Osterman Research

White Paper by Osterman Research
Published **March 2025**
Sponsored by **BIO-key International**

CISO and CIO Investment Priorities for Cybersecurity in 2025

Executive summary

CISOs and CIOs are prioritizing cloud infrastructure security, internal cybersecurity talent, and the ethical control of data in 2025. The threat environment continues to change, with AI-driven cyberthreats escalating the potential damages on the offensive side in parallel with tightening cybersecurity insurance requirements forcing a recalibration of the defensive side.

More organizations are experiencing a higher number of cybersecurity incidents each year, which drives the need to re-assess the efficacy of current posture against the organization's desired standard of performance. Having done so, the CISOs and CIOs in this research are investing in protections to shore up the critical areas above. In addition to the overall prioritization of cybersecurity areas, we offer a more nuanced analysis of CISO and CIO priorities within the areas of applications, cloud platforms and services, identities, and data.

KEY TAKEAWAYS

The key takeaways from this research are:

- **Cybersecurity driven by changing threat response calculus**
  Increasing prices for cybersecurity insurance, the growing use of AI in cyberattacks, software supply chain compromise, and return-to-office mandates for employees are the top trends and challenges driving how CISOs and CIOs approach cybersecurity in 2025. All force a reevaluation of how best to address current and emerging threats.

- **Cloud infrastructure security, cybersecurity talent availability, and control and ethical processing of data top the priority stack**
  Out of 24 potential investment areas for cybersecurity, two thirds of organizations assigned the highest priority to cloud infrastructure, internal cybersecurity talent, and compliant data processing. They see weaknesses in their current posture that are misaligned with where they want to be and are investing the resources to do something about it.

- **Budgets continue to rise, showing resilience across economic cycles**
  Almost all organizations have received a higher budget for cybersecurity over the previous two years, and most believe they could put even more budget to productive and effective use.

- **Strong risk management disciplines make a significant difference**
  Organizations with higher efficacy in managing the business risks associated with key cybersecurity areas such as applications, cloud, and identities show much higher commitment to address security weaknesses and are spending accordingly. Being able to see what is and isn't happening drives change.

- **Organizations must do the work to understand their priorities**
  Investment priorities for any given organization must be set within the context of their current posture, real-world threat data, and known areas of concern (and unknown areas of weakness). This is the fundamental work that cybersecurity decision-makers and influencers must coordinate.

CISOs and CIOs are prioritizing cloud infrastructure security, internal cybersecurity talent, and the ethical control of data in 2025.

ABOUT THIS WHITE PAPER

BIO-key International sponsored this white paper. Information about BIO-key International is provided at the end of this paper.

METHODOLOGY

The data presented in this white paper is based on a survey of 268 CISO or CIO respondents at organizations in the United States with more than 1,000 employees. Methodology details and respondent breakdowns are provided on page 33.

WHAT IS AN "INVESTMENT PRIORITY?"

This research presents a deep dive into investment priorities for cybersecurity in 2025. To do so, we analyzed the data collected from the CISO and CIO respondents to our survey in line with two principles:

- **Evidence of alignment essential**
  Merely espousing something as a priority was not enough. Among the survey responses, we looked for alignment with both current posture and intended expenditure before labeling something as a priority. For example, if an investment area was stated as a priority in one question but there was no sense of concern around current shortcomings nor an expressed intent to address the area through financial investment in other questions, we didn't give it the "priority" label.

- **Merely spending more does not make something a priority, just as merely spending less does not necessarily render something not a priority**
  The level of spending required depends on the current state and what is needed. It is the gap between the two which says what investment is required, and in the case where an organization needs to double its expenditure to reach its desired state, doing significantly less than that indicates it is not a priority in any given year.

COMPARISONS WITH OUR 2023 RESEARCH

This is our second biannual research on CISO and CIO investment priorities for cybersecurity. The first was published two years ago in February 2023—see CISO and CIO Investment Priorities for Cybersecurity in 2023. All comparisons to our previous research on this topic are against this 2023 report.

The majority of the data in this current report and our 2023 report provide a look-forward perspective on investment priorities for the coming year. The data from one question in both research cycles—on cybersecurity incident types experienced—profiles experiences from the previous 12 months; it is look-back data. For accuracy, these are referenced as data from calendar year 2022 and calendar year 2024.

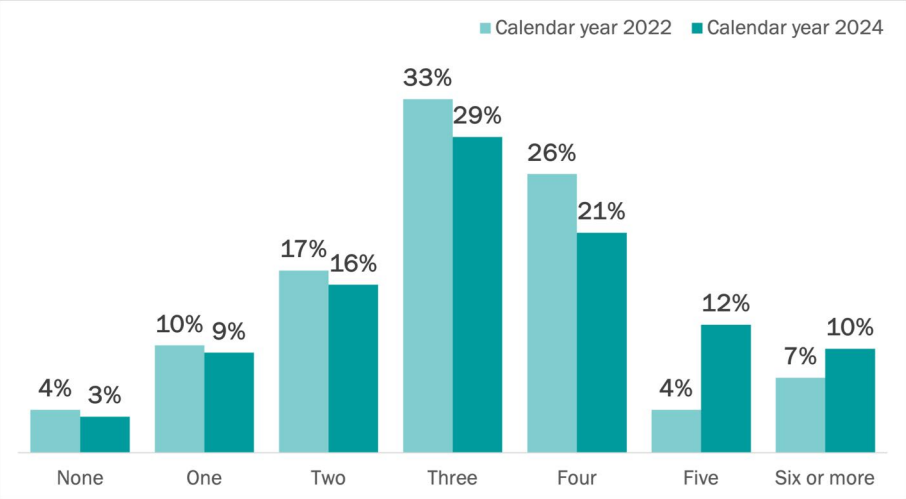
Cybersecurity incident types

Of all potential indicators for assessing the efficacy of current posture, a cybersecurity incident provides the strongest evidence of vulnerability. Incidents are a costly and disruptive signal that current security protections are insufficient. Our research found:

- 72% of organizations experienced three or more types of cybersecurity incidents over the previous 12 months (during calendar year 2024), up slightly from 70% in our 2023 research report (highlighting incidents from calendar year 2022).[1] In both time periods, we asked about the types of incidents experienced, not the number of incidents within each type.
- The shape of the incident type count graph is similar across both time periods, although fewer organizations in our latest research indicated four or fewer incident types. More organizations are experiencing a higher number of incident types; the trend line is moving in the wrong direction.

See Figure 1.

Figure 1
Number of cybersecurity incident types experienced: 2022 and 2024
Percentage of respondents



Source: Osterman Research (2025)

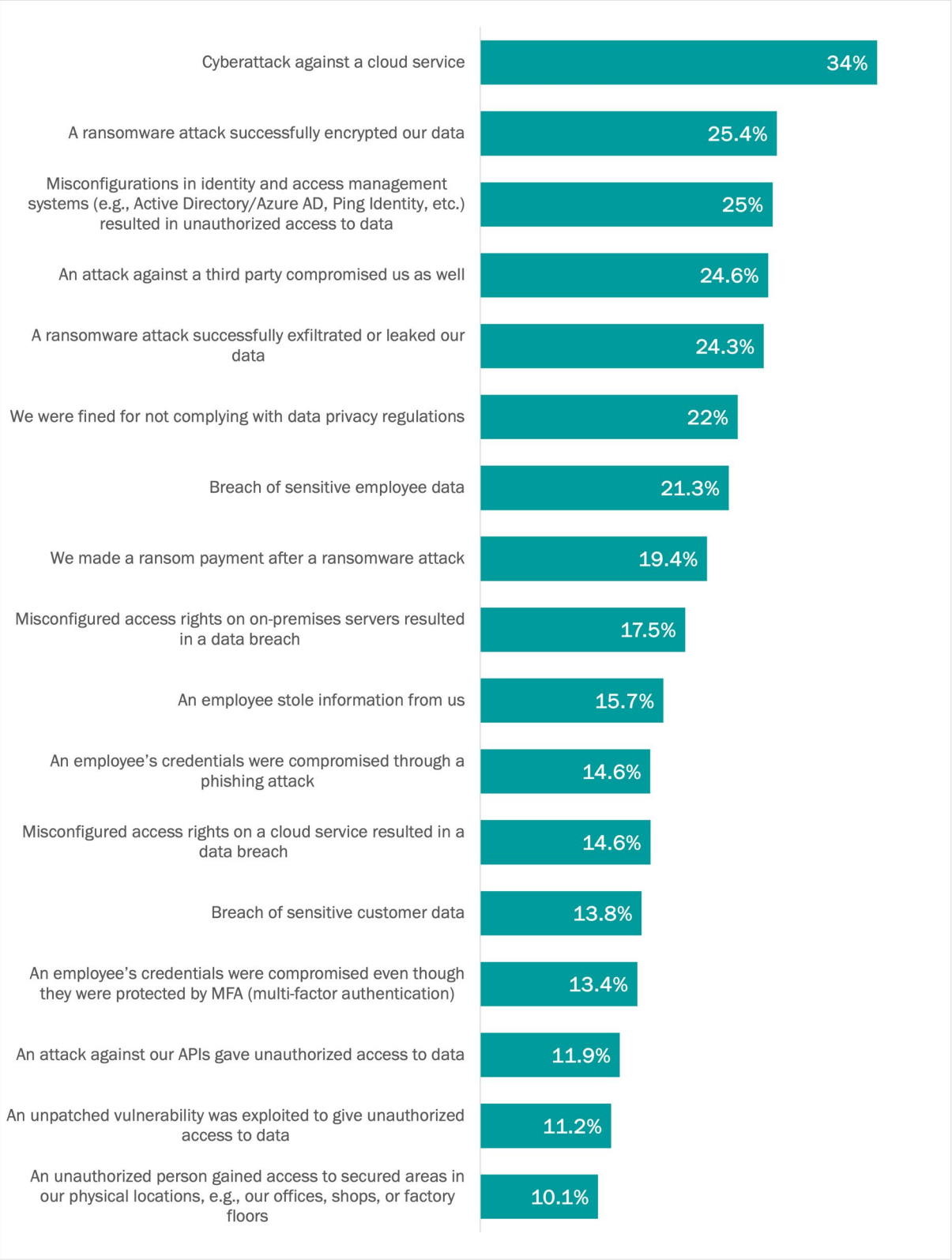
More organizations experienced higher numbers of cybersecurity incident types during calendar year 2024 than in calendar year 2022.

