Gartner Research

CISO Effectiveness: Address Talent Shortage by Fostering Emerging Talent

Victoria Cason, Fadeen Davis, Richard Addiscott

12 February 2024

Gartner

CISO Effectiveness: Address Talent Shortage by Fostering Emerging Talent

Published 12 February 2024 - ID G00799728 - 15 min read

By Analyst(s): Victoria Cason, Fadeen Davis, Richard Addiscott

Initiatives: Cybersecurity Leadership; Build and Optimize Cybersecurity Programs

Organizations are struggling to find and retain talent to fill cybersecurity roles due to salary, attrition and work-life balance. Cybersecurity leaders should focus on fostering and retaining promising employees to build succession plans and sustain longer-term security program effectiveness.

Overview

Key Findings

- Cybersecurity leaders have seen the global talent deficit steadily increase upward from 2.7 million individuals in 2021 to 3.9 million individuals in 2023. This upward trend suggests the global talent deficit will continue to accelerate.
- Less than half of cybersecurity employees are satisfied with what their current employer provides for respect and development opportunities.
- Key frustrations of cybersecurity talent include limited support from the organization for personal and skills development via training, a scarcity of financial investment in professional certifications, limited recognition of personal contributions to enterprise success, and ambiguous or absent routes for career advancement.

Recommendations

To combat the ongoing cybersecurity talent deficit and foster emerging talent for their security program, cybersecurity leaders should:

- Understand the impact of the cybersecurity talent deficit on the cybersecurity program by addressing employee burnout and frustration.

- Develop a cybersecurity workforce strategy that includes demonstrable investment in skills development, a leadership succession plan and a “promote from within” policy to showcase investment for employees’ career growth as cybersecurity professionals and demonstrate a viable career path.
- Mitigate the cybersecurity workforce’s frustrations by continuously assessing employee burnout and prioritizing workloads.
- Evaluate longer-term strategies, such as internships, to foster future security talent and identify opportunities to create capacity for mentoring and talent development.

Introduction

Year over year, the global talent shortage continues to affect the cybersecurity industry. In 2023, the industry saw a deficit of 3.9 million individuals, which has grown an additional 12.6% from the previous year. [1] The numbers are alarming as the workforce gap has steadily increased since 2021. Cybersecurity leaders have seen the deficit increasingly trend upward from 2.7 million individuals in 2021, [2] 3.4 million individuals in 2022, [3] and now 3.9 million individuals in 2023. This dismal forecast suggests the deficit will continue to accelerate and highlights the importance of fostering emerging cybersecurity talent.

Organizations cannot hire their way out of this talent deficit. Instead, they must increase the number of competent security personnel by fostering skills development in the enterprise’s existing personnel. Continually seeking external talent to fill existing skills gaps and improve team performance exacerbates the struggle and breeds attrition. Cybersecurity leaders need to revamp their talent strategies by fostering emerging talent along with sustaining internal cybersecurity talent to increase retention and career satisfaction.

Analysis

Understand the Impact of the Cybersecurity Talent Deficit on Your Cybersecurity Program

Organizations cannot expect cybersecurity talent to thrive and excel as subject matter experts and future leaders if they are not given the opportunities to exercise and expand their knowledge. Concurrently, cybersecurity leaders also need to be mindful of workplace stressors that affect themselves and their personnel. The cybersecurity field itself is stressful due to its protector-like role to defend individuals and organizations from malicious actors seeking to inflict harm or damage.

In a perfect world, with the number of personnel proportionate to what the organization requires, workplace stressors could be maintained through even distribution of responsibilities to establish a work-life balance. In reality, however, the cybersecurity talent deficiency is leading to:

- Attrition among personnel
- Increased workload and responsibilities
- Lack of a true work-life balance, causing burnout

Cybersecurity leaders should investigate how burnout and frustration resulting from the cybersecurity talent deficit impact their organization's cybersecurity capability.

