Enterprise Strategy Group™ by TechTarget

Operationalizing Encryption and Key Management

Jack Poller | Senior Analyst
ENTERPRISE STRATEGY GROUP

DECEMBER 2023

Research Objectives

The potential for serious business disruptions from breaches makes securing data critical. Ransomware, software supply chain compromise, and targeted penetration attacks are just some of the looming threats that can result in data loss, compliance violations, brand damage, and lost revenue. Additionally, ransomware actors are changing their tactics to focus on data extortion: holding exfiltrated data hostage to public exposure.

As a result, organizations are turning to encryption to maintain cyber-resiliency in response to a successful data breach as well as to ensure data privacy and compliance. Although organizations understand how encryption protects data, they struggle with the implementation, specifically how encryption and key management solutions balance security, usability, performance, compatibility, and costs. Further compounding these problems is quantum computing's potential to break current encryption protocols, representing another challenge to securing sensitive data. Vendors need to demystify and simplify encryption and key management.

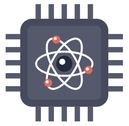
To gain more insights into these trends, TechTarget's Enterprise Strategy Group surveyed 387 IT, compliance, DevOps, and cybersecurity professionals at organizations in North America (US and Canada) involved with encryption and data security technology and processes.

This study sought to:

Determine which cyberthreats and attack vectors inspire an increased focus on encryption and key management strategies.

Understand the challenges organizations have encountered with encryption that have limited its usage.

Establish the level of understanding organizations have about the full capabilities of encryption and key management solutions.



Highlight how new technologies like quantum computing disrupt legacy encryption and key management approaches.

BACK TO CONTENTS

KEY FINDINGS

CLICK TO FOLLOW

Encryption Is Pervasive and Growing

PAGE 4

Operational Issues Plague Encryption Deployments

PAGE 9

A Lack of Encryption Was the Primary Contributor to All-too-common Data Loss

PAGE 12

The Post-quantum Cryptography Journey Has Started

PAGE 16

Encryption Is a Strategic Security Activity

PAGE 19

More Spending Is Ahead for Encryption Initiatives

PAGE 23

Encryption Is Pervasive and Growing

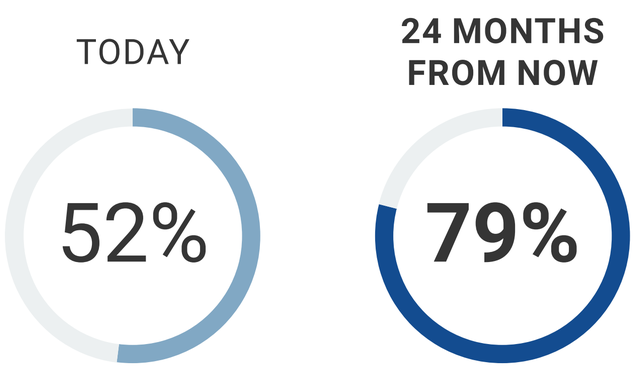
Encryption for All Three Data Use Cases Will Increase

Data at rest is data housed physically on computer data storage in any digital form that is not being accessed or used (e.g., cloud storage, SAN, NAS, databases, archives, backups, mobile devices, etc.). On average, 60% of data at rest is encrypted, and this is expected to increase to 78% in 24 months.

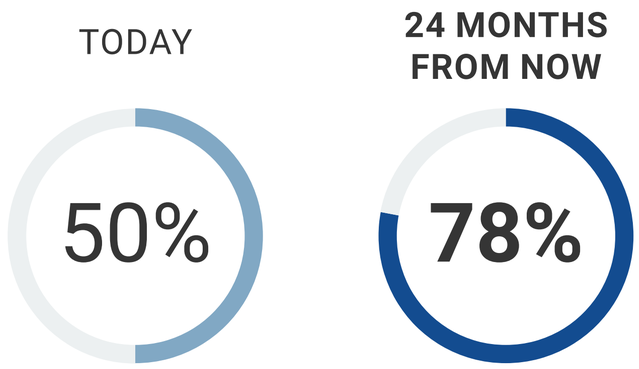
Data in motion, also known as data in transit or data in flight, is data moving from one location to another, such as across the internet, through a private network, or between services. On average, 59% of data in motion is encrypted, and this will increase to 77% in 24 months.

Data in use is data currently being updated, processed, accessed, or read by a system. This type of data is actively moving through parts of an IT infrastructure and is stored in a non-persistent digital state, such as computer RAM, CPU caches, or CPU registers. On average, 60% of data in use is encrypted, and this will likely increase to 77% in 24 months.

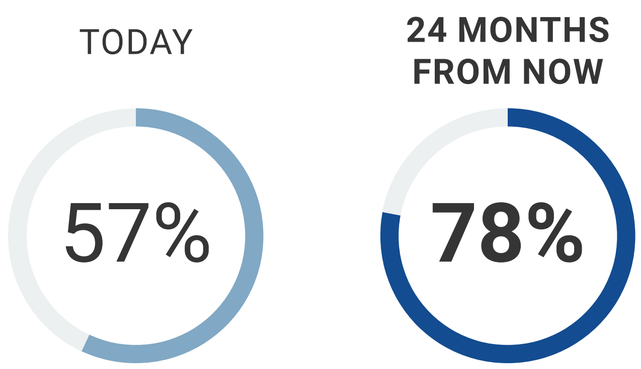
Organizations that encrypt more than 60% of their **data at rest.**



Organizations that encrypt more than 60% of their **data in motion.**



Organizations that encrypt more than 60% of their **data in use.**

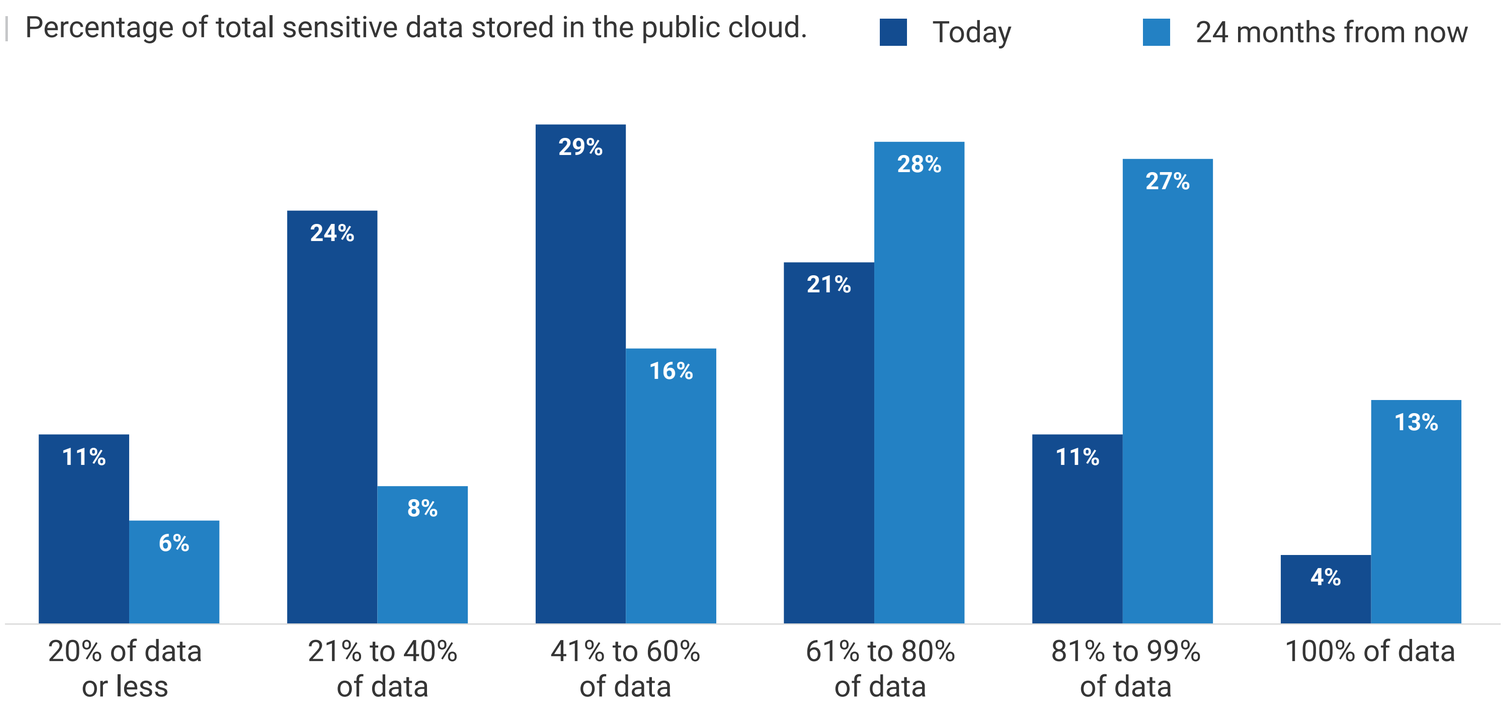


BACK TO CONTENTS

Sensitive Data Continues to Move to the Cloud, Protected by Encryption

Public cloud services are now ubiquitous. Digital transformation initiatives, business intelligence, data analytics, and the rapid explosion in the use of generative AI have accelerated the migration of sensitive data assets to the cloud. On average, 51% of an organization's sensitive data is stored in the cloud, and this will likely grow to 68% in 24 months. Specifically, 36% of respondents said that more than 60% of their sensitive data resides on public cloud services today. This is expected to increase to 68% of organizations within 24 months. More surprisingly, 4% of organizations store all their sensitive data in the cloud, which is expected to more than triple to 13% of organizations within 24 months.

