

BITS, BYTES, AND LOYALTY

HOW TO IMPROVE
TEAM RETENTION

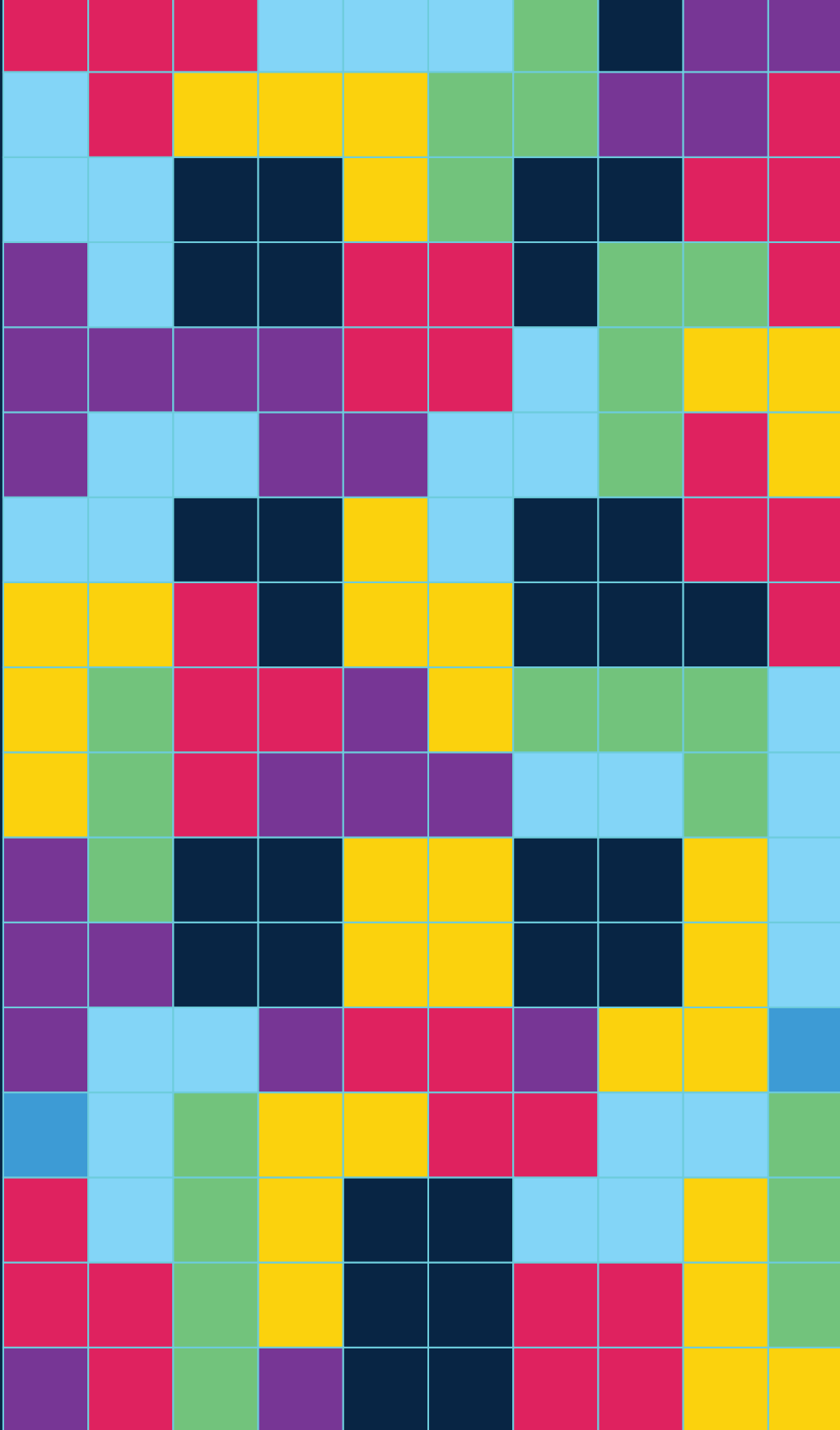
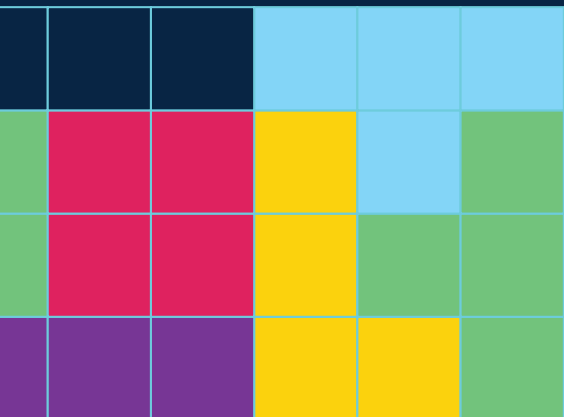