The most frequently occurring types of incidents during the past 12 months were:

- **For one in three organizations**
  Cyberattack against a cloud service.
- **For one in four organizations**
  Ransomware attack that encrypted data, misconfigured identity and access management systems, supply chain attack, and ransomware attack that exfiltrated data.
- **For one in five organizations**
  Fined for not complying with data privacy regulations, breach of sensitive employee data, and making a ransom payment after a ransomware attack.

See Figure 2, which excludes five incident types occurring at less than 7% of organizations, e.g., threat actor bypassing safety features of AI-enabled cyber defenses.

Figure 2
Cybersecurity incident types experienced in 2024
Percentage of respondents



Source: Osterman Research (2025)

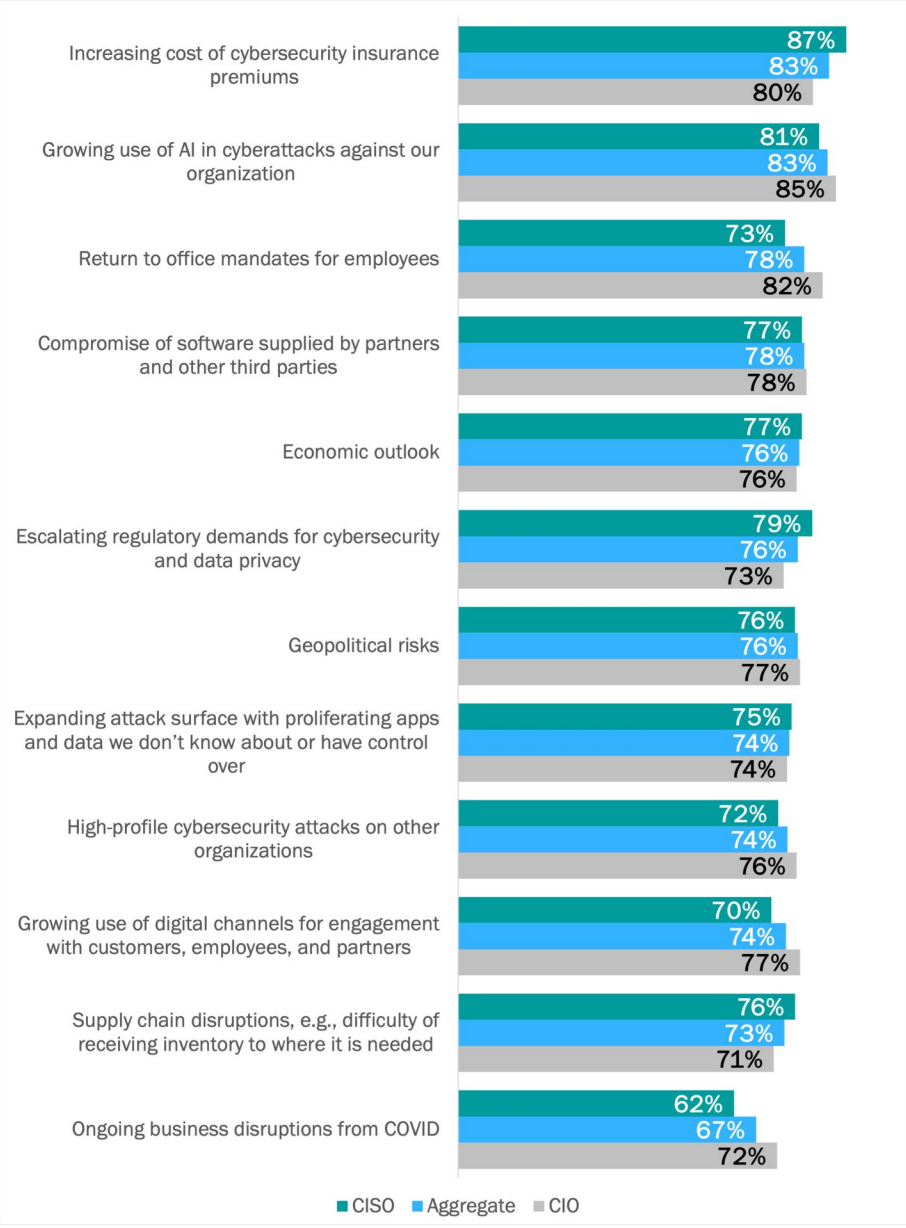
Trends, challenges, priorities

We explore the trends and challenges driving cybersecurity's prioritization in 2025.

TRENDS AND CHALLENGES DRIVING CYBERSECURITY

CISOs and CIOs are closely aligned in how they assess the impact of many trends and challenges on cybersecurity in 2025. Two trends top the list with 83% of all respondents indicating a "very impactful" or "extremely impactful" rating. The increasing cost of cybersecurity insurance premiums is followed closely by the growing use of AI in cyberattacks. See Figure 3.

Figure 3
Trends and challenges impacting how organizations approach cybersecurity
Percentage of respondents indicating "very impactful" or "extremely impactful"



Source: Osterman Research (2025)

Risk coverage for cybersecurity weaknesses and dealing with new AI-enabled cyberattacks are driving the cybersecurity agenda in 2025.

The top four trends and their impact on cybersecurity are:

- **The increasing cost of cybersecurity insurance premiums**
  Higher premium costs and elevated minimum requirements for securing coverage push organizations to rebalance where their cybersecurity budget is spent. Few organizations could now afford to rely on cybersecurity insurance alone, even if that were a possibility. If security protections and resilience are weak, potential insurers are unwilling to extend coverage at affordable rates—if at all. This prices the cost of inaction and low efficacy in stark terms for organizations. More CISOs rated this trend or challenge as highly impactful compared to CIOs, indicating the higher relative responsibility carried for addressing systemic issues. This trend has increased in impact from fourth overall in our 2023 research to first place this year.

- **The growing use of AI in cyberattacks**
  That cybercriminals are already using AI in cyberattacks is widely recognized,[2] but how far that usage will extend is uncharted territory for most. Organizations are already investing in AI-powered cyber defenses to mitigate growing threats. Still, the net effect of escalating offensive threats against an increasingly AI-powered defensive posture has not yet played out sufficiently. CISOs and CIOs rate this challenge almost equally. We did not ask about this challenge in our 2023 research program.

- **Compromise of software supplied by partners and other third parties and return-to-office mandates for employees (tied for third)**
  Two trends or challenges tied for third place overall. CISOs and CIOs ranked one equally: the compromise of software supplied by partners and other third parties. During 2024, the CrowdStrike incident bore witness to the devastating consequences of trusted partners getting something wrong. The other trend tied for third place is return-to-office mandates for employees, which CIOs view as more highly impactful than CISOs.

That cybercriminals are already using AI in cyberattacks is widely recognized, but how far that usage will extend is uncharted territory for most.

CISOs and CIOs provided almost equal ratings for half of the trends. Among the other half, the most significant differences were for:

- Ongoing business disruption from COVID, which CIOs rated 10% higher than CISOs (72% versus 62%).

- Return-to-office mandates for employees, with a 9% higher rating by CIOs than CISOs (82% versus 73%).

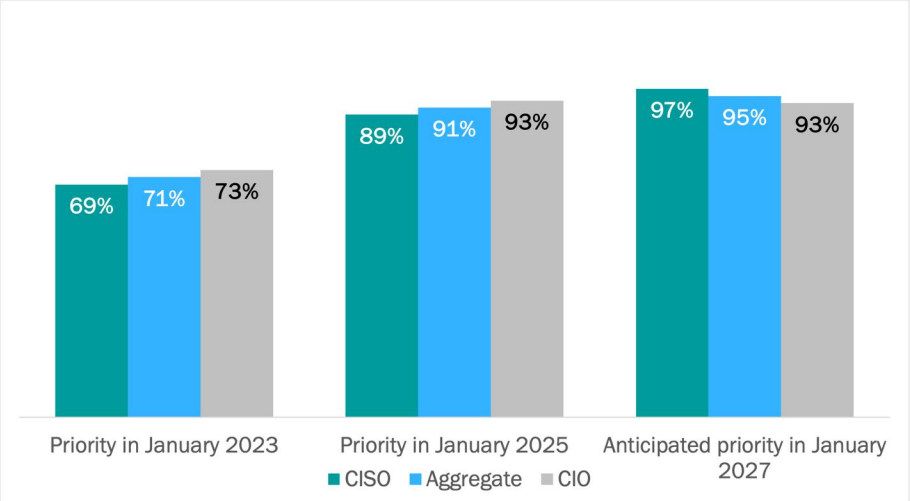
- Increasing cost of cybersecurity insurance premiums, with a 7% higher rating among CISOs (as discussed above).

These variations may reflect enduring role-specific differences between CISOs and CIOs or signal areas where each can better assist the other. For example, a CISO could initiate a conversation with the CIO to see if there are cybersecurity aspects to ongoing COVID disruptions and return-to-office mandates that the CISO is systematically under-addressing. Likewise, if there are aspects of DevOps where security considerations are under-addressed that negatively impact cyber insurance requirements for the CISO, a conversation with the CIO would be prudent.

PRIORITIZING CYBERSECURITY ISSUES HAS BECOME ESSENTIAL

Given the continued rise of cyberthreats, the growing menace of AI-enabled cyberattacks, the devastating consequences of triple-threat ransomware attacks, and massive data breaches that resulted in the victim organization filing for bankruptcy (e.g., National Public Data), it would take a brave CISO or CIO to dismiss the importance of cybersecurity to their organization's success. The data from this research shows this is not happening. Addressing cybersecurity issues is already a high or extreme priority at more than nine out of ten organizations, with continued growth in priority anticipated over the next two years. See Figure 4.

Figure 4
Assessing the priority of cybersecurity issues to organizations
Percentage of respondents indicating "high priority" or "extreme priority"



Source: Osterman Research (2025)

Organizations place high and intensifying priority on addressing cybersecurity issues.

