NICE | community coordinating council

EMPOWERING ORGANIZATIONS TO RETAIN SKILLED CYBERSECURITY TALENT FOR LONG-TERM SUCCESS

January 2025

A project of the public Modernize Talent Management (MTM) working group, led by NICE under the National Institute of Standards and Technology (NIST) at the U.S. Department of Commerce. NICE is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development.

Authors

Jessie Bolton, *Bolt Resources*

Jo Justice, *Leidos*

Terry Leach, *Astrolytes/CyberCo-op*

Olesya Menon, *Google*

Marian Merritt, *NICE, National Institute of Standards and Technology*

Arianna Schuler Scott, *Virginia Tech*

Student co-authors

Alexander Ibacache, *Virginia Tech*

Sidney Laden, *Virginia Tech*

Kamalanand Sangameswaran, *Virginia Tech*

Published January 2025

Abstract: The NICE Modernize Talent Management (MTM) working group project team was launched to advance the broader NICE Strategic Plan, directly supporting Strategic Objective 3.1, "Enhance the capabilities of organizations and sectors to recruit, hire, develop, and retain the talent needed to manage cybersecurity-related risks, and Strategic Objective 3.4, "Encourage and enable ongoing development and training of employees, including rotational and exchange programs, to foster and keep current talent with diverse skills and experiences."[1] This research offers insights for employers, HR professionals, and talent acquisition leaders, emphasizing that retaining cybersecurity talent is crucial for organizational security, innovation, and reputation. High turnover in these roles leads to operational costs, knowledge gaps, and security risks, impacting legal, financial, and reputational aspects. By understanding the factors driving attrition, organizations can improve employee satisfaction, loyalty, and performance through tailored retention strategies like career development, impactful workplace initiatives, and mental health support. These efforts foster a committed, engaged, and stable cybersecurity team, strengthening the organization's security posture and adaptability to the changing cyber threat landscape.

Keywords: Cybersecurity, Talent Retention, Employee Development, HR Strategies, Organizational Culture, Employee Engagement

Audience: HR leaders, hiring managers, cybersecurity managers, organizational executives, and industry stakeholders

Acknowledgements: We want to acknowledge the contributions of HR leaders, cybersecurity managers, and professionals who shared their insights and experiences, and to thank the NICE Program Office team, led by Director Rodney Petersen and Deputy Director and Liaison to the Modernize Talent Management Working Group Marian Merritt, for their dedication to advancing best practices in cybersecurity talent management.

[1] https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan#Goal%203

Table of Contents

.

I. Introduction

In today's digital age, the specter of cyberattacks casts a long shadow over organizations of all sizes. A staggering 90% of organizations suffered breaches last year, each costing an average of $3.86 million. According to the IBM Cost of a Data Breach Report[2], more breached organizations report more severe staffing shortages (up 26%) and significantly higher breach costs compared to well-staffed companies. In order to mitigate these losses and safeguard sensitive data, we must urgently address a critical challenge: the cybersecurity talent shortage. High turnover rates exacerbate this issue, leaving organizations vulnerable to exploitation. We must understand the root causes of employee turnover and implement effective retention strategies to build a resilient cybersecurity workforce.

This NICE Modernize Talent Management (MTM) working group report aims to illuminate these challenges and provide actionable solutions. By discussing the factors driving cybersecurity professionals to leave their roles, we can empower organizations to create engaging and supportive work environments. This research will identify key retention strategies and offer insights to foster a workforce capable of meeting current and future cybersecurity demands.

II. Problem Statement

The cybersecurity industry is grappling with a severe talent shortage, with nearly 457,000 unfilled positions in the U.S. alone (CyberSeek, 2024). This critical gap, intensified by high turnover rates, poses a significant threat to national security and organizational resilience. Traditional human resources (HR) strategies are insufficient to address the unique challenges facing cybersecurity professionals. A recent study by Black Fog[3] revealed that a quarter of CISOs and IT security decision makers are considering leaving their roles, primarily due to the overwhelming stress they feel in their roles. This stress stems from excessive workloads, long

[2] https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs
[3] https://privacy.blackfog.com/wp-content/uploads/2024/10/BF_CISO_Research.pdf

hours, feelings of isolation, and unrealistic expectations. Compounding this, a reported 71% of cybersecurity professionals have been told to keep breaches quiet, potentially exposing them to regulatory and compliance risk as well as personal legal trouble, according to a 2023 BitDefender report.[4] Overwork, stress, feelings of isolation, needing to keep secrets? Is it any wonder the global cybersecurity talent pool has a shortage and a retention problem.

To mitigate this crisis, we must delve deeper into the root causes of turnover and develop targeted retention strategies. By addressing factors such as burnout, lack of career progression, and unsupportive work cultures, organizations can foster a more resilient and engaged cybersecurity workforce.