More than two-thirds (68%) of organizations employ encryption to protect their cloud-resident sensitive data. Encryption was the second most often used security technology for protecting sensitive data stored in the public cloud, just behind cloud security management tools such as CNAPP, CSPM, CIEM, etc.



"68% of organizations use data encryption technology to protect their cloud-resident sensitive data."

BACK TO CONTENTS

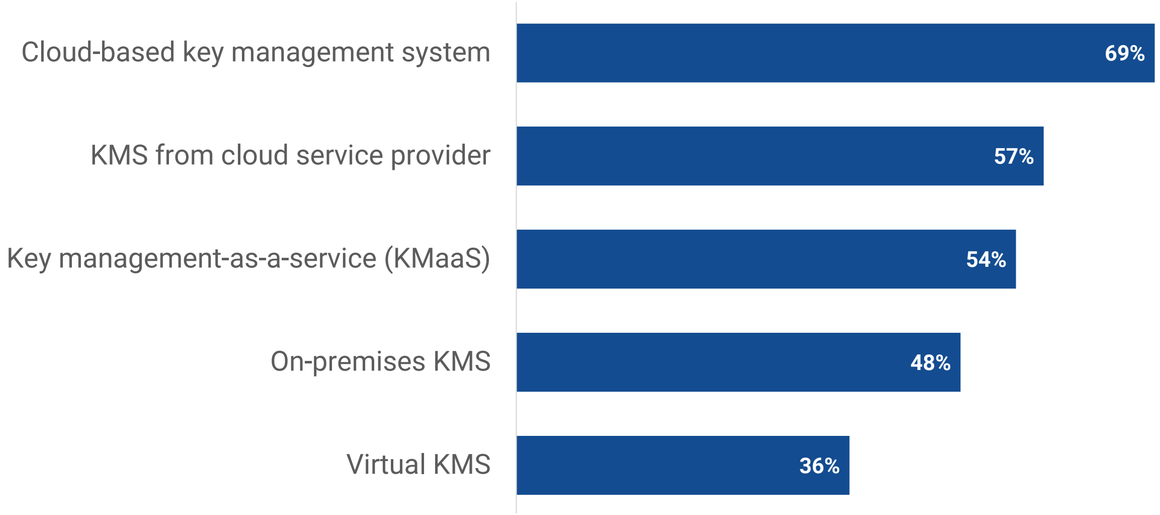
Although Cloud Deployment Is Preferred, the Majority Currently Employ a Hybrid Cryptographic Infrastructure

As with data, the flexibility, scalability, and cost structure of the cloud make it more favorable and ubiquitous for infrastructure deployments. Thus, more organizations deploy cloud-based or CSP-provided key management systems (KMSs) to manage cryptographic keys throughout the key lifecycle. Likewise, more organizations deploy cloud-based hardware security modules (HSMs) to perform encryption and safeguard and manage secrets and keys.

While cloud-based solutions are preferred, overall, the majority employ a hybrid cryptographic infrastructure via both cloud-based and on-premises KMSs, HSMs, and other cryptographic solutions.

Hardware security modules in use for sensitive data.

Key management systems in use.



Cryptographic infrastructure deployment.

57%
Hybrid, combining both on-premises and cloud-deployed cryptographic infrastructure

24%
All cryptographic infrastructure is deployed in the cloud

19%
All cryptographic infrastructure is deployed on premises

BACK TO CONTENTS

Cryptographic Solutions Are Making a Positive Impact

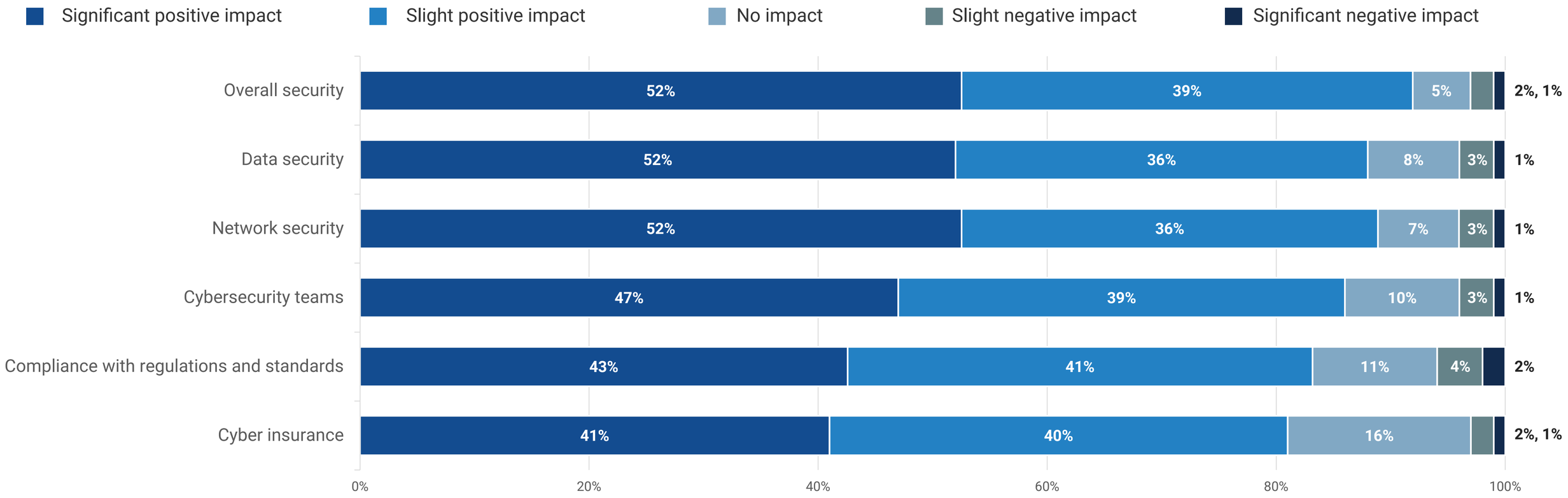
While organizations expect, and commonly experience, an improvement in overall security when deploying cryptographic solutions, encryption provides other benefits such as:

Compliance with regulations such as PCI-DSS, Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), and others.

Improved availability and cost of cyber insurance due to encryption's perceived protection for data exfiltration/data hostage-taking during ransomware attacks and other cyber attacks.

Reduced workload for cybersecurity teams responding to alarms, threats, and attacks.

Impact of cryptographic policies and deployment of encryption solutions.



BACK TO CONTENTS

Operational Issues Plague Encryption Deployments

Despite the Clear Cloud Preference, Organizations Face Internal Operational Challenges When Migrating to the Cloud

The top challenges associated with migrating the cryptographic infrastructure to the cloud share the common thread of internal operating issues. Specifically, more than a quarter (26%) of organizations lack sufficient cybersecurity staff. The chronic global cybersecurity skills shortage[1] is most likely a contributing factor to this and the other challenges. With too much to do and not enough people, encryption often falls off the high-priority task list and is frequently perceived as difficult to coordinate in a complex environment.

Likewise, lack of expertise makes determining where and when to apply encryption a difficult task.

Most difficult encryption tasks.

12%
Determining where and when to apply encryption

10%
Managing and validating certificate chains of trust

10%
Encrypting to ensure regulatory compliance

Top five cryptographic infrastructure cloud migration challenges.

26%
Lack of sufficient cybersecurity staff

24%
Higher priorities than encryption

24%
Expense associated with cloud-based cryptographic infrastructure solutions

24%
Difficulties coordinating encryption in a complex environment

22%
Level of effort to deploy and integrate cloud-based cryptographic infrastructure solutions

[1] Source: Enterprise Strategy Group Research Report, *2023 Technology Spending Intentions Survey*, November 2022.