In looking at the data:

- **The composition of priority is shifting dramatically**
  More CISOs and CIOs ranked priority as "high" in January 2023 rather than "extreme." For both respondent groups, however, this switched for the January 2025 and 2027 rankings, with more indicating "extreme priority." Among CISOs, almost two thirds said "high" for 2023 but "extreme" for 2027.
- **The level of priority rose more than anticipated two years ago**
  Our previous research assessing cybersecurity investment priorities saw CISOs and CIOs forecasting only a marginal uplift in cybersecurity priority within their organizations over the subsequent two years, from an average of 77% indicating the two highest importance rankings to 81%. We wrote at the time that "*neither CISOs nor CIOs are currently able to perceive that cybersecurity could still become significantly more important than it is today*." In retrospect, another conclusion would have been better: that neither CISOs nor CIOs could perceive that *the attention paid to cybersecurity issues* within their organization could be significantly higher. On the tail of SolarWinds, multiple global Exchange Server incidents, and the shock of crippling ransomware attacks against critical infrastructure organizations, many assessed their organizations as nearing maximum attentional capacity two years ago.

Assessing investment priorities against cybersecurity posture

In this section, we analyze respondents' assessment of their cybersecurity posture in 24 areas and the investment required to improve posture.

METHODOLOGY

We asked respondents to provide an assessment of their current cybersecurity posture in 24 areas. For each area, we asked three numerical rating questions:

1. **Level of concern about current posture**
   The level of concern with the current cybersecurity posture of a given area at their organization, e.g., security of endpoints. Each respondent was asked to answer the question based on how their organization approached each area—that is, against their own internal framework, standard, or baseline. The question did not seek any assessment against an external framework or imposed baseline. Respondents had to balance their assessment of current strengths, weaknesses, opportunities, and threats for each of the 24 areas.
2. **Level of investment required to meet the organization's standard or desired level of posture**
   The level of investment required to raise the cybersecurity posture of a given area to the internal standard or framework set by their organization. This question was phrased as an internal rating rather than seeking alignment with any universal standard, external framework, or imposed baseline. Hence, in conjunction with the first question, respondents defined investment required against their own internal assessment of the current and desired state.
3. **Level of priority in 2025 of investing in each area**
   The level of priority within the organization for improving the cybersecurity posture of a given area in 2025.

See Figure 5.

Determining investment priorities requires assessing the gap between current and desired posture.

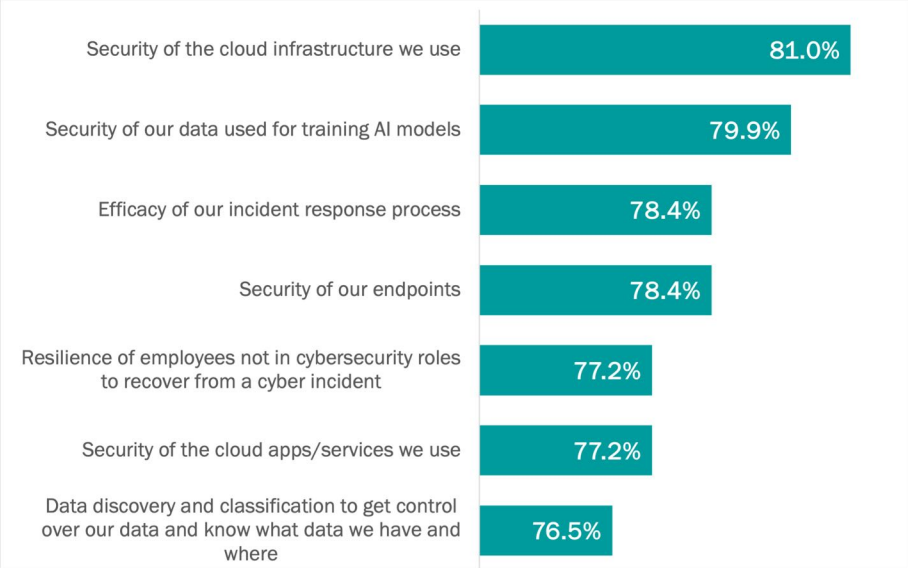
Figure 5
Methodology for assessing overall cybersecurity priorities

Source: Osterman Research (2025)

TOP SEVEN PRIORITIES

Cloud infrastructure security, AI model training data security, incident response efficacy, and endpoint security lead the list of cybersecurity investment priorities for organizations in 2025 in this research. See Figure 6.

Figure 6
Cybersecurity posture investment priorities in 2025: Top seven
Percentage of respondents indicating "high priority" or "extreme priority"



Source: Osterman Research (2025)

Many of the top seven priorities align with the data we have explored above on incident types with higher annual incidence rates and trends and challenges driving cybersecurity in 2025. See Figure 7.

Figure 7
Aligning priorities, incidents, and trends/challenges

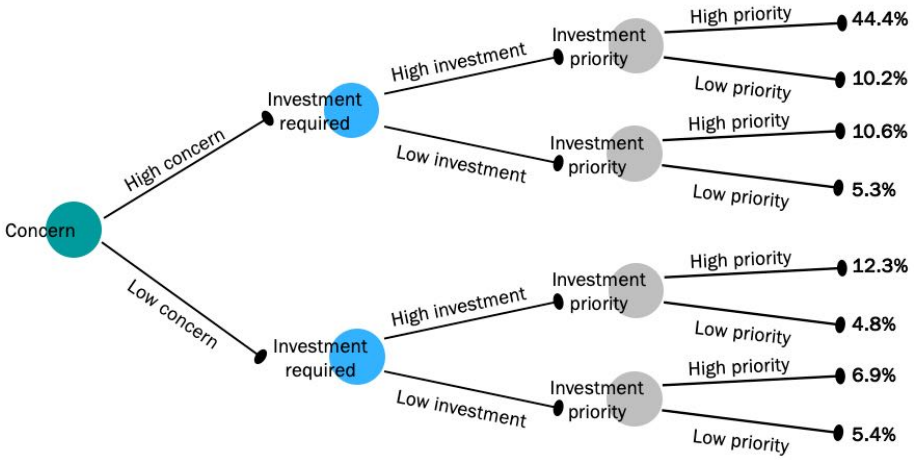
Priority (Figure 6)	Incidents (Figure 2) (% annual incidence rate)	Trends and challenges (Figure 3) (% impactful)
Cloud infrastructure security (#1) Cloud apps/services security (#6)	Cloud service cyberattacks (#1, 34%) Data breach due to misconfigured access rights on a cloud service (#12, 15%)	
Security of data used for training AI model (#2)		Growing use of AI in cyberattacks against our organization (#2, 83%)
Efficacy of incident response processes (tied for #3) Employee resilience to recover from a cyber incident (#5)	97% of respondents experienced one or more incident types in 2024 (see Figure 1)	
Endpoint security (tied for #3)	Successful MFA bypass attacks (#14, 13%)	Return-to-office mandates (#4, 78%)
Data discovery and classification (#7)	Ransomware attack exfiltrated data (#5, 24%) Sensitive employee data breached (#7, 21%) Sensitive customer data breached (#13, 14%)	Expanding attack surface with unknown or uncontrolled data (#8, 74%)

Source: Osterman Research (2025)

CORRELATING CONCERN, INVESTMENT LEVELS, AND PRIORITY IN 2025

The data in Figure 6 above presents the raw data for investment priorities in 2025. To analyze investment intent more deeply, we correlated the answers to the three questions assessing concern, required investment, and investment priority. We divided the responses to the three questions into two groups each, creating eight combinations. See Figure 8.

Figure 8
Correlating concern, investment required, and investment priority in 2025
Percentage of respondents



Source: Osterman Research (2025)

Respondents evidence four primary patterns. See Figure 9.

Figure 9
Dominant patterns of investment priorities correlated with concern and expected investment to mitigate

Pattern	Name	Explanation	Example
High concern High investment High priority	High-High-High **44.4%**	Where high concern over current posture and high required investment spending coalesces for high priority in 2025. This pattern was expected to dominate.	Security of cloud infrastructure (57%)
Low concern High investment High priority	Low-High-High **12.3%**	Signals areas subject to uncertainty, chaotic possibilities, or imposed external conditions that override preferred internal risk assessments. For example, where investment to stop data exfiltration is prioritized due to negative consequences in the case of a breach despite low concern about current posture.	Availability of cybersecurity talent for internal roles (16%) Preventing data exfiltration (15%)
High concern Low investment High priority	High-Low-High **10.6%**	Areas prioritized since high concerns (perceived weaknesses) can be mitigated with low relative investment expenditure.	Incident response efficacy (14%) Employee preparedness (14%)
High concern High investment Low priority	High-High-Low **10.2%**	Areas not prioritized in favor of focusing on other areas. Can signal high market volatility in the efficacy of possible mitigations (e.g., immature solutions with a high rate of change between vendors).	Security of applications developed internally (15%) Gen AI data security (15%)

Source: Osterman Research (2025)

Figure 10
Assessing cybersecurity posture: Correlating concern, investment, and priorities in 2025
Percentage of respondents (sorted by the sum of the Low-High-High and High-High-High patterns)

Source: Osterman Research (2025)

Comparing the raw prioritization of the Top 7 in Figure 6 with the correlated analysis in Figure 10 leaves several priorities unchanged but others moderately to dramatically different. Key changes are:

- **Prioritization remains unchanged for both cloud areas**
  Security of cloud infrastructure ranks first in both lists, and security of cloud apps/services ranks sixth in both lists. These are the only two items that remain unchanged in relative rank ordering between the lists.

- **Three priorities fell off the Top 7 list based on correlated ratings**
  Security of data used for training AI models drops from second in the Top 7 to eighth in the correlated list, and post-incident recovery resilience of employees not in cybersecurity roles drops from fifth in the Top 7 to ninth. The most dramatic change is for the efficacy of the incident response process, which dives from third in the Top 7 to 16th. For each of these, while the priority is asserted, we don't see the flow-through from current concern around posture nor intended budgetary adjustments. For some organizations, the reason could be that knowing what to do to address weaker areas is unclear. For example, securing data used for training AI models is still an emerging area with a lot of uncertainty around which products work best. Market education, product maturity, and ranking vendors takes time to get right, but once there, investment decisions and associated budgetary implications are easier.