III. Methodology

The project team chose to investigate retention risks in cybersecurity through fielding a targeted survey and conducting an environmental scan of published research into cybersecurity workforce stress, morale, and retention topics. The survey gathered quantitative and qualitative data from HR leaders, cybersecurity managers, and individual contributors, offering insights into industry challenges. Despite limitations, including a small sample size and U.S.-focused data, this approach provides initial findings to inform retention strategies. The environmental scan further contextualizes results with relevant industry reports and literature.

1. Retention Risks Survey

The project team conducted an online survey to explore specific challenges within the cybersecurity field, offering actionable insights that could lead to improved organizational practices. However, it is essential to note that the survey sample was small, with fewer than 100 responses, and future research or additional data collection would help provide more reliable and representative findings.

[4] https://www.infosecurity-magazine.com/news/twofifths-it-pros-told-keep/

2. Survey Methodology

The survey targeted three key groups: HR leaders, cybersecurity managers, and individual contributors. Quantitative (e.g., Likert scale) and qualitative (open-ended) questions were used to gather numerical data and in-depth insights. The survey was distributed online through professional networks, industry associations, and partnering organizations.

3. Limitations and Scope

While the survey provided valuable information, there were limitations in the study's scope. The sample size, under 100 responses, limits statistical power and generalizability. The study was primarily U.S.-based, meaning the findings may only partially reflect global trends. The six-month study period may not capture long-term or seasonal variations, and the voluntary nature of the survey could introduce self-selection bias, potentially favoring more engaged professionals. Efforts representing diverse industries and organizational sizes have left some sectors underrepresented. Moreover, due to the rapidly evolving nature of cybersecurity, the findings may need to be updated quickly.

4. Environmental Scan

The project team also conducted an environmental scan to supplement the survey and provide additional context. This scan included a comprehensive review of existing literature, industry reports, and best practices in cybersecurity talent retention. Additionally, publicly available data on cybersecurity job market trends and turnover rates were analyzed.

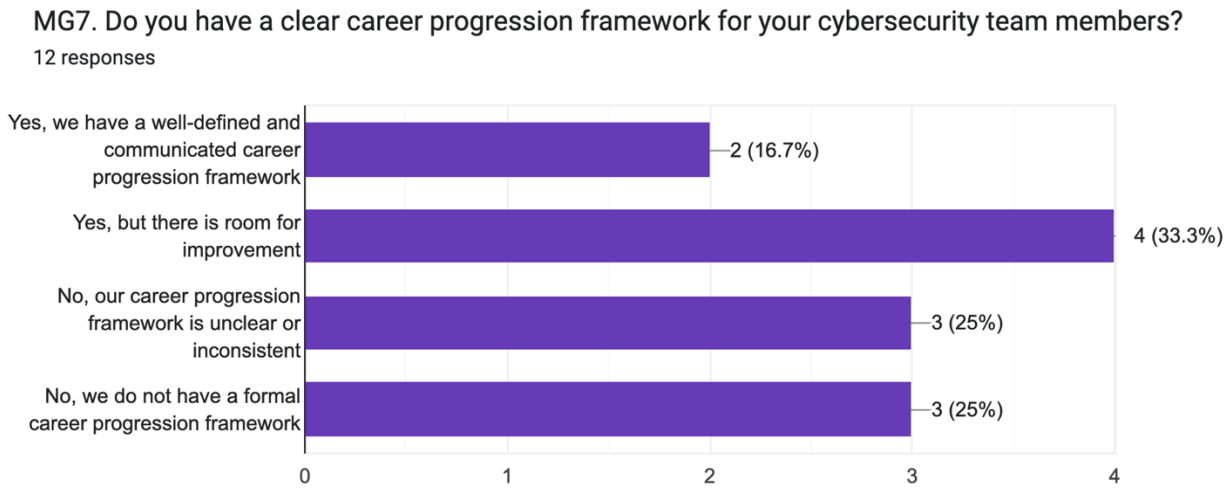
IV. Data

Cybersecurity talent retention is a growing challenge driven by inadequate employee support, poorly defined career pathways, and burnout. The "Cybersecurity Talent Retention Survey" fielded by the Modernize Talent Management working group, led by NICE at NIST, highlights these critical issues that contribute to high turnover rates and a heightened risk of security breaches. Organizations must proactively address these concerns in order to retain skilled professionals and ensure a secure, effective workforce.