BACK TO CONTENTS

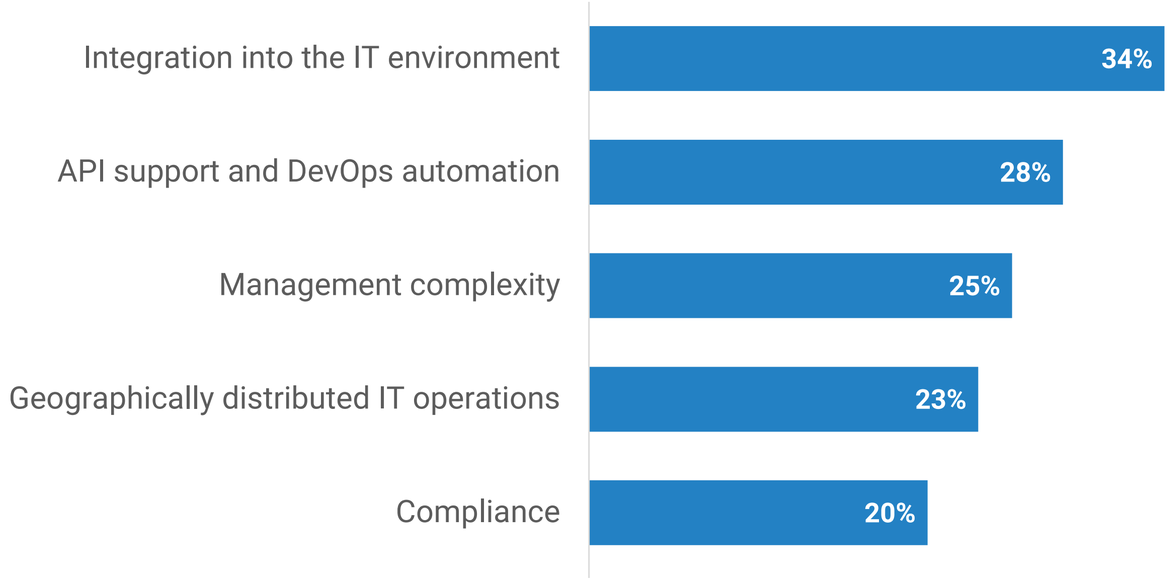
Complexity Leads to KMS and HSM Integration Challenges

To operate properly, cryptographic infrastructure, especially hardware security modules and key management systems, must interoperate with myriad devices, systems, and applications throughout the ever-more complex IT environment. This makes integrating encryption into the IT environment the most cited challenge for both KMSs and HSMs.

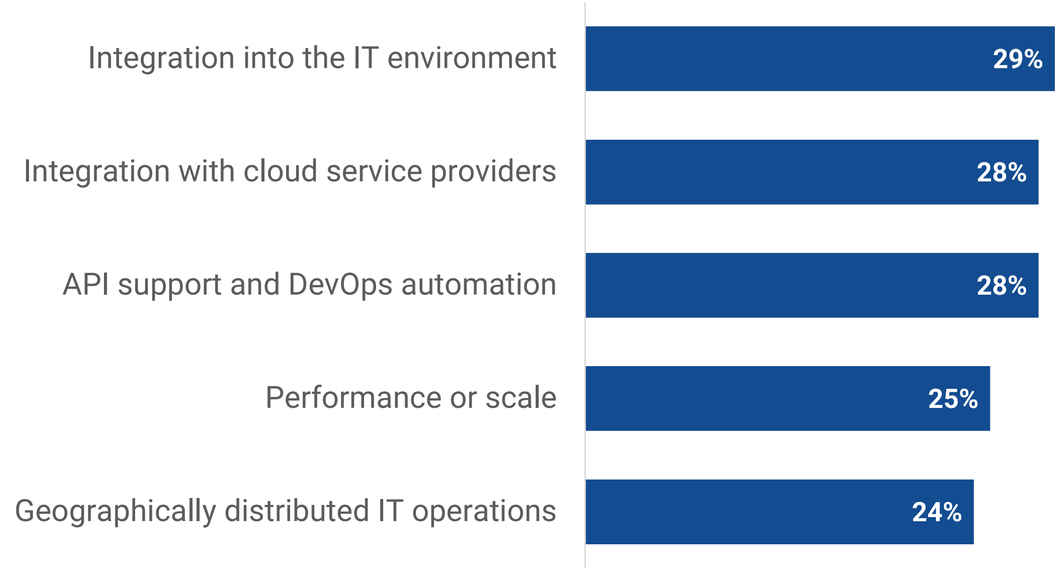
Given encryption's long history, it's not surprising that cryptographic solutions haven't completed the transition from supporting traditional waterfall development to supporting modern automated DevOps paradigms. Thus, while organizations want to use encryption to protect their internally developed applications, more than a quarter said that they faced challenges using the KMS APIs and automating KMSs in their DevOps environments.

Furthermore, HSMs, being primarily hardware-based solutions, also proved to be challenging to integrate into non-owned cloud service provider environments.

Top five key management challenges.



Top five hardware security module challenges.



BACK TO CONTENTS

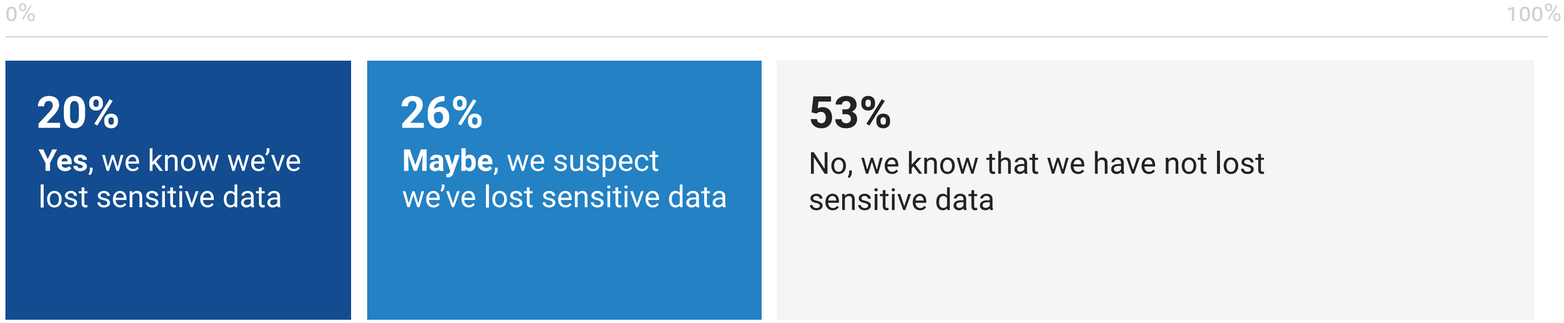
A Lack of Encryption Was the Primary Contributor to All-too-common Data Loss

Loss of Sensitive Data Is Common and Suspected

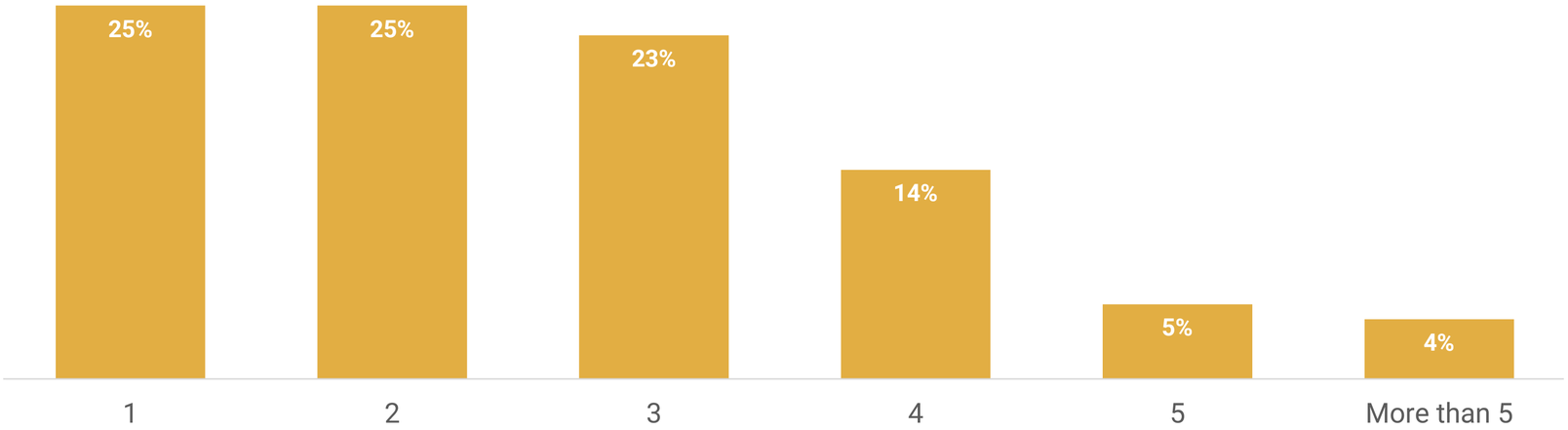
One in five (20%) respondents know their organization has lost sensitive data. Of greater concern are the 26% who suspect they've lost sensitive data but don't know for sure because they don't have the tooling or expertise to find out. These organizations are failing to learn from and respond to data loss, resulting in multiple incidents.