TABLE OF CONTENTS

EXECUTIVE SUMMARY

PAGE 2

APPROACH AND ACKNOWLEDGMENTS

PAGE 3

CURRENT THREAT LANDSCAPE

PAGE 6

KEY DRIVERS OF ATTRITION IN CYBERSECURITY

PAGE 8

BURNOUT AND STALLED GROWTH

RECOMMENDATIONS FOR PROFESSIONAL DEVELOPMENT AND RETENTION

PAGE 16

CONCLUSION

PAGE 23

THE VALUE OF INVESTING IN PEOPLE

CALL TO ACTION

PAGE 26

TURNING RECOMMENDATIONS INTO ACTION

GET INSPIRED

PAGE 28

SAMPLE CYBER PROFESSIONAL DEVELOPMENT
AND RETENTION PROGRAMS

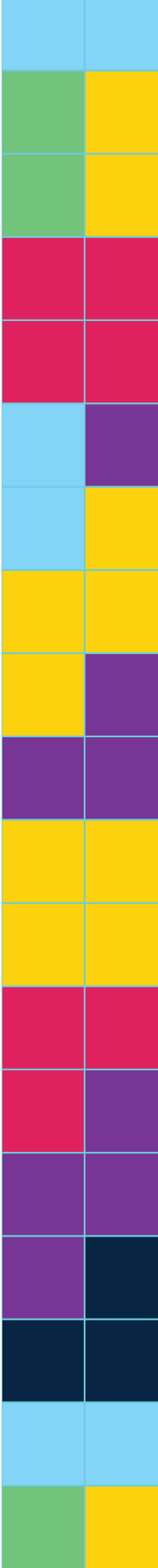
EXECUTIVE SUMMARY

The cybersecurity industry faces an acute talent crisis marked by high turnover rates and millions of unfilled roles across the world. Organizations struggle to remain skilled enough to protect critical networks and data as cyberattacks rapidly evolve. All this fuels the challenge of both recruiting necessary talent and developing the right retention and development efforts to maintain existing staff. This report provides recommendations on addressing the primary drivers of cybersecurity talent attrition and burnout: 1) excessive workloads and 2) lackluster career development opportunities.

These include anti-burnout employee wellbeing programs like flexible work options, continuous learning sessions, competitive rewards packages, community service opportunities, and transparent communication structures. Proactive retention and development measures offer many advantages, from cost savings due to reduced recruitment expenses plus stronger security postures through empowered teams and better knowledge retention.

Cybersecurity leaders interested in building more resilient workforces should use the findings from this report to identify areas for improvement at their own organizations. While industry-wide cooperation is a must for addressing the talent shortage, positive changes start with nurturing and empowerment activities that foster mutual success between organizations and employees.

This report provides recommendations on addressing the primary drivers of cybersecurity talent attrition and burnout: 1) excessive workloads and 2) lackluster career development opportunities.





APPROACH AND ACKNOWLEDGMENTS

TIMELINE

This paper concept was developed in virtual and in-person meetings of the Cyber Workforce and Education Coalition from November 2022 to November 2023.

ABOUT THE ASPEN U.S. CYBERSECURITY GROUP

The Aspen US Cybersecurity Group is a cross-sector public-private forum composed of former government officials, Capitol Hill leaders, industry executives, and respected voices from academia, journalism, and civil society that have come together to translate pressing cybersecurity conversations into action. At its November 2022 meeting, the group created a Cybersecurity Workforce & Education Coalition and created a list of workforce topics that could be addressed. To streamline our work, both groups focused efforts on cybersecurity workforce professional development and retention issues as well as recommendations.

CONTRIBUTORS

ASPEN U.S. CYBER WORKFORCE AND EDUCATION COALITION

Marene Allison
Former CISO

David Ames
Partner for
Cybersecurity, Privacy &
Forensics, PwC

Tatyana Bolton
Security Policy Manager,
Google

Judy Cheong
Recruiting Manager,
Cloudflare

Michael Daniel
President & CEO, Cyber
Threat Alliance

Brett DeWitt
Vice President, Global
Cyber & Tech Policy

Donald R. Dixon
Co-Founder &
Managing Director,
ForgePoint Capital

James Durbano
Senior Director,
Technical Talent
Development, Northrop
Grumman Corporation

Nathaniel Gleicher
Director and Head of
Security Policy, Meta

Beth Harvey
Director of People and
Culture, IronNet Security

Niloofer Howe
Senior Operating
Partner, Energy Impact
Partners

Bruce Johnson
Director, Federal Affairs
–Labor, Workforce, and
Education Policy, The
Boeing Company