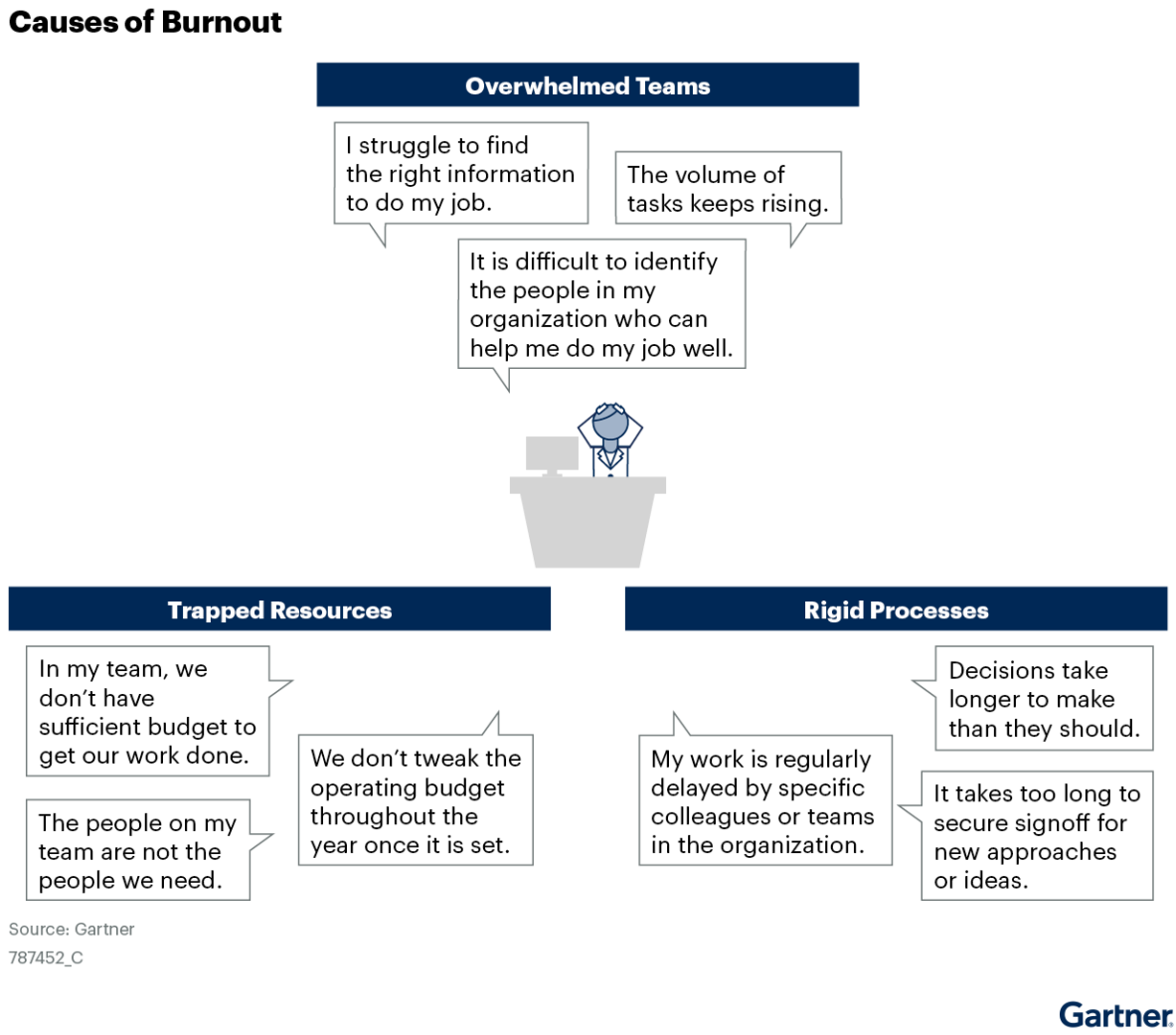
Expectations for employee developmental excellence without a clear path for success is a breeding ground for frustration and attrition.

Cybersecurity Burnout

Burnout in the workplace is an ever-present topic permeating all organizational functions, including cybersecurity. An overabundance of tasks, overwork due to staff or skills shortages, and inadequate resources to sufficiently protect the organization are among the top contributions of burnout and low morale stemming from the global talent deficit of cybersecurity professionals. [1] By shining a spotlight on burnout, you can examine how the ongoing talent deficit contributes to burnout in both leadership and personnel.