Unfortunately, nearly three-quarters (71%) of organizations with confirmed or suspected data loss incidents indicate this has happened at least twice in the past 12 months, with almost half (46%) reporting three or more data loss events.

Sensitive data loss incidents within the last 12 months.



Number of sensitive data loss incidents.



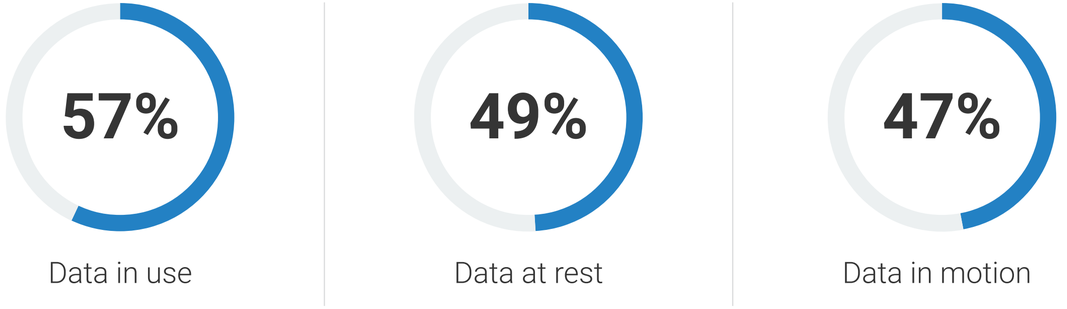
BACK TO CONTENTS

Contributors to Sensitive Data Loss

While the focus is often on data at rest and data in motion because the protection technology is mature and well-understood, more than half (57%) of organizations have actually experienced loss of data in use.

This raises questions regarding the organizational understanding of data-in-use security controls and the prevalence of data-in-use attacks.

Data has been lost across all use cases.



Causes of sensitive data loss.

POLICY

- Sensitive data was not encrypted when it should have been: **33%**
- Incorrect/insufficient security policies: **28%**
- Unsanctioned apps/services: **27%**
- Encryption key was too small, leading to unauthorized decryption: **25%**
- Shadow data: **18%**

MISCONFIGURATION

- Misconfiguration of encryption of data in motion: **33%**
- Misconfiguration of encryption of data at rest: **26%**
- Misconfiguration of encryption of data in use: **25%**

ACCESS

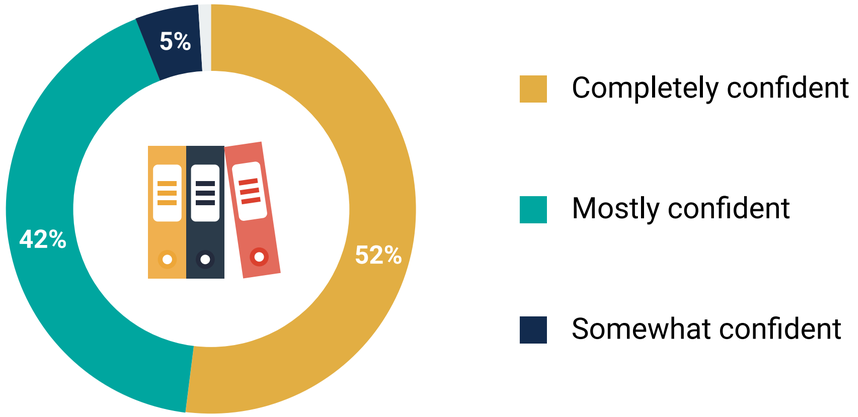
- Malicious actor exfiltrated unencrypted data: **32%**

BACK TO CONTENTS

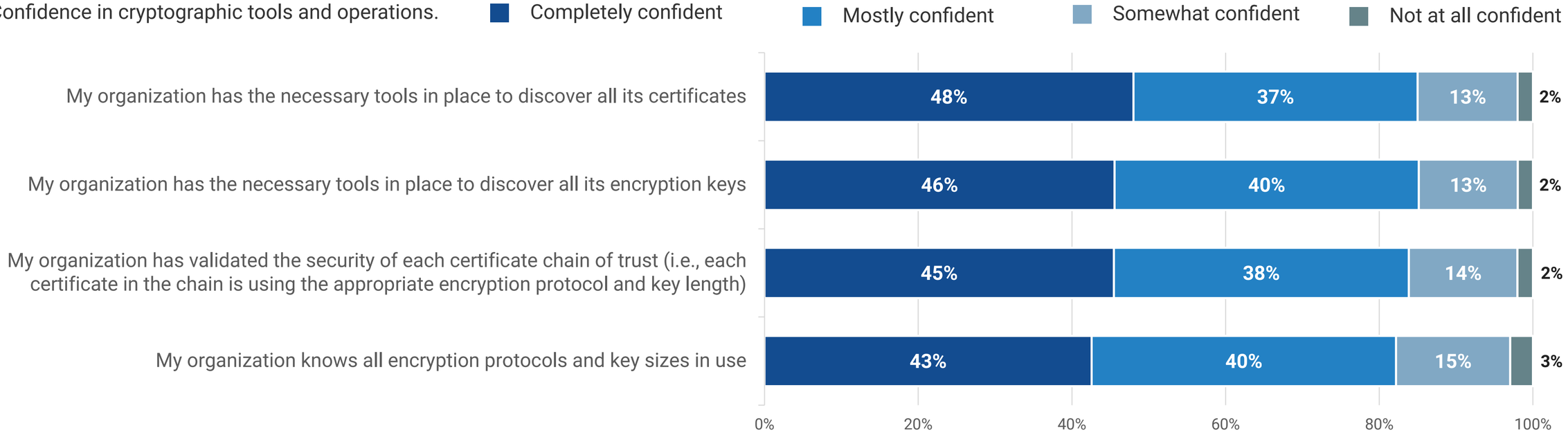
Overconfidence in Cryptographic Capabilities?

Most organizations place a premium on knowing what sensitive data they have and where that data is located, so confidence in these abilities is high. Specifically, 94% of respondents were mostly or completely confident in their organization's ability to discover and identify sensitive data. However, as seen previously, 18% of organizations attribute a sensitive data loss event within the past year to undiscovered shadow data, and more than a quarter (27%) say that they lost data in shadow apps and services. Confidence levels are similarly high in knowing all encryption protocols and key sizes in use despite the fact that 25% of organizations attributed a sensitive data loss event to using too small an encryption key, leading to unauthorized decryption.

Confidence in ability to discover and identify all sensitive data.



Confidence in cryptographic tools and operations.