Jodie Kautt
Vice President, Cyber
Security, Target

Bonnie Leff
Senior Vice President,
Corporate Security
Program Management,
Mastercard

Herb Lin
Senior Research Scholar,
Research Fellow,
Stanford University

Nicole McKoin
Director of External
Engagement, Target

Chandra McMahon
CISO, CVS Health

Stacy O'Mara
Head of Advanced
Cybersecurity Solutions
& Partnerships,
Mandiant Public Sector

Nancy Schuehler
Head of Cyber Strategy
and PMO, Verizon Cyber
Security

Richard Seiersen
Chief Risk Officer,
Resilience

ASPEN U.S. CYBERSECURITY GROUP

GROUP CO-CHAIRS

Yvette Clarke
Co-Chair, U.S House of
Representatives

Yasmin Green
CEO, Jigsaw Google

Christopher Krebs
Co-Chair Senior,
Newmark Fellow in
Cybersecurity, Aspen
Digital

Gary Steele
President & CEO,
Splunk

GROUP LEADERSHIP

Nicole Tisdale
Senior Advisor, Cyber
Workforce and
Education, Aspen
Digital

Yameen Huq
Director, US
Cybersecurity Group,
Aspen Digital

Robert Taj Moore
Former Director, US
Cybersecurity Group,
Aspen Digital

Katie D'Hondt Brooks
Director, Global
Cybersecurity Group,
Aspen Digital

Jeff Greene
Senior Director,
Cybersecurity Programs,
Aspen Digital

John P. Carlin
Strategic Advisor and
Chair Emeritus for
Cybersecurity, Aspen
Digital

GROUP MEMBERS

Katherine Adams

Senior Vice President
and General Counsel,
Apple

Marene Allison

Former CISO

Sara Andrews

Global CISO and Senior
Vice President, PepsiCo

Monika Bickert

Head of Product Policy
and Counterterrorism,
Facebook

Geoff Brown

Senior Vice President,
Arete

Tom Burt

Corporate Vice
President, Customer
Security and Trust,
Microsoft

Vinton G. Cerf

Chief Internet
Evangelist, Google

Dr. Lorrie Cranor

Director, CyLab Security
& Privacy Institute

Michael Daniel

President, Cyber Threat
Alliance

Noopur Davis

Corporate EVP, Chief
Information Security and
Product Privacy Officer,
Comcast

John Demers

Corporate Secretary,
The Boeing Company

Jim Dempsey

Policy Advisor, Stanford
Program on Geopolitics,
Technology, and
Governance

Donald R. Dixon

Co-Founder &
Managing Director,
ForgePoint Capital

Sue Gordon

Rubenstein Fellow, Duke
University

Vishaal Hariprasad

Co-founder and CEO,
Resilience

Niloofar Razi Howe

Senior Operating
Partner, Energy Impact
Partners

Sandra Joyce

VP, Mandiant
Intelligence at Google
Cloud

Sean M. Joyce

Head of Global and US
Cybersecurity and
Privacy, PwC

Jodie Kautt

Vice President, Cyber
Security, Target

Sam King

CEO, Veracode

Dr. Herb Lin

Senior Research Scholar
for Cyber Policy and
Security, Stanford
University

Brad Maiorino

Corporate Vice
President and CISO,
Raytheon Technologies

Jeanette Manfra

Global Director for
Security and
Compliance, Google

Chandra McMahon

CISO, CVS Health

Tim Murphy

Chief Administrative
Officer, Mastercard

Craig Newmark

Founder, Craig
Newmark Philanthropies

Dr. Gregory Rattray

Adjunct Professor,
Columbia University
SIPA

Nasrin Rezai

Senior Vice President
and CISO, Verizon

David Sanger

National Security
Correspondent, The
New York Times

Dr. Phyllis Schneck

Vice President and
CISO, Northrop
Grumman Corporation

Bruce Schneier

Fellow, Berkman-Klein
Center & Lecturer,
Harvard Kennedy School

Charley Snyder

Head of Security Policy,
Google

Alex Stamos

Adjunct Professor,
Stanford University

Alissa Starzak

Vice President Global
Head of Public Policy,
Cloudflare

Bobbie Stempfley

Vice President of
Cybersecurity, Dell
Technologies

Scott C. Taylor

Board Member,
Strategic Advisor, and
Former General Counsel

Dr. Hugh Thompson

Managing Partner,
Crosspoint Capital
Partners

Jack Weinstein

Professor, Boston
University

Dr. Jonathan W.