1. Manager vs. Individual Contributor Perspectives

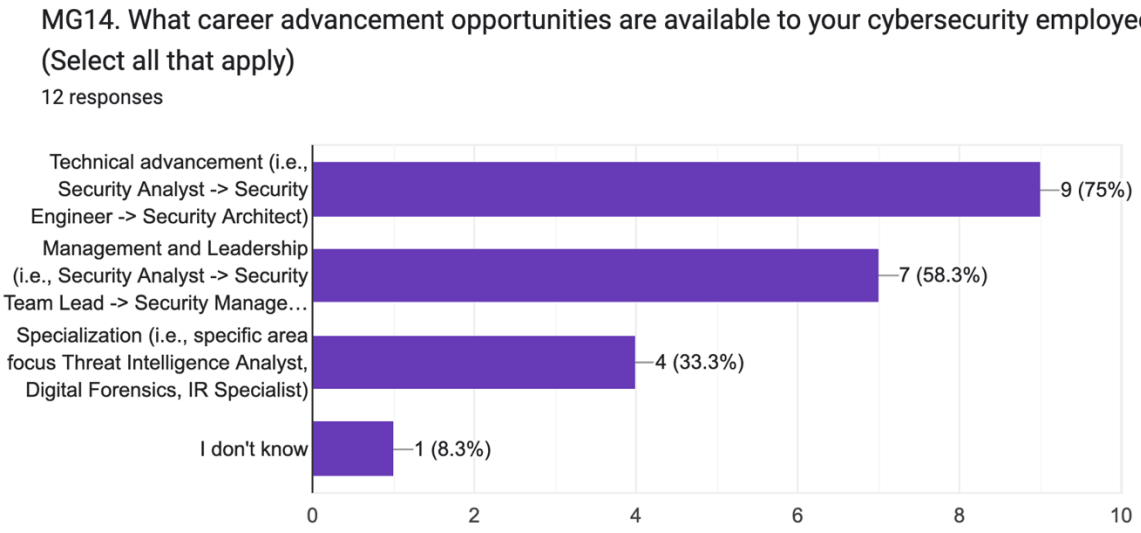
Differences in perspectives between managers and individual contributors were revealed in this research. Managers reported relative satisfaction with recruitment and onboarding efforts, while acknowledging areas for improvement. Over half of the manager respondents felt their organization's onboarding programs needed improvement. The project team believes it is a best practice for organizations to assess their employees for skills gaps on a regular basis in order to accomplish two things: to identify learning opportunities for their employees that align to career growth; and to spot gaps in competencies that can lead to cybersecurity risks for the organization. When asked whether their organization offered a program to assess for skills gaps, 67% reported having a program while the remaining third do not. The vast majority of employers offer opportunities for employees to participate in training and learning programs that are tied to their ongoing skill development.

The "Cybersecurity Talent Retention Survey" found that half of the managers believe their employer offers a clear career framework for employees on the cybersecurity team. Organizations that offer a well-defined career progression acknowledge this can serve as an incentive for employees to remain with their employer to continue developing knowledge and skills and rise in their profession.



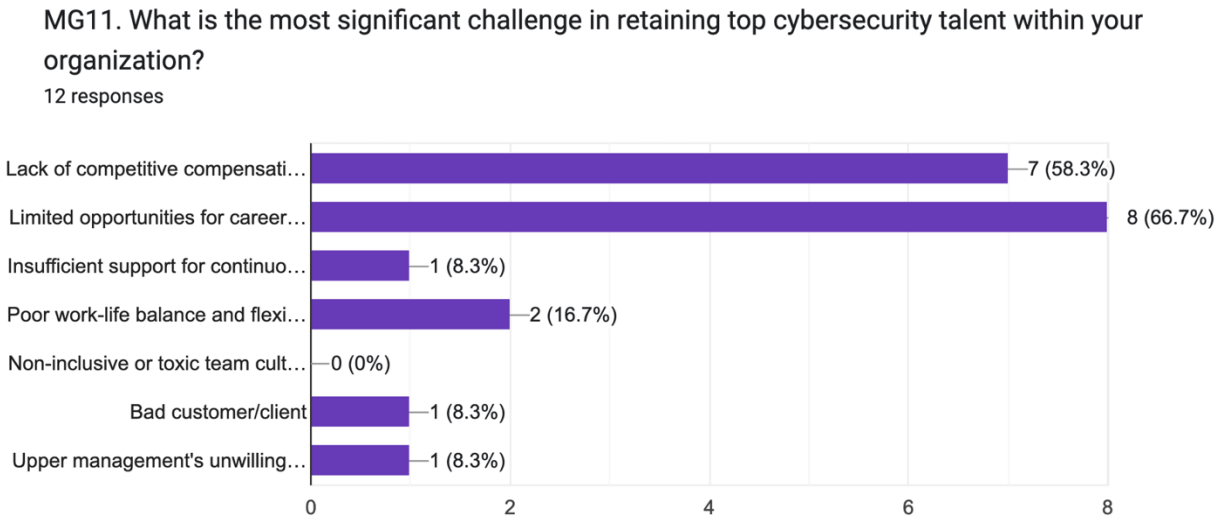
,.

It is useful to see how managers view typical career paths for their cybersecurity team. The chart below depicts common responses for career advancement in their organization. The most common pathways were for technical and managerial advancement. Note again that the dataset is small, and more research is warranted but for those individuals with an interest in specialization, it may be that those pathways are less frequently part of a standard program.