- **Three priorities join the correlated ratings list that aren't on the Top 7**
  Three areas that didn't make the Top 7 are highly rated on the correlated list. Availability of cybersecurity talent for internal roles is in second place, and level of control and ethical processing of data in third. Network security also joins the correlated list, in seventh place.

- **Data discovery and classification becomes more important**
  The ability to discover and classify data moves from seventh place in the Top 7 to fourth in the correlated list. It sits directly after a related area—the level of control and ethical processing of data (in third place, as above). It has become essential for organizations to be able to discover and classify data in response to a changing regulatory environment where greater differentiation of data types is required.

Cloud security, finding good cybersecurity talent, and understanding data risks rank at the top of the priority list for cybersecurity investments in 2025.

DISCUSSION

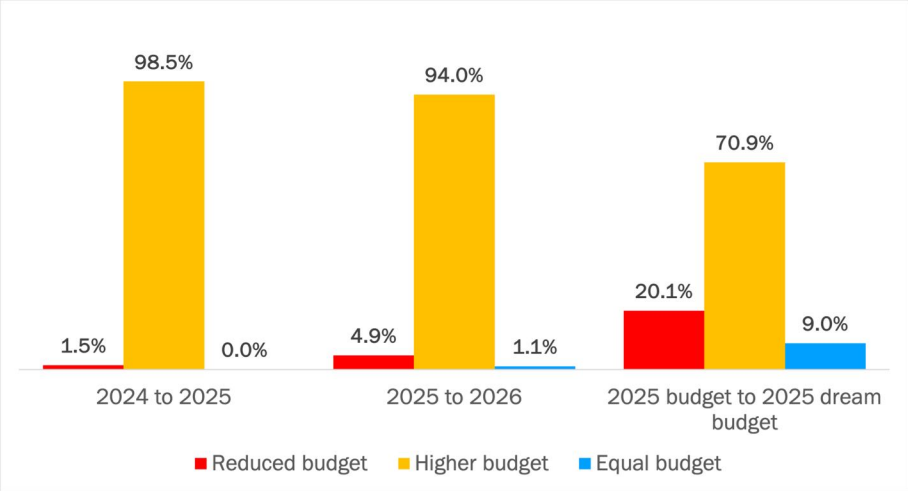
Some priorities are quickly espoused. Others become clearer only when contextual reasoning and intended consequential actions align. This research shows the enduring importance of strengthening cloud security (for infrastructure primarily, and apps/services secondarily), having the right people in cybersecurity roles, and upleveling various aspects of data security. These are the major themes and priorities for 2025.

Having the right people in cybersecurity roles is necessary but insufficient in the ongoing fight against cybersecurity threats. Organizations cannot solely hire their way to success, because there aren't enough people or resources available to do so. Having the right tools, technologies, mitigations, and protections available to deflect attacks, provide early warning signals, and enable resilient recovery are equally essential. The two go together.

Budget outlook

The predominant pattern is higher budgets year on year, with the greatest frequency of increase for the 2024 to 2025 years (at 98.5% of organizations). The percentage of respondents expecting a higher budget in 2026 compared to 2025 is slightly lower, although still very high. See Figure 11.

Figure 11
Year-on-year budget changes for cybersecurity
Percentage of respondents



Source: Osterman Research (2025)

The most surprising budget finding is that when asked about their dream or ideal budget for 2025—assuming every dollar could be put to productive and effective use—only 70.9% wanted a higher budget. In other words, almost 30% wanted the same or less, and the data says those wanting less were twice the amount of those wanting the same. By comparison, in our 2023 research, the percentage wanting a higher dream budget was the highest of the three data sets. Speculatively, this could represent financial fatigue at the relentless growth in cybersecurity budgets, a preference for shifting to platform offerings that combine multiple point solutions at a lower overall net cost, or an acknowledgement—at least among some organizations—that they hit maximum absorption capacity for new cybersecurity solutions for the time being. We will need another cycle of research data to determine if this is a trend or a blip in normal operations.

Cybersecurity budgets remain resilient, with almost all organizations reporting continued year-on-year growth.

Four areas of focus for 2025

In the following sections, we investigate investment priorities for CISOs and CIOs in four focus areas. This section talks methodology for that analysis.

DIGGING DEEPER

Complementary to the assessment of overall posture, required investment, and investment priority in 2025 in the opening sections above, we asked respondents to provide deeper insight into their security posture and investment priorities in four specific areas. These were chosen for their importance to cybersecurity in 2025. The four areas are applications, cloud platforms and services, identities, and data.

METHODOLOGY

For each of the four areas, we asked respondents to provide a rating across three related questions:

- **Efficacy at managing the associated business risks**
  For each topic or issue in the focus area, we asked for a rating of how well the organization is currently managing the associated business risks. The "business risks" as such were not defined, leaving it up to each respondent to answer in terms of the visibility and optics into the business risks seen at their organization. Respondents answered on a five-point scale: poor, fair, good, very good, and excellent.
- **Priority of security in 2025**
  For each topic or issue, we asked for a rating of how the organization is prioritizing security in 2025. Respondents answered on a five-point scale: not a priority, low, medium, high, and extreme.
- **Budget change in 2025 compared to 2024**
  For each of the topics or issues within the focus area, we asked for a rating of how the budget allocated to the topic is changing in 2025 compared to 2024. Respondents answered on a seven-point scale, ranging from a budget decrease of 20% or more to a budget increase of 20% or more.

In the subsequent four sections, we present the following analysis for each area:

- **Overall risk management posture, priorities, and budget change**
  Across all organizations and on average, what is the overall level of risk management efficacy, security priority, and budget change in 2025? These answers present an overall picture of the data without correlating the answers for each respondent.
- **Correlating risk management posture with priorities and budget change**
  The current assessment of risk management efficacy is used to split the data on priorities and budget change in 2025. Correlating the answers in this way provides a different view of the data than the overall one. A near-universal finding across the four focus areas is that organizations with higher risk management efficacy place higher priority on security in 2025 and are allocating a greater budget increase as well. By implication, organizations with a lower rating of risk management efficacy manifest lower priority and a lower intent to invest in improvements in 2025.

A discussion on each area follows the quantitative analysis.

Organizations with higher risk management efficacy place higher priority on security in 2025 and allocate a greater budget increase.

Applications

Focusing on API security is essential due to the specific vulnerabilities they pose and the serious repercussions of API breaches, such as data loss and financial harm

TOPICS FOR APPLICATIONS

We investigated six topics in the applications focus area:

- Assessing security vulnerabilities when introducing new applications.
- Ensuring data is kept safe when migrating away from legacy or unused applications.
- Developing APIs without introducing new security risks.
- Discovering APIs as they are developed.
- Managing API security posture across our organization.
- Preventing data from leaking from an application to other applications with reduced security.

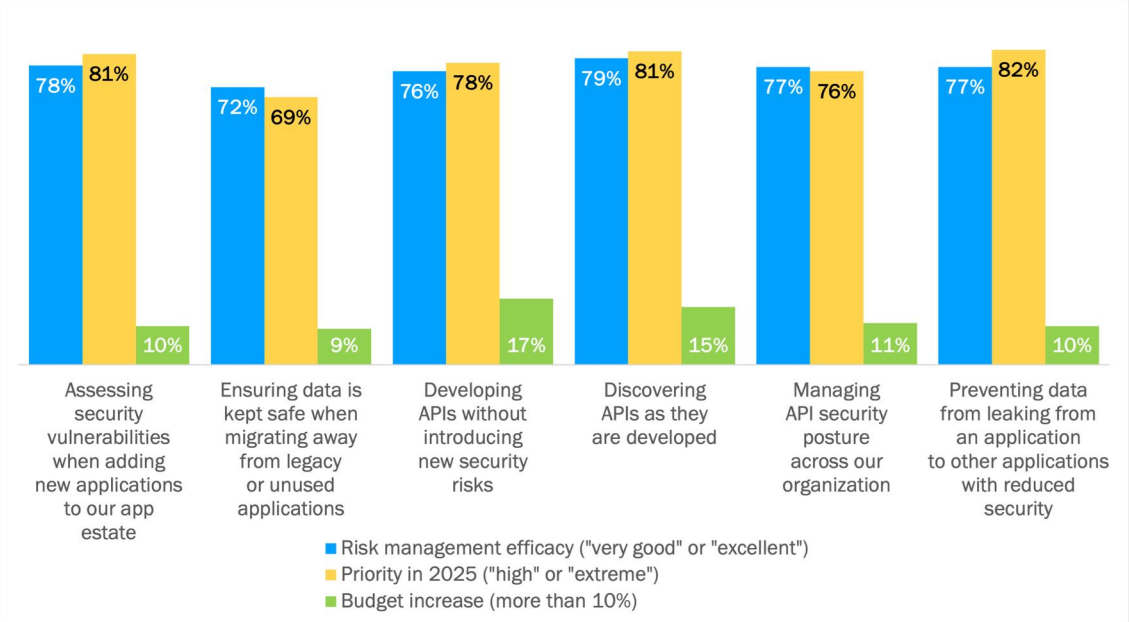
OVERALL PRIORITIES IN 2025

In looking at the rankings given to the six issues (see Figure 12):

- Risk management efficacy is evenly distributed across the six issues, with only a net variation of 10%. Highest efficacy is for discovering APIs as they are created. Lowest is ensuring data is kept safe when migrating away from legacy or unused applications.
- Spending priority is highest for preventing data leakage, discovering APIs as they are created, and assessing security vulnerabilities when new applications are introduced. The second and third of these issues are about promptly detecting changing conditions in the design and functioning of applications.
- Two of the API-related issues have the highest anticipated budget increase: developing APIs (17% of respondents expected a budget increase of more than 10%) and discovering APIs as they are created (15%).

Common API vulnerabilities like broken authentication, excessive data exposure, and security misconfiguration can be targeted by attackers seeking unauthorized access to confidential data and systems.