Welburn
Researcher, RAND
Corporation

Michelle Zatlyn

Co-founder & COO,
Cloudflare

CURRENT THREAT LANDSCAPE

Organizations of all types require qualified security staff to protect their critical systems and data assets. Global demand for cybersecurity talent dramatically outpaces supply, resulting in a workforce shortage reaching crisis proportions. Estimates vary, but one study found a shortage of 3.12 million cybersecurity professionals globally.¹ This staggering figure underscores the immense recruitment needs facing the field.

Retaining skilled employees is equally crucial for building a robust workforce pipeline in the long-term. Losing and replacing employees carries substantial costs, often equivalent to 20% or more of the departing employee's annual salary when factoring in lost productivity and training expenditures during the vacancy period.

Losing and replacing employees carries substantial costs, often equivalent to 20% or more of the departing employee's annual salary.

INADEQUATE STAFFING LEVELS

Many organizations lack adequate cybersecurity staffing to secure systems effectively. In a 2022 survey, 70% of cybersecurity workers reported feeling their employer doesn't have an adequate cybersecurity team to be effective.² This indicates teams are severely understaffed, hampering an organization's security posture. The talent shortage leads directly to issues with understaffing and its consequences.

¹ (ISC)². "2021 Cybersecurity Workforce Study." International Association of Privacy Professionals, <https://iapp.org/resources/article/isc2-2021-cyber>.

² (ISC)². "2022 Cybersecurity Workforce Study." ISC2. <https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf>

HEAVY WORKLOADS AND BURNOUT

Understaffing frequently results in excessive workloads and employee burnout. In 2020, 70% of surveyed cybersecurity professionals stated they are directly affected by talent shortages.³

Understaffing frequently results in excessive workloads and employee burnout.

PLANNED EXODUS

Turnover intention, or the self-reported likelihood or intention to leave their current job or position in the near future, among cybersecurity professionals is worryingly high.⁴ A survey revealed 30% of cybersecurity workers plan to “move to a different career or profession at some point in the future.”⁵ This signals deeper systemic issues influencing job satisfaction and retention. Without addressing these problems, organizations will continue to bleed talent and suffer from instability in their security teams. All these factors combine to produce troubling turnover levels.

Proactive retention strategies are essential for building productive, stable teams that can secure systems over the long haul.

These statistics paint a sobering picture of the cybersecurity retention crisis. While recruitment remains important, organizations need to couple it with engagement initiatives focused on

- ³ Security Staff. “71% of organizations are impacted by cybersecurity skills shortage.” *Security Magazine*. September 5, 2023. <https://www.securitymagazine.com/articles/99865-71-of-organizations-are-impacted-by-cybersecurity-skills-shortage>.
- ⁴ ZDNet. “Bad News: The Cybersecurity Skills Crisis is About to Get Even Worse.” ZDNet, <https://www.zdnet.com/article/bad-news-the-cybersecurity-skills-crisis-is-about-to-get-even-worse/>.
- ⁵ Trellix. “Trellix Survey Findings: A Closer Look at the Cyber Talent Gap.” Trellix, <https://www.trellix.com/en-us/about/newsroom/stories/perspectives/trellix-survey-findings-a-closer-look-at-the-cyber-talent-gap.html>.

the workforce already in place. Proactive retention strategies are essential for building productive, stable teams that can secure systems over the long haul. Tackling cybersecurity's retention challenges must become a priority.

KEY DRIVERS OF ATTRITION IN CYBERSECURITY: BURNOUT AND STALLED GROWTH

Understanding what causes cybersecurity professionals to leave their roles is crucial for developing effective retention strategies. A review of recent research and surveys has revealed two primary factors driving talent loss in the field: burnout from unrelenting workloads and the constant threat of system disruptions and attacks as well as insufficient career development and continuous skills training opportunities.⁶ By exploring the dynamics and impacts of these two key attrition drivers, organizations can gain insights into creating policies and programs to improve retention.

The always-on nature of defending systems from persistent and evolving threats is mentally taxing. There are no “off-days” in cybersecurity like there are for even other demanding jobs.

⁶ ZDNet. "Cybersecurity Burnout is Real and It's Going to be a Problem for All of Us." ZDNet, <https://www.zdnet.com/article/cybersecurity-burnout-is-real-and-its-going-to-be-a-problem-for-all-of-us/>.

BURNOUT FROM THE “ALWAYS ON” CULTURE

In many industries, burnout is a concern—but perhaps none more so than cybersecurity. The always-on nature of defending systems from persistent and evolving threats is mentally taxing. There are no “off-days” in cybersecurity like there are for other demanding jobs like investment bankers, surgeons, or first responders. In fact, attacks actually spike over holidays for a variety of reasons.⁷ The threats never sleep and by extension neither can security analysts, engineers, and leaders. This unceasing threat landscape forces many cybersecurity teams into a persistent state of high alert. New attacks barrage systems daily, eliminating any downtime. Working long hours and being on call for overnight emergency response becomes a regular expectation.

