Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **February 2023**
Sponsored by **Quest**

CISO and CIO Investment Priorities for Cybersecurity in 2023

Executive Summary

CISOs and CIOs view cybersecurity as a significantly higher priority than two years ago and are investing in multiple areas to meet escalating regulatory demands, protect new digital channels, and counteract ongoing cyber incidents. Improving protections for cloud services and platforms is the top-rated priority (attacks against cloud services were the most-seen incident type during the past year), followed by protections against ransomware attacks. CISOs and CIOs see a range of issues within apps, cloud platforms, data, and on-premises infrastructure requiring ongoing and higher investment in 2023. They are budgeting accordingly.

The data presented in this white paper is from a survey of CISO and CIO respondents at 284 organizations in the United States with more than 1,000 employees. Further details on the survey methodology are provided on page 34.

CISOs and CIOs view cybersecurity as a significantly higher priority than two years ago and are investing in multiple areas to meet escalating regulatory demands, protect new digital channels, and counteract ongoing cyber incidents.

KEY TAKEAWAYS

The key takeaways from this research are:

- **Regulation, digital channels, and economics driving cybersecurity**
  The top trends and challenges driving how organizations approach cybersecurity in 2023 are escalating regulatory demands for cybersecurity and data privacy; growing use of digital channels for engagement with customers, employees, and partners; and the declining economic outlook. CISOs attribute greater impact to all trends and challenges than the CIO (with one exception).
- **Top priorities are cloud security, ransomware protections, and data**
  Cloud security and ransomware protections are the top two investment priorities in 2023 out of more than 20 areas. For the investment priority to be high, the most common pre-conditions are high concern that the current security protections are insufficient along with the requirement for a significant financial outlay to bring the area up to the internal standard of the organization.
- **Better risk management leads to higher security prioritization and budget**
  Organizations with a greater ability to manage the business risks associated with apps, cloud platforms, data, and on-premises infrastructure assigned higher security prioritization to the key issues associated with each area, as well as a higher budget, compared to organizations with lower risk management efficacy.
- **Budgets have increased 11% since last year and are expected to increase further**
  The average budget increase from 2022 to 2023 is 11%, with a further average increase of 19% forecast for the 2023 to 2024 budget cycle. However, CISO and CIO respondents believe they could put an average of twice as much budget to productive and effective use in 2023. Some CISOs and CIOs say they could put three to five times as much budget to productive use in 2023.
- **How the board views cybersecurity has significant flow-on effects**
  Boards that view cybersecurity as a business risk show greater proclivity toward proactive investment, concern with technical risks, and approval of funding. Among these boards, fewer take a reactive approach to cybersecurity threats. If the board only pays attention to cybersecurity threats after a breach or incident, cybersecurity is viewed as a technical risk and budget is approved only grudgingly.

ABOUT THIS WHITE PAPER

This white paper is sponsored by Quest. Information about Quest is provided at the end of this paper.

Setting the Scene

This section defines "investment priority" and presents data on recent incidents.

WHAT MAKES SOMETHING AN "INVESTMENT PRIORITY"?

The strategic intent of this research is to explore what CISOs and CIOs view as investment priorities for cybersecurity in 2023. We have based our analysis of the answers to the survey questions on the following three principles:

- **A priority requires a thinking and conceptual component**
  It is essential that a case can be made for why something is a priority. This requires being able to explain the underlying logic.
- **A priority requires aligned action**
  Actions flowing from a declared or espoused priority provide evidence that the priority is more than mere words. An aligned action could be continued investment in an area or increased investment year on year.
- **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. If the required investment is 100% more than what is spent currently, spending only 15% more indicates that it is not a priority.

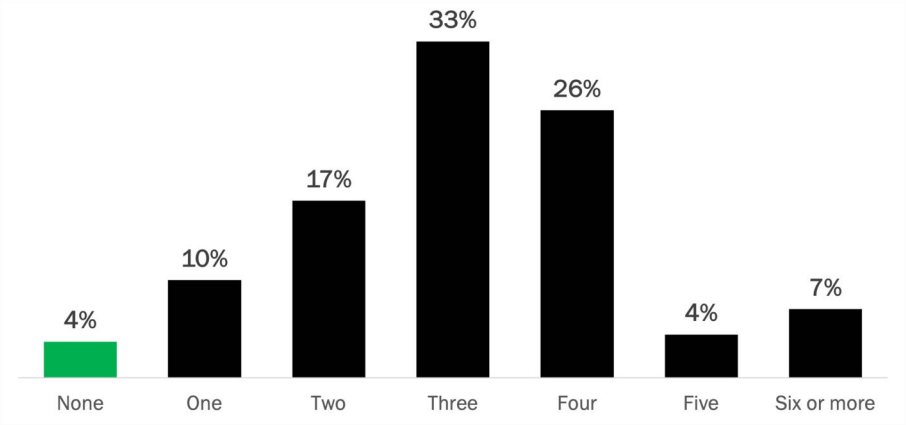
In other words, we dug into the data to look for alignment and consistency across multiple questions, not merely simple adherence to a single question.

CYBERSECURITY INCIDENT TYPES DURING 2022

Seventy percent of organizations experienced three or more types of cybersecurity incidents in 2022 (see Figure 1). Incidents signal areas where organizations are vulnerable and current security protections are insufficient. Of all assessment actions, an actual incident provides the strongest reality check for an organization—albeit a costly and disruptive one.

Seventy percent of organizations experienced three or more types of cybersecurity incidents during 2022.

Figure 1
Number of Cybersecurity Incident Types Experienced in 2022
Percentage of respondents

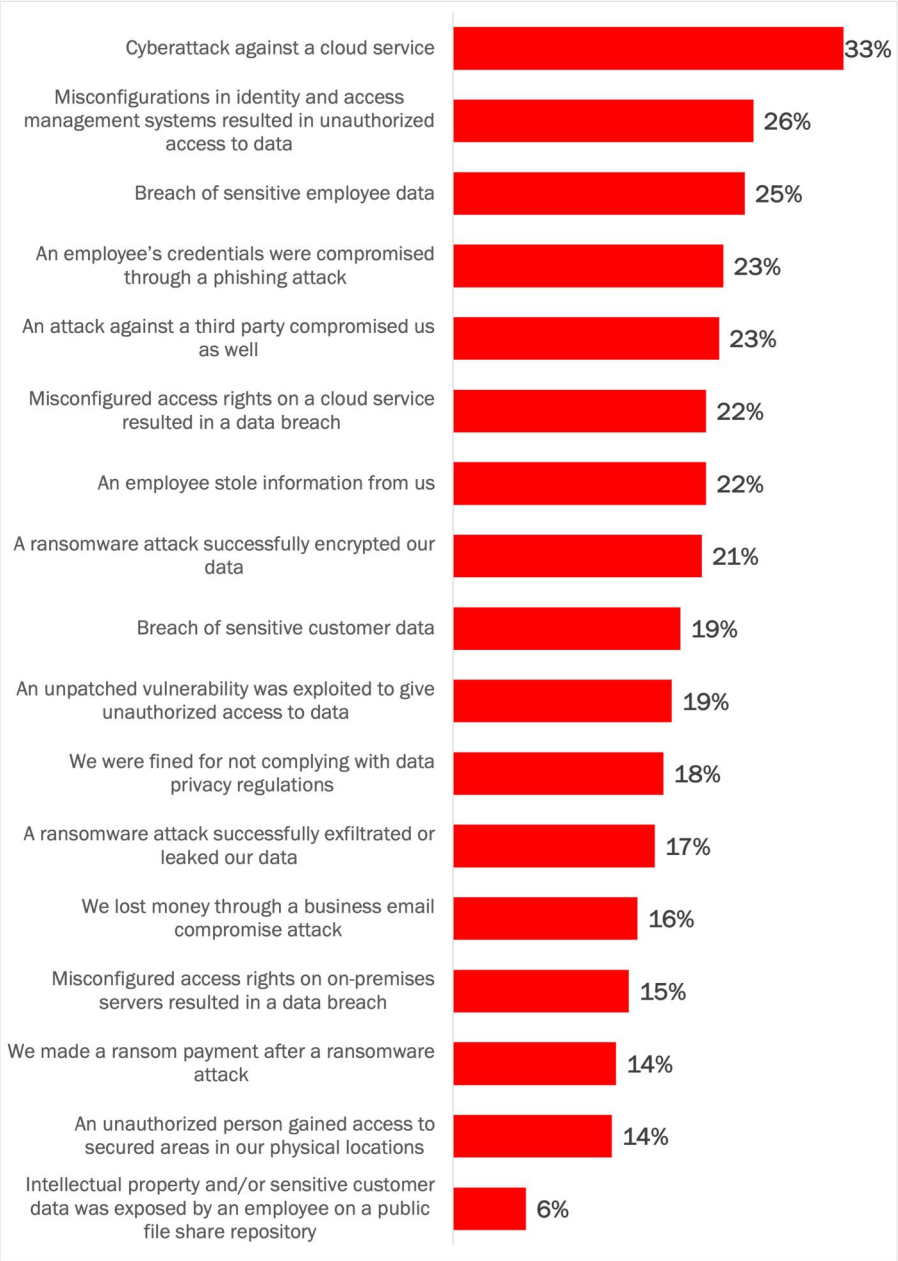


Source: Osterman Research (2023)

The numbers in Figure 1 refer to types of incidents experienced, not the number of incidents per se. With most organizations experiencing three or more different types of incidents, threat fighting increases in difficulty and post-breach capabilities in importance. Threat prevention measures are essential, but no less so than recovery capabilities.

The most frequently occurring types of incidents during the past 12 months were a cyberattack against a cloud service, unauthorized access to data due to misconfigurations in identity and access management systems (e.g., Active Directory/Azure AD, Ping Identity), and breach of sensitive employee data. See Figure 2.

Figure 2
Cybersecurity Incident Types Experienced in 2022
Percentage of respondents



Source: Osterman Research (2023)

One third of organizations experienced at least one cyberattack against a cloud service during 2022.