Managing team needs contributes to burnout among CISOs. As strategic demands increase, CISOs are expected to delegate operational and technical responsibilities to their staff. These added responsibilities increase the amount of hours needed for their staff to complete tasks responsibly and efficiently. This, in turn, leads to overwhelmed teams, trapped resources and rigid processes — each of which contributes to burnout, as shown in Figure 1.

Figure 1: Causes of Burnout



These burnout impacts can decrease the work-life harmonization that cybersecurity talent desire. Some CISOs who have observed the impact of burnout on their teams have implemented the following actions to address this talent risk: [4]

1. Put monitoring in place to ensure an employee does not work more than three months straight without taking any personal time off.

2. Collect data to make a case for increased headcount when needed.

3. Leverage contracting services as a type of quick hire to prevent team members from burnout.

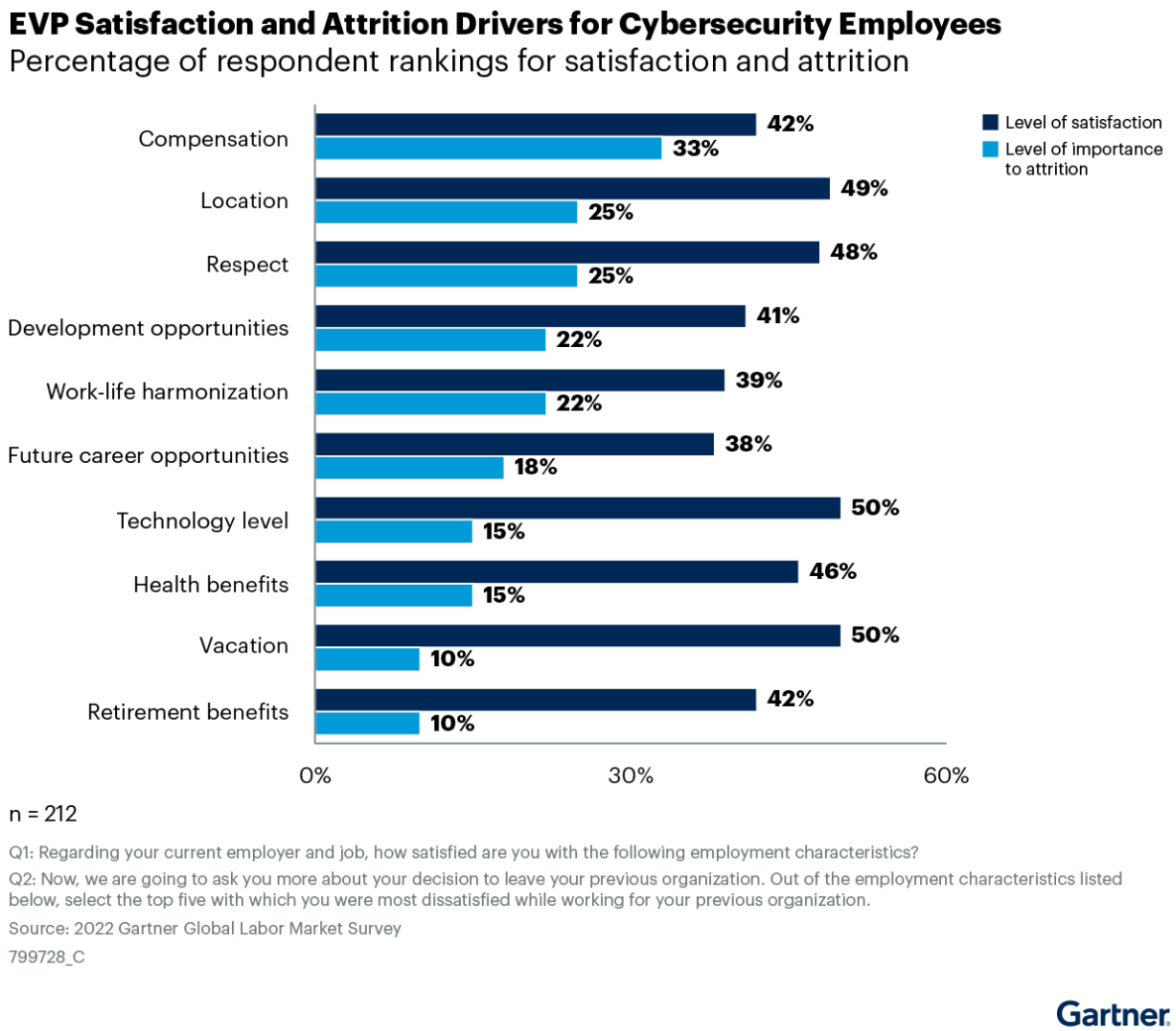
4. Automate repeatable and lower-level tasks where possible.