Workforce gaps commonly leave teams understaffed, exacerbating burnout by spreading existing employees dangerously thin.

Excessive workloads also contribute heavily to burnout levels. Surveys find a majority of cybersecurity professionals report concerning symptoms like anxiety, depression, and exhaustion. Workforce gaps commonly leave teams understaffed, exacerbating burnout by spreading existing employees dangerously thin.

HEAVY WORKLOADS COMPOUND BURNOUT

Excessive workloads also contribute heavily to cybersecurity burnout levels. A recent survey found 62% of cybersecurity professionals reported a spike in their workload and responsibilities over the past few years.⁸

⁷ Wetzig, Cayley. “Cyber Attacks During Holidays: Why The Spike?” *ThriveDX*, 2 Nov. 2022, <https://thrivedx.com/resources/article/cyber-attacks-during-holidays>.

⁸ Information Systems Security Association (ISSA) & Enterprise Strategy Group (ESG): “The Life and Times of Cybersecurity Professionals 2021.” ISSA & ESG, <https://www.issa.org/wp-content/uploads/2021/07/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Jul-2021.pdf>.

UNDERSTAFFING OVERBURDENS EMPLOYEES

With the severe talent shortage, teams are chronically understaffed and each employee has to take on bigger workloads. A study found 1 in 10 CISOs labor an extra 20-24 hours per week on top of their regular full-time role.⁹ Even frontline analysts are not immune—an industry report revealed 39% of the surveyed businesses receive a volume of alerts ranging from 100 to 1,000 each day.¹⁰

This state of constant overload and stress drives professionals to eventually burn out and leave the field entirely. Without better workload balancing and a focus on mental health, the cybersecurity industry will continue to lose top talent to exhaustion and burnout.

Many employers fail to adequately invest in training programs and growth initiatives. Without the ability to actively expand their skills, employees become dissatisfied, leading to departures.

INSUFFICIENT GROWTH OPPORTUNITIES

Besides burnout, employees often leave roles because of insufficient opportunities for career development and continuous skills training. With rapidly growing technologies, methodologies, and regulations, ongoing learning is essential for cybersecurity professionals to stay relevant and add value. However, many cybersecurity employees currently do not believe they are getting adequate professional development or career growth opportunities from their employers. This lack of investment in talent hampers retention efforts across the industry. Many employers fail to adequately invest in training programs and growth initiatives. Without the ability to actively expand their skills, employees become dissatisfied, leading to departures.

⁹ Tessian: "Reclaiming Hours Lost to Cybersecurity Incidents." Tessian, https://www.tessian.com/research/ciso-research/?utm_medium=online&utm_source=pr&utm_campaign=losthours-2111

¹⁰ Torgersen, Dana. "The automation hype is real for SOC teams: unpacking the Dimensional Research '2020 State of SecOps and Automation' report." *Dimensional Research*, 9 July 2020. <https://www.tessian.com/resources/report-cisos-lost-hours>.

TOO FEW GET ADEQUATE TRAINING

As one expert observed, “There is a cumulative impact here: You don’t have enough people, the people you have don’t have the right skills and the people that you have aren’t getting the right training.”¹¹ Studies validate this concern—a recent report found only 38% of cybersecurity professionals feel their organization provides the appropriate level of training to keep their skills current amidst business and IT changes.¹²

STAGNATING SKILLS INCREASE TURNOVER

Without consistent access to upskilling, employees’ expertise can stagnate as the field advances. Stalled skills development may leave professionals feeling dissatisfied, making them more likely to quit. Turnover intention grows without growth opportunities.

FEAR OF LOST INVESTMENT IN HUMAN CAPITAL


Some organizations shy away from investing in development out of fear employees will leave afterwards. However, avoiding growth opportunities can be counterproductive. Losing tenured staff means losing years of accumulated experience and institutional knowledge that is not easily replaced. At the same time, continuous learning is key for maintaining talent. A survey revealed 76% of employees say they’re more likely to stay with a company that offers continuous training opportunities to upgrade their skills.¹³

Developing cybersecurity talent takes time and dedication, and continuous professional development is essential in the rapidly changing cybersecurity landscape.

¹¹ Information Systems Security Association (ISSA) & Enterprise Strategy Group (ESG): “The Life and Times of Cybersecurity Professionals 2021.” ISSA & ESG, <https://www.issa.org/wp-content/uploads/2021/07/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Jul-2021.pdf>.