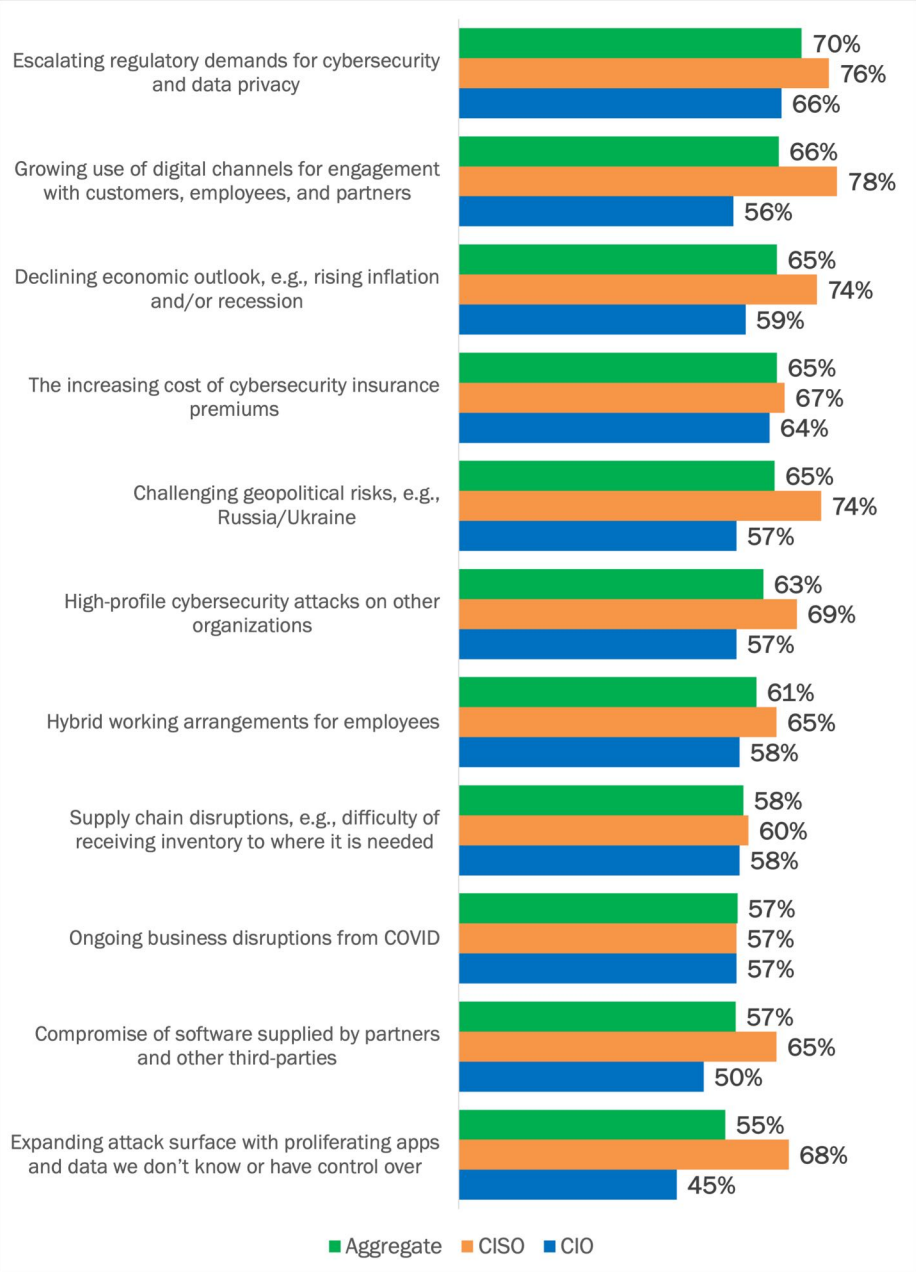
Trends, Challenges, Priorities

This section examines the trends and challenges driving how organizations approach cybersecurity in 2023, and hence the growing priority of cybersecurity.

TRENDS AND CHALLENGES DRIVING CYBERSECURITY IN 2023

The trends and challenges making the greatest impact on how organizations approach cybersecurity reflect changing and highly uncertain business realities. In all cases but one, CISOs attribute greater impact to the trends and challenges than CIOs. 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 (2023)

Escalating regulatory demands, new digital engagement channels, and the declining economic outlook are the trends and challenges having the most impact on cybersecurity in 2023.

The impacts of the top four trends and challenges on cybersecurity include:

- **Escalating regulatory demands for cybersecurity and data privacy**
  Organizations (and public company officers) can be subject to financial and other penalties for lack of compliance even if there is no evidence of compromise or an active incident. Changing regulatory expectations force investment in areas that many organizations have historically ignored or under-prioritized. One in five organizations have already been fined for non-compliance (see Figure 2).
- **The growing use of digital channels for engagement with customers, employees, and partners**
  The use of new channels increases the potential attack surface. New channels and apps increase complexity and decrease security posture due to unverified cybersecurity ratings on apps; expanded third-party connections; and a growing number of identities to provision, manage, and secure. Newness equates with uncertainty, and often insufficient visibility. The cost of downtime is also raised due to increased dependency on digital channels. Connectivity and cloud service availability becomes essential to business operations.
- **The declining economic outlook, particularly rising inflation and/or the likelihood of a global recession in 2023**
  Cybersecurity budgets may be reduced or flat, resulting in greater difficulty in procuring the necessary talent, solutions and protections that will be required.
- **The increasing cost of cybersecurity insurance premiums**
  More expensive premiums change the risk calculus in cybersecurity planning. Organizations may previously have relied on cybersecurity insurance to mitigate the costs of an incident, but the increasing cost and difficulty of acquiring coverage places higher relative importance on actually addressing cybersecurity weaknesses instead of operating on the assumption that the insurance company will mitigate the financial cost of any incident.

Changing regulatory expectations force investment in areas that many organizations have historically ignored or under-prioritized.

The systematic differences in impact weighting between CISOs and CIOs is informative. We make the following observations on the difference:

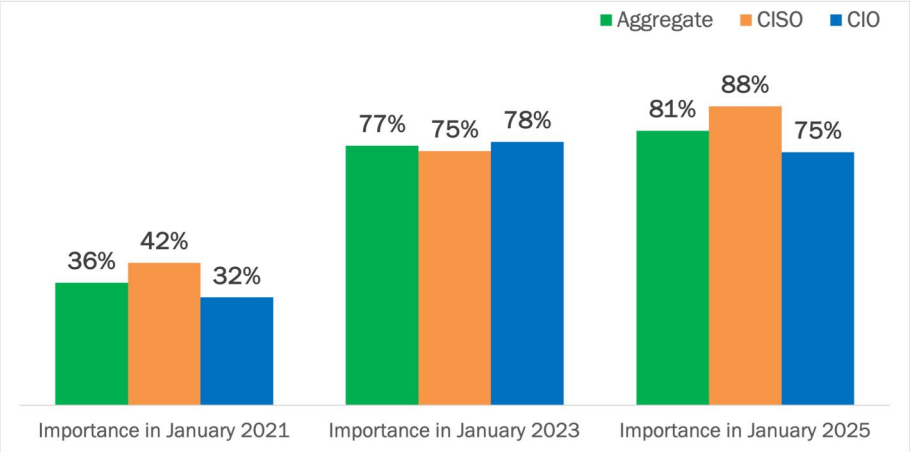
- **More CISOs report to CIOs than the other way around**
  Assigning a higher impact weighting as a CISO indicates taking responsibility for the trend or challenge, thus reducing the weight of the trend or challenge on the CIOs shoulders. Some issues that are much more impactful to CISOs—such as growing use of digital channels at 78% vs. 56% for CIOs—reflect heightened security concerns that a CISO needs to take care of. Other issues with large differences—such as challenging geopolitical risks at 74% vs. 57% for CIOs—could reflect a greater awareness by the CISO of the specific security ramifications when sanctions against Russia (and by implication, Russian cybercrime gangs) are lifted.
- **The CIO role has been around for longer, with greater business exposure**
  The CIO is a more established business leader role than the CISO role. CISOs are moving away from their technical origin story, but their exposure to business risk assessment generally lags behind those in CIO roles. CISOs may be systematically over-assessing impact.
- **CISOs will need to educate CIOs where significant differences exist**
  The issue of least importance to CIOs (45%, 11th place) is right in the middle of the CISOs' ranking (68%, 6th place): the expanding attack surface with proliferating apps and data that are unknown and uncontrolled. This specific challenge links directly with the two top-rated trends and challenges: escalating regulatory

demands for cybersecurity and data privacy, and the growing use of digital engagement channels. Failing to get the expanding attack surface under control will, by implication, undermine the organization's ability to mitigate the threats of the two top trends. There is an educational role for CISOs to CIOs on this topic.

THE PRIORITY OF CYBERSECURITY IN ORGANIZATIONS HAS DOUBLED

Twice as many CISOs and CIOs indicate that their organization places the highest levels of priority on cybersecurity today as compared with two years ago. In the aggregate, even more organizations are expected to do so in 2025, although the level of expected increase is marginal. This may indicate that CISOs and CIOs perceive their current cybersecurity defenses are almost completely adequate to meet future threats, or alternatively that they perceive innovation in the cybercriminal community will be less robust in the future. See Figure 4.

Figure 4
Priority of Cybersecurity Issues to Organizations
Percentage of respondents indicating "important" or "extremely important"



Source: Osterman Research (2023)

Neither CISOs nor CIOs are currently able to perceive that cybersecurity could still become significantly more important than it is today.

The increasing level of priority for cybersecurity over the past two years is unsurprising given the well-publicized cybersecurity incidents that have occurred since January 2021. The SolarWinds compromise started in December 2020 and its impacts were still unfolding in January. Microsoft Exchange Server has been the target of numerous global incidents during the past two years. And the devastating ransomware incidents against Colonial Pipeline, JBS, and others were pivotal in driving awareness around the ransomware threat for boards and senior leaders.

We don't yet know what headline-grabbing incidents will occur over the next two years. By implication, while CISOs and CIOs expect only a marginal uplift in priority during this time, the reality could be very different. If this question is asked in a survey in January 2025, we are likely to find that the comparison between 2023 and 2025 is again a doubling of importance, not a marginal uplift. Neither CISOs nor CIOs are currently able to perceive that cybersecurity could still become significantly more important than it is today.

The different ratings between CISOs and CIOs is interesting. CISOs say their organization placed the highest priority on cybersecurity two years ago (42%) and will do so in two years (88%). For 2023, CIOs slightly lead (78%), perhaps due to greater interaction with the CEO and board over the immediate urgency around cybersecurity.

Assessing Investment Priorities Against Cybersecurity Posture

In this section, we look at how respondents assess their overall cybersecurity posture in 22 areas and the investment required to improve posture.

METHODOLOGY

We asked respondents to provide an assessment of their current cybersecurity posture in 22 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. The question did not seek any comparison or assessment against an external framework or an imposed baseline. Each respondent was asked to answer the question based on how their organization approached a given area—that is, against their own internal framework. Respondents had to implicitly balance an assessment of current strengths, weaknesses, opportunities, and threats for each of the 22 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 standard set by their organization. This question was phrased as an internal rating rather than seeking alignment with any universal standard, external framework, or an 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 2023 of investing in each area**
   The level of priority within the organization for improving the cybersecurity posture of a given area in 2023.

Organizations must assess the gap between their current and desired security posture.

TOP SEVEN PRIORITIES

The top seven priorities for the organizations in this research are shown in Figure 5, with cloud security, ransomware protections, and protecting identities leading the list. These top seven priorities link to many of the trends and challenges driving cybersecurity in 2023 (see Figure 3 on page 5):

- **Security of cloud apps and services**
  The adoption of cloud apps and services continues to skyrocket and 33% of organizations in this research experienced an attack against their cloud services in the last year. As new apps and services are embraced, the volume of business data contained in these apps and services increases. When security is lacking, insufficient, or incorrectly configured, the risk of exposure and data breach is high. With the growing regulatory demands for data privacy (the top-rated trend or challenge impacting how organizations approach cybersecurity), exposure and breach become significant incidents for an organization.
- **Protecting against ransomware attacks**
  Ransomware attacks can devastate the ability of an organization to operate, compromise intellectual property and customer data through pre-detonation data exfiltration, and result in lost business opportunities and financial standing.[1] This second highest–rated priority links to several of the trends and challenges in Figure 3, including the increasing cost of cybersecurity insurance premiums (much of which has been driven by exorbitant ransomware-related payouts) and high-profile cybersecurity attacks on other organizations. Protecting against ransomware attacks requires an approach that covers the full lifecycle of protections, including prevention and recovery.
- **Protecting user identities from attack and compromise**
  As the number of digital channels for engagement with customers, employees, and partners increases, organizations must manage and secure a growing range of user identities. Protecting these user identities from attack and compromise is the third-highest priority in 2023. It was the second most common attack in 2022.