Figure 12
Overall investment priorities in 2025: Applications
Percentage of respondents



Source: Osterman Research (2025)

CORRELATING RISK POSTURE WITH PRIORITIES AND BUDGET CHANGE

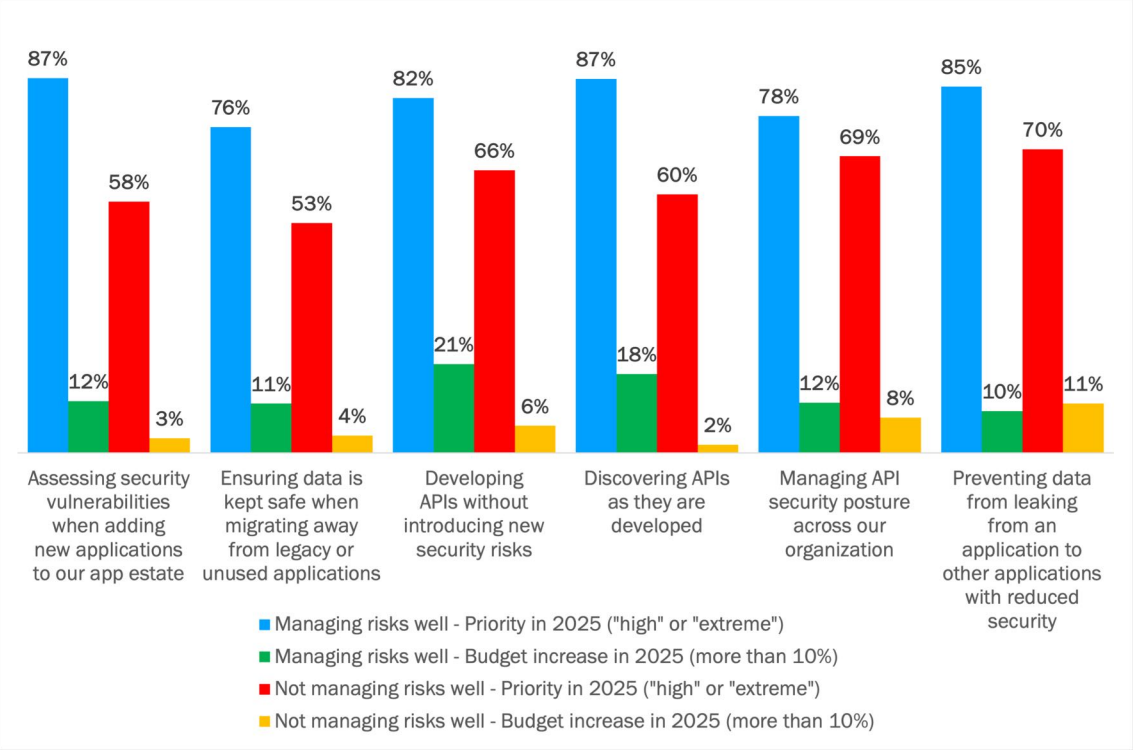
There is a dramatic difference in investment priorities and anticipated budget increases between organizations that are and are not appropriately managing the business risks of each issue. Organizations that are managing the business risks well place higher priority on each issue in 2025. They have also allocated a larger budget increase in all but one situation—preventing data from leaking from an application to other applications with reduced security.

The data in this research positions two of the three API issues as high priority in 2025 and with the largest anticipated budget increases out of the six issues. APIs are critical to modern application design and functioning. Being able to securely develop and discover APIs as they are developed are ranked more highly than managing API security posture as such. API security posture can be managed to some extent by strengthening the guardrails for the other two issues, and hence the relative ratings make sense to some degree. But it is vital to understand that API security posture governance extends beyond just reducing risks during development. Continuous monitoring and safeguarding of APIs in production are key to identifying and addressing threats as they arise. This encompasses the integration of runtime protection, mechanisms for threat detection, and automated response capabilities to maintain continuous API security. Organizations would be shortsighted to ignore API security posture entirely, but the data in this research doesn't support that conclusion. API security posture attracts a somewhat lower prioritization, not outright abandonment.

Continuous monitoring and safeguarding of APIs in production are key to identifying and addressing threats as they arise.

See Figure 13.

Figure 13
Correlating risk management efficacy with investment priorities and budget: Applications
Percentage of respondents



Source: Osterman Research (2025)

Only 29% of respondents say their organization is "very good" or "excellent" at managing the business risks for all six application-related issues we asked about. The majority (71%) have differing levels of risk management efficacy across the six issues.

DISCUSSION ON INVESTMENT PRIORITIES FOR APPLICATIONS IN 2025

Under both ways we examined the data, the organizations in this research place high priority on the ability to promptly detect changing conditions in the design and functioning of applications. This means the ability to assess vulnerabilities when net new applications are introduced to the organization, and to minimize security risks when application design constructs—such as APIs—are created or updated. This includes the ability to identify and secure hidden or unmanaged APIs ("shadow APIs"), which represent a significant security risk to organizations.

With new AI coding assistants being increasingly used across DevOps teams, the velocity of developing new APIs and code is dramatically increased. By implication, so too is the risk of introducing vulnerabilities that bypass access controls, give access to commercially sensitive process logic, and allow unauthorized access to data for breach and extortion attacks. AI coding assistants can only generate APIs and other code based on underlying training data, and any prominence of security weaknesses in training data gets perpetuated in future development cycles.

The risks and threats against APIs are reflected in the OWASP API Security Top 10 list for 2023,[3] which identifies prevalent API vulnerabilities like broken authentication, excessive data exposure, and security misconfiguration. These weaknesses can be targeted by attackers seeking unauthorized access to confidential data and systems. Focusing on API security is essential due to the specific vulnerabilities they pose and the serious repercussions of API breaches, such as data loss and financial harm.

Focusing on API security is essential due to the specific vulnerabilities they pose and the serious repercussions of API breaches, such as data loss and financial harm.

AI-driven API security solutions offer organizations a way to level up their API security posture. AI-driven solutions can analyze API traffic, identify anomalies, and detect threats in real-time, providing crucial defense against advanced attacks. Integrating AI into API security helps organizations manage the complexity of modern development and protect its vital assets.

Migration of data away from legacy or unused applications ranked in last place for efficacy at managing the associated business risks well. It also had the second to lowest budget increase across the collection of topics we investigated. One possibility is that organizations have largely completed their digital transformation efforts and legacy applications are a minor issue, and therefore it is of lower relative priority. Another possibility is that organizations are blind to what's happening with legacy and unused applications and the data stored inside, creating an exposed and uncontrolled vector for data breach. It would be good for organizations to double-check if unsure.

Cloud platforms and services

Cyberattacks against a cloud service were the most common incident type respondents experienced. Organizations with good risk management capabilities are all in on dealing with everything that needs to be strengthened to make the cloud as secure as possible.

TOPICS FOR CLOUD PLATFORMS AND SERVICES

Cloud incidents and the prioritization of cloud security feature prominently in this research. In taking a deeper look at the cloud, we asked respondents about six topics:

- The use of shared passwords when accessing cloud platforms and services.
- Managing configuration of access rights on cloud platforms and services to prevent unauthorized access to data, including the difference between up-to-date access rights and MFA protections.
- Addressing inconsistencies between security capabilities (and hence diverging security policies) when using multiple cloud platforms to host applications.
- Finding appropriately trained cybersecurity talent to protect cloud platforms and services.
- Implementing data-centric security to protect sensitive data in use for secure data portability and sharing across multiple cloud platforms.

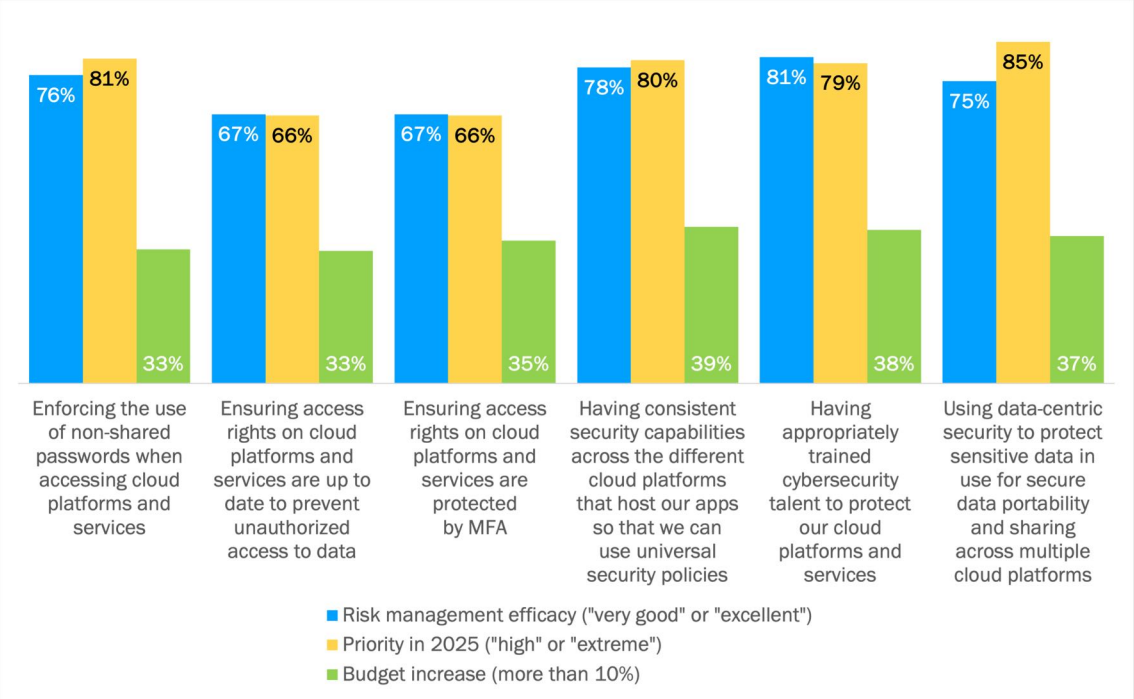
OVERALL PRIORITIES IN 2025: CLOUD PLATFORMS AND SERVICES

In looking at the rankings across the six issues (see Figure 14):

- Risk management efficacy is lowest for the two issues related to access rights—having them up to date and protecting access with MFA. Access rights are a fundamental control and weakness in this area is highly concerning.
- Spending priority is highest for data-centric security. This is unsurprising given the frequency of data breaches affecting cloud platforms and services.
- The budget numbers are essentially the same (ranges 33% to 39%).