BACK TO CONTENTS

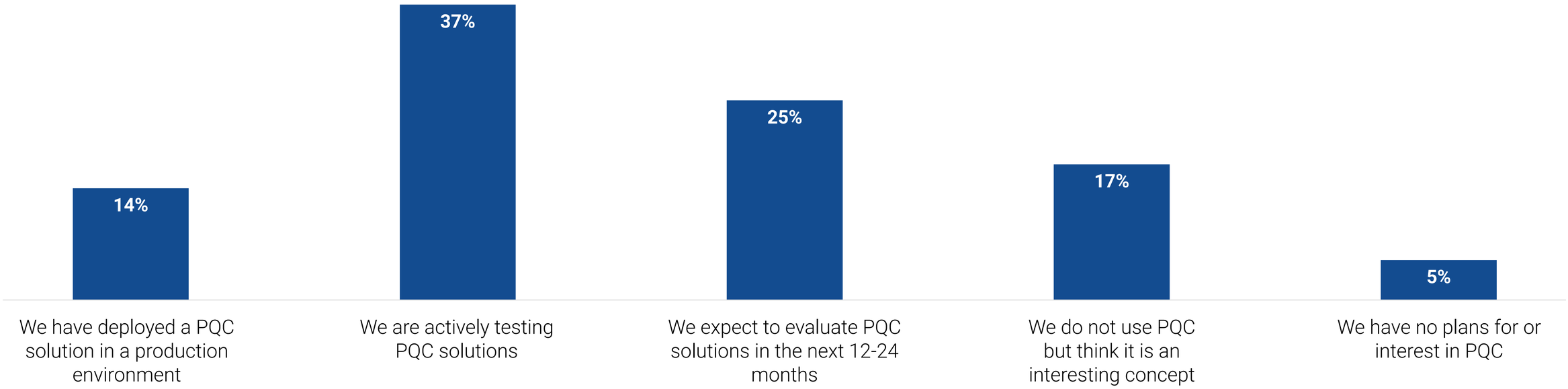
The Post-quantum Cryptography Journey Has Started

Half Have Started Their Post-quantum Cryptography Journey

Quantum computing harnesses the principles of quantum mechanics to process information using quantum bits (qubits), enabling the simultaneous representation of multiple states and the potential to solve certain problems, such as encryption, exponentially faster than classical computers. Thus, the National Institute of Standards and Technology (NIST) has begun the process of standardizing encryption algorithms designed to withstand attacks by quantum computers.

Although no quantum computers are currently big enough to break encryption algorithms, with billions of dollars being invested in building bigger and faster quantum machines, current encryption algorithms may become insecure at any time. Thus, vendors have already commercialized quantum-safe or post-quantum cryptographic (PQC) algorithms, and more than half of organizations have started their journey to replace their current encryption with PQC. Another 25% will start in the next 12-24 months.

Usage of or plans for post-quantum cryptography.



BACK TO CONTENTS

PQC Is Making a Positive Impact

While organizations expect and experience an improvement in data security when deploying post-quantum cryptographic solutions, PQC provides many other benefits such as:

- Improved overall security.
- Compliance with new and existing standards and regulations.
- Eligibility to obtain cyber insurance or reduce rates.

Top five PQC migration issues.

24%
Expense associated with PQC solutions

23%
Lack of sufficient cybersecurity staff

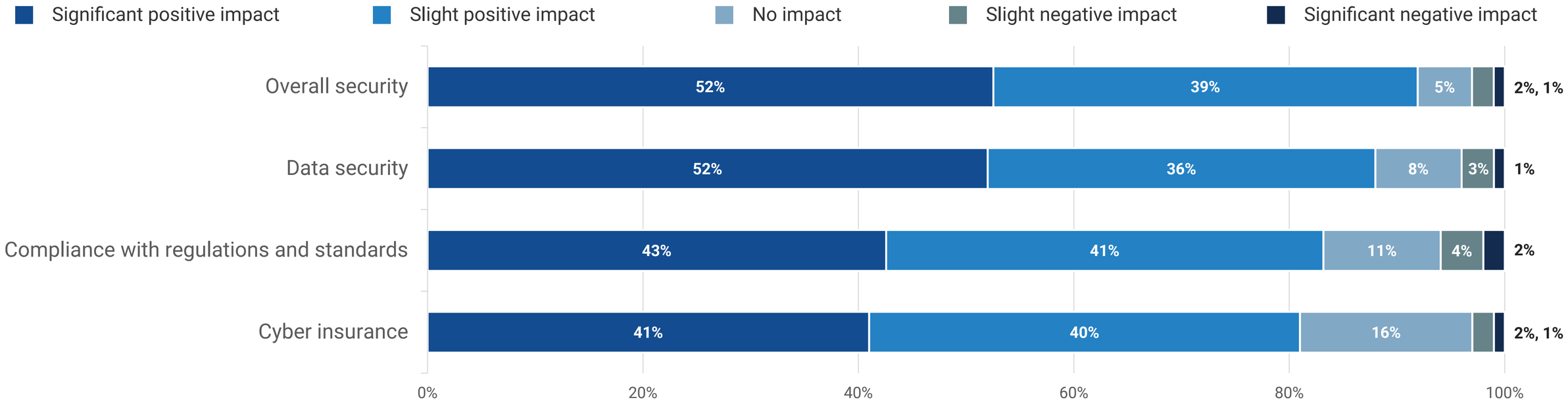
22%
Higher priorities than encryption

21%
Lack of sufficient cybersecurity budget

21%
Lack of tools for building consolidated key inventories

However, migrating an organization's cryptographic infrastructure to PQC is not always easy. Indeed, the top five PQC migration issues are mostly operational and include the expense associated with PQC solutions, lack of sufficient cybersecurity staff, higher priorities, lack of budgets, and lack of tools for building consolidated key inventories.

Impact that PQC has had or will have in certain areas.



BACK TO CONTENTS

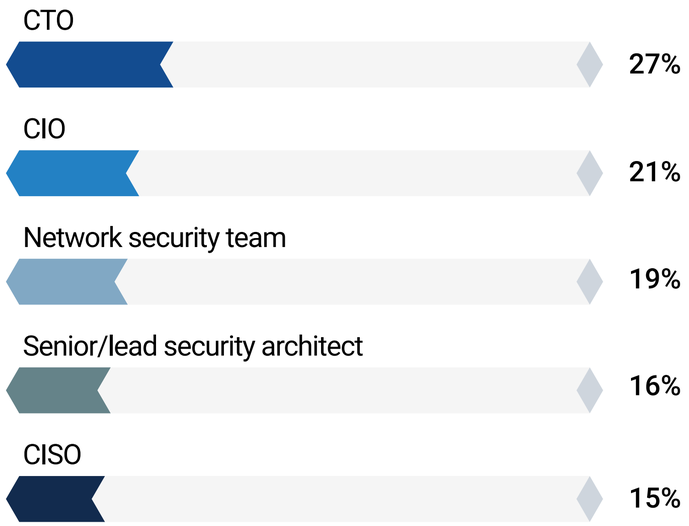
Encryption Is a Strategic Security Activity

Majority Have a Formal Cryptographic Program

Nearly three-quarters (71%) of organizations have adopted a formal cryptographic program, with half of those organizations applying a well-defined and articulated cryptographic policy across their entire organization.

Likewise, 81% of organizations have a team dedicated to encryption, key management, and certificate management. For more than half of those organizations, this encryption team is well established, having been in place for more than a year. Sixty-three percent of the encryption teams report to the C-level (i.e., CTO, CIO, or CISO). This charter indicates that the cryptographic program is of strategic importance to the organization.

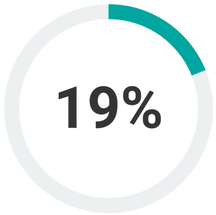
Encryption team reporting structure.



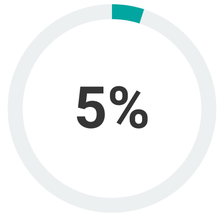
Adoption of a formal cryptographic program.

We've implemented or begun to implement a well-defined and articulated cryptographic policy across the entire organization

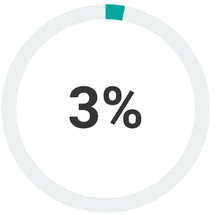
We've implemented or begun to implement a formal cryptographic policy for specific parts of our environment or use cases



We're planning to adopt and implement a formal cryptographic policy

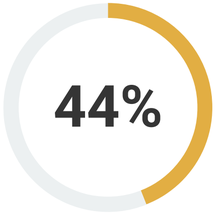


We're interested in developing a formal cryptographic policy

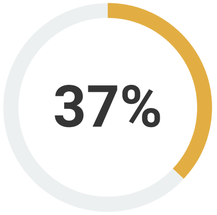


We have no plans for or interest in a formal cryptographic policy

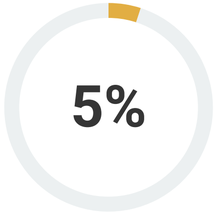
Implementation of an encryption team.