As the number of digital channels for engagement with customers, employees, and partners increases, organizations must manage and secure a growing range of user identities.

Figure 5
Cybersecurity Posture Investment Priorities in 2023: Top Seven
Percentage of respondents indicating "high priority" or "essential"

Source: Osterman Research (2023)

CORRELATING CONCERN, INVESTMENT LEVELS, AND PRIORITY IN 2023

Beyond the raw data shown above, the interplay between the three questions provides an approach for assessing investment intent. To do so, we divided the responses to the three questions into two groups for each question, creating eight combinations (see Figure 6). We expected to see two dominant patterns in the data:

- **High concern → High investment required → High priority in 2023**
  If a respondent indicates high concern for a given area, in most cases, they should also rate the investment required to bring the area up to their internal standard as being high. If the required standard is not rated as being high, in many cases they should not be highly concerned. If concern is high and the investment required is high, the priority of investment in 2023 should normally also be high. This combination of high concern with high required investment and high investment priority is the most common pattern seen in the joint ratings across the three questions, occurring on average 34.7% of the time across all posture areas.
- **Low concern → Low investment required → Low priority in 2023**
  The second expected pattern is the inverse of the first. If a respondent indicates low concern, in most cases, they should also say that the investment required is low, and that the investment priority in 2023 is low. Rather than being the second most frequently occurring pattern, it was actually in third place (occurring 11.5% of the time).

If concern is high and the investment required is high, the priority of investment in 2023 should normally also be high.

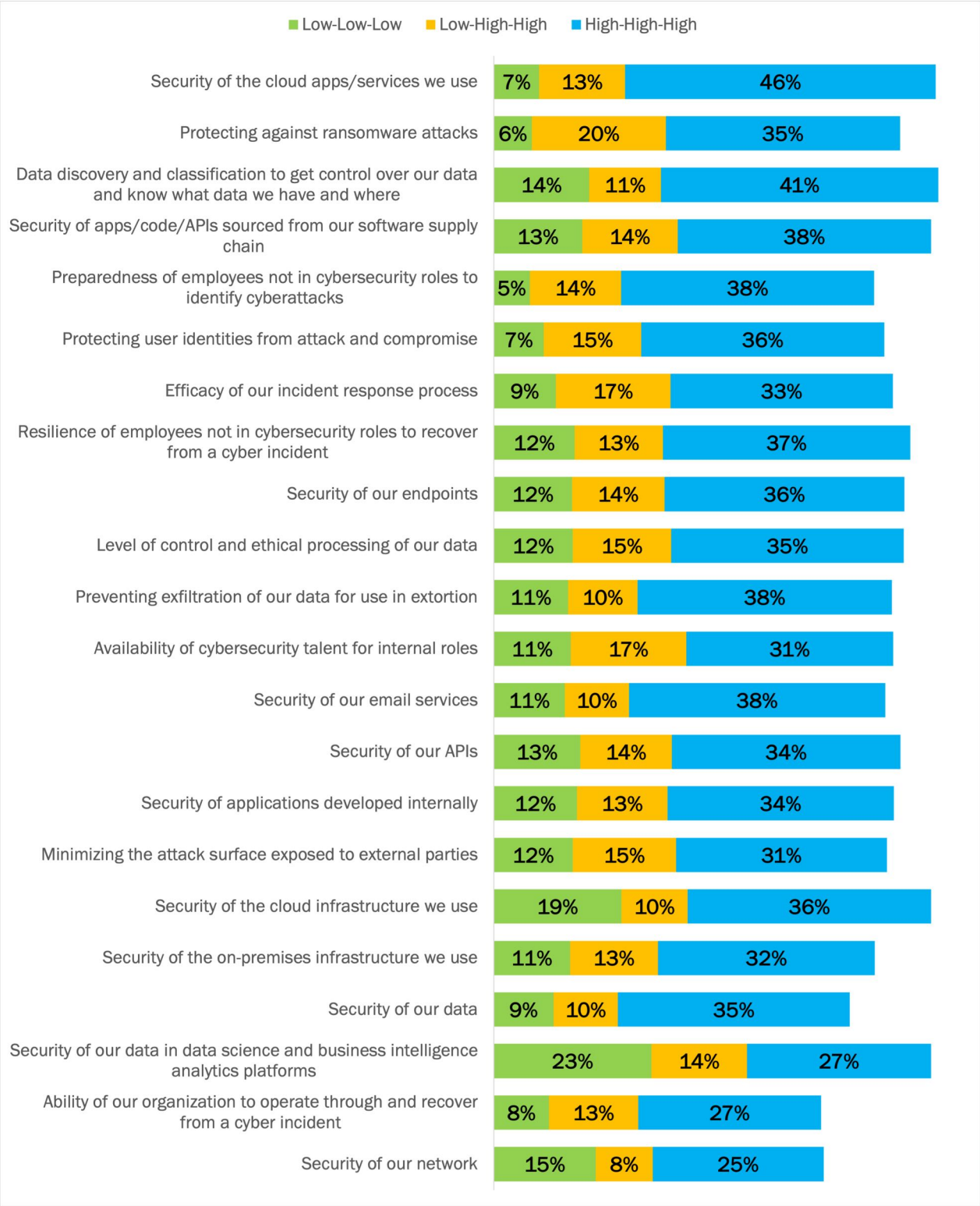
Figure 6
Correlating Concern, Investment Required, and Priority in 2023
Percentage of respondents

Level of current concern	Level of investment required	Priority of security spending in 2023	Percentage	Rank
High concern	High investment	High priority	34.7%	1
High concern	High investment	Low priority	8.4%	5
High concern	Low investment	High priority	11.0%	4
High concern	Low investment	Low priority	6.9%	7
Low concern	High investment	High priority	13.3%	2
Low concern	High investment	Low priority	6.4%	8
Low concern	Low investment	High priority	7.7%	6
Low concern	Low investment	Low priority	11.5%	3

Source: Osterman Research (2023)

The second most frequent pattern was not expected to occur so often. This pattern combines low concern with high investment required and high investment priority in 2023. In looking at the individual posture areas where this pattern happened most often (see Figure 7)—protecting against ransomware attacks (20%), availability of cybersecurity talent for internal roles (17%), and level of control and ethical processing of our data (15%)—these areas give the sense of uncertain, chaotic, or imposed external conditions that override the internal-facing assessment of current posture. This pattern was unexpected because its closest counterpart—low concern with high investment required and low investment priority—was the pattern that occurred the least overall (6.4%). When concern is low and the required investment is high, deciding to do little or nothing can be the correct approach.

Figure 7
Assessing Cybersecurity Posture: Concern, Investment Required, and Priority in 2023
Percentage of respondents (sorted by the sum of Low-High-High and High-High-High)



Source: Osterman Research (2023)

Correlating the level of concern with the investment required and priority in 2023 (as shown in Figure 7 above) changes the relative ordering of priorities in 2023 in almost half of cases compared to the ordering based on priority alone (as shown in Figure 5). See Figure 8 for a comparison of ordering between the two lists. The four types of changes are:

- **Three priorities remain the same**
  The top two priorities remain unchanged between the two lists—both cloud security and ransomware protections are of high priority under multiple viewpoints. Security of apps/code/APIs sourced from the software supply chain is also unchanged between the two lists, in fourth place.
- **One priority moves lower in the Top 7 list based on Correlated Ratings**
  Protecting user identities from attack and compromise moves lower in the Correlated Ratings analysis, from third place to sixth place.
- **Three new priorities move into the Top 7 list of Correlated Ratings**
  Three priorities that are ranked in the Top 7 of the Correlated Ratings list are not on the Top 7 list by Priority Only. Data discovery and classification ranks third on the Correlated Ratings list, preparedness of employees not in cybersecurity roles to identify cyberattacks is fifth, and the efficacy of the incident response process is in seventh place.
- **Three priorities from the Top 7 list on Priority Only don't make the Top 7 list on Correlated Ratings**
  Security of applications developed internally drops from fifth to 15th place (the most significant re-ordering of a Top 7 area), security of endpoints from sixth to nineth, and security of email services from seventh from to 13th.

Figure 8
Comparing Priority Only with Correlated Concern, Investment Required, and Priority
Percentage of respondents

	Priority-Only Rating		Correlated Ratings		
	Percentage of respondents indicating "high priority" or "essential"		*Percentage of respondents indicating "Low-High-High" and "High-High-High"*		
	RANK	PERCENTAGE	CHANGE	RANK	PERCENTAGE
Security of the cloud apps/services we use	1	75%	=	1	59.1%
Protecting against ransomware attacks	2	74%	=	2	54.8%
Protecting user identities from attack and compromise	3	70%	↓	6	50.7%
Security of apps/code/APIs sourced from our software supply chain	4	69%	=	4	52.0%
Security of applications developed internally	5	69%	↓	15	47.2%
Security of our endpoints	6	69%	↓	9	49.5%
Security of our email services	7	68%	↓	13	47.7%
Data discovery and classification to get control over our data and know what data we have and where	Not top 7		↑	3	52.0%
Preparedness of employees not in cybersecurity roles to identify cyberattacks	Not top 7		↑	5	51.3%
Efficacy of our incident response process	Not top 7		↑	7	50.2%

Source: Osterman Research (2023)

Four Specific Focus Areas in 2023

In this and the subsequent four sections, we present the investment priorities for CISOs and CIOs in four specific focus areas: apps, cloud platforms, data, and on-premises infrastructure.

DIGGING DEEPER

In addition to the assessment of overall posture, required investment, and investment priority in 2023 for the 22 areas above, we asked respondents to provide insight into their security posture and investment priorities in four specific focus areas. These were:

- **Apps**
  Several types of apps are used in organizations for productivity, collaboration, business processes, and more. We asked about apps approved and sanctioned by IT, those tolerated by IT that don't support common identity and provisioning standards, and unsanctioned apps that are used by employees without approval by IT.
- **Cloud platforms**
  Organizations are migrating on-premises workloads to Microsoft Azure, Google Cloud Platform, and Amazon Web Services. We asked about managing access rights, security policies across cloud platforms, cybersecurity talent, and data centric security in the cloud.
- **Data**
  Discovering, classifying, protecting, and having the ability to restore data after a cyber incident were among the topics of assessment explored for the data focus area.
- **On-premises infrastructure**
  Few organizations are fully cloud-only. In most cases, organizations also have on-premises infrastructure to secure against cybersecurity threats. We looked at four topics: post-incident recovery, integrating new security solutions into legacy infrastructure, cybersecurity talent, and data privacy.

How are organizations approaching apps, cloud, data, and on-premises infrastructure in 2023?

METHODOLOGY

For each of these four specific focus 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, how well the organization is currently managing the associated business risks. These business risks 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 2023**
  How the organization is prioritizing security for each topic or issue within a focus area in 2023. Respondents answered on a five-point scale: none, low, medium, high, and essential (with "essential" meaning that it must be done).

- **Budget change in 2023 compared to 2022**
  For each of the topics or issues within an area, how the budget allocated to the topic is changing in 2023 compared to 2022. Respondents answered on a five-point scale: a reduction of 10% or more, a reduction of 5% to 10%, about the same (meaning a range from -5% to +5%), an increase of 5% to 10%, and an increase of more than 10%.

In the subsequent four sections, we present the following analysis for each focus 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 2023? 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 2023. Correlating the answers in this way provides a different view of the data than the overall one. A common finding across all four focus areas is that organizations with higher risk management efficacy place higher priority on security in 2023 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 spend in 2023.

A discussion on each of the focus areas follows the numerical analysis.