¹² Ibid

¹³ TalentLMS and the Society for Human Resources Management (SHRM): “The State of L&D in 2022.” TalentLMS, <https://www.talentlms.com/employee-learning-and-development-stats>.



Developing cybersecurity talent takes time and dedication, and continuous professional development is essential in the rapidly changing cybersecurity landscape. However, many organizations do not invest enough in ongoing training opportunities. This skills stagnation contributes to talent losses. With new threats constantly emerging, cybersecurity professionals need to regularly expand their skills and knowledge. A study found 82 percent of employers report a shortage of cybersecurity skills.¹⁴ 71 percent believe these talent gaps directly damage their organizations.¹⁵ Without consistent access to new training, employees' expertise can stall and lead to stagnant, inefficient teams.

BENEFITS OF ADDRESSING BOTH BURNOUT AND LACK OF DEVELOPMENT

DEVELOPMENT INVESTMENTS CAN BOOST LOYALTY

Robust training often boosts loyalty over exit by developing stronger ties between employers and employees. Employees appreciate when employers facilitate their growth and are more inclined to stay. Investing in an employee's career trajectory and skills shows commitment to their success. This nurturing environment fosters motivation, engagement, and loyalty.

RETENTION CREATES COMMUNITY

Developed talent who stay also foster community within organizations. They mentor newer employees, share knowledge, and lead teams. Keeping tenured professionals is vital for building connections. Long-time employees become pillars of the organizational culture. They set standards, share history, and pass on knowledge that benefits the entire community.

STABILITY ATTRACTS TOP TALENT

A strong learning culture also better positions organizations to attract talent externally. Professionals seek environments that will nurture their skills. In competitive hiring climates, skilled cybersecurity job seekers actively look for employers invested in continuous development. A robust training culture signals an appealing work environment.

¹⁴ Center for Strategic and International Studies: "The Cybersecurity Workforce Gap." CSIS, <https://www.csis.org/analysis/cybersecurity-workforce-gap>.

¹⁵ *ibid*

STRONGER SECURITY POSTURE

Burned out staff struggle to implement best security practices and respond decisively to incidents. Empowered professionals operating at full capacity better identify and mitigate risks. Similarly, underdeveloped teams lack the continuous training required to defend against rapidly evolving threats. Investment in continuous learning ensures teams have cutting-edge skills to secure critical systems and data.


INCREASED PRODUCTIVITY

Burnout severely hampers workforce productivity through disengagement, sickness, and absenteeism. Preventing fatigue allows for optimal idea generation and execution. Insufficient growth opportunities also dampen productivity by leaving staff ill-equipped for new challenges. Providing continuous skills development maximizes workforce efficiency and innovation capabilities.

Burnout does not affect all cybersecurity employees equally. Marginalized groups, including women and professionals of color, often take on additional duties. These extra responsibilities can compound burnout.

INEQUITABLE IMPACTS ON MARGINALIZED GROUPS

Burnout does not affect all cybersecurity employees equally. Marginalized groups, including women and professionals of color, often take on additional duties like mentoring and supporting diversity initiatives. On top of their existing heavy workloads, these extra responsibilities can compound burnout. However, more research needs to be conducted to fully understand how burnout disproportionately affects underrepresented groups in cybersecurity. Without equitably distributing workloads and considering the unique challenges faced by minority groups, cybersecurity risks losing diversity, in addition to losing talent overall.



Lack of career development and continuous learning also tends to affect marginalized professionals inequitably. Marginalized professionals suffer more when there are no programs or opportunities that provide formal continuous learning for professional enhancement. Minority employees often report lower access to sponsorships, high-visibility projects, and training programs than their non-minority counterparts. As technology transforms rapidly in their field, marginalized employees are left behind without access to initiatives for skill development that benefit all. These workers can't keep up with the latest technology if they don't have access to it. By promoting ongoing professional development, underrepresented groups can gain access to leadership positions and organizations increase their diversity.

If we don't consider the unique challenges faced by minority groups and allocate equal workloads and resources, diversity in cybersecurity will be lost.

The pressure to prove yourself by highlighting your capabilities are disproportionately felt by marginalized groups in cybersecurity. Prioritizing inclusive strategies for development is essential. Marginalized groups in cyberspace face added pressure in their efforts to establish themselves and show their abilities.

Minorities are often under pressure to perform better and exceed expectations than their majority counterparts to achieve advancement and opportunities in society. Overtime work compounds these effects, increasing burnout risk. Cultural pressure often leads individuals to give up their unique qualities or authenticity to conform to expectations. The cognitive or "mental" burden associated with code-switching (altering one's language, behavior, and expressions to fit different cultural or social contexts) often increases and causes fatigue.