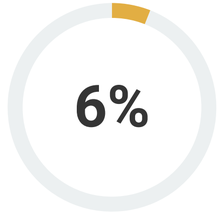
This position(s) has been in place for at least a year



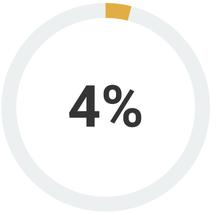
This position(s) was recently established (i.e., within the last 12 months)



We are actively hiring for this position



We plan to establish this type of position(s) within the next 12 to 24 months



We will likely establish this type of position(s) sometime in the future

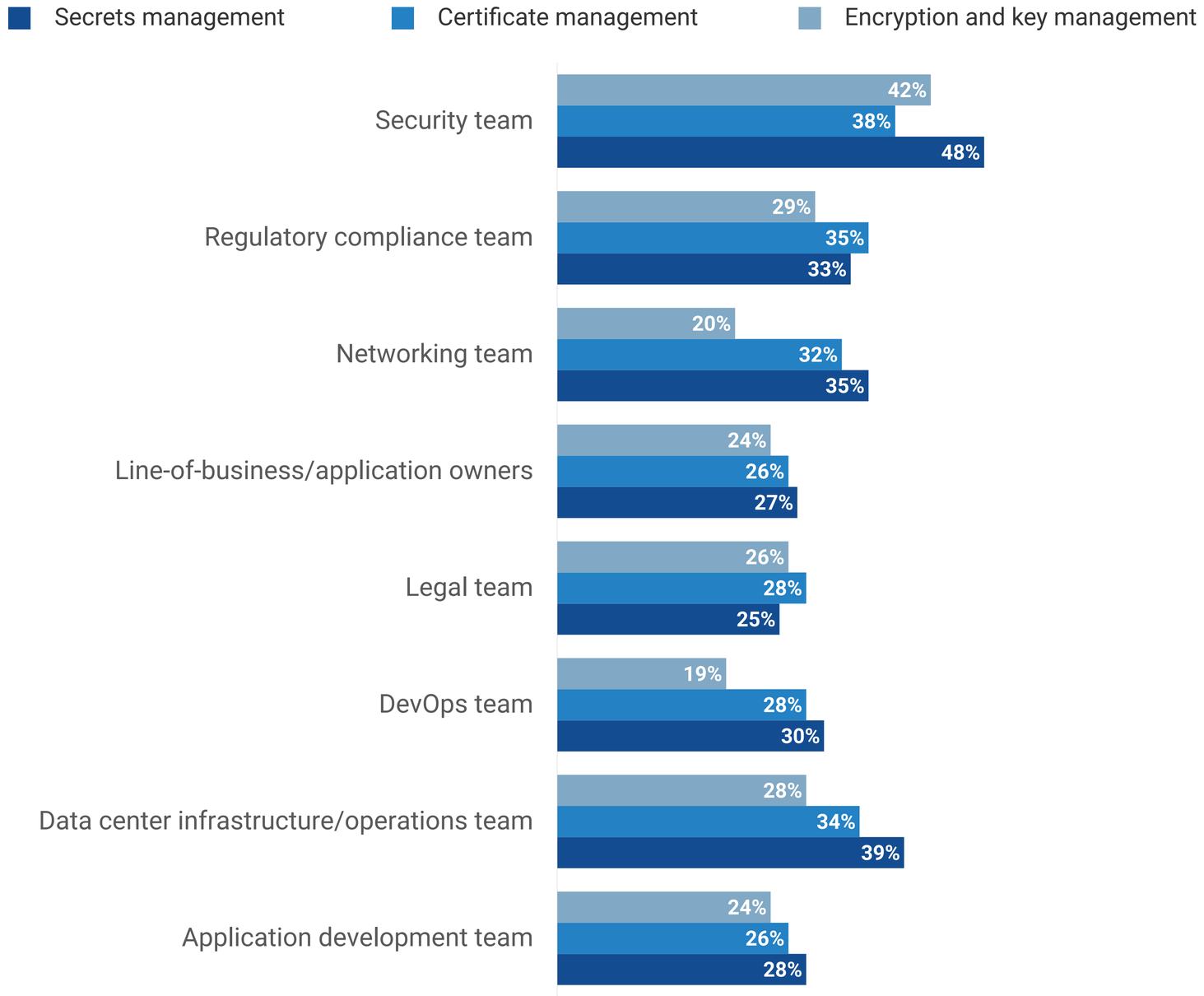
BACK TO CONTENTS

Encryption Is a Team Sport

Even with a formal encryption team, many others are involved in an organization's cryptographic program.

In terms of the individuals or groups that are directly involved in creating policies for secrets management, certificate management, or encryption and key management, the security team takes the lead. However, they are not alone, with other groups representing various interests and responsibilities participating in this process as well, including those in regulatory compliance, networking, lines of business, and legal.

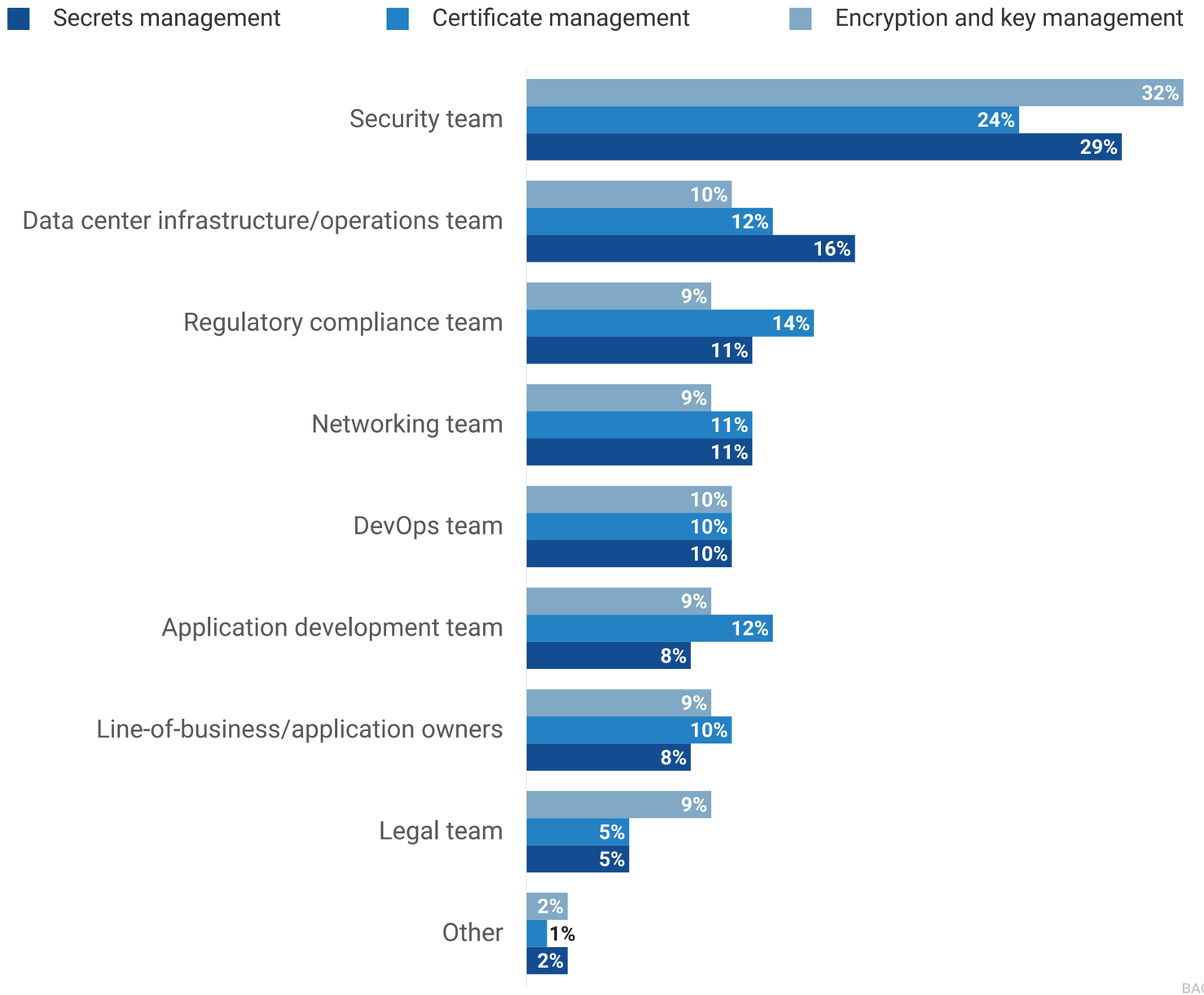
Groups responsible for creating encryption policies.



BACK TO CONTENTS

Similarly, the security team takes the lead in defining the requirements for encryption, certificate, and key management products and services, joined by the data center infrastructure/operations team, regulatory compliance, networking, and DevOps.

Groups responsible for defining requirements for encryption products and services.