Organizations with higher risk management efficacy place higher priority on security in 2023 and are allocating a greater budget increase.

Priorities for Apps

Within the Apps focus area, we asked about three types of apps used in organizations:

- Applications that are approved and sanctioned by the IT team and security teams. This frequently includes Microsoft 365, Salesforce, and more.
- Applications that are tolerated by IT for use in an organization, even though they do not meet common standards that are important to security teams, e.g., for identity and provisioning. Many critical business functions are run through these types of apps, yet management of identity and access is performed manually and through brittle workarounds, increasing vulnerability to data breach and exposure.
- Unsanctioned applications that neither the IT team or security team have approved, but are still used by employees for various reasons.

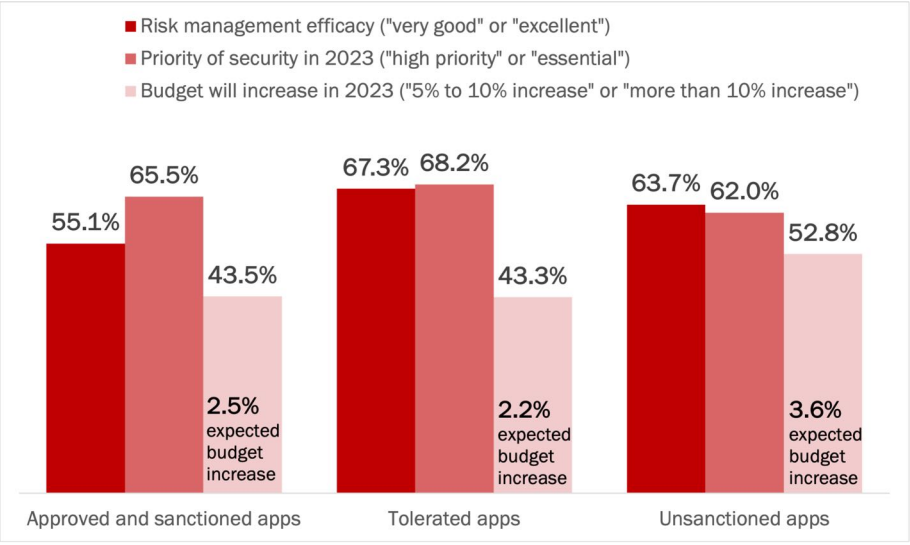
OVERALL APP PRIORITIES IN 2023

Respondents indicated the following risk posture and priorities (see Figure 9):

- Efficacy of managing risks is lowest for approved and sanctioned apps (55.1% indicated "very good" or "excellent") and highest for tolerated apps (67.3%).
- Priority of security in 2023 is highest for tolerated apps (68.2%). Including tolerated apps in the automated provisioning and deprovisioning capabilities of identity management solutions extends identity security and provisioning automation to a whole group of critical apps that organizations have failed to secure. Priority of security in 2023 is lowest for unsanctioned apps (62.0%).
- Increased budget for security in 2023 compared to 2022 is the highest for unsanctioned apps (52.8%), which is ironic since the priority of security is lowest for these apps. The overall net budget change is 3.6%.

Many critical business functions are run through tolerated apps, yet management of identity and access is performed manually and through brittle workarounds, increasing vulnerability to data breach and exposure.

Figure 9
Overall Investment Priorities in 2023: Apps
Percentage of respondents



Source: Osterman Research (2023)

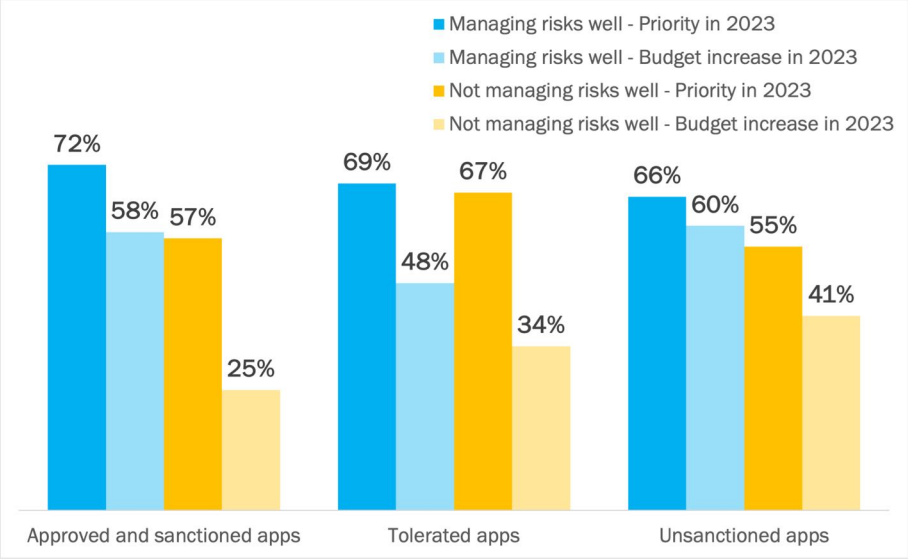
CORRELATING RISK POSTURE WITH PRIORITIES AND BUDGET CHANGE

Organizations with a stronger risk management posture (that is, management of the business risks associated with each of the types of apps is "very good" or "excellent") place a higher priority on security in 2023 and are allocating a greater budget increase to each of the types of apps as well. Organizations with a weaker risk management posture place a lower priority on security and are spending less (see Figure 10):

- **Better risk management equals higher security priority in 2023**
  Organizations that indicate they have a higher ability to manage the business risks associated with an app type, also indicate a higher priority in security in 2023. For the apps category, better risk management capabilities include greater visibility into and awareness of apps in use, identifying configuration drift, and automated lifecycle management of identities and access. This leads to a higher overall priority to do something about rectifying the weaknesses and shortcomings seen. This is most evident for approved and sanctioned apps (15% net difference) and unsanctioned apps (11% net difference).
- **Better risk management equals higher budget increase in 2023**
  Organizations with better risk management capabilities also plan to spend more in 2023 to improve risk positioning. For organizations with this better risk management ability, 58% of respondents indicate that the budget assigned to approved and sanctioned apps will increase in 2023, compared to 25% where risk management capabilities are lacking (a 33% difference). This same trend is also seen for the other two types, although not to the same extent.

Better risk management capabilities for apps includes greater visibility into and awareness of apps in use, identifying configuration drift, and automated lifecycle management of identities and access.

Figure 10
Correlating Risk Management with Investment Priorities in 2023: Apps
Percentage of respondents



Source: Osterman Research (2023)

Only 22% of respondents say their organization is "very good" or "excellent" at managing the business risks for all three types of apps. The majority (78%) indicate variability in risk management approaches. Since these types of apps will continue to be used across organizations, and business processes will continue to be managed through these different types, organizations should pursue a better balance of risk management capabilities across the three types of apps.

DISCUSSION ON INVESTMENT PRIORITIES FOR APPS

We were the most concerned by the rating given for the ability to manage business risks for approved and sanctioned apps in comparison to the other two types of apps. Overall, respondents indicated their organizations were least effective at managing risks for this group of apps (55.1%), and yet these are the approved and sanctioned applications that store and process an increasing share of the organization's intellectual property; sensitive corporate data; and personal data on customers, employees, and others. The latter types of data are subject to new and emerging data privacy and protection regulations, hence the ability to manage the risks associated with these apps is significantly lagging the changing regulatory environment.

The tolerated apps type presents an interesting mix of data points. Respondents indicate that they have the highest ability to manage the business risks associated with tolerated applications and are placing the highest priority in 2023 on addressing the revealed weaknesses, threats, and concerns. New solutions are available that replace manual efforts and workarounds for managing identity, provisioning, and access requirements for tolerated apps, transforming ad hoc approaches into repeatable and scalable approaches using process automation. While the expected budget increase is the lowest of the three types, that could merely signal that the requisite cost outlay for the other two types is comparatively higher. Bringing as many tolerated apps as possible in line with best practices for identity, provisioning, and access is of great value to organizations for safeguarding data, meeting regulatory demands, and reducing the threat of opportunistic breach.

The number of unsanctioned apps used in an organization is often several orders of magnitude higher than the number of apps across the other two types. Employees use unsanctioned apps for a slew of reasons, ranging from better fit to a team's requirements to outright rejection of the official standard. However, any app that is used to store or process business, operational, or customer-related data must be managed to reduce the security risk to the organization. Unauthorized access through credential compromise is a risk, as is ongoing access by terminated employees and exposure of customer data by an opportunistic hacker or threat researcher.

Using app discovery capabilities enables organization to figure out which apps are being used by employees, and wherever possible, to prioritize unsanctioned apps that can be incorporated into the identity and provisioning workflows of identity solutions. Organizations lacking the optics to identify the difference between unsanctioned and tolerated apps must put up with a much higher risk of data breach and exposure compared to organizations that can see the different types of apps in use and extend security controls to as many as possible.

Bringing as many tolerated apps as possible in line with best practices for identity, provisioning, and access is of great value to organizations for safeguarding data, meeting regulatory demands, and reducing the threat of opportunistic breach.

Priorities for Cloud

Within the Cloud focus area, we investigated four topics:

- Managing configuration of access rights on cloud platforms and services that enable unauthorized access to data—in other words, detecting misconfigured access rights before they lead to a data breach or exposure
- Managing inconsistencies between security capabilities across different cloud platforms that host apps that result in diverging security policies
- 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

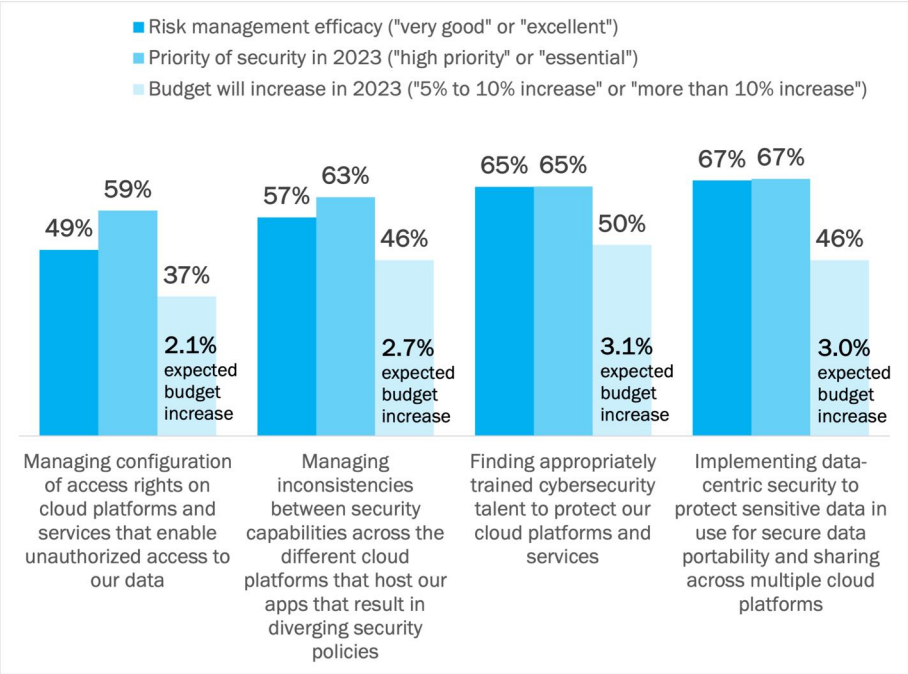
OVERALL CLOUD PRIORITIES IN 2023

Respondents indicated the following risk posture and priorities (see Figure 11):

- Efficacy of managing risks is lowest for managing configuration of access rights (49% indicated “very good” or “excellent”) and highest for implementing data-centric security (67%).
- Priority of security is highest for implementing data-centric security (67%) and lowest for managing configuration of access rights (59%).
- Increased budget for security in 2023 compared to 2022 is the highest for finding trained cybersecurity talent (50%), with an overall net budget change of 3.1%.