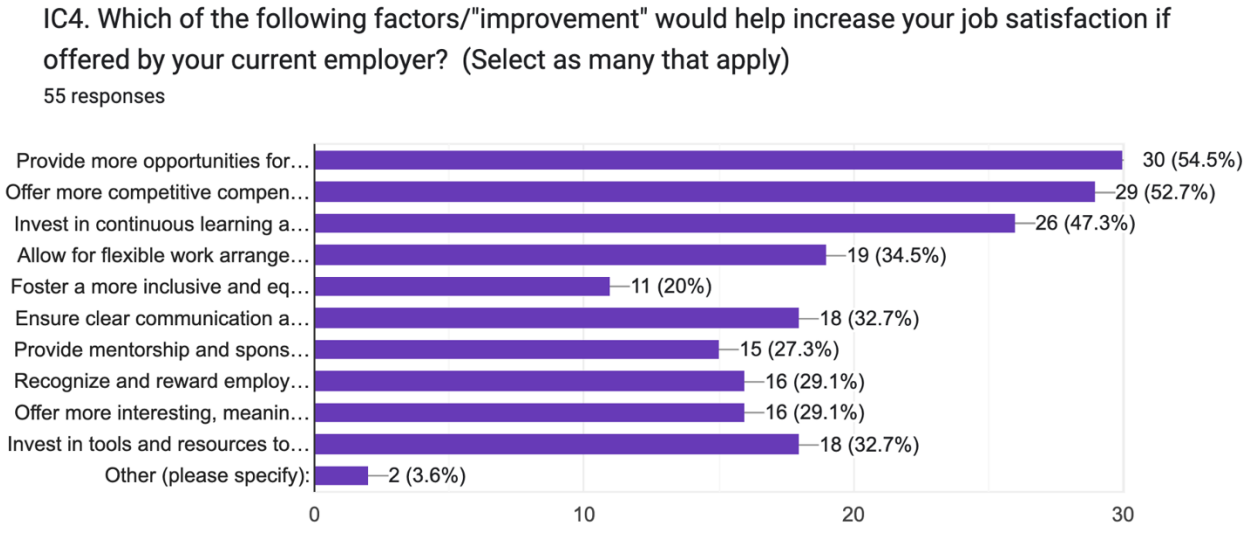


Managers' ratings for how satisfied they were personally with their organization's workplace flexibility and autonomy indicated they were pretty satisfied 3.75 (on a scale of 1-5). Interestingly, most managers believed that compensation and opportunities for advancement

were crucial for retaining talent.

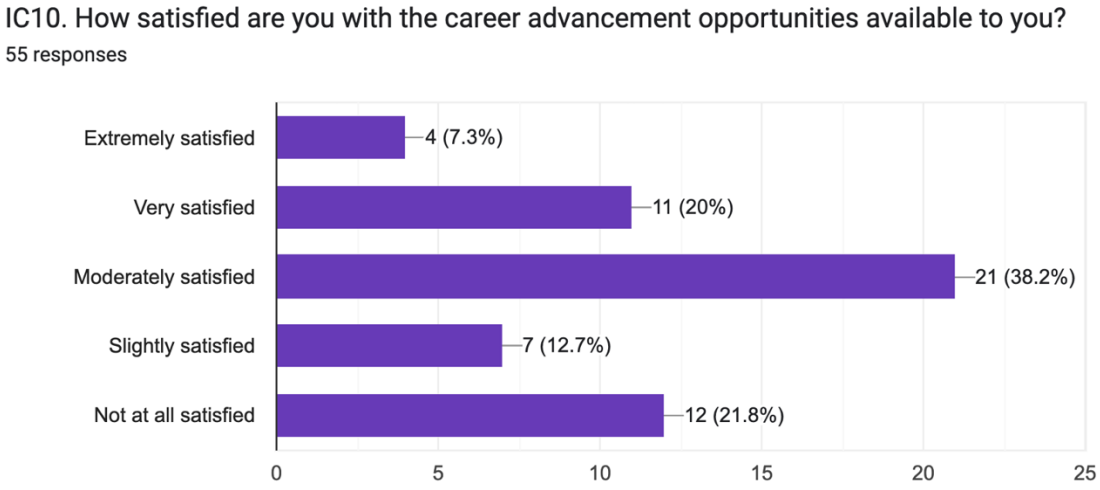


Individual respondents show similar concerns to those of managers. (Note, managers and individual contributors were able to provide responses to the individual contributor questions.) The sample was skewed towards experienced cybersecurity professionals with over 72% having 5 or more years of experience. 44% have been with their current employers for five or more years. The individual contributors reported moderately high ratings of personal happiness with their current employer, or 3.45 (on a scale of 1-5). When asked what would increase their happiness, the respondents led with career growth, competitive compensation, and opportunities for continuous learning (see chart below):



Most of the individual contributors feel their skills are being utilized in their roles. But a third do feel underutilized or mismatched and this could additionally cause concern for their longevity.

Two-thirds (66%) report a degree of satisfaction with their career progression – putting them at odds with managers' responses about likely retention issues and also the same individual contributors' identifying it as a factor that could increase satisfaction in their current position. Therefore, measurements of career satisfaction might be easily misunderstood in meetings with employees; someone might say they are satisfied yet still be looking for more structured programs and learning opportunities. Managers should seek to proactively ask employees what career track they see themselves on and create programs to help the employee achieve their goals.