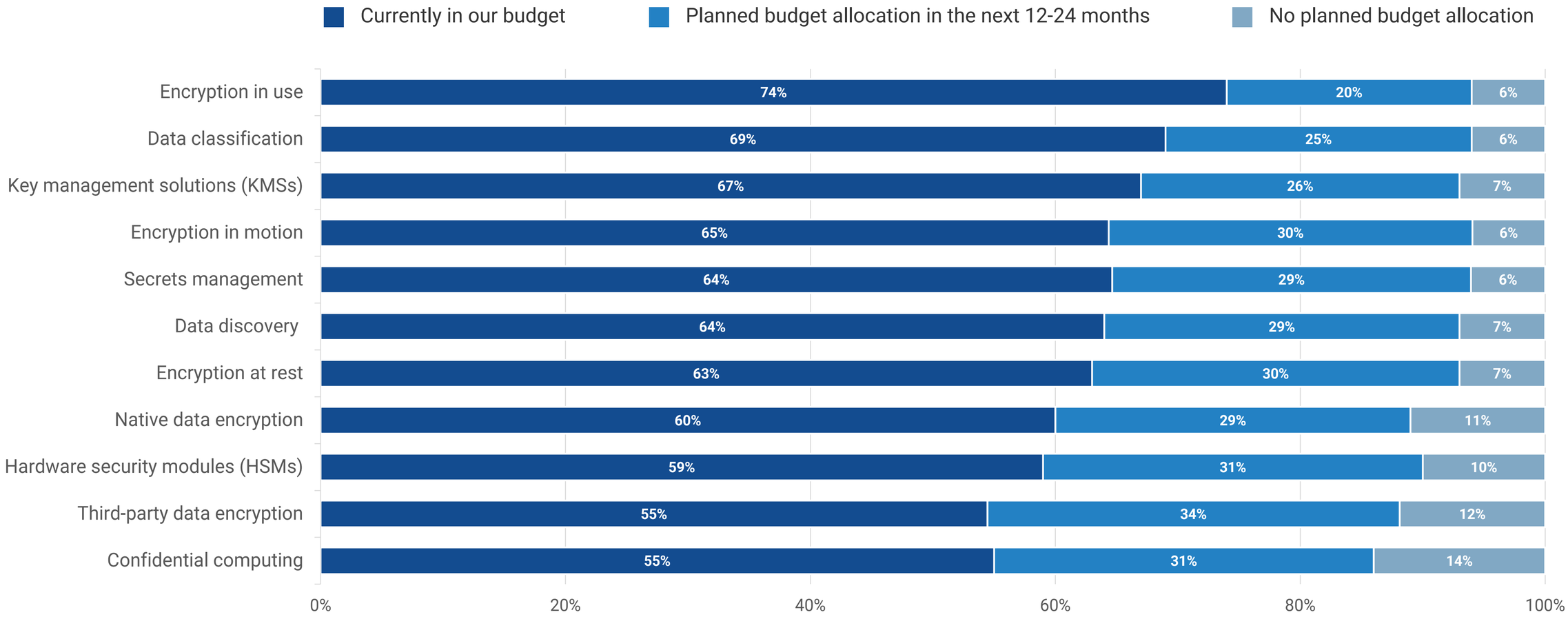
BACK TO CONTENTS

More Spending Is Ahead for Encryption Initiatives

Encryption in Use Is the Most Popular Budget Line Item and Next Activity

Even with encryption of data in use technology being relatively new compared with encryption of data at rest and data in motion, three-quarters of organizations currently budget for encryption in use, and another 20% plan to allocate budget in the next 12-24 months. Other top budget items include data classification and key management solutions.

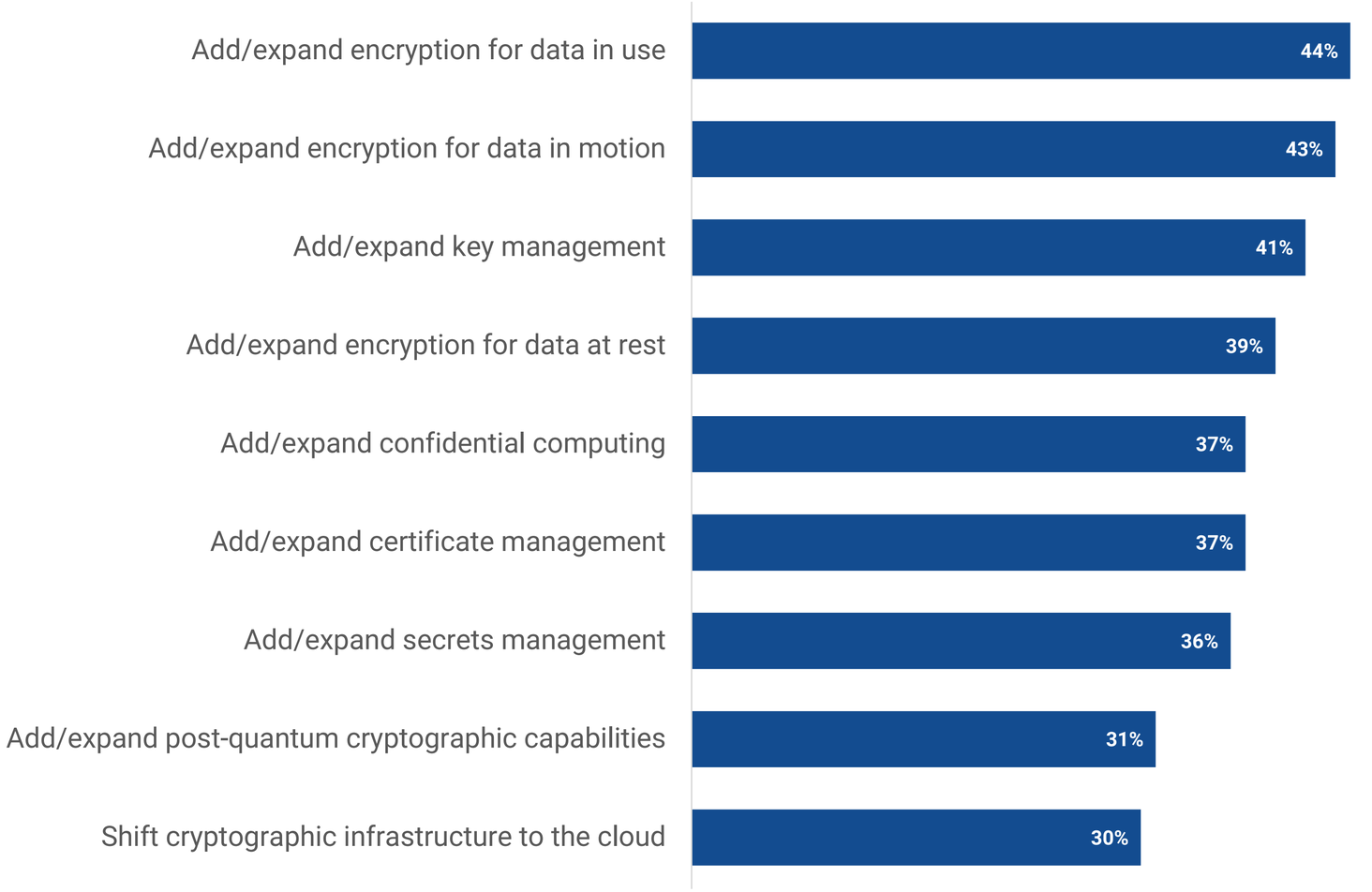
Budget plans for data security controls over the next 12-24 months.



BACK TO CONTENTS

The desire to secure data in use is most likely the result of the expanded use of shared infrastructure services in public and private cloud architectures. With virtual machines or container infrastructures, multiple workloads may be running on the same physical machines, and security teams are concerned that rogue applications may be able to access another workload's data in the physical machine's memory or processors. Thus, adding or expanding encryption for data in use is the most popular encryption activity planned in the next 12-18 months.

Encryption activities planned for the next 12-18 months.