When risks are unknown, invisible, or unquantified, it is very difficult to summon the will to act—particularly among those holding budget purse strings.

Figure 11
Overall Investment Priorities in 2023: Cloud
Percentage of respondents



Source: Osterman Research (2023)

CORRELATING RISK POSTURE WITH PRIORITIES AND BUDGET CHANGE

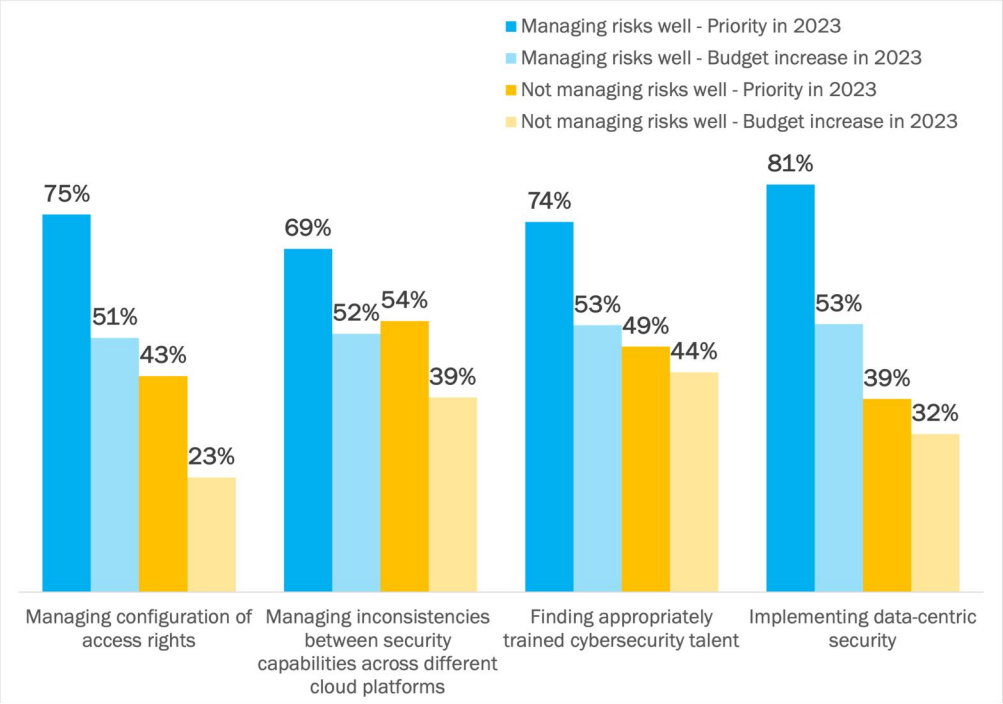
Among organizations with better risk management capabilities, the security priority in 2023 is higher than for organizations lacking strong risk management capabilities. The largest differences are seen with implementing data-centric security (42% difference) and managing configuration of access rights (32% difference). Second, better risk management is linked with a greater intent to allocate more budget to addressing current issues. See Figure 12. These two patterns were also seen in the Apps focus area.

Among organizations that are managing risks well, splitting the ratings changed the relative weighting of the security priority for the first topic (managing configuration of access rights) from last place in the overall ratings to second place below. Better risk management equals better visibility of risk, and risk that is more visible elevates the desire to do the basic principles of access rights better.

The percentage of organizations allocating an increasing budget for each of the four topics evened out among the "managing risks well" cohort after splitting the ratings. Between 51% and 53% of organizations in this cohort plan to spend more across all four topics in 2023. Among those not managing risks well, the intent to spend more is more unevenly distributed (ranging from 23% to 44%), with the highest change going to finding appropriately trained cybersecurity talent.

Too many organizations continue to hire expensive cybersecurity talent and assign them repetitive tasks that would be better done by an automated solution.

Figure 12
Correlating Risk Management with Investment Priorities in 2023: Cloud
Percentage of respondents



Source: Osterman Research (2023)

Only 17% of respondents say their organization is "very good" or "excellent" at managing the business risks for all four topics of managing cloud platforms and services. The majority (83%) have differing capabilities across the four topics.

DISCUSSION ON INVESTMENT PRIORITIES FOR CLOUD

Organizations should lean in the direction of automating as many cloud security tasks as possible. Automation allows calculated predictability and repeatability of process. At organizations without automated approaches, manual effort is required to keep everything working all the time. These efforts are thus more subject to error and are usually more expensive since appropriately trained cybersecurity talent must be hired and retained. Resolution of errors with automated processes requires re-establishing controls and process flow. If there are systematic errors with manual approaches, the only answer is more and better training, which is costly, disruptive, and hard to schedule.

What organizations must spend on finding appropriately trained cybersecurity talent is often significantly more than the outlay required for a solution to automate a given aspect of cloud security. While the two should go hand in glove—great people plus great tools—too many organizations continue to hire expensive cybersecurity talent and assign them repetitive tasks that would be better done by an automated solution. In the early days of a new cloud platform, manual effort is often required to facilitate learning, but cloud has been around for long enough that less reliance on manual effort should be the way forward.

Higher ratings for risk management efficacy drive higher security priority and increased budget. There are a range of cloud security solutions that offer elevated visibility and optics into the state of risks against cloud platforms, including early detection of misconfigured access rights, threat activity, and ongoing assurance that configuration settings are adhering to internal standards and external frameworks. Investing in solutions to drive this visibility leads to a better awareness of the business risks at play, which in turn is likely to drive increased urgency to do something about it. When risks are unknown, invisible, or unquantified, it is very difficult to summon the will to act—particularly among those holding budget purse strings.

We do not have a budget baseline for the four topics explored in the cloud focus area, so the net budget increase must be set in the context of each topic. For example, the baseline budget for cybersecurity talent will be much higher than the baseline budget for managing the configuration of access rights. The two are priced differently, so in turn, the magnitude of the budget increase will also be different.

The top priority for organizations that are managing risks well is different to those not managing risks well:

- **Managing risks well: the priority is data-centric security**
  Implementing data-centric security is a fine-grained security mechanism for protecting data. It reduces the scope for data breach and exposure and is a control that aligns with new and emerging data privacy regulations.
- **Not managing risks well: the priority is managing inconsistencies between security capabilities across different cloud platforms**
  Managing inconsistencies between security capabilities in different cloud platforms is usually about access rights and limitations. This is a coarser-grained security control than data-centric security.

Data-centric security that is 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 a removal of protection when independent security capabilities are used, unlike when cloud-specific protections are embraced.

Data-centric security that is managed independently of the cloud provider ensures secure data portability and secure data sharing irrespective of the cloud in use.

Priorities for Data

Within the Data focus area, we asked about the priority of six topics or issues:

- Discovering where data is stored
- Automatically classifying data, 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., stopping the theft of personally identifiable information, intellectual property, classified information, and other sensitive information
- The ability to restore all data after a cyber incident, such as a ransomware attack that maliciously encrypts files and documents

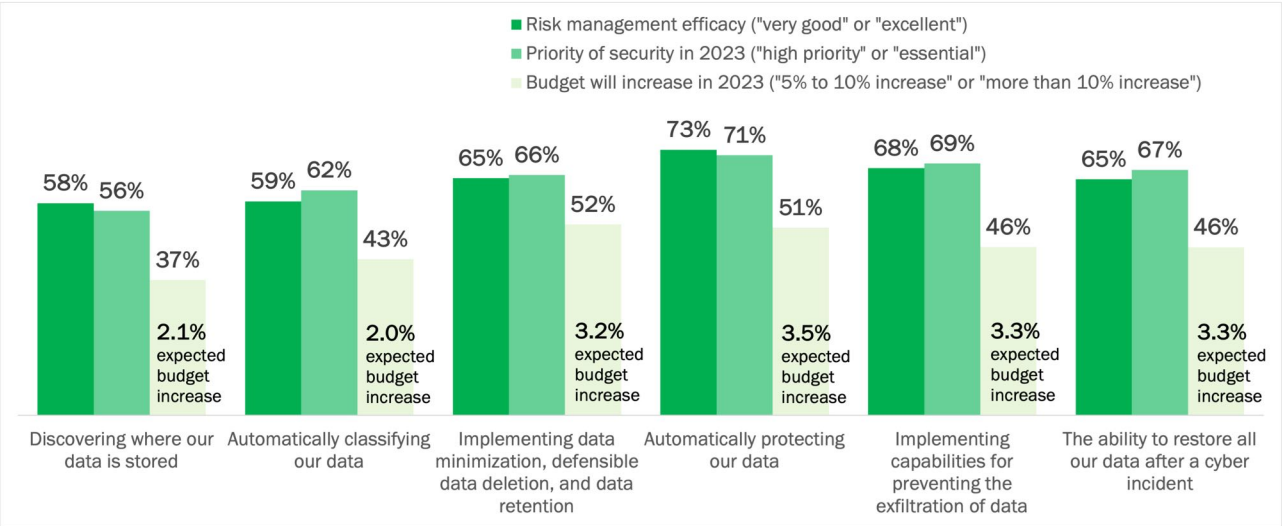
Automatic protection of data through encryption, tokenization, and other methods of obfuscation offers a fast track to meeting compliance regulations and assuring data privacy.

OVERALL DATA PRIORITIES IN 2023

Respondents indicated the following risk posture and priorities (see Figure 13):

- Efficacy of managing risks is lowest for discovering where data is stored (58% indicated “very good” or “excellent”) and highest for automatically protecting data, e.g., with encryption (73%).
- Priority of security is highest for automatically protecting data (71%) and lowest for discovering where data is stored (56%).
- Increased budget for security in 2023 compared to 2022 is highest for implementing data minimization (52%), but the highest overall net budget change belongs to automatically protecting data (3.5% uplift).