When managers were asked questions about their own roles and relative work satisfaction, the responses were a mixed bag. Relative happiness with their role was 3.42 (on a scale of 1-5). The survey then provided an open response text box for the managers to provide more detail for their personal happiness response:

Positive remarks include:

"Access to training and toolkits to help employees, leadership support"; "Competitive salary, awesome work/life balance, hybrid work from home"; Mission focus and importance, complex problem-solving, high visibility and exposure in the company."

Negative remarks include:

"Lack of career progression and compensation"; "Toxic work environment"; "I am limited in my ability to bring important change"; "Compensation is not competitive"; "We need more bodies to get real work done"; "Leadership lack of openness to change and prevention"; "They'd rather 'pay the fine.'"

For the individual contributors, when asked if they would ever consider leaving the cybersecurity field, half would if given the right circumstances. When asked why, they mentioned issues with lack of career opportunities, issues with compensation, and issues with their team's culture. Most individual contributors believe their employer supports their professional needs and well-being.

Yet the open ended query into how frequently they feel overwhelmed or burned out elicited some interesting remarks:

“Very often, we are being asked to do more with less.”

“Often. Lack of adequate funding”

“Too many projects in parallel”

“When there are numerous competing demands for my time and attention” and in particular, “This is one of the main reasons I have left every job I’ve had in security operations…I have had to switch jobs…to recover.”

Not everyone feels so overwhelmed by their jobs. Some additional remarks include:

“While I have a large workload, I do not feel overwhelmed.”

“I just feel I am compensated incorrectly”

“Sometimes but the cybersecurity profession is stressful by nature of the work. People who endeavor to enter this field should account for stress and weigh if it fits their expectations.”

Organizations that regularly evaluate their compensation packages and communicate this information to their employees have an opportunity to improve employee satisfaction and address any pay discrepancies. Currently, employee satisfaction with compensation is divided, with many unsure what constitutes fair pay for their work. Often managers believe compensation is the primary driver for employees to leave but these comments show that employees need their work-life balance measures met first and foremost. Even those who accept that stress comes with the job should have reasonable accommodations (e.g. flexible hours, time off after a crunch period, recognition from leadership); it simply isn’t healthy for employees to be under duress throughout their career.

V. Data Interpretation

1. Support, Career Growth, and Work-Life Balance

According to the survey, over 75% of individual contributors report having a healthy work-life balance, with about half mentioning room for improvement in support-related areas. Some show needs of support in addressing work-life issues that may lead to resignation. Several key factors were identified as having a significant impact on retention, including limited opportunities for career advancement, inadequate work-life balance, lack of organizational support, and insufficient training and development programs. Participants expressed dissatisfaction with the limited opportunities for career progression, which aligns with trends reported by ISC2 and ISACA. Burnout, often resulting from excessive workloads and poor work-life boundaries, was a major contributor to turnover within the industry. Many employees reported feeling disconnected from their managers, leading to decreased engagement in seeking training and career development opportunities. Technical and soft skills training were identified as areas of deficiency, with employees expressing a desire for more on-the-job learning and skill enhancement. These findings highlight the critical nature of the situation, as dissatisfaction with career development remains a significant driver of turnover in the cybersecurity industry, per the ISC2 Cybersecurity Workforce Study.

2. Addressing Training and Skills Development

To address the need for more training and skills development, employers must prioritize creating a culture of ongoing skill development and offer new opportunities for staff. Although salary is often seen as a primary motivator, surveys suggest retention is more nuanced. Cybersecurity professionals need opportunities to develop both technical and professional skills. Managers should encourage staff to engage in activities like writing reports, making presentations, attending senior staff meetings, and rotating through different parts of the organization. By identifying areas of professional interest and facilitating on-the-job learning programs, employers and managers can actively contribute to staff growth, fostering loyalty and retention.

3. Organizational Culture and Psychological Safety

Organizational culture and psychological safety also play a critical role in retention. The survey results indicate a strong correlation between inclusive organizational cultures and employee satisfaction. Psychological safety is vital for fostering innovation and open communication within cybersecurity teams. Most respondents report feeling comfortable to voice their concerns, ideas and suggestions (31% are extremely comfortable; 26% are very comfortable.) Employees in psychologically safe environments are more likely to report security concerns and contribute to team effectiveness. Many respondents reported feeling disconnected from their managers, which led to decreased engagement and participation in career development opportunities. Organizations that prioritize inclusive cultures, valuing openness to all employee perspectives and contributions, tend to have lower turnover rates and higher job satisfaction. Moreover, fostering psychological safety encourages collaboration and knowledge sharing, which is essential for addressing complex cybersecurity challenges.

4. Disconnection from Management and Its Impact

When employees feel disconnected from their managers, they are less likely to participate in training programs or formal and informal learning opportunities. This can lead to dissatisfaction, causing employees to consider leaving the company or even the cybersecurity profession altogether. Respect from both the organization and managers towards their cybersecurity teams is a critical concern that must be addressed to retain talent and maintain a productive, innovative workforce.

