# HEALTHCARE CISOs:

## *A Deep Dive into Talent & Leadership Trends*

2023 – 2024 WittKieffer
CISO Executive Survey Results

WittKieffer

# TABLE OF CONTENTS

WittKieffer conducted a comprehensive survey of healthcare Chief Information Security Officers (CISOs) to explore the role, scope, and compensation of these leaders.

To enrich the survey findings, we also carried out proprietary research on the career paths of CISOs at the top 100 health systems nationwide.


# HEALTHCARE CISO DEEP DIVE

## THREE DISTINCT PHENOTYPES

- **Hybrids (approx. 55%):** Information security professionals who gained experience in other sectors (e.g., in technology, financial services, IT consulting) and transitioned into healthcare, eventually becoming CISOs.
- **Recent healthcare "transplants" (approx. 30%):** Leaders who transitioned directly from another industry (mainly technology) into a CISO role at a health system.
- **Healthcare natives (approx. 15%):** Those who joined healthcare very early in their careers and cultivated their expertise within IT departments of healthcare organizations.

## HIRING TRENDS

- Most current health system CISOs (61%) have been **recruited externally** rather than hired from within their organizations.
- There is **significant leadership turnover** among health system CISOs: 42% of CISOs were appointed within the last three years. Notably, we observe a trend toward **attracting experienced "chiefs"** (52% of recently appointed CISOs have held a similar position before), indicating access to a more experienced talent pool and a preference for a low-risk approach.
- Over half (52%) of healthcare CISOs are within the **base salary range of $301k and above**.

## TALENT FORCES

- A notable shift in the working model emerged, with a significant 61% of CISOs expressing a **preference for remote work**, opting to be onsite only on rare occasions in their next roles (vs. hybrid and onsite scenarios).
- In most cases, the **reporting line is still to a CIO** (70% of respondents), but we observe a rise in alternative reporting structures (e.g., reporting lines to a COO, Legal, and even a CEO).
- Over 60% of the respondents face **challenges in recruiting and developing their teams**, and almost 50% indicate challenges related to talent retention.

# CISO PHENOTYPES

The Chief Information Security Officer (CISO) role is a relatively recent addition to the healthcare sector, and its path to attainment lacks a conventional trajectory. Our examination of the career paths of sitting CISOs unveiled three discernible patterns.

A majority (55%) of CISOs at leading health systems fall into the "hybrid" category—professionals who cultivated their information security expertise in different industries before transitioning to the information security department of a healthcare organization. Another notable group comprises "recent healthcare transplants" (30%)—seasoned professionals who transferred directly into the top information security role at a healthcare organization after amassing significant experience in another industry, often technology-related. A smaller proportion, less than a fifth (15%), are "healthcare natives" who embarked on their careers in healthcare organizations, steadily ascending through the ranks to attain their CISO expertise.

While approximately a third of healthcare CISOs have a graduate degree, most leaders in this field rely heavily on accumulated job experience and on-the-job training. It remains unclear how an expanding landscape of formalized training and educational opportunities in information security will affect the future trajectory of CISO roles within the healthcare sector.

### HYBRIDS (APPROX. 55%)

Information security professionals who gained experience in other sectors (e.g., in technology, financial services, IT consulting) and transitioned into healthcare, eventually becoming CISOs.

### RECENT HEALTHCARE “TRANSPLANTS” (APPROX. 30%)

Leaders who transitioned directly from another industry (mainly technology) into a CISO role at a health system.

### HEALTHCARE NATIVES (APPROX. 15%)

Those who joined healthcare very early in their careers and cultivated their expertise within IT departments of healthcare organizations.