Figure 13
Overall Investment Priorities in 2023: Data
Percentage of respondents



Source: Osterman Research (2023)

CORRELATING RISK POSTURE WITH PRIORITIES AND BUDGET CHANGE

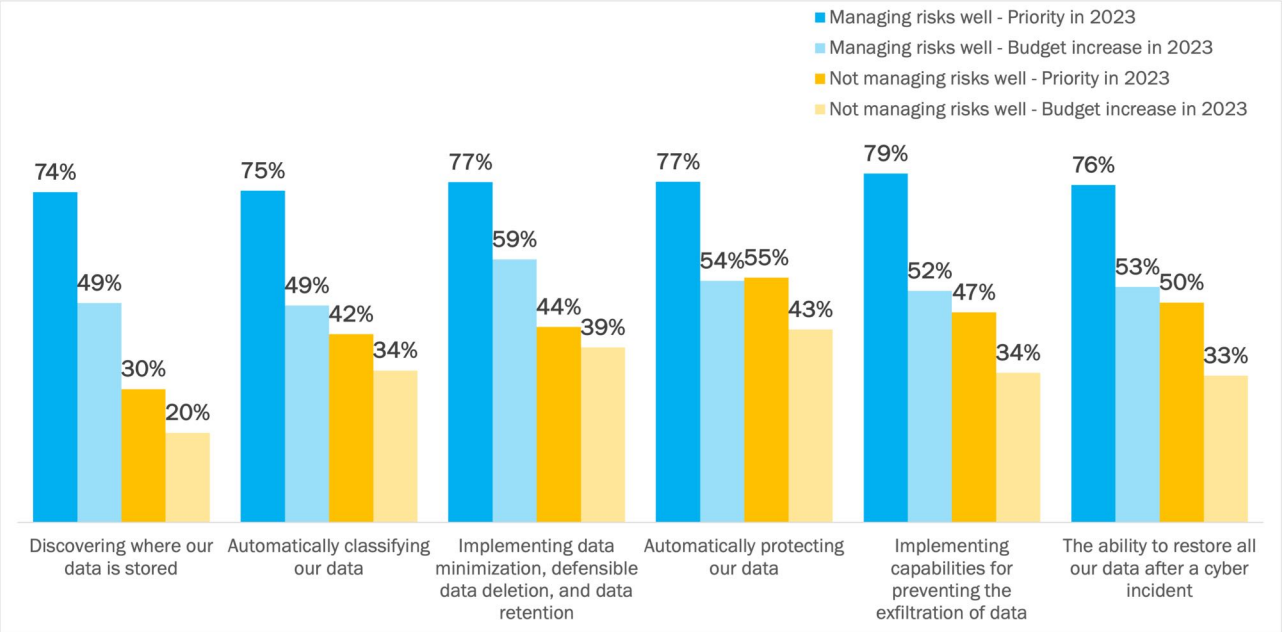
Implementing capabilities for preventing the exfiltration of data is the highest-rated priority for organizations that are managing risks well (79%), up from 69% and second place in the overall analysis. Automatically protecting data drops from first in the overall analysis (71%) to second place in the split analysis (76.7%, ahead of data minimization, defensible data deletion, and data retention by 0.1%), although the percentage of organizations increasing their budget spend in 2023 is highest for data minimization, defensible data deletion, and data retention (59% among organizations managing risks well). See Figure 14.

Splitting the data reduces the variation in priority of security for each of the six topics at organizations that are managing risks well, with the highest at 79% and the lowest at 74%. In the overall analysis, the variation runs from 71% to a low of 56%.

Organizations that are not managing risks well place the highest priority on the ability to automatically protect data (55%), followed by the ability to restore data after a cyber incident (50%). Data discovery (30%) and automatic data classification (42%) are rated as the two least important areas for this cohort, giving the sense of opting for automatic data protection to negate the need for discrete discovery and classification tasks. How well that works with escalating regulatory demands for data privacy remains to be seen, but at this juncture, it appears a risky strategy.

Data minimization and defensible data deletion reduce the volume of data stored and processed, and by implication the volume of potential data that can be breached or exposed through any means.

Figure 14
Correlating Risk Management with Investment Priorities in 2023: Data
Percentage of respondents



Source: Osterman Research (2023)

Only 17% of respondents say their organization is “very good” or “excellent” at managing the business risks for the six aspects of managing data we asked about. The majority (83%) lack unified and consistent risk management approaches across all six.

DISCUSSION ON INVESTMENT PRIORITIES FOR DATA

In the overall analysis, automatically protecting data is the highest priority for organizations (71%), as well as the topic with the highest net budget change in 2023 compared to 2022. In the split analysis, it is the second-highest rated priority among organizations that are good at managing the business risks of data, and the highest among those that are not. Automatic protection of data through encryption, tokenization, and other methods of obfuscation offers a fast track to meeting compliance regulations and assuring data privacy—which was the top-rated trend or challenge driving how organizations are approaching cybersecurity in 2023 (see Figure 3 on page 5).

Preventing the exfiltration of data is the other side of the automatically protecting data coin. Anti-data exfiltration offers the same fast track to meeting compliance regulations and assuring data privacy. Automatic protection means that data is protected from unauthorized access when it is under the control of the organization. Automatic protection also renders exfiltrated data unreadable in the case of a data breach or exposure (thus reducing the severity of data breach notification processes) and unusable for extortion (thus significantly reducing the threat of modern ransomware attacks). Preventing data exfiltration adds a complementary level of protection when data is already protected through encryption, and in cases when encryption for protection is not used, it provides an alternative method for stopping data breach, exposure, and extortion avenues. All organizations should do both but must do at least one very well.

Data minimization, defensible data deletion, and data retention provide structured ways of reducing the volume of data collected and retained, thereby embracing privacy-by-design mandates. When data must be retained to meet compliance, legal, and internal requirements, data retention offers an automated approach for keeping what is required for the specified timeframe and then deleting it. Data minimization and defensible data deletion have the effect of reducing the volume of data stored and processed, and thus the volume of potential data that can be breached or exposed through any means (while also supporting environmental and sustainability imperatives through reduced energy and carbon usage). Not capturing or retaining what is not essential means that that data can never be breached. The highest number of organizations in both the overall analysis (52% in Figure 13) and for organizations that are currently managing the risks of data well (59% in Figure 14) indicate that budget allocated to these areas will increase in 2023 compared to 2022.

The ability to restore all data after a cyber incident, such as a ransomware attack, is the third highest–rated topic in the overall analysis in both priority and expected budget increase (the latter at 3.26%, just 0.01% behind second place of anti-data exfiltration at 3.27%). Automatically protecting data through encryption and anti-data exfiltration provide pre-attack protection mechanisms, but when cyber defenses fail and an incident happens, being able to recover quickly, fully, and at minimum cost becomes the holy grail. While organizations must strengthen protections and defenses against attack, losing sight of the equivalent mandate for preparedness and resilience to recover is only asking for trouble.

The underlying capabilities of data discovery and automatic classification are rated in the last two places for both sides of the split data, although among those managing risks well, the margin between the other topics is very small. Overall, one way to interpret this is that organizations have less interest in these as standalone and isolated capabilities. Discovery for the sake of discovery is not enough, nor is classification for the sake of classification.

While organizations must strengthen protections and defenses against attack, losing sight of the equivalent mandate for preparedness and resilience to recover is only asking for trouble.

Priorities for On-Premises Infrastructure

In the focus area of on-premises Infrastructure, we asked about the following four topics:

- The ability to recover from a cyber incident against on-premises infrastructure and return to normal business operations
- Managing challenges with integrating new security technologies into legacy on-premises infrastructure
- Finding appropriately trained cybersecurity talent to protect on-premises infrastructure
- The likelihood of non-compliance with data privacy regulations due to immature data protection approaches in on-premises infrastructure

OVERALL ON-PREMISES PRIORITIES IN 2023

Respondents indicated the following risk posture and priorities (see Figure 15):

- Efficacy of managing risks is lowest for recovering after a cyber incident against on-premises infrastructure (58% indicated “very good” or “excellent”) and highest for finding appropriately trained cybersecurity talent (67%).
- Priority of security is highest for non-compliance with data privacy regulations (69%). It is lowest for recovering after a cyber incident against on-premises infrastructure and the challenge of integrating new security technologies into legacy on-premises infrastructure (tied for third at 62%).
- Increased budget for security in 2023 compared to 2022 is highest for finding appropriately trained cybersecurity talent (55%), with an overall net budget change of 3.4%.

Finding and retaining the right people with the right skills is essential for any organization reliant on on-premises infrastructure.

Figure 15
Overall Investment Priorities in 2023: On-Premises Infrastructure
Percentage of respondents

Source: Osterman Research (2023)

CORRELATING RISK POSTURE WITH PRIORITIES AND BUDGET CHANGE

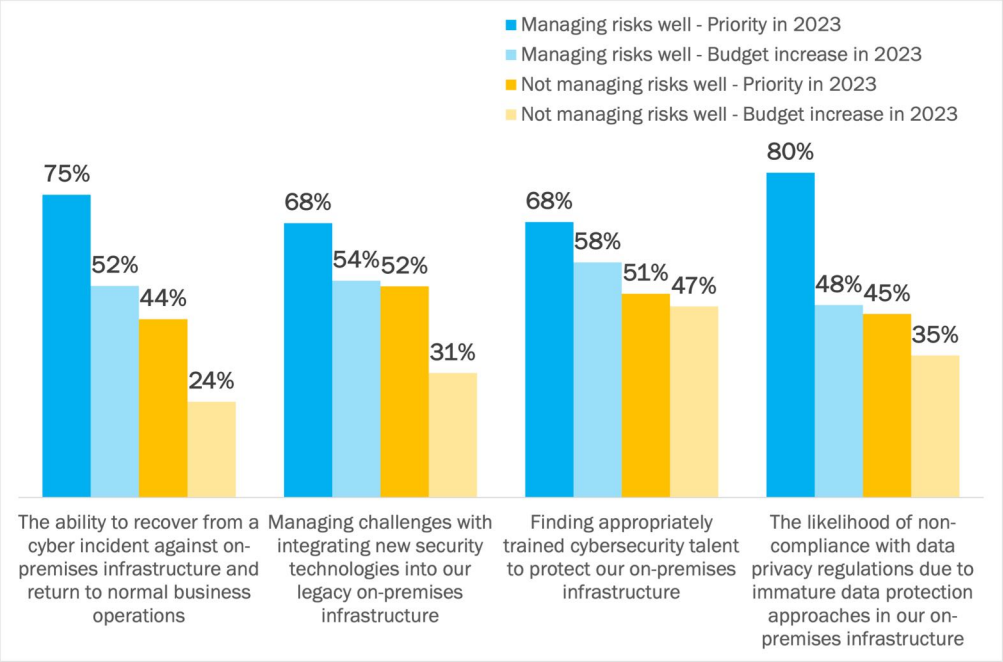
Correlating risk management with security priorities and budget change presents two different pictures for organizations managing risks well and those that are not. For those managing risks well, the highest priority issues are non-compliance with data privacy regulations (80%) and recovery after a cyber incident (75%). These are higher-order and more advanced issues surrounding on-premises infrastructure. For organizations not managing risks well, managing challenges with integrating new security technologies into legacy on-premises infrastructure comes first (52%), followed closely by finding appropriately trained cybersecurity talent to protect on-premises infrastructure (51%). Organizations in this cohort continue to struggle with the technical and staffing requirements of an on-premises approach. See Figure 16.

In all cases—for the overall analysis (55%), for the cohort of organizations managing risks well (58%), and for the cohort not managing risks well (47%)—the area with the highest budget increase in 2023 compared to 2022 is cybersecurity talent. Finding and retaining the right people with the right skills is essential for any organization with ongoing reliance on on-premises infrastructure.

In Figure 16, the difference in ranking for the non-compliance issue is striking. It is the top-rated priority among organizations managing risks well (80%), but almost the last-equal priority among organizations not managing risks well (45%). Clarity and current competence drive the awareness of the compliance obligation. Lack of clarity and low current competence with on-premises infrastructure obfuscates it.

Most organizations must manage a hybrid combination of multiple cloud platforms and on-premises infrastructure.

Figure 16
Correlating Risk Management with Investment Priorities in 2023: On-Premises
Percentage of respondents



Source: Osterman Research (2023)

Only 21% of respondents say their organization is “very good” or “excellent” at managing the business risks for the four aspects of managing on-premises infrastructure. The majority (79%) have a mix of approaches.