Each of these actions helps CISOs in mitigating burnout by establishing a work-life harmonization culture for their staff. Behind compensation, work-life harmonization is the leading employee value proposition (EVP) attribute for cybersecurity talent, with 34% placing this attribute as the most important when considering employers. [5]

Cybersecurity Talent Frustration

When reviewing the most important attributes for cybersecurity employees, respect and development opportunities were in the top 10 for attrition. Interestingly, when analyzing the level of satisfaction for respect and development opportunities, less than half of the surveyed employees are satisfied with what their current employer provides (see Figure 2). [5] This led us to investigate the underlying emotional and subliminal conflict between the two attributes.

Figure 2: EVP Satisfaction and Attrition Drivers for Cybersecurity Employees



n = 212

Q1: Regarding your current employer and job, how satisfied are you with the following employment characteristics?

Q2: Now, we are going to ask you more about your decision to leave your previous organization. Out of the employment characteristics listed below, select the top five with which you were most dissatisfied while working for your previous organization.

Source: 2022 Gartner Global Labor Market Survey

799728_C

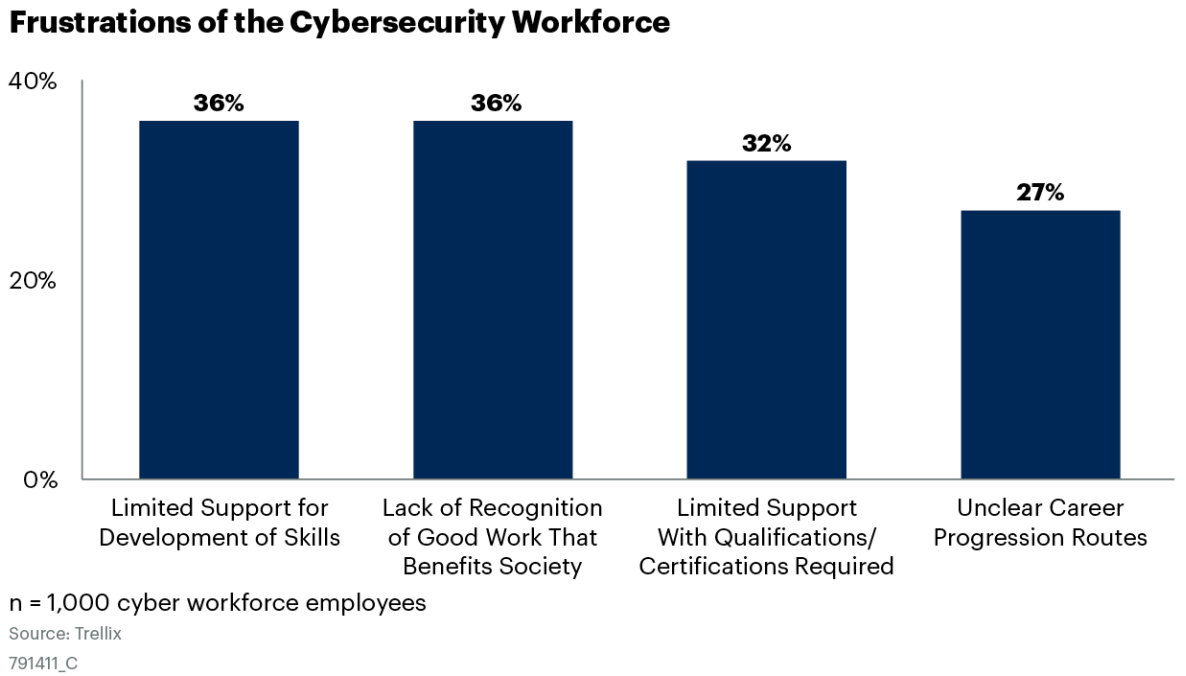
Gartner

Frustration is often the root cause of the conflict between the aforementioned attributes. Many cybersecurity professionals have this feeling, and it has been exploited due to the global talent deficit. For example, frustrations related to respect could be exemplified in noncompetitive compensation. Companies often hold the misconception that salaries for cybersecurity talent are interchangeable with salaries for IT professionals. While the two industries overlap at times, that misconception can lead to noncompetitive compensation offers, resulting in a continuous struggle to attract and/or retain cybersecurity talent.

Noncompetitive salary is one of many leading frustrations stemming from the global talent deficit that could be tied to respect. Lack of representation in underrepresented talent, diverse skill sets and realistic job expectations are other key examples. However, lack of employee development is an emerging frustration. This frustration occurs when organizations offer limited training or financial support for development, skills or acquiring certifications.

Lack of recognition and unclear career progression routes are also leading frustrations among cybersecurity talent (see Figure 3). [6] Cybersecurity talent desire respect and opportunities for growth within their organization. However, if these desires are disregarded, attrition at the organization will increase and the talent deficit will continue to grow.

Figure 3: Frustrations of the Cybersecurity Workforce



What You Need to Do

One of the key game-changing behaviors exhibited by leading CISOs is becoming a workforce architect. [7] Workforce architects are effective CISOs who have a future-focused talent strategy to meet their enterprises' growing skills needs. This behavior results in a leader whose overall security workforce is better prepared for challenges through developing a formal strategic workforce plan.