## ROUTE TO THE TOP

### Academic background


### Immediate prior industry

**72%** Healthcare

**8%** Technology

**20%** Other
(education, government, financial services, transportation, retail, consumer goods and services, etc.)

Source: WittKieffer’s proprietary research on the career paths of 100 CISOs at leading health systems, 2023

# HIRING TRENDS

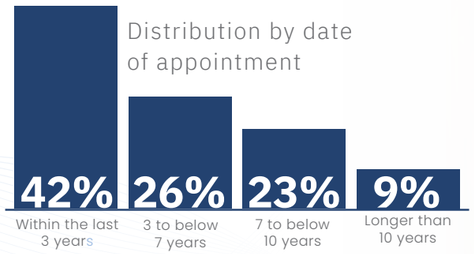
## Past Role & Tenure

A majority of CISOs at leading health systems (61%) were appointed from outside of the organization, rather than receiving internal training and promotion. CISO turnover is notably high, with 42% having been appointed within the past three years. More than half (51%) had immediate past roles as a CISO, CIO, or CTO, suggesting healthcare executives and boards recognized the increased importance information security posed to their organizations and responded by hiring "experienced chiefs."

While this low-risk approach may be an appropriate strategic response to fortify an organization's security practices swiftly, leadership should not overlook the value of developing internal talent and "building a bench" of internal successors in this area. Long-term institutional knowledge is crucial for an information security leader, as it enables them to make informed decisions aligned with the organization's unique context, culture, and technology landscape. This deep understanding facilitates the development and implementation of effective security strategies and fosters strong relationships with key stakeholders. Leadership should prioritize developing individuals who combine institutional knowledge with a willingness to adapt, be agile, and evolve to address the dynamic nature of information security.

### Current Position

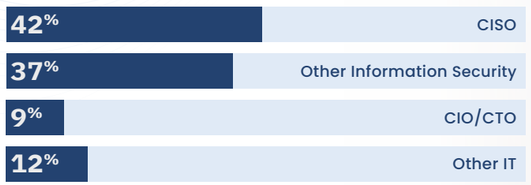
**5.3Y**
Tenure in current position




EXTERNAL APPOINTMENTS
**61%**

**39%**
INTERNAL PROMOTIONS

### Immediate Prior Role



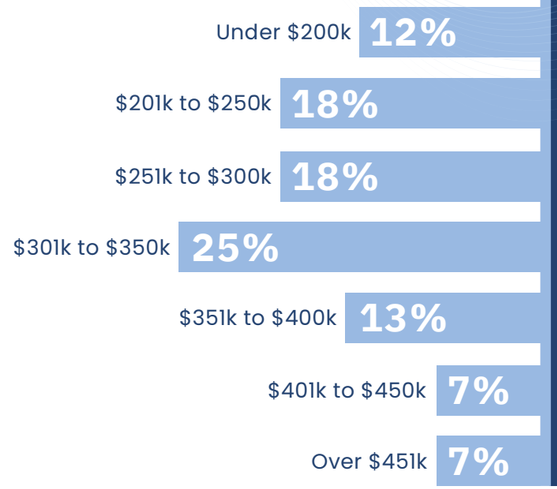

Source: WittKieffer's proprietary research on the career paths of 100 CISOs at leading health systems, 2023

# HIRING TRENDS Compensation

A significant majority of surveyed CISOs disclosed base salaries surpassing $250,000 per annum, with the prevalent pay range falling within $300,000 to $350,000 per year. While the majority (89%) experienced incremental raises in their base pay, typically within the range of 5% or less, a noteworthy 43% affirmed eligibility for bonuses ranging from 11% to 20% of their annual salary.

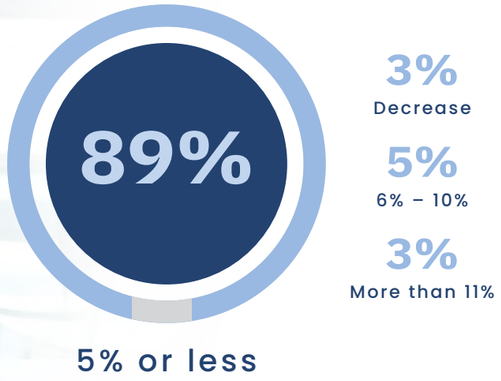
This trend suggests that, beyond the recruitment of seasoned professionals for CISO roles, numerous institutions actively incentivize exemplary performance by CISOs and their steadfast safeguarding of company information through the provision of performance-based bonuses. This dual approach reflects a strategic alignment of competitive compensation structures with the imperative to attract and retain top-tier cybersecurity leadership.