It is not indulgent to be able to be fully present at work. If we don't consider the unique challenges faced by minority groups and allocate equal workloads and resources, diversity in cybersecurity will be lost. Instead of putting this burden on marginalized professionals, organizations should focus on ways to improve performance and integrate their systems. Increased retention will be achieved by ensuring equal access, inclusive cultures, and real empowerment.

BENEFITS OF SUPPORTING MARGINALIZED GROUPS

STRENGTHENING DIVERSITY, EQUITY, INCLUSION, AND ACCESSIBILITY

By taking concrete steps to achieve DEIA goals, an organization shows that it is committed to diversity and equity. All professionals have the same opportunity to excel. Providing equitable access to wellness resources and growth initiatives shows an organization's commitment beyond words. It ensures professionals from all backgrounds can thrive.

RETAINING DIVERSE PERSPECTIVES

Acknowledging and preventing disproportionate fatigue and skills stagnation enables retention of diverse perspectives and identities within teams. This fosters creativity, innovation and understanding.

UNLOCKING SUPERIOR PERFORMANCE

Reduced fatigue and stagnant skills help teams to keep different perspectives, while creating a collaborative working environment. When diverse, equitable, inclusive, and accessible teams work together efficiently, team performance is enhanced and drives business outcomes. Supporting minority employees maximizes the potential of the entire team.

ENHANCING COMMUNITY TIES

The key to strengthening local ties is by engaging unrecognized groups within shared communities. This opens the door for volunteerism, partnerships, and peer learning. Supporting under-represented groups fosters community connections.

LIVING ORGANIZATIONAL VALUES

Engaging with minority employees helps foster core values like belonging, justice, and empowerment. It builds an ethical and humane organizational culture.



RECOMMENDATIONS FOR PROFESSIONAL DEVELOPMENT AND RETENTION

To invest in employees and increase retention, organizational strategic priorities must include employee health, empowerment, and development. Potential initiatives include:

COMMUNITY OUTREACH AND VOLUNTEER OPPORTUNITIES

Enabling employees to give back to their communities develops their skills and leadership abilities. This boosts engagement, well-being, and retention by connecting work to a larger purpose. Collaborate with nonprofits, schools, and other community groups to facilitate cybersecurity volunteer initiatives for employees. Potential partners and projects could include:

1. Cybersecurity education programs with schools and youth organizations.
2. Providing cybersecurity services to nonprofits at low or no cost.
3. Joining industry groups offering pro bono services.
4. Sponsoring hackathons and coding events for students.
5. Guest speaking at conferences and community events.
6. Mentoring students interested in cybersecurity careers.
7. Volunteering with diversity-focused groups.

Organizations offering aligned programming include:

- [CyberPeace Institute's CyberPeace Builders Program](#)
Connects corporate cybersecurity professionals to nonprofits needing support.
- [Girl Scouts' Cybersecurity Basics badge](#)
Equips girls grades 1–12 with cybersecurity skills.
- [Vets in Tech Mentorship Program](#)
Facilitates cybersecurity career mentoring for veterans and military spouses.
- [WiCyS Mentorship Program](#)
Provides career development mentoring for women in cybersecurity.

COMPETITIVE COMPENSATION BENCHMARKING

Retaining cybersecurity professionals requires more than just a paycheck. Standard benefits, such as health insurance, retirement contributions, and paid time off, form the cornerstone of a benefits package. But the changing ethos of the modern workplace mandates creative, tailored offerings. To retain top cybersecurity talent, it's imperative to offer competitive compensation packages that adapt to the evolving workplace. A mix of foundational benefits, modern perks, innovative offerings, and budget-friendly bonuses can ensure a satisfied and committed workforce. Regularly review and equitably adjust compensation packages including salary, benefits, and perks to ensure offerings remain competitive compared to industry standards. Sample offerings:

1. Core Benefits

- Health insurance, retirement contributions, and paid time off are foundational.

2. Modern Perks

- Rejuvenation: Offer 1-2 month sabbaticals for refreshment and refocusing.
- Community Involvement: Support pro bono work for nonprofits.

- Wellness: Introduce massage services, fitness sessions, and counseling.
- Education: Promote continuous learning via stipends or leave.
- Flexibility: Embrace remote work, varied hours, and generous time-off.

3. Innovative Offerings:

- Family Support: Provide onsite childcare or stipends.
- Financial Relief: Assist with student loan repayments.
- Guidance: Offer career coaching.
- Remote Work: Supply home office stipends.
- Team Unity: Organize team bonding activities.
- Eco-Friendly Commute: Incentivize green commuting methods.

4. Budget-friendly Benefits:

- Balance: Prioritize additional paid time off and remote work.
- Recognition: Boost morale with simple, regular acknowledgments.
- Learning: Offer modest professional development stipends.
- Community: Host informal team gatherings.
- Milestones: Recognize tenure and give bonuses for successful employee referrals.