5. Mental Health

The mental health concerns for the cybersecurity professional are tied up in many of the concerns previously discussed in this report. When employees feel overwhelmed by the demands made of them in the workplace and feel psychologically unsafe, their mental health will suffer. Organizations often provide resources for the employee's mental well-being, but it is important that employees can access these services without concern for any negative impact to their careers. In the Tines study of the mental health of the cybersecurity professional, 27% reported a decline in their mental health over the previous year, with two-thirds reporting stress that impacts

their work. Half reported getting medication to help them cope with their work-based stress. [5] Most organizations in the Tines study (57%) offer such resources. In the Modernize Talent Management research, we only asked HR leaders about these offerings and there were too few responses for conclusive results. Therefore, we can only recommend that the evidence can be seen from the environmental scan of the need for mental health support for cybersecurity staff as part of the whole suite of wellness resources to ensure a positive work-life balance for the understaffed cybersecurity team is invested in by the organization.

VI. Proposed Solutions

This section outlines three key strategies to address the issues raised in this study: career development opportunities, organizational strategies, and work/life balance and burnout prevention. These strategies are likely to support organizations in retaining cybersecurity talent, enhancing employee support, fostering career development, promoting work-life balance, and creating a supportive and open workplace culture. This is important because this helps companies mitigate their business risk. Additionally, it covers the importance of monitoring engagement and the role of leadership in supporting well-being and professional growth. These approaches address retention challenges and build a sustainable, motivated cybersecurity workforce.

1. Career Development Opportunities

Organizations can increase employee satisfaction and retention by providing clear career paths, skill development opportunities, and structured training, mentorship, and growth programs. Rotational and exchange programs can further diversify skill sets and enhance the work experience. Competitive pay, performance incentives, and recognition programs can also improve employee satisfaction and reduce attrition. Ongoing technical and soft skills training helps employees address emerging threats and challenges, while a culture of continuous learning boosts confidence, commitment, and organizational resilience. Ultimately, employee recognition, career development opportunities, and competitive compensation contribute to a thriving and

[5] https://www.tines.com/reports/state-of-mental-health-in-cybersecurity/

engaged workforce. Smaller organizations may not be able to provide every employee with their choice of advanced career opportunities but having a better skilled workforce will pay off even if the employees are retained for only a few additional years. We can look to the retention impact of apprenticeship programs where organizations invest in the dedicated education, training, and mentorship of employees – the positive return on investment and extended retention of these individuals demonstrates the value of providing employees with career progression opportunities including on-the-job learning (Apprenticeship.gov data).

2. Support Career Development through Structured Plans and Mentorship

To retain top talent, cybersecurity professionals need clear career pathways and regular opportunities for skill enhancement. Structured career development plans emphasizing leadership opportunities and promotions can help employees see a long-term future within the organization. With mentorship programs, especially for candidates who might be career switching or upskilling, organizations can increase engagement and foster a sense of belonging. An ISC2 study in 2024 shows that mentorship is vital for retaining such talent. To implement this effectively, we recommend:

a. Provide employees with a clear and achievable career path, emphasizing promotions and lateral moves. Clear progression pathways motivate employees to envision their future within the organization.

b. For less experienced employees, mentorship creates a sense of community and guidance, improving retention. Senior professionals should be assigned to mentor junior staff. Create a defined mentoring program that establishes goals for the year, with expected numbers of hours the mentor/mentees will meet, activities for them to work on. Recognize excellence for those who participate and help to develop and retain junior talent.

c. Regular access to certifications (e.g., CISSP, CompTIA Security+) and training ensures that employees remain engaged and up-to-date in their skills. According to the "7 Proven Strategies to Recruit and Retain Remote Cyber Talent" report (ISC2, 2024), continuous education is critical to combating professional stagnation. Provide opportunities to learn during work hours – expecting

employees to pursue education and certifications during their after work time and on weekends leads to furthering the sense of burnout. Offering opportunities to attend in-person training, especially with senior staff can be seen as a form of recognition of talent.

3. Organizational strategies

To effectively improve employee retention and engagement in cybersecurity teams, HR leaders, talent acquisition staff, senior managers, and non-managerial staff must collaborate as part of an advisory team to implement regular employee surveys. These surveys, ideally conducted once per quarter, can provide valuable insights into team satisfaction, work-life balance, and professional development. Additionally, recommended "check-in" questions should be integrated into weekly 1:1 meetings between managers and their direct reports to ensure ongoing feedback. This combination of regular surveys and check-ins ensures continuous dialogue and allows for proactive adjustments.