CISOs can exhibit this behavior by proactively mitigating the future implications arising from an emerging talent shortage for their organization by leveraging one or more of the recommendations provided below:

Adopting the workforce architect behavior as a CISO is fundamental to fostering, sustaining and protecting the organization's pipeline of emerging security talent to ensure the sustainability and continuous improvement of its cybersecurity risk posture.

Implement a Cybersecurity Workforce Management Strategy

Use Performance and Career Discussions to Identify, Evaluate and Foster Emerging Talent

CISOs can use regular performance and career conversations as an opportunity to attract and develop talent to address any skills capability gaps within their program along with mitigating the increasing workload demands on their staff (see Ignition Guide to Creating a Strategic Workforce Plan for Cybersecurity). CISOs should leverage both the external and internal talent ecosystems to identify emerging talent. For the external talent ecosystem, CISOs can use various hiring channels and talent pools to identify new talent. For the internal talent ecosystem, they can use quiet hiring practices.

Some examples of quiet hiring practices include internal job postings, mentorship programs and upskilling opportunities provided through collaboration with other IT and business teams. When leveraging either ecosystem, CISOs must proactively create compelling career progressions and development plan conversations to this aspiring talent group.

Develop a Cybersecurity Talent Succession Plan

A succession plan is a useful way to forecast and establish, over time, the operational capabilities required to ensure the cybersecurity function can meet business demand as it advances its digital and strategic ambitions. As the security function evolves to meet that demand, CISOs should also ensure any workforce management strategy outcomes include establishing the capacity and ability to coach, mentor, and/or lead as new talent joins the organization, and as existing talent must upskill.

Promote From Within When Looking for, and Filling, Internal Cybersecurity Roles

Promoting from within does two things. First, it helps to establish a succession plan for team leaders, middle management and, ultimately, CISO-level roles; and therefore, it establishes the longer-term sustainability and advancement of the organization's security program (see Case Study: Actionable CISO Succession Planning).

Second, it will help retain top security talent by showing them a clear and attainable career path should they stay at the organization. CISOs can partner with the CHRO to co-create the necessary initiatives that will improve the security team's talent strategies (see Tool: A CISO's Guide for Conversations With the CHRO).

Compile a Leadership Competency Profile and Inventory

CISOs should work with the organization's HR function to define the critical leadership competencies required within their organizational context. They should then conduct a skills assessment across the security and IT workforce that includes an evaluation of current leadership competencies. This will help identify which team members have the leadership attributes, aptitude and interest that could be fostered for future leadership roles.