DISCUSSION ON INVESTMENT PRIORITIES FOR ON-PREMISES

The top-rated security priority in the overall analysis (67%) and among the cohort of organizations that are managing the business risks of on-premises infrastructure well (80%) is the likelihood of non-compliance with data privacy regulations due to immature data protection approaches. This emphasis aligns with the top-rated trend and challenge driving how organizations are approaching cybersecurity in 2023—that of escalating regulatory demands for cybersecurity and data privacy (see Figure 3). These demands are blind to delivery mechanism and infrastructure context; organizations don't get a free pass just because they have workloads that are not in the cloud. Organizations continuing to run workloads using on-premises infrastructure face two significant challenges in addressing compliance at this point:

1. **Lack of digital transformation**
   Organizations have missed out on the digital transformation activities that go along with migrating workloads to the cloud—unless the migration was simply lift-and-shift of workloads.
2. **Very old infrastructure and applications**
   Organizations have legacy infrastructure and applications to contend with, much of which was created decades before data privacy regulations became a thing. The access and data controls, along with the nuances needed for least privilege, data masking, and field-level encryption, are often missing in legacy infrastructure and applications.

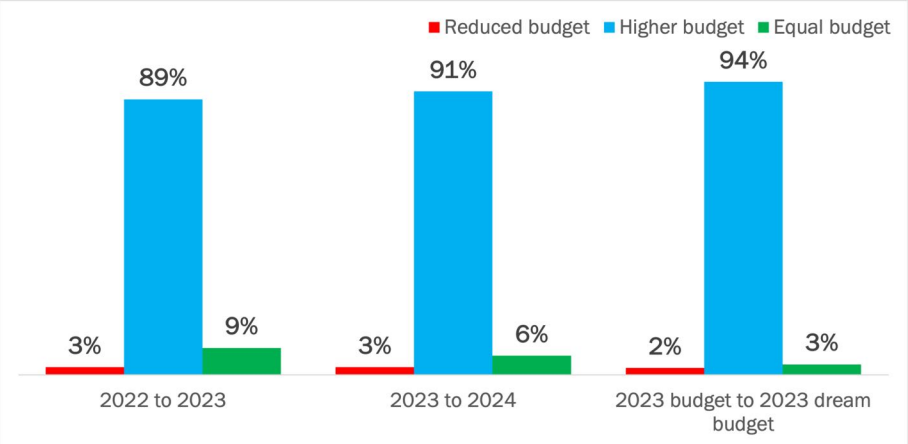
Few organizations are at the extremes of cloud vs. on-premises. Some organizations are cloud-only or cloud-native, and some are exclusively on-premises, but the vast majority are somewhere in between. All such organizations must manage a hybrid combination of multiple cloud platforms and on-premises infrastructure. In the context of this research, they must wrestle with the security challenges profiled in both the cloud and on-premises focus areas.

Escalating regulatory demands are blind to delivery mechanism; organizations don't get a free pass just because they have workloads that are not in the cloud.

Budget Outlook

The budget for cybersecurity increased from 2022 to 2023 at 89% of organizations and is expected to increase from 2023 to 2024 at 91% of organizations. Almost all respondents said their dream budget for 2023 is higher than their actual budget for 2023. Across all respondents, budgets have increased 11% from 2022 to 2023, and are expected to increase 19% from 2023 to 2024. See Figure 17.

Figure 17
Year-on-Year Budget Changes for Cybersecurity
Percentage of respondents

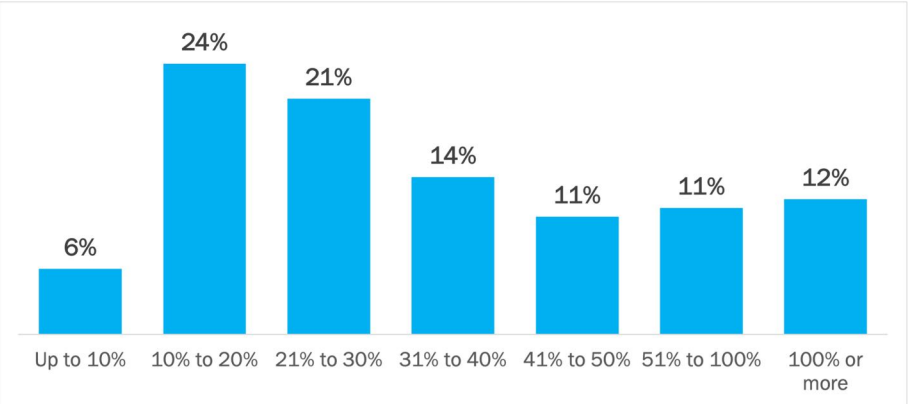


Source: Osterman Research (2023)

We asked respondents what their dream or ideal total budget for cybersecurity in 2023 would be, assuming they could put every dollar to productive and effective use. Ninety-four percent of respondents said their dream or ideal budget would be higher than their actual budget for 2023, with an overall median increase of 30%. The average increase is 97%—in other words, twice as much budget—but this number is significantly skewed by the respondents who wanted three to five times the amount of their 2023 budget. Figure 18 presents a distribution of budget increases across seven ranges to reduce the effect of outliers skewing the data.

Ninety-four percent of respondents said their dream or ideal budget in 2023 would be higher than their actual budget for 2023.

Figure 18
Distribution of Actual Budget 2023 vs. Dream Budget 2023 Ranges
Percentage of respondents with a higher dream budget (n=254)



Source: Osterman Research (2023)

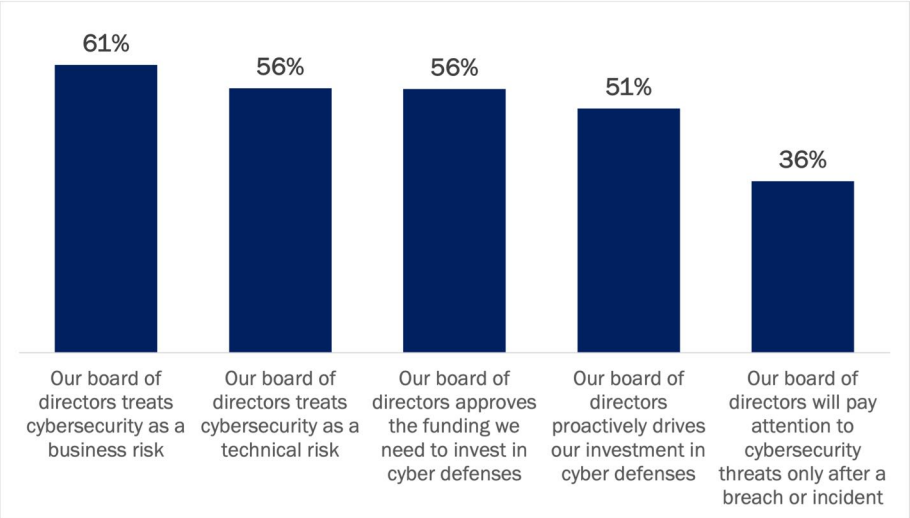
Organizational Issues

In this section, we look at the impact of the board of directors on cybersecurity approaches, reporting lines for CISOs and CIOs, and how CISOs and CIOs assess the criticality of cybersecurity.

THE BOARD OF DIRECTORS HAS A SIGNIFICANT IMPACT ON CYBERSECURITY APPROACHES

At more than half of organizations, the board of directors treats cybersecurity as a business risk (61%) and a technical risk (56%) and approves the funding needed to invest in cyber defenses (56%). At more than a third of organizations, however, the board of directors will pay attention to cybersecurity threats only after a data breach or incident. See Figure 19.

Figure 19
Board of Directors on Cybersecurity
Percentage of respondents indicating "agree" or "strongly agree"



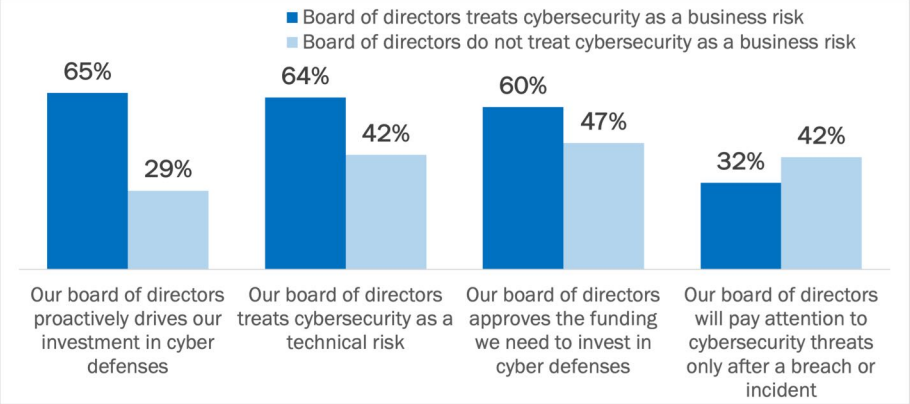
Source: Osterman Research (2023)

Cybersecurity is both a business risk and a technical risk, but more boards assign primacy to the business risk view.

The board of directors' stance on cybersecurity has significant flow-on impacts:

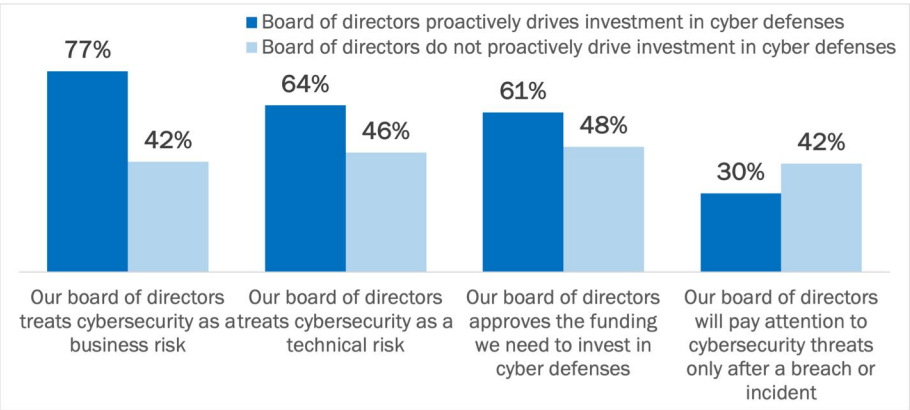
- **Treating cybersecurity as a business risk**
  Among organizations where the board treats cybersecurity as a business risk, there is greater proclivity toward proactive investment, concern with technical risks, and approval of funding. In addition, fewer take a reactive approach to cybersecurity threats. See Figure 20.
- **Proactively driving investment in cyber defenses**
  The same pattern of outcomes is evident among organizations where the board proactively drives investment in cyber defenses. Treating cybersecurity as a business risk, concern with technical risks, and approval of funding are all higher, and reactivity is lower. See Figure 21.
- **Paying attention to cybersecurity only after a breach or incident**
  At organizations where the board only pays attention to cybersecurity threats after a breach or incident, there is greater proclivity to view cybersecurity as a technical risk and to approve budget funding only grudgingly. See Figure 22.