By fostering a feedback-driven culture, organizations can identify and address challenges such as extended work schedules, unmet training needs, and mental and physical health concerns. To support this, we recommend the following key metrics and processes to evaluate employee engagement:

a. **Establish a Peer Network**. A peer network allows employees to share experiences and provide mutual support. This network can be instrumental in creating a sense of community and belonging, which is particularly important in high-stress industries like cybersecurity. Having opportunities for guest-speakers can allow cross-departmental information sharing, deepening relations across the organization. Employees who feel supported by their peers are more likely to remain engaged and committed to their work.
b. **Cultivate Safe Spaces for Feedback without Retaliation**. For feedback to be meaningful, employees must feel safe to voice their concerns and suggestions without fear of retaliation. Organizations should establish anonymous feedback systems, ensuring that all employees have a platform to express their opinions freely. To build trust, leadership must actively listen to feedback and respond empathetically, reinforcing a culture where feedback is valued and acted upon.

Implementing a zero-tolerance policy for retaliation and addressing feedback promptly demonstrates a commitment to transparency and a positive employee-supported culture, both of which are key to long-term employee satisfaction and retention.

c. **Building a Resilient and Innovative Cyber Workforce**. It takes more than creative hiring strategies to foster a resilient and innovative cybersecurity workforce. It requires intentional efforts to create a workplace where all employees feel respected, supported, and empowered to contribute. According to the Deloitte 2023 Global Human Capital Trends Report,[6] employee support is critical to engagement and retention. Organizations should create psychologically safe environments where all talent can thrive, and all employees are motivated to stay and innovate. Our key recommendations for achieving this include:

    i) A psychologically safe workplace ensures that all employees feel valued and supported, particularly for recent career entrants. Open communication and mentorship opportunities are essential for retaining junior talent.

    ii) Leaders must actively work to foster a supportive culture by prioritizing creative efforts in hiring and advancement, providing support to junior talent, and breaking down cultural norms that hinder employee career progress.

d. **Employee Engagement Scores**. Regular surveys are essential to capturing employee engagement levels within the cybersecurity team. Utilizing metrics such as the Employee Net Promoter Score (eNPS) allows organizations to gauge overall sentiment and satisfaction, clearly indicating team morale and engagement. Regularly assessing this metric helps organizations track engagement and implement timely interventions if needed.

e. **Turnover and Retention Rates**. Organizations should continuously monitor turnover rates within their cybersecurity teams to better understand employee retention and attrition trends. A closer look at the reasons behind departures—

[6] https://www2.deloitte.com/us/en/insights/focus/human-capital-trends/2023.html

whether due to burnout, lack of career growth, or other factors—can inform retention strategies. Analyzing these trends and focusing on retaining top performers and critical roles will enable organizations to reduce turnover and build a more stable, experienced team.

f. **Foster a Positive Workplace Culture**. A positive workplace culture that values innovation and employee engagement is essential for retention, especially cybersecurity. A lack of engagement can lead to high turnover. According to 2023 WiCyS research, exclusion is a significant factor in attrition. Leaders who foster respect and engagement contribute to higher retention and morale. Additionally, engaged teams drive innovation and are better equipped to solve complex problems. Research from WiCyS and the N2K Cyber Talent Study reveals that such leadership helps "break the glass ceiling" and fosters environments where innovation thrives.

g. **Organizational strategies.** Management can cultivate a more robust cybersecurity workforce by fostering a respectful, transparent, and psychologically safe workplace culture. Such an environment promotes collaboration, innovation, and open communication, leading to increased job satisfaction and reduced turnover. Engaged leadership, offering regular feedback and career development support, is essential for employee retention.

4. Work-Life Balance and Burnout Prevention

Strong leadership is indispensable to retain top talent and drive long-term engagement in today's cybersecurity environment. A key element of effective leadership is a genuine commitment to employee well-being and development. With growing evidence of the mental health challenges faced by cybersecurity professionals, leadership must prioritize proactive, structured programs that focus on mental health, emotional intelligence, and continuous development. According to the a study from Tines in 2024, 64% of cybersecurity professionals report that their mental health impacts their productivity, emphasizing the need for leaders to support and enhance employee well-being initiatives actively.

By committing to these initiatives, organizations can create an environment that values personal and professional growth. The following structured programs are essential for fostering a healthy, engaged workforce:

a. **Implement Regular Well-being Check-Ins**. Organizations should establish regular mental health check-ins to identify potential stressors early and provide support. These check-ins, whether through one-on-one meetings with HR or direct access to mental health professionals, ensure employees have a safe space to discuss their well-being. Create a conversation starter for managers to use in their employee one-on-one meetings to help guide appropriate and supportive conversations.

b. **Work-Life Balance Indicators**. Evaluating work-life balance is critical to preventing burnout and ensuring long-term employee well-being. Key metrics such as hours worked, overtime frequency, and leave usage can provide insight into potential overwork. If these indicators show excessive work demands, taking immediate action is essential by reviewing workloads and offering solutions such as adjusted schedules or additional support to help employees maintain a healthier work-life balance.

