Adoption Roadmap for Larger Enterprises Survey,” February 2024.
5. Eileen Yu, “Employees input sensitive data into generative AI tools despite the risks,” ZDNet, February 22, 2024.
6. “2024 Global Threat Report,” CrowdStrike, February 2024.
7. “Despite increased budgets, organizations struggle with compliance,” Help Net Security, May 24, 2024.
8. “Data Protection and Privacy Legislation Worldwide,” U.N. Trade & Development, accessed June 7, 2024.
9. “U.S. State Privacy Legislation Tracker,” IAPP, last updated May 28, 2024.
10. Martin Armstrong, “EU Data Protection Fines Hit Record High in 2023,” Statistica, January 8, 2024.
11. “Health Information Privacy: Enforcement Highlights,” U.S. Health and Human Services, accessed April 30, 2024.
12. “2024 Data Breach Investigations Report,” Verizon, April 2024.
13. “2023 Data Breach Report,” ID Theft Center, January 2024.
14. “Cost of a Data Breach Report 2023,” IBM Security, July 2023.
15. Ibid.
16. “2024 Global Threat Report,” CrowdStrike, February 2024.
17. “2024 Data Breach Investigations Report,” Verizon, May 2024.
18. “Privacy in Practice 2024,” ISACA, January 2024.
19. “Fortinet Global Zero Trust Report Finds Majority of Organizations Are Actively Implementing Zero Trust But Many Still Face Integration Challenges,” Fortinet Press Release, June 20, 2023.

Kiteworks

June 2024

www.kiteworks.com