Figure 20
Board of Directors on Cybersecurity: The Business Risk Pivot
Percentage of respondents indicating "agree" or "strongly agree"



Source: Osterman Research (2023)

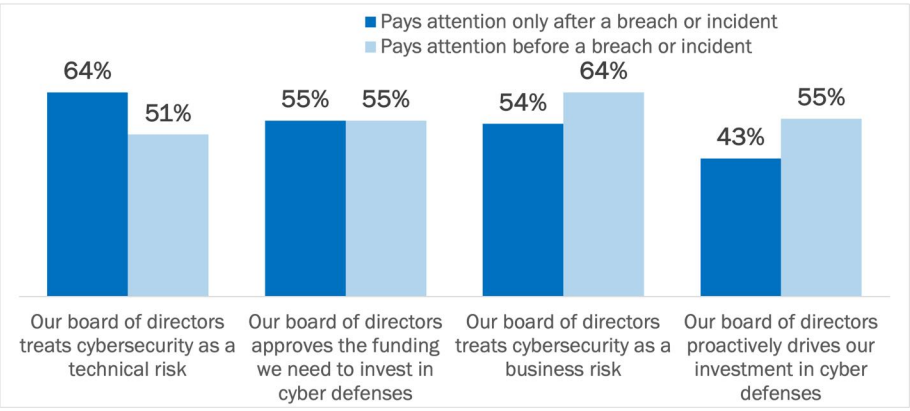
Figure 21
Board of Directors on Cybersecurity: The Proactive Investment Pivot
Percentage of respondents indicating "agree" or "strongly agree"



Source: Osterman Research (2023)

Boards that treat cybersecurity as a business risk are more likely to make proactive investments, evaluate technical risks, and approve funding.

Figure 22
Board of Directors on Cybersecurity: The Paying Attention Pivot
Percentage of respondents indicating "agree" or "strongly agree"

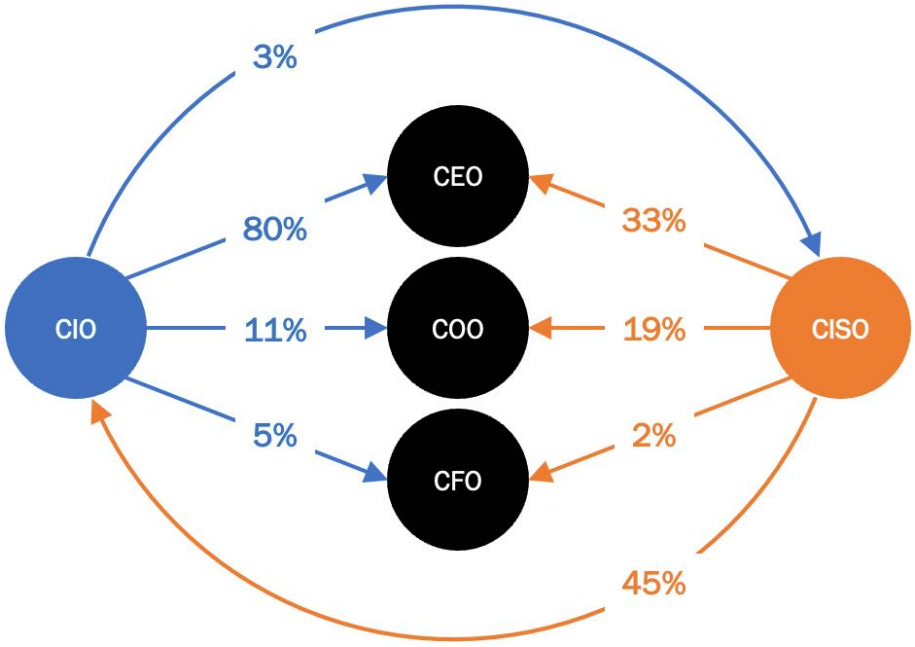


Source: Osterman Research (2023)

REPORTING LINES FOR CISOs AND CIOs

Most CIOs report directly to the CEO (80%), followed by reporting to the COO (11%). By contrast, most CISOs report to the CIO (45%), followed by a direct reporting line to the CEO (33%). Reporting to the CFO is the least commonly occurring pattern for the organizations in this research (5% for CIOs, and 2% for CISOs). See Figure 23.

Figure 23
Reporting Lines: CISOs and CIOs
Percentage of respondents



Source: Osterman Research (2023)

With respect to reporting lines:

- **For CISO: from CIO to the CEO, as cybersecurity is increasingly a business issue**
  Reporting to the CIO is the traditional reporting line for CISOs. But for one third of organizations, the CISO now reports directly to the CEO, indicating the maturation of cybersecurity as a business risk on one hand and a business priority on the other. Getting cybersecurity wrong is becoming a costly business and regulatory issue of high concern to the CEO and board of directors, not just a matter of downtime that can be dealt with solely as a technical issue.
- **For CIO: a small number report directly to the CISO**
  The majority of CIOs report to CEOs (80%), although this is the expected pattern. What is interesting—even though it's the least commonly occurring pattern for CIOs—is the 3% of CIOs that report to the CISO. Reporting to the CISO makes a strong organizational statement that security is core and central to IT, not an afterthought.
- **For both CISOs and CIOs: minority report to COO or CFO**
  16% of CIOs and 21% of CISOs report to the COO or CFO, roles that take responsibility for the internal operations of the organization and its financial management. As IT and security become core to external operations, customer engagement, and organizational performance, however, these reporting lines no longer make sense.

One third of CISOs report directly to the CEO, indicating the maturation of cybersecurity as a business risk and priority.

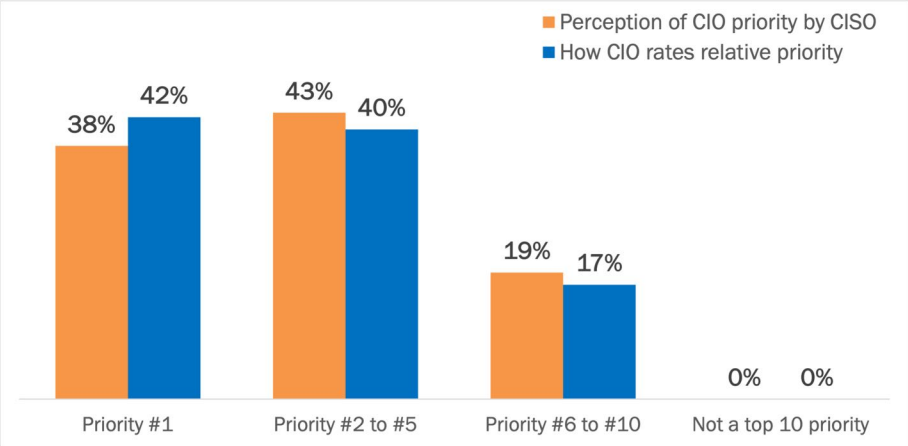
CRITICALITY OF CYBERSECURITY TO THE CIO

CISOs and CIOs are closely aligned in how the CIO assesses the level of priority of cybersecurity relative to all other IT initiatives at their organization (which was an undefined list, but would include initiatives such as cloud migration, zero trust, modernization, and building new channels for customer engagement). We asked the CISO respondents to the survey for their opinion on how their CIO ranks the priority of cybersecurity, and we asked the CIO respondents for their rating of priority. The results are shown in Figure 24:

- **More CIOs indicate "Priority #1" than CISOs believe to be the case**
  Around 10% more CIOs say that cybersecurity is their top overall priority compared with CISOs who believe their CIO ranks cybersecurity in first place. Given what is at stake from ineffective cybersecurity protections and recovery mechanisms, this level of prioritization by the CIO is not surprising. At some organizations, therefore, the CISOs should stop underplaying their work and contribution to the success of the organization.
- **CIOs are taking lead from the board of directors**
  At organizations where the CIO's priority on cybersecurity is priority #6 to #10, the board of directors is 26% more likely to pay attention to cybersecurity threats only after a breach or incident and 25% less likely to treat cybersecurity as a business risk.
- **Cybersecurity is a top 10 priority at all organizations**
  No CISOs or CIOs indicated that cybersecurity is less than a top 10 priority relative to all other IT initiatives. Any CISO or CIO who holds that view is unlikely to remain in their role for very long.

More CIOs view cybersecurity as their #1 priority than CISOs believe to be the case.

Figure 24
Relative Priority of Cybersecurity to the CIO
Percentage of respondents



Source: Osterman Research (2023)

Conclusion

The top investment priorities in cybersecurity for CISOs and CIOs in 2023 focus on cloud security, ransomware protections, and improving underlying data disciplines such as discovery and classification. CISOs and CIOs also indicate a range of specific priorities within the areas of apps, cloud platforms, data, and on-premises infrastructure, and are assigning budget accordingly. The results in this white paper present a snapshot of priorities across a representative sample of organizations in the United States, but the priorities for any given organization must be set within the context of their current posture and areas of concern.

Decision-makers and influencers on cybersecurity should keep the following three principles in view as priorities are acted out in 2023:

- **Approach protection across the lifecycle, not merely pre-breach**
  Strengthening cybersecurity protections to prevent or counteract an attack is essential, along with the optics and visibility to detect new and emerging threats. Organizations ignore these steps at their peril. At the same time, since the arms race against bad actors is never-ending, organizations must strengthen their ability to recover quickly and completely from successful incidents. Cyber insurance won't cover it anymore.
- **Improve the efficacy of managing the business risks of cybersecurity**
  With 61% of boards treating cybersecurity as a business risk, CISOs and CIOs must ensure they have the systematic ability to capture, identify, and manage the business risks of cybersecurity. In each of the four specific focus areas explored in this research, organizations with better business risk management efficacy always prioritized security and budget higher compared to organizations with lower efficacy. In other words, sort out optics and visibility, and action is highly likely to follow. Escalating regulatory demands for cybersecurity and data privacy view a lack of business risk management as a sign of deliberate negligence, not an exemption.
- **Counteract the cybersecurity skills shortage**
  The organizations in this research signaled a clear increase in the priority of cybersecurity and its associated budget allocations. This intent, however, will be undermined if organizations are hampered by the inability to hire and retain cybersecurity professionals, and if the professionals they do have are assigned menial security tasks such as triangulating alerts and running inefficient incident response processes. Moving beyond current well-known but ineffective cybersecurity solutions requires professionals having time to explore, experiment, and embrace what they currently do not know.

Escalating regulatory demands for cybersecurity and data privacy view a lack of business risk management as a sign of deliberate negligence, not an exemption.

Sponsored by Quest

Quest solutions work together to protect your hybrid Active Directory (AD) environment and manage risk. Our software allows customers to align their AD security controls to the NIST framework and compliance requirements, thus increasing cyber resiliency while mitigating gaps that bad actors can exploit. Quest helps enterprises discover and eliminate potential attack paths, identify risky changes, control group policy chaos, and quickly recover from AD disasters like ransomware. And we've been conquering What's Next in the Microsoft platform management market for two decades. We are the Active Directory leaders, and we have been since our Microsoft story first started in 2000.

Learn more at www.quest.com.

www.quest.com

@Quest

+1 800 306 9329

Methodology

This white paper is based on findings from a survey conducted by Osterman Research. Two hundred eighty-four (284) respondents in CISO and CIO roles were surveyed during December 2022 and January 2023. 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 equivalent role)	42.6%
CIO (or equivalent role)	57.4%

INDUSTRY

Agriculture, Forestry, Mining	3.2%
Chemicals	0.4%
Computer Hardware or Computer Software	9.2%
Data Infrastructure, Telecom	7.0%
Education	7.7%
Energy, Utilities	5.6%
Financial Services	8.8%
Healthcare	8.1%
Hospitality, Food, Leisure Travel	5.6%
Industrials (Manufacturing, Construction, etc.)	8.8%
Life Sciences	4.2%
Media, Creative Industries	3.9%
Professional Services (Law, Consulting, etc.)	10.6%
Public Service, Social Service	4.2%
Retail / eCommerce	5.3%
Safety and Environmental Support	0.4%
Transport, Logistics	7.0%

[1] Osterman Research, Ransomware Attacks: Strategies for Prevention and Recovery, October 2022, at https://ostermanresearch.com/2022/10/14/orwp_0355/