   According to the Gallup report[7], employees who can provide feedback anonymously are 4.6 times more likely to feel empowered to perform their best work. The report highlights that anonymous feedback mechanisms contribute to a more open and honest dialogue between employees and management, leading to better decision-making and improved employee satisfaction.

c. **Develop a Comprehensive Employee Assistance Program (EAP)**. Investing in a comprehensive Employee Assistance Program (EAP) is crucial for providing employees access to various support services. These services should include mental health counselling, financial advice, and legal assistance, which can significantly reduce stress and contribute to overall well-being. A strong EAP supports employees and demonstrates the organization's commitment to their holistic health.

[7] https://www.gallup.com/workplace/349484/state-of-the-global-workplace.aspx

d. **Create a Leadership Training Program Focused on Emotional Intelligence**. Effective leadership in cybersecurity requires more than technical expertise; it demands emotional intelligence (EQ). Leadership training programs should prioritize EQ to help managers develop the skills to understand, support, and motivate their teams. Leaders with high emotional intelligence are better equipped to foster trust, manage stress, and create a positive, supportive work environment, ultimately contributing to higher employee engagement and retention.

e. **Promote Work-Life Balance to Combat Burnout**. Burnout remains one of the top reasons cybersecurity professionals leave their jobs. To combat this, organizations should focus on promoting a healthy work-life balance. Flexible work arrangements such as remote options and flexible hours can significantly alleviate stress and prevent burnout. Moreover, actively managing workloads and setting boundaries for after-hours work can ensure employees maintain a healthy balance, reducing turnover risk. The 2023-2024 SHRM State of the Workplace Report[8] shows that neglecting work-life balance leads to higher turnover. Therefore, we recommend:

    i. Offering remote work, flexible hours, and condensed workweeks can significantly improve work-life balance and reduce stress.

    ii. Regularly assess and adjust employee workloads to ensure they are manageable, especially during peak periods such as major security incidents.

    iii. Set clear expectations for after-hours work. Avoiding excessive after-hours communication helps employees (and their managers) maintain a good work-life balance.

    iv. Managers must set the right example and demonstrate a meaningful commitment to their employees' well-being. Do not reward those who stay in the office at all hours of the day and night; encourage people to use their earned vacation and other leave time; check-in regularly with

[8] https://www.shrm.org/topics-tools/research/2023-2024-shrm-state-workplace

team members. When times of extra-long work are required due to cybersecurity events or operating system updates and application patching, managers and leadership should endeavor to “make it right” for their teams by helping them schedule some time off or stagger schedules.

VII. Conclusion

The cybersecurity industry is characterized by rapid evolution and increasing complexity, leading to a heightened demand for skilled professionals who can navigate these challenges. However, research indicates that retaining these valuable employees remains a significant issue for many organizations. Key factors influencing an employee's decision to stay or leave include workplace culture, which fosters a sense of belonging and loyalty, and the level of organizational support, including access to resources and training. Additionally, work-life balance is crucial; employees who feel overwhelmed or lack flexibility are more likely to explore other opportunities. Opportunities for career advancement, such as professional development programs and clear pathways to promotion, are essential for maintaining engagement and motivation.

There may be additional strategies that highly effective organizations will investigate to get ahead of shortages in staff, such as investments in new technologies, machine learning, and artificial intelligence. These discussions are outside of the scope of this report, where the authors have chosen to focus on actions that HR leaders and cybersecurity managers can put into immediate effect to address some of the most crucial cybersecurity retention challenges.

To tackle these challenges effectively, organizations must implement targeted and empathetic strategies that address the unique needs of their workforce. This could involve creating mentorship programs, promoting mental health resources, and enhancing communication channels to ensure employees feel heard and valued. By prioritizing employee well-being and

growth, companies can significantly improve retention rates, boost overall job satisfaction, and ultimately cultivate a more robust and resilient cybersecurity workforce.

VIII. References

1. NICE Strategic Plan (2021-2025)
2. Verizon 2024 Data Breach Investigations Report
3. IBM Cost of a Data Breach Report 2024
4. Black Fog 2024 Report, "Managing Expectations and Job Satisfaction for IT Security Leaders"
5. WiCyS 2024 Research
6. ISC2 July 2024 White Paper: "7 Proven Strategies to Recruit and Retain Remote Cyber Talent"
7. Gartner Predicts 2023 | Cyber Industry Focused on the Human Deal
8. National Institute of Standards and Technology (NIST), "Preparing a Cyber Ready Workforce," NIST IR 8355, 2024
9. The White House, Connecting Americans to Good Paying Jobs, Service for America initiative
10. ISACA Cybersecurity and Burnout: The Cybersecurity Professional's Silent Enemy
11. ISC2 Research
12. Cybersecurity Ventures and Evolution Equity Partners, 2024
13. The Deloitte 2024 Global Human Capital Trends Report
14. Fortinet Global Cybersecurity Skills Gap Report, 2024
15. Gallup, "State of the Global Workplace Report," 2024
16. SHRM, State of the Workplace Report, 2023-24
17. Tines research
18. SANS-GIAC Cyber Workforce Research Report, 2024
19. CyberSeek