The general intent across all organizations is to spend more on all aspects of cloud security in 2025.

Figure 14
Overall investment priorities in 2025: Cloud platforms and services
Percentage of respondents



Source: Osterman Research (2025)

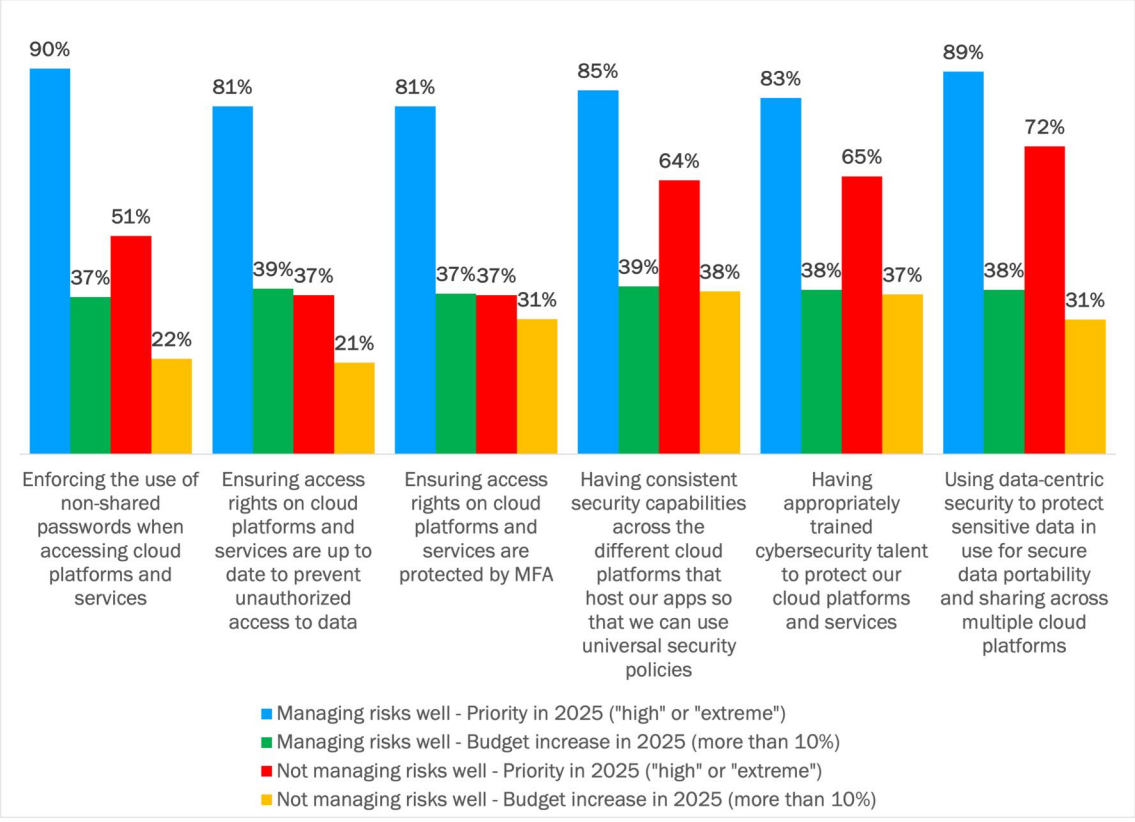
CORRELATING RISK POSTURE WITH PRIORITIES AND BUDGET CHANGE: CLOUD PLATFORMS AND SERVICES

When splitting the data on cloud investment priorities and budget increases based on risk management efficacy, the anticipated variation in priorities remains. In all cases, those managing risks well place a higher priority on all six issues (average 85% versus 54%). For anticipated budget increases across the six issues, however, current efficacy drives less of a differentiation (average 38% versus 30%). In other words, irrespective of how well organizations are currently managing the risks of cloud platforms and services, the general intent is to increase budget in 2025 for all the issues we asked about. See Figure 15.

Among organizations who are currently managing risks well, there is little variation in the priority given to the six issues, and little variation in budget allocations, too. They are all in—dealing with everything that needs to be strengthened to make the cloud as secure as possible. By contrast, among those not currently managing risks well, there's a greater degree of variation in priorities. Highest priorities are data-centric security (72%), cloud talent (65%), and consistent security policies (64%). Lower priorities are identity and access. For this group, choosing the best cloud platforms available and having the talent to run it is essential, but without the operationalization of security through strong identity and access, much is lost.

Without the operationalization of cloud security through strong identity and access, much is lost.

Figure 15
Correlating risk management efficacy with investment priorities and budget: Cloud platforms and services
Percentage of respondents



Source: Osterman Research (2025)

Only 29% of respondents say their organization is "very good" or "excellent" at managing the business risks for all the issues related to cloud platforms and services. The majority (71%) have differing levels of risk management efficacy.

DISCUSSION ON INVESTMENT PRIORITIES FOR CLOUD PLATFORMS AND SERVICES IN 2025

Cloud represents a significant strategic bet for most organizations, and by implication, security needs to be as well. With cyberattacks against a cloud service the most common incident type experienced by the organizations in this research—affecting one out of three organizations during the past 12 months—and with other incident types giving access to sensitive data for failings including misconfigured access rights, organizations know they must do better.

The difference in rankings given to data-centric security and access rights in the overall analysis (see Figure 14) feels backward. Why is a comparatively higher priority put on securing data in the cloud for secure data portability (85%) versus stopping unauthorized access to the cloud and its data (66%)? Isn't that just like leaving the front door open? The correlated analysis in Figure 15 provides a potential answer: there's a significant difference in access rights as a priority among those that are managing risks well versus those not doing so. For this group, priorities must be re-evaluated. It is insufficient to merely have the best cloud platforms and talent available; matters pertaining to identity and access control are fundamental.

Having the right talent available is rated as a high priority, but the details matter in what that talent is then tasked with. Repetitive tasks should be the domain of automated cloud security systems for operational efficiency, not cybersecurity talent. Automation allows for consistent application of defined controls and real-time re-alignment of configuration drift against established policies. Trying to maintain this with human talent alone is a losing proposition.

The majority of respondents (71%) were not consistently good at managing the business risks for all six issues related to cloud platforms and services. If some of the issues we asked about are unimportant to a particular organization, then such variation is appropriate. However, if the issues are all important, it would be good to see investment in developing more consistent risk management practices across the six. That should be a priority for organizations in itself.

Data-centric security managed independently of the cloud provider ensures secure data portability and secure data sharing irrespective of the cloud in use. Moving data from one cloud environment to another does not require the removal of protection when independent security capabilities are used, unlike when cloud-specific protections are embraced. As organizations embrace a multi-cloud posture for resilience and business advantage, re-evaluating how to achieve cloud-independent data security and policy adherence becomes a more significant issue.

Automation of cloud security processes allows for consistent application of defined controls and real-time re-alignment of configuration drift against established policies.

Identities

A username and password alone for gaining access to a resource, device, or application no longer offers sufficient strength to prevent unauthorized access.

TOPICS FOR IDENTITIES

Compromised identities feature prominently in many cyberattacks. We asked about eight identity-related issues in assessing investment priorities for this area:

- Tightening identity requirements in three different ways.
- Protecting against attacks that seek to compromise human identities.
- Protecting against attacks that seek to compromise non-human identities.
- Managing identity security posture.
- Governing user identities and access rights.
- Ensuring that credentials for offboarded employees are promptly revoked.

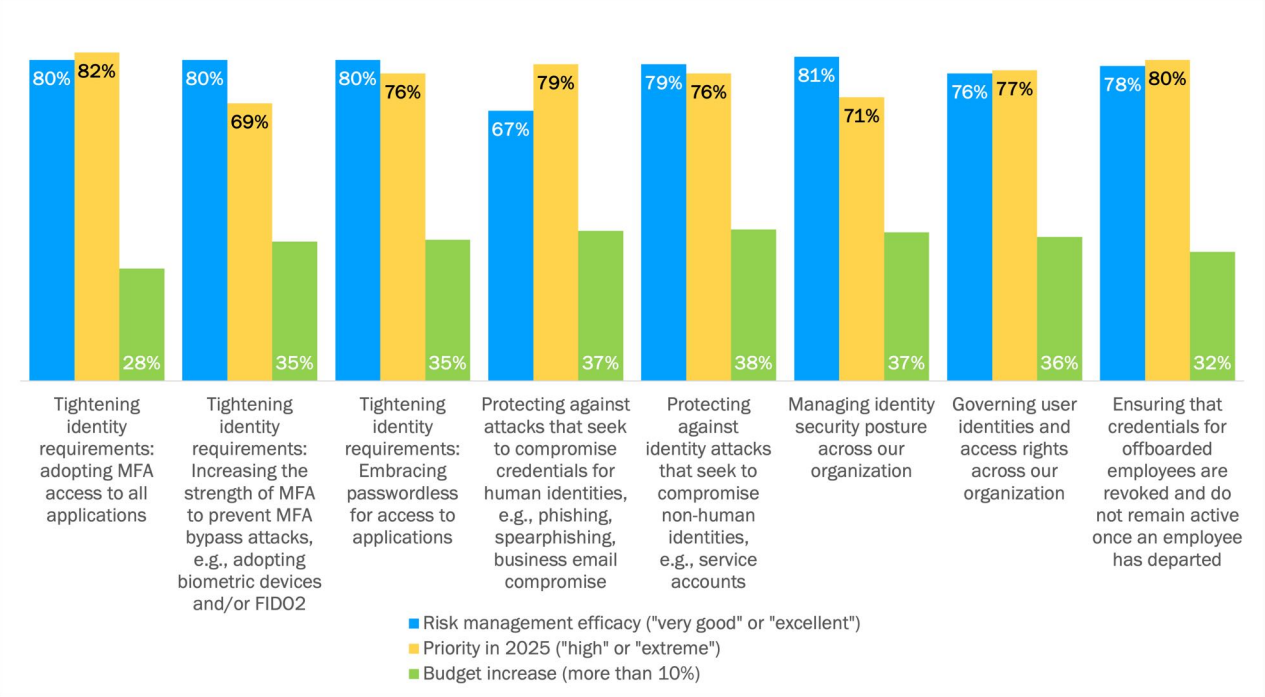
OVERALL PRIORITIES IN 2025: IDENTITIES

From an overall perspective for identities in 2025 (see Figure 16):

- Around 80% of respondents claim high-risk management efficacy across all eight issues. The notable exception is the lower rating for protecting against attacks that seek to compromise human identities, such as phishing.
- Investment priorities for six of the issues are relatively similar (average 77% for issues 3 to 8 below). The data varies on which approach to take to MFA (issues 1 to 2 below). The priority for enforcing MFA for all applications is higher than increasing the strength of MFA methods, e.g., adopting biometric devices.
- The anticipated increase in budget numbers is very similar, with an average of 36% for the middle six issues below. MFA for all applications and revoking credentials for departed employees are on the low end of the increase scale.