## What is your current 2023 base salary?*

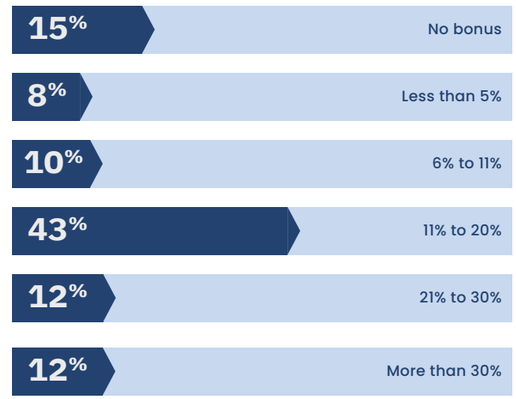



CISOs changing employers in the past year indicated that the move had minimal impact on their total compensation, with the majority experiencing an **increase of less than 10%**. This suggests that factors beyond financial considerations, such as work location flexibility and autonomy, significantly influence their decision to change positions.

## What was the percentage increase in your 2023 base salary from 2022?*




## If you are eligible for a bonus, what percentage of your salary is it?*




*CISO responses only

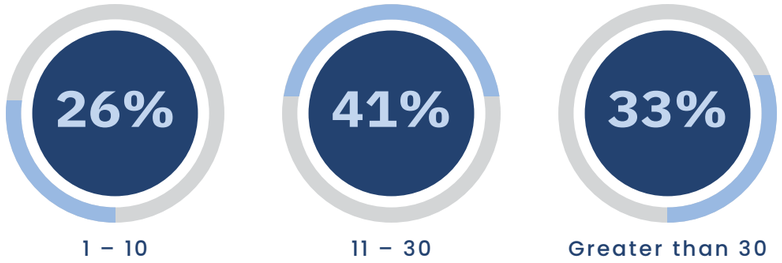
# HIRING TRENDS

## Building a Team

A substantial majority (74%) of CISOs at health systems oversee teams consisting of more than 10 full-time employees. This statistic underscores the significant investment that healthcare organizations are making in bolstering their information security functions. Our findings suggest that many of them face challenges related to underdevelopment and the ongoing struggle to attract and retain talent.

In the current landscape, where numerous organizations are actively expanding their information security functions, it is imperative that leaders proactively address these challenges. This necessitates a concerted effort to offer competitive compensation packages and provide work location flexibility. Moreover, leaders must articulate clear pathways for professional development and avenues for career advancement. Ensuring that CISOs can build and lead a top-notch team is paramount in fortifying the organization's overall cybersecurity position. By strategically addressing talent-related challenges, healthcare leaders can foster an environment conducive to the growth and success of their information security teams.

### What is the total FTE (full-time employee) count on your staff (excluding contractors)?




### What talent-related challenges does your team currently face?

# TALENT FORCES

## Remote Work

A prominent trend observed among the surveyed CISOs was the increasing prevalence of remote work within this leadership cohort. A noteworthy majority (55%) expressed infrequent onsite presence, typically occurring quarterly or every few weeks. Additionally, 61% identified the ability to work remotely as a pivotal factor in considering their next professional role.

While there may be a perception that a key organizational figure such as a CISO should maintain a more regular onsite presence, it is imperative to contextualize this within the work settings of their teams. A substantial 61% reported that their teams operate entirely in a remote capacity with occasional onsite visits, with a mere 6% managing entirely onsite teams. Recognizing these dynamics, organizational leadership must acknowledge the evolving landscape of work preferences within the information security domain. Embracing a degree of flexibility in work location is paramount to attracting and retaining top-tier talent in this space. This strategic approach aligns with the broader industry shift toward flexible work arrangements and enhances the organization's capacity to recruit the best information security leaders.