Typical competencies expected of emerging security leaders include adaptability, the ability (and willingness) to coach and mentor junior staff, communication, stakeholder management, business acumen, decisiveness, and diversity of opinion.

Continuously Assess Employee Burnout and Prioritize Workloads

Assess and Address the Impact of Employee Burnout

On a weekly basis, make time to engage with your personnel and identify potential changes in employee behavior that may mask burnout and frustration. While some signs and symptoms of employee burnout could materialize in the below engagement and performance items, these are not absolute indicators:

- Surges in preventable operational errors

- Lack of team participation and disengagement
- Obsession with small work projects/programs
- Declines in overall confidence

Each employee's experience with burnout is unique to them. Some may show immediate burnout symptoms, while others could have a "slow burn" effect where the feelings of frustration linger and grow over time. CISOs must demonstrate empathic leadership when addressing the impact of burnout. Address each employee's individual source of burnout with questions that can lead to a heartfelt discussion without implying a performance improvement tone that may alarm employees. [8] Some examples of questions that can leveraged include:

- How are you feeling about your work?
- Has anything changed about your day-to-day experience?
- Has anything been creating additional pressure or causing you frustration?
- Is there anything I can do to support you and/or to make your experience better?

Prioritize Workloads

CISOs must also proactively support employees' well-being or risk increased attrition. This can be accomplished by setting the tone and leading the cybersecurity department's efforts to prioritize workloads. CISOs can leverage our Tool: Team Prioritization Matrix to Reduce Burnout to help align their efforts in prioritizing team workloads and maximizing operational efficiency through:

- Determining the level of effort and resources that should be assigned to different activities and projects based on potential impact to strategic goals
- Reevaluating the results of this exercise on a monthly or quarterly basis to ensure effort is still aligned with impact and employee workloads are manageable
- If necessary, rebalancing or rightsizing employee workloads to protect workforce health and individual's well-being

Evaluate Longer-Term Opportunities for Talent Development

Engage With HR to Build Internship Programs

Internship programs can be highly beneficial for fostering and retaining emerging cybersecurity talent as they allow for increased exposure to the organization and the cybersecurity field along with creating opportunities to collaborate with other business units (see Case Study: Building a Diverse Talent Strategy [T-Mobile]). This is very helpful for extending personal networks and building productive working relationships beyond immediate team structures within, or outside, the organization. This program can also aid in creating a talent funnel to provide opportunities to join the organization once the internship is complete.

Seek Coaching and Mentoring From Business Leaders for Emerging Security Leaders

Another key attribute of an effective CISO is the ability to define risk appetite through collaboration with senior business decision makers. [7] Enabling emerging security leaders to be exposed to experienced business mentors and coaches internally will help them to become more familiar with the organization's business operations, context, strategic objectives and risk appetite in a friendly and safe setting.

In turn, it will allow them to begin developing critical leadership competencies earlier, shortening the runway to full effectiveness once appointed to their new leadership roles. It will also help business leadership by fostering greater familiarity of its specific operational objectives within the cybersecurity team, which over time will make for more business-centric security advice and improved information risk decision making.

Establish a Security Champion Program

As outlined in our research, Quick Answer: Do I Need a Business Information Security Officer?, latent security talent may exist outside of the IT and/or security team, especially when it comes to strategic business skills. Establishing a security champion program will help in identifying emerging talent considering a career change to cybersecurity. A security champion can also partner with a business information security officer who can coach and mentor the champions to aid in their transition over time.

Create and Fund an Ongoing M.B.A. Scholarship Program

CISOs could use a portion of any increased funding for directly developing leadership talent. The knowledge imparted via external, business-centric courses, such as M.B.A. and/or executive M.B.A. programs, will help emerging security leaders to gather the foundational knowledge, skills and business acumen required to better understand their organization's business context. In turn, this will help them communicate more effectively with their business peers and senior executive stakeholders.

Scholarship funds can be awarded on an annual basis, based on performance, to encourage ongoing study and performance improvement. Awarding scholarship funds across multiple individuals not only sends positive signals about potential career development to the rest of the workforce but also enables multiple emerging leaders to be developed at the same time.