Organizations place higher priority on enforcing MFA for all applications than increasing the strength of MFA methods.

Figure 16
Overall investment priorities in 2025: Identities
Percentage of respondents



Source: Osterman Research (2025)

CORRELATING RISK POSTURE WITH PRIORITIES AND BUDGET CHANGE: IDENTITIES

Only 25% of respondents say their organization is "very good" or "excellent" at managing the business risks for all the issues related to identities. Most (75%) have differing levels of risk management efficacy. This low result could highlight why many organizations struggle with detecting and stopping identity-based attacks.

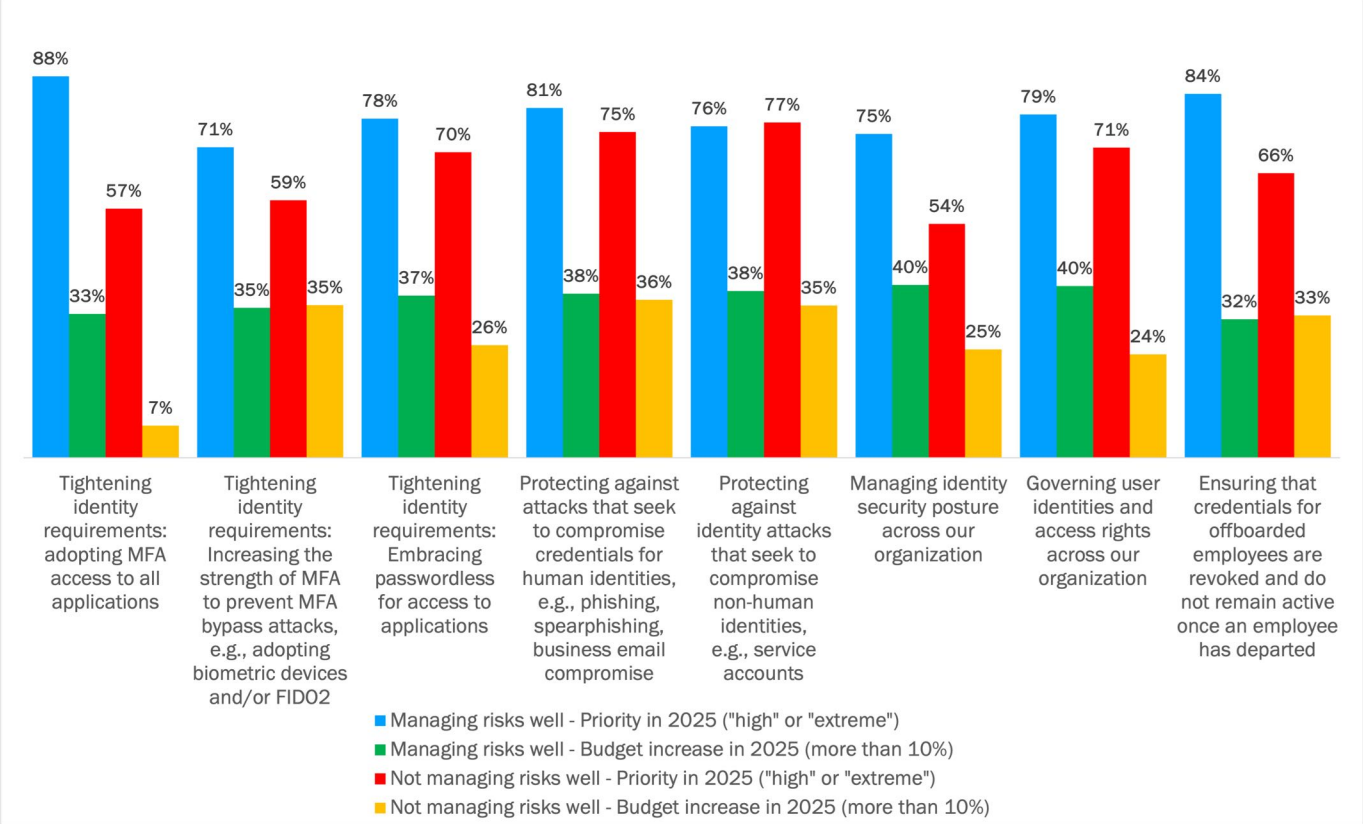
Splitting the data on investment priorities and anticipated budget increases for 2025 by current risk management efficacy results in several issues being indifferent to the correlation. The priority and anticipated budget increase for protecting against credential compromise attacks of both human and non-human identities are essentially the same, irrespective of current risk management efficacy. In other words, all organizations know they need to do better as a matter of urgency, irrespective of whether they have the risk management processes in place already. Other issues in the list are similar but not the same, e.g., governing user identities and tightening identity requirements with stronger MFA methods. This indifference to current risk management efficacy is not seen to the same extent in the other deep-dive areas in this research.

All organizations know they need to do better with identity security as a matter of principle.

Protecting against identity attacks that seek to compromise non-human identities is the only issue across all four areas where the security priority in 2025 is higher among those not managing risks well compared to those who are. This is an unaddressed issue for too many organizations, and the warning bells are sounding.

See Figure 17.

Figure 17
Correlating risk management efficacy with investment priorities and budget: Identities
Percentage of respondents



Source: Osterman Research (2025)

DISCUSSION ON INVESTMENT PRIORITIES FOR IDENTITIES IN 2025

A username and password alone for gaining access to a resource, device, or application no longer offers sufficient strength to prevent unauthorized access. Credentials have been too easily compromised through phishing attacks in recent decades, and unrelenting data breaches have given threat actors a treasure trove of credentials that can be used in attacks. Mitigating or compensating controls on credentials and their usage has become essential for organizations, and often mandatory for some industries and any organization looking for cyber insurance coverage. MFA is one example of a compensating control, and there are clear signals in the data that senior leaders are placing priority in 2025 on widening the usage of MFA and strengthening MFA devices. Passwordless is another compensating control, and that too is attracting high interest and budgetary investment in 2025. Finally, managing identity security posture—having the optics to see who is logging in where and how and if there are abnormalities in patterns that may signal malicious activity—is a third. Something must be added to the use of a username and password, and the embrace of a multi-level defensive posture is showing up in the data. These are positive movements.

Protecting non-human identities (e.g., service accounts) has received less cut-through compared to human identities, and hence many organizations have significantly lower optics and visibility into their risk factors. Such a situation is ideal for threat actors. If they can compromise access to a service account—especially ones that are highly privileged and where access patterns are not regularly audited—the longer the potential footprint becomes for unauthorized data access and subsequent lateral movement. In the data from this research, the priority for protecting both human and non-human identities is closely aligned. This is a promising sign that organizations are elevating attention on both.

Deactivating credentials for offboarded employees had the second highest priority in both the overall chart and the correlated one for organizations that are managing business risks well. Failing to close out the possibility of such credentials being used raises the risk of surreptitious usage by threat actors and ex-employees alike. Hardening offboarding controls and processes for identities prevents a whole set of downstream compromise incidents.

Hardening offboarding controls and processes for identities prevents a whole set of downstream compromise incidents.

Data

Classification for classification's sake is a less compelling proposition than using that analysis to drive automated and elevated protections over data.

TOPICS FOR DATA

Data is targeted in many cyberattacks, as its exfiltration, unauthorized publication, or threatened irreversible destruction has proven an effective method of financial extortion. Data is always in the crosshairs; it's the thing that threat actors are after. We looked into six issues about data:

- Data discovery, e.g., where data is stored
- Automatic data classification, e.g., personal data subject to privacy regulations
- Implementing data minimization, defensible data deletion, and data retention in support of privacy compliance and risk reduction
- Automatically protecting data, e.g., encrypting personal data subject to privacy regulations
- Implementing capabilities for preventing the exfiltration of data, e.g., to stop the leakage of personally identifiable information (PII), intellectual property (IP), classified information, and other sensitive information
- The ability to restore data after a cyber incident

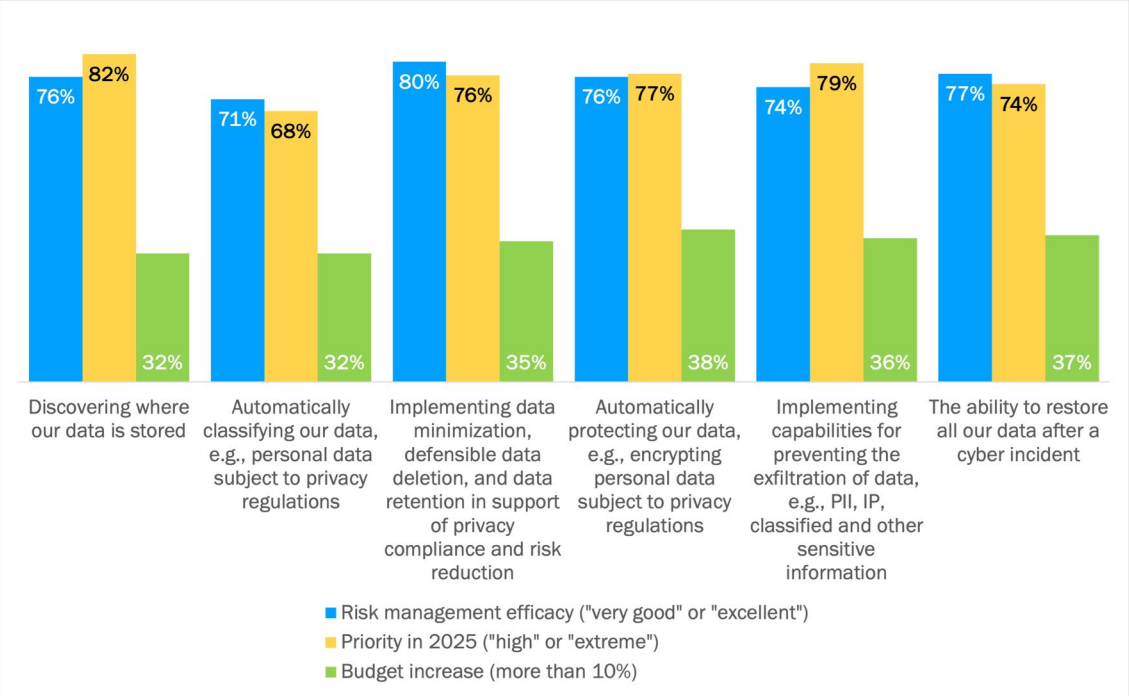
Data is always in the crosshairs; it's the thing that threat actors are after.