### Where are your teams currently situated?

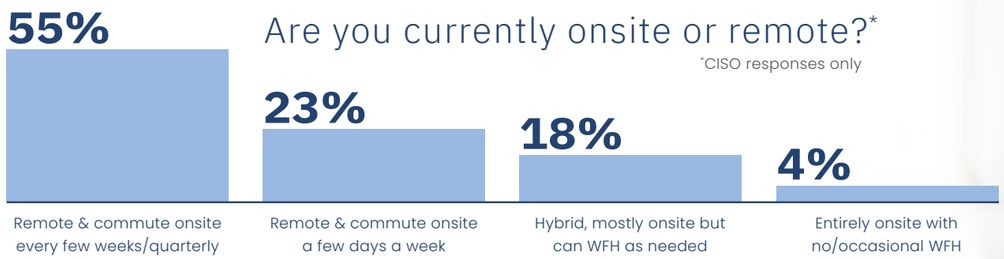
**61%** Entirely Remote

**33%** Partially Remote

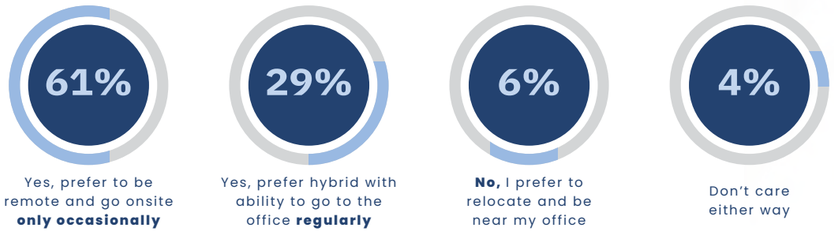
**6%** Entirely Onsite

### Are you currently onsite or remote?*

*CISO responses only




### Will the ability to be remote be important in your next role?

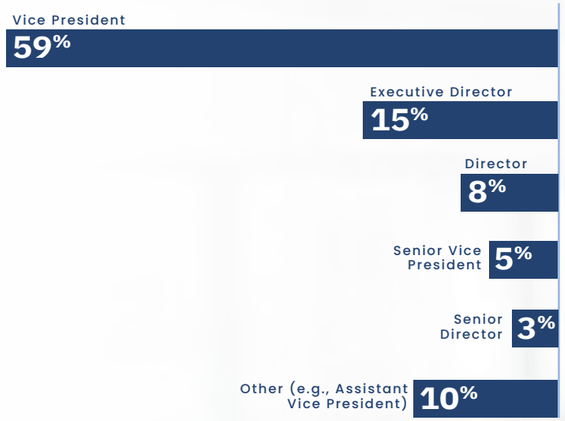


# TALENT FORCES
## Reporting Lines

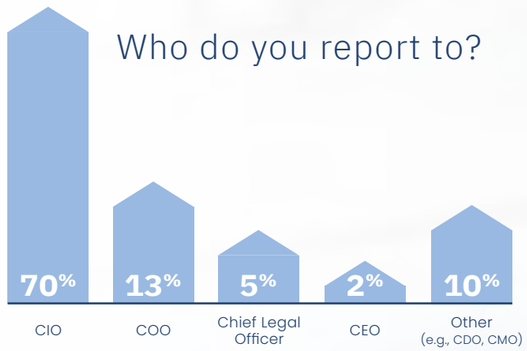
Typically designated as vice presidents of information security, healthcare CISOs exhibit a distinct reporting pattern, with a higher likelihood of reporting to a chief information officer (CIO) and a lesser likelihood of reporting to a chief operating officer (COO) or chief legal officer. This trend may be indicative of the relatively recent establishment of formalized information security teams within healthcare organizations. As CISOs and their security protocols become more deeply integrated into the organizational framework, the potential for conflicts of interest may necessitate a reevaluation of reporting structures to ensure the protocols remain independent and unbiased. This may call for aligning them more closely with operational leadership, such as the COO, chief legal officer, or even the chief executive officer (CEO).

While reporting to top executives endows CISOs with heightened strategic influence and unit autonomy, a potential downside lies in the risk of creating disconnections with the Information Technology (IT) department, if not managed judiciously. Striking a delicate balance is imperative, wherein CISOs are granted the latitude to shape strategy while concurrently collaborating closely with IT. This collaborative approach ensures the seamless integration of security measures and a thorough understanding of specific technology-related risks, optimizing the effectiveness of cybersecurity efforts within the organization.

### What is the level of your role?*




### Who do you report to?




### Reporting Structure Across Industries

| 54% | 12% | 2% | 5% | 27% |
|---|---|---|---|---|
| | | | | (e.g., Risk, CFO, Global CISO) |

Heidrick & Struggles, Global CISO Survey, 2023.