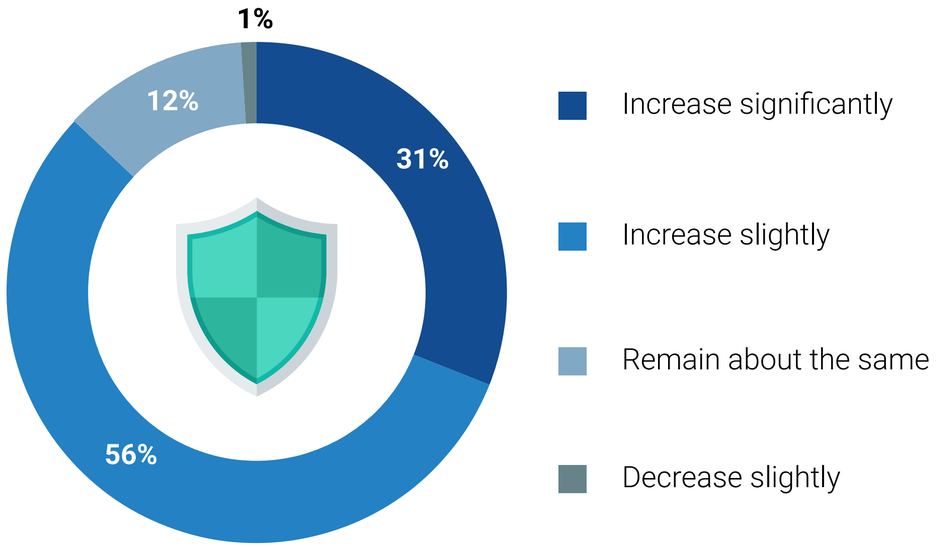
BACK TO CONTENTS

Encryption to Garner Larger Share of Security Budget, Driven by the Need for Simplification

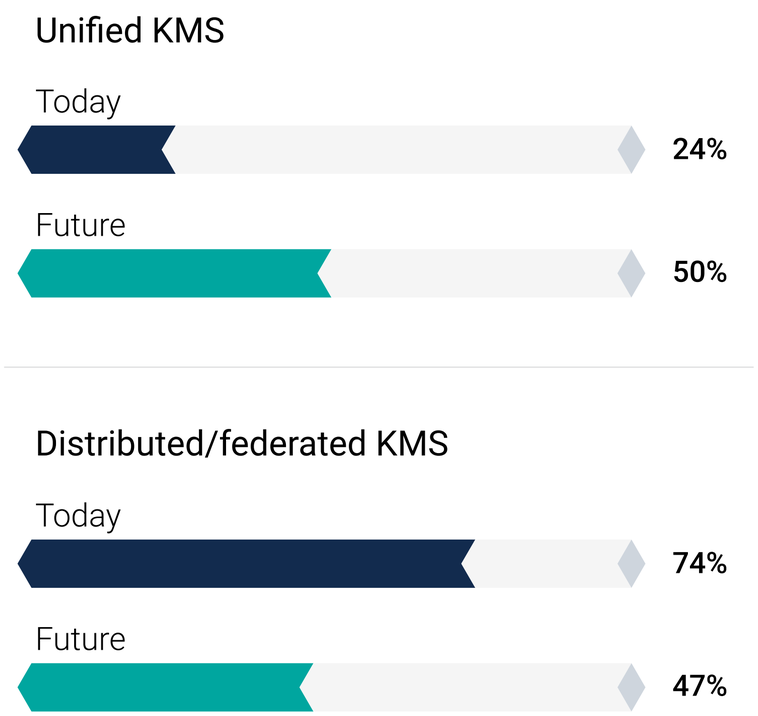
The publicity of data exposure through ransomware data exfiltration and other cybersecurity attacks along with the publicity surrounding the rapid progress in quantum computing have made data and security leaders aware of encryption's role in increasing data security. It's not surprising, then, that 87% of organizations expect to increase their spending on encryption technologies relative to other areas of cybersecurity in the next 12 months, with nearly a third classifying this increase as significant.

Recognizing that encryption, especially migrating to post-quantum cryptography, needs to be uniformly implemented organization-wide for the best security, many organizations are shifting their key management strategies. While three-quarters of organizations employ distributed and federated key management today, the favored strategy for the future is a unified KMS. Thus, 32% of organizations will invest their increased encryption budget into a comprehensive encryption solution.

Encryption technology investment in the next 12 months.



Encryption activities planned for the next 12-18 months.



"32% of organizations will invest their increased budget into a comprehensive encryption solution."

BACK TO CONTENTS

Fortanix®
Look. Know. Further.

Fortanix's data-first approach helps businesses of all sizes to modernize their security solutions on-premises, in the cloud, and everywhere in between. Enterprises worldwide, especially in privacy-sensitive industries like healthcare, fintech, financial services, government, and retail, trust Fortanix for data security, privacy, and compliance. Fortanix investors include Goldman Sachs, Foundation Capital, Intel Capital, In-Q-Tel, Neotribe Ventures, and GiantLeap Capital. Fortanix is headquartered in Santa Clara, CA. Fortanix – Look. Know. Further.

LEARN MORE

ABOUT ENTERPRISE STRATEGY GROUP

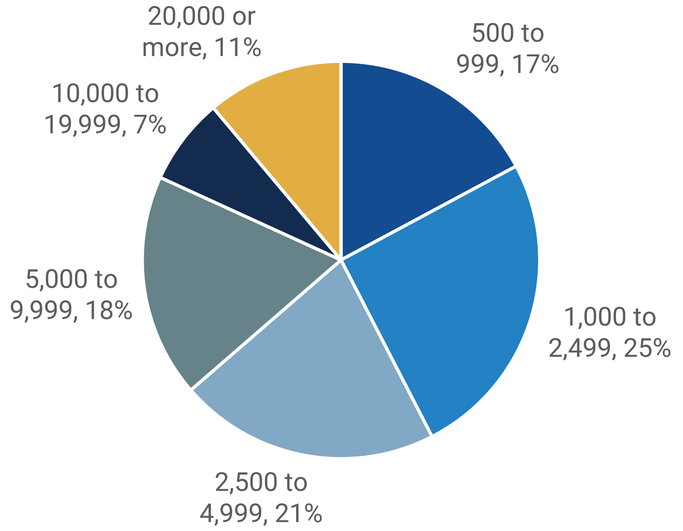
TechTarget's Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

Research Methodology and Demographics

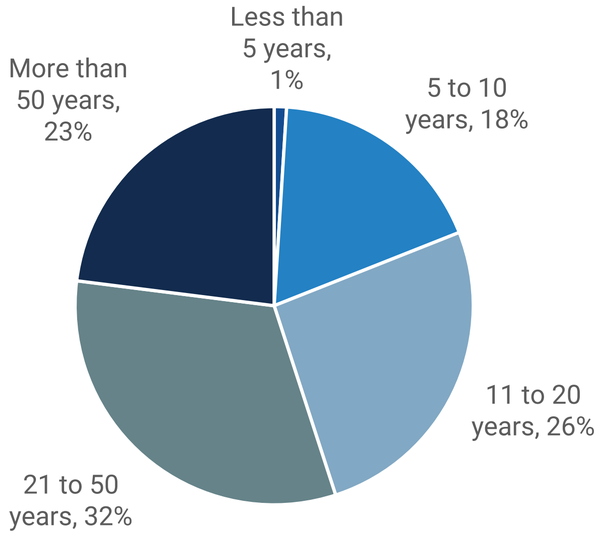
To gather data for this report, TechTarget's Enterprise Strategy Group conducted a comprehensive online survey of IT, compliance, DevOps, and cybersecurity professionals from private- and public-sector organizations in North America between September 26, 2023 and October 11, 2023. To qualify for this survey, respondents were required to be involved with encryption and data security technology and processes. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 387 IT, compliance, DevOps, and cybersecurity professionals.

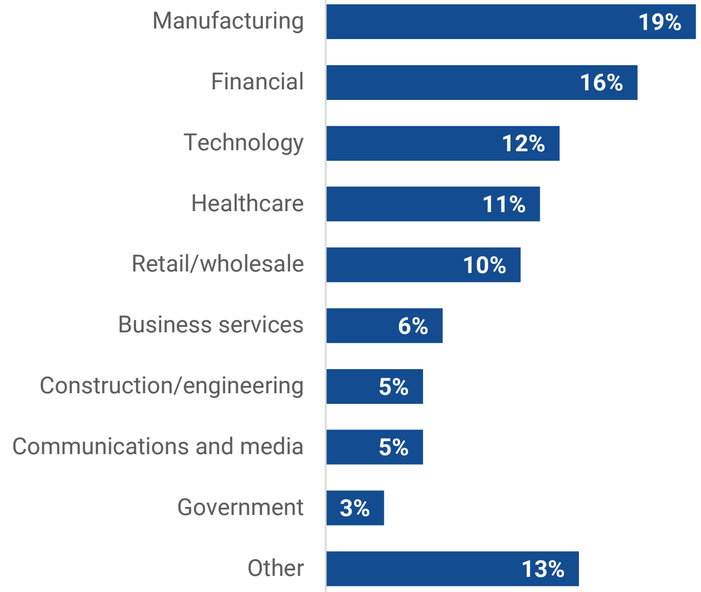
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY AGE OF ORGANIZATION



RESPONDENTS BY INDUSTRY



BACK TO CONTENTS

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.