OVERALL PRIORITIES IN 2025: DATA

The overall viewpoint on data in 2025 is (see Figure 18):

- In sum, risk management efficacy is fairly evenly distributed across the six issues.
- The highest investment priorities in 2025 are data discovery and stopping data exfiltration. There is often a relationship between these in attacks: exfiltrated data was somewhere unknown.
- There is not a lot of variation in the budget increase numbers (average 35%).

Figure 18
Overall investment priorities in 2025: Data
Percentage of respondents



Source: Osterman Research (2025)

CORRELATING RISK POSTURE WITH PRIORITIES AND BUDGET CHANGE: DATA

Only 22% of respondents say their organization is "very good" or "excellent" at managing the business risks for all the issues related to data. Most (78%) have uneven levels of risk management efficacy across the six data issues. As data is continually targeted in cyberattacks—by ransomware, data breaches, and as a result of misconfigured access rights (see Figure 2 earlier)—strengthening these controls is linked directly with shrinking the accessible attack space.

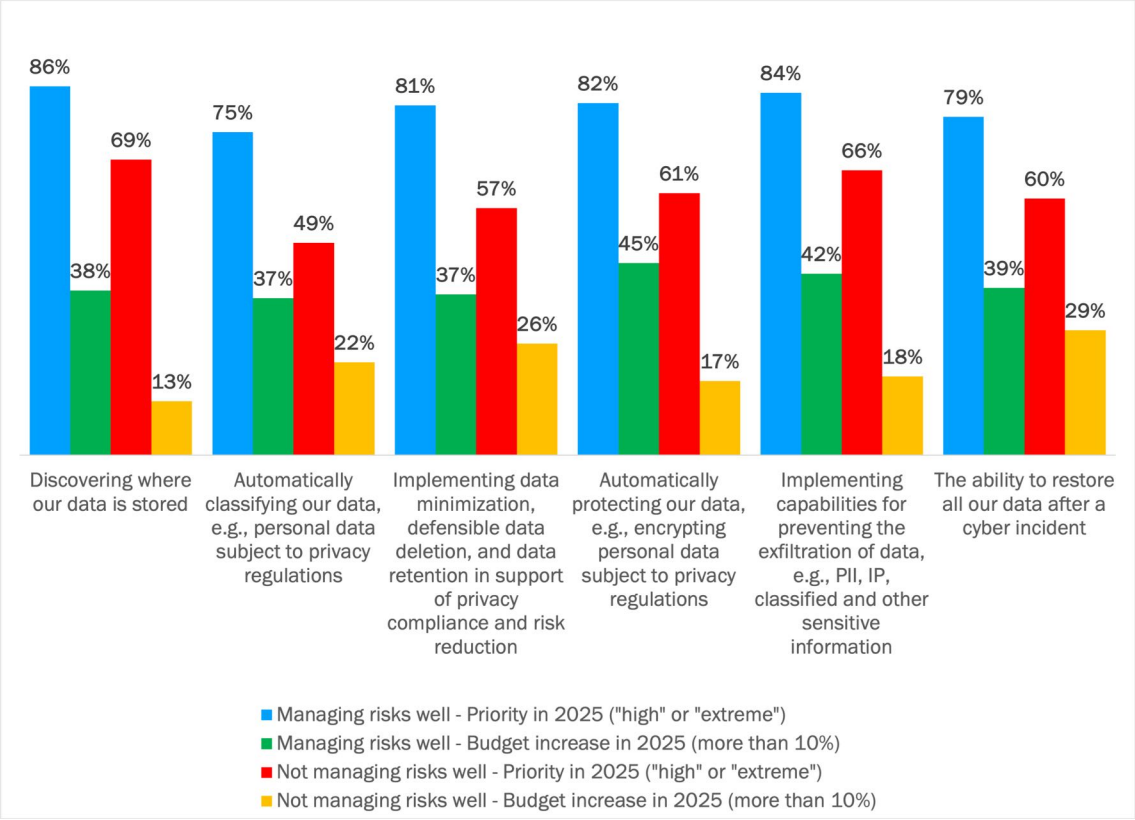
Among organizations managing risks well, there is slight variation around the priority associated with the six data issues in 2025 (ranging from 75% to 86%). Budgets, too, are similar, although the largest budget increases are targeted for automatically protecting data with encryption and preventing data exfiltration. The first often enables the second, or at minimum, eliminates the threat carried by the second if the encryption approach can withstand brute-force decryption attempts.

Several budget increase comparatives have significant variations between those managing risks well and those not doing so. The largest percentage variation is for automatically protecting data with encryption (28%); the second largest is for data discovery (25%). By contrast, some are much closer. The ability to restore all data after a cyber incident has the smallest variation (10%), indicating that irrespective of current risk management efficacy, being able to get back to business after a cyber incident is highly important to many organizations.

Encryption aids in preventing data exfiltration by eliminating the threat if the encryption approach can withstand brute-force decryption attempts.

See Figure 19.

Figure 19
Correlating risk management efficacy with investment priorities and budget: Data
Percentage of respondents



Source: Osterman Research (2025)

DISCUSSION ON INVESTMENT PRIORITIES FOR DATA IN 2025

The relative priority around the two potential automatic actions taken on data is interesting and something we saw in the 2023 research too. There is higher priority for both groups of respondents in Figure 19—those managing risks well and those not managing risks well—to automatically protect data with encryption rather than merely automatically classifying data. There's a strong case to be made for strengthening data classification methods. Still, if that's where it ends—in classification only—it's not as compelling as using that classification to drive automated and elevated protections over data. Encryption is a key contender for reducing the fallout from data breaches.

Conclusion

The priorities presented in this white paper around cloud, talent, and data reflect a snapshot of representative organizations in the United States for the 2025 calendar year. The CISO and CIO respondents who engaged in this survey have shared their perspective and plans across a wide selection of cybersecurity areas, along with a deeper dive into topics associated with the specific areas of applications, cloud platforms and services, identities, and data.

The priorities presented in this white paper may not, however, immediately resonate for your organization. Investment priorities for any given organization must be set within the context of their current posture, real-world threat data, and known areas of concern (and unknown areas of weakness). This is the fundamental work that cybersecurity decision-makers and influencers must coordinate within their own organizations. Do that work, assess what is needed, and use this white paper as an external reference point to ensure the right issues are being addressed.

Investment priorities for any given organization must be set within the context of their current posture, real-world threat data, and known areas of concern.

Sponsored by BIO-key International

BIO-key is revolutionizing authentication and cybersecurity with biometric-centric, multi-factor identity and access management (IAM) software securing access for over forty million users. BIO-key allows customers to choose the right authentication factors for diverse use cases, including phoneless, tokenless, and passwordless biometric options. Its cloud-hosted or on-premises PortalGuard IAM solution provides cost-effective, easy-to-deploy, convenient, and secure access to computers, information, applications, and high-value transactions.

www.BIO-key.com

BIO-key.com

@BIOkeyIntl

Methodology

This white paper is based on findings from a survey conducted by Osterman Research. Two hundred sixty-eight (268) respondents who have responsibility for planning and managing the cybersecurity strategy at their organization, including evaluating and selecting cybersecurity solutions and determining spending priorities, were surveyed during January 10 to 22, 2025. To qualify, respondents had to work at organizations with at least 1,000 employees. All surveys were conducted in the United States. The survey was cross-industry, and no industries were excluded or restricted.

JOB ROLE

CISO, or some other role that has this responsibility	48.9%
CIO, or some other role that has this responsibility	51.1%

ORGANIZATION SIZE

1000 to 4999 employees	41.8%
5000 to 9999 employees	29.5%
10,000 to 19,999 employees	10.4%
20,000 or more	18.3%

INDUSTRY

Agriculture, forestry or mining	4.5%
Computer hardware or computer software	1.5%
Data infrastructure or telecom	1.9%
Education	5.2%
Energy or utilities	6.7%
Financial services	9.7%
Government	2.2%
Healthcare	10.8%
Hospitality, food or leisure travel	4.1%
Industrials (manufacturing, construction, etc.)	8.2%
Information technology	13.8%
Life sciences or pharmaceuticals	3.7%
Media or creative industries	3.0%
Professional services (law, consulting, etc.)	1.9%
Public service or social service	0.4%
Retail or ecommerce	10.1%
Transport or logistics	12.3%

[1] Osterman Research, CISO and CIO Investment Priorities for Cybersecurity in 2023, February 2023, at https://ostermanresearch.com/portfolio/orwp_0356-investment-priorities-2023/

[2] Osterman Research, Using AI to Enhance Defensive Cybersecurity, November 2024, at https://ostermanresearch.com/portfolio/orwp_0363/

[3] OWASP, OWASP Top 10 API Security Risks - 2023, at https://owasp.org/API-Security/editions/2023/en/0x11-t10/