These programs could become a differentiating employee value proposition, helping to attract new talent to the organization in a tight labor market. CISOs should also work with the business to set up secondments or other work placement opportunities. This will help emerging leaders to make the most of the knowledge and skills that they acquired through their courses in other parts of the organization.

Identify Opportunities to Free Up Time for Talent Development

In many cases, organizations have limited time to dedicate to developing emerging talent. This is especially the case for smaller security teams (where members are often performing multiple, cross-disciplinary roles) and in large teams (where individuals are fully utilized in single-focus roles).

Regardless of whether their organizations have a formal security workforce management strategy in place, CISOs should look to find the talent development time needed by identifying opportunities to create capacity and operational efficiency within the function. This might be achieved by:

- Outsourcing more commoditized security functions to managed security service providers
- Reskilling to ensure organizational generative AI capabilities for cybersecurity
- Leveraging security orchestration, automation and response, robotic process automation and AI-enabled capabilities to reduce time spent on day-to-day standardized security processes

Evidence

[1] How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce, 2023, (ISC) [2] Cybersecurity Workforce Study.

[2] A Resilient Cybersecurity Profession Charts the Path Forward Cybersecurity Workforce Study, 2021, (ISC) [2]

[3] Cybersecurity Workforce Study, 2022, (ISC) [2]

[4] Wondering If Infosec Folks Consider the Risk of Burnout to Be an Unavoidable Part of Cybersecurity Roles? Gartner Peer Community, April through December 2023.

[5] 2022 Gartner Global Labor Market Survey. This survey was based on responses from 72,000 employees globally, including 7,004 IT employees and 212 cybersecurity employees. Cybersecurity employees were defined as IT employees who selected security architecture/engineering, security operations, or security policy, governance and risk management as their department. Responses were collected monthly across 40 different countries in 15 languages and then aggregated to generate yearly findings.

[6] Trellix Survey Findings: A Closer Look at the Cyber Talent Gap, Trellix.

[7] The 2020 Gartner CISO Effectiveness Survey. We surveyed 129 heads of information risk functions globally across industries, geographies and revenue bands in January 2020 to identify the beliefs and behaviors of leaders who effectively deliver against key security outcomes. We used descriptive statistics to ensure all outcomes were normally distributed, and created a measure of effectiveness that determines a CISO's ability to execute against those outcomes. We defined "effective CISOs" as those who scored in the top one-third of our CISO effectiveness measure. To identify the factors that impact effectiveness, we used correlation analysis and analyzed a set of 60 different behaviors and mindsets, background traits, and organizational factors against the effectiveness index.

[8] Address Burnout by Keeping Employees S.A.N.E.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

CISO Effectiveness: How to Attract, Retain and Release Cybersecurity Talent

CISO Effectiveness: Key EVP Attributes for Cybersecurity Talent

Tool: Identifying Adjacent Talent for Key Cybersecurity Roles

Case Study: Actionable CISO Succession Planning

CISO Effectiveness: Start Practicing 3 Burnout-Avoiding Behaviors Now

Tool: A CISO's Guide for Conversations With the CHRO

Case Study: Building a Diverse Talent Strategy (T-Mobile)

Actionable, objective insight

Position your organization for success. Explore these additional complimentary resources and tools for cybersecurity leaders:

Report

Cybersecurity Trends: Optimize for Resilience and Performance

Equip your cybersecurity function for greater resilience.

Download Now

Roadmap

IT Roadmap for Cybersecurity

Create a resilient, scalable and agile cybersecurity strategy.

Download Now

Research

CISO Foundations: Cybersecurity Talent Strategies for CISOs

Discover tried-and-tested guidance for building skilled cybersecurity teams.

Download Now

Conference

Gartner Security & Risk Management Summit

Join your peers for the unveiling of the latest insights at Gartner conferences.

Reserve Your Spot

Already a client?
Get access to even more resources in your client portal. Log In

Connect With Us

Get actionable, objective insight that drives smarter decisions and stronger performance on your mission-critical priorities. Contact us to become a client:

U.S.: 1 866 263 8917

International: +44 (0) 03301 628 476

Become a Client

Learn more about Gartner for Cybersecurity Leaders
gartner.com/en/cybersecurity

Stay connected to the latest insight

Gartner®