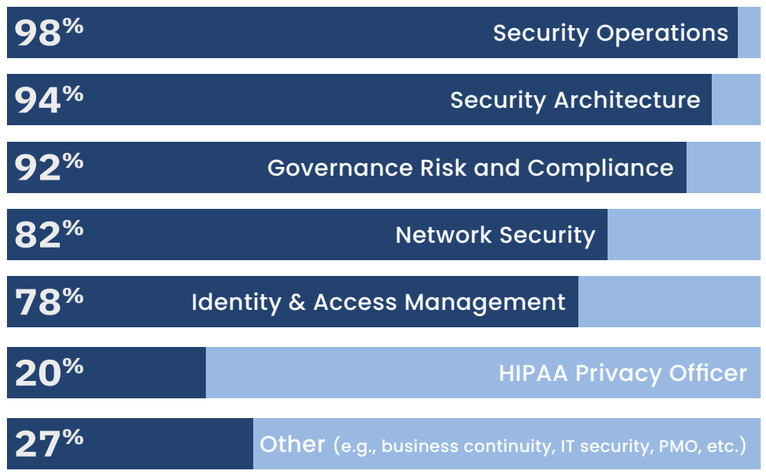
# TALENT FORCES
## Succession Planning

A comprehensive view of the roles undertaken by CISOs reveals that over 9 in 10 are actively engaged in critical functions such as Security Operations (98%), Security Architecture (94%), and Governance Risk and Compliance (92%). The prominence of these responsibilities underscores their increasing importance in safeguarding the health and longevity of businesses, thereby solidifying the integral role of CISOs in essential operational frameworks.

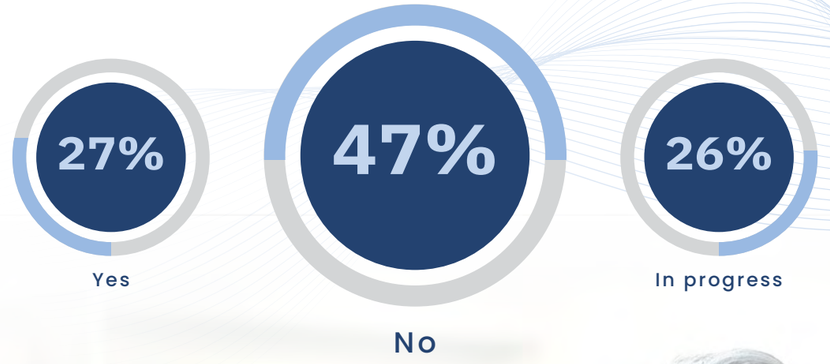
Despite the undeniable significance of their contributions, a notable observation arises concerning succession planning. Astonishingly, only a quarter (27%) of CISOs reported the existence of a succession plan for their current role. Particularly for CISOs, whose responsibilities are pivotal in maintaining the robustness of an organization's security operations, the absence of a succession plan poses a considerable risk. Such plans are indispensable to mitigate potential security vulnerabilities that may emerge in the absence of a seamless transition, thereby fortifying the organization against potential cyber threats.

In recognizing the unique and critical nature of the CISO role, organizations are compelled to prioritize and formalize succession planning. Establishing clear pathways for leadership continuity not only safeguards against security lapses but also ensures the sustained effectiveness of security operations in an ever-evolving threat landscape. As businesses increasingly rely on the expertise of CISOs, proactive and strategic succession planning becomes an imperative component of comprehensive information security governance.

### What is your scope of responsibility?




### Is there a succession plan for your current role in place?



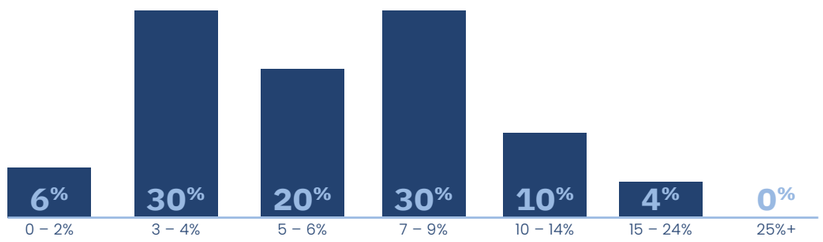

# TALENT FORCES Budget

A crucial factor influencing an organization's capacity to attract premier information security talent and sustain high job satisfaction lies in the volume of budget allocated and the autonomy granted for its management. Notably, a mere 39% of CISOs possess an independent budget, with the majority falling within the $1 million to $10 million range annually for information security. To contextualize, over half of CISOs reported budgets constituting less than 7% of the total IT or departmental budget.

Despite Gartner's report that the average IT security spend across industries was 5.2% of IT budget in 2022[1], such allocations may prove inadequate for effectively mitigating prevailing information security risks. According to cybersecurity solution provider SenseOn, an optimal budget should range between 7% and 20% of the IT budget.[2]

The stakes for CISOs have intensified, particularly since October 2023 when the SEC made a groundbreaking decision to file a formal complaint against a company and its CISO.[3] The allegations included securities fraud and failures tied to significant cybersecurity weaknesses and risks. Organizations must recognize that withholding adequate budgets and resources not only makes the CISO's job more challenging and exposes the organization to heightened risk but could also render them personally liable in the face of regulatory actions.

## What percentage of the IT or other departmental budget is spent on security?




According to Gartner, **5.2%** of IT budgets were spent on IT security in 2022[1].

However, cybersecurity solution provider SenseOn strongly recommends businesses spend **7%** to **20%** of their budget on cyber security to adequately mitigate risk[2].

[1] Gartner, IT Key Metrics Data 2023: IT Security Measures, December 2022

[2] SenseOn, How Much Should a Business Spend on Cybersecurity, October 2023

## If you have a budget, where is it based?


## What is your total annual information security budget?

# TALENT FORCES Challenges

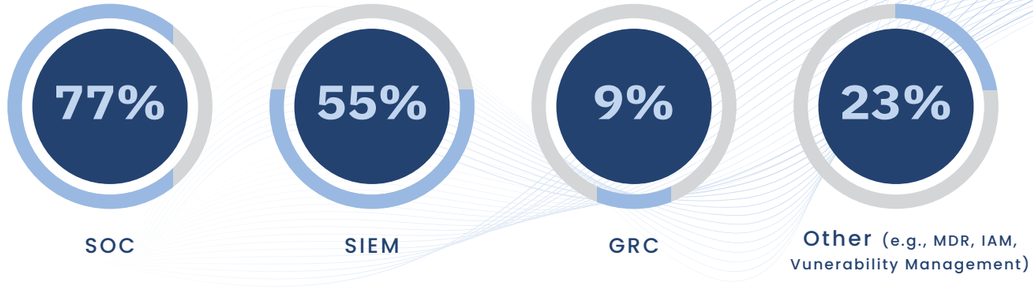
Information security leaders have identified Talent Management as one of their top three security concerns alongside Security Operations and Cloud & Technology. Specific challenges within Security Operations include continuous monitoring, ransomware, and managing third-party risks. Despite occasional outsourcing of functions like Security Operations Centers (SOC), a prevailing trend highlights the majority's preference for maintaining security protocols in-house.

Given the trajectory of rising risks and the simultaneous surge in protocols, information security leaders must adopt a more strategic approach. This entails a meticulous evaluation of the benefits and drawbacks associated with retaining all capabilities in-house versus introducing additional risks through engagements with external vendors. While developing internal talent may require time, it presents a potential trade-off worth considering. As the information security landscape evolves, CISOs must navigate these strategic decisions with heightened discernment to fortify their organizations against emerging threats.

## What are your **three** most pressing information security challenges today?

Cyber converge over the full organization
People Factor **TALENT MANAGEMENT**
**Adaptive Risk** Privileged access management
Email based threats **Behavioral & Cultural**
**Asset Management** Vulnerability Management
The Basics **SECURITY OPERATIONS**
People **Budget & Funding** Ransomware
Privileged access management **Phishing**
**Data Protection** Attack surface management
Cyber threats **CLOUD & TECHNOLOGY**
**Business Continuity & Resilience** IT Risk
Changing organization behaviors to be cyber aware
**Users** Stragic Alignment & Risk Management

## What kinds of functions do you outsource, partially or fully, to an MSSP or vendor?



# RECOMMENDATIONS FOR LEADERS

## VARIED EXPERTISE AMONG HEALTHCARE SECURITY LEADERS

Cultivate an environment that positions healthcare as an attractive destination for skilled information security leaders. Actively seek professionals with varied backgrounds and experiences, emphasizing the unique opportunities, challenges, and impact the healthcare sector offers in the realm of information security. Emphasize the vital role of safeguarding patient data and supporting the broader healthcare mission to create an influx of top talent.

## PRIORITIZE THE TALENT PIPELINE

While external hires can bolster security practices swiftly, leaders should also prioritize developing talent internally who may one day be suitable for CISO roles. Long-term institutional knowledge is invaluable for effective decision-making. Leaders must balance the need for experienced chiefs with the advantages of promoting individuals possessing institutional knowledge, adaptability, and agility.

## ADDRESS TALENT CHALLENGES PROACTIVELY

In light of the substantial investment in information security functions, leaders must proactively address talent-related challenges. Offering competitive compensation packages with performance incentives, work location flexibility, and clear pathways for professional development will contribute to building and leading top-notch teams, fortifying the organization's overall cybersecurity position.

# Appendix:
## Demographic Profile of Respondents

WittKieffer conducted proprietary research on the career paths of the current CISOs at the top 100 health systems nationwide (by revenue), using publicly available information from late 2023, including data from organization websites, BoardEx, and LinkedIn.

To gain a better understanding of the healthcare CISO role, scope, and compensation as well as to acquire insights on how these executives are addressing talent and leadership challenges, we surveyed 50+ CISOs in the healthcare industry. The following provides an overview of their backgrounds and composition.

| GENDER | SHARE OF RESPONDENTS |
|---|---|
| Male | **86%** |
| Female | **10%** |
| Prefer not to answer | **4%** |

| RACE / ETHNICITY | SHARE OF RESPONDENTS |
|---|---|
| White | **80%** |
| Hispanic / Latino | **8%** |
| Asian | **4%** |
| Black / African American | **2%** |
| Multi-racial | **2%** |
| Prefer not to answer | **4%** |

| TITLE | SHARE OF RESPONDENTS |
|---|---|
| CISO | **78%** |
| Director | **8%** |
| Deputy CISO | **4%** |
| Other | **10%** |

| ORGANIZATION'S GROSS REVENUE | SHARE OF RESPONDENTS |
|---|---|
| Over $3B | **55%** |
| $1.1B to $3B | **23%** |
| $501M – $1B | **10%** |
| $101M – $500M | **6%** |
| Less than $100M | **6%** |

| TYPE OF ORGANIZATION | SHARE OF RESPONDENTS |
|---|---|
| Integrated delivery network | **31%** |
| Multi-hospital system | **25%** |
| Academic medical center | **18%** |
| Community hospital | **10%** |
| Medical group | **4%** |
| Payor | **4%** |
| Children's hospital | **2%** |
| Other | **6%** |

# About the **AUTHORS**

### NICHOLAS (NICK) GIANNAS

A principal at WittKieffer devoted to the IT practice since 2006, Nick dedicates his practice to identifying outstanding leaders for traditional and emerging information technology roles in healthcare and higher education, including CISOs, CIOs, CTOs, digital, and analytics leaders.

Nick can be reached at: **ngiannas@wittkieffer.com**

### ZACHARY DURST

A conusltant in the Information Technology Practice at WittKieffer, Zachary dedicates his search practice and work to identifying exceptional leaders in information security, digital, and data analytics, with an emphasis on serving healthcare and higher education institutions.

Zachary can be reached at: **zdurst@wittkieffer.com**

## Improving quality of life through impactful leadership.

### ABOUT WITTKIEFFER

WittKieffer is the premier executive search and leadership advisory firm developing impactful leadership teams for organizations that improve quality of life. We work exclusively with organizations in healthcare, science, and education — the Quality of Life Ecosystem — and provide essential knowledge, analysis, and perspective that produce effective leaders and inclusive cultures. Through our executive search, interim leadership, and leadership advisory solutions, we strengthen organizations that make the world better. WittKieffer is proud to be 100 percent employee-owned. Visit **wittkieffer.com** to learn more.

*WittKieffer*