FACILITATED MENTORSHIP OPPORTUNITIES

Creating mentorship opportunities within your organization can facilitate organic learning and growth opportunities.

Pairing junior employees with more experienced staff enables knowledge sharing and nurtures professional development.

Consider “Reverse Mentorships” where younger or newer employees are paired with experienced or senior leaders. The junior employee mentors the leader on newer topics like emerging technologies, social media, diversity issues, etc to facilitate cross-generational learning. Potential program elements include:

1. Allowing staff to volunteer as mentors or request to be paired with one.
2. Formalizing mentor-mentee relationships and expectations.
3. Providing tools and resources to support meaningful mentorships.
4. Hosting group mentoring events to network and share experiences.
5. Recognizing outstanding mentors and mentees.
6. Tracking program participation and satisfaction rates.
7. Soliciting feedback to improve the program.

HEALTH AND WELLNESS OFFERINGS

Prioritizing flexibility, rest, health, and sustainability fosters positive culture and prevents fatigue. Employees who feel empowered to manage their wellbeing are more engaged, productive, and loyal. Implement policies and programs focused on employee wellbeing and work-life balance to prevent cybersecurity professional burnout. Consider introducing flexible schedules, remote work options, meditation resources, counseling services, and other wellness benefits because sustainability and work-life balance can prevent burnout. Potential offerings include:

1. Flexible work hours and location policies.
2. Generous paid time off allowances.
3. Remote work and telecommuting options.
4. Onsite wellness services like massages, fitness classes, counseling.
5. Emergency child care assistance.
6. Sabbatical programs to allow extended time off.
7. No-meeting times to allow focused work.
8. Boundaries on after hours contact and notifications.
9. Evaluating workloads and reallocating responsibilities if needed.

INTERNAL AND EXTERNAL CERTIFICATION PROGRAMS

Helping staff achieve certifications shows commitment from organizations. It empowers employees to prove their competencies while enabling growth. This retention strategy ensures workers have current credentials. Actively encourage and assist employees in obtaining relevant cybersecurity certifications through financial support and allotted study time. Supporting certification attainment enables skill development and career advancement. Example activities include:

1. Offering skill-based certifications, which validate expertise and upskill employees on skills relevant for current and potential future job expectations.
2. Facilitating prep courses for certification exams onsite or through subscriptions.
3. Providing stipends to cover exam fees and study materials costs.
4. Allowing use of professional development time allotments for certification study.
5. Being flexible with schedules to accommodate exam dates and preparation needs.
6. Rewarding certifications with bonuses, increased compensation, and recognition.
7. Reimbursing recertification fees to maintain active status.

REGULAR SKILLS TRAINING ON EMERGING THREATS AND TECHNOLOGIES

Offer training courses and learning opportunities to help employees stay updated on the latest cybersecurity threats, technologies, regulations, and mitigation best practices.

Ongoing training demonstrates commitment to nurturing talent with current expertise. Regular training initiatives not only empower the workforce with updated expertise but also foster loyalty and retention by showing investment in development. Example activities include:

1. Requiring annual or semi-annual required training on new attack methods, tools, and compliance issues.
2. Hosting voluntary training webinars from cybersecurity vendors on their latest product features.
3. Sponsoring conferences, workshops, and events related to relevant skill development.
4. Holding internal “lunch & learns” where employees present on projects and technologies.

ROTATIONAL PROGRAMS OFFERINGS


Develop rotational programs that allow employees to gain exposure to new roles and teams while breaking through stagnant talent development, growth and retention efforts.

Rotational training offers both cross-training benefits, as well as new perspectives. Examples might include:

- Rotating between various departments and projects on an annual or quarterly basis.
- Discovering other organization roles by job shadowing.
- Offering short-term projects or assignments designed to expand our capabilities.
- Offering debriefing sessions to reflect on lessons learned.

SAFE SPACES FOR EMPLOYEE FEEDBACK

Create formal channels to solicit employee feedback and listen to challenges and suggestions. The key is not just gathering feedback but showing it is heard—closing the loop—which is crucial for building trust. Responding to input shows care and fosters goodwill. Take action on concerns, implement ideas, and communicate changes being made based on input. Transparent communication channels give employees voice and influence. When organizations are responsive, retention and morale improve. Examples include:

- 
1. Conduct engagement surveys, then share results and action plans.
 2. Host open office hours for employees to ask leadership questions, then distribute a Q&A summary afterward.
 3. Create an anonymous suggestion channel, then implement highly voted ideas and announce which were selected.
 4. Perform stay interviews asking about retention drivers, then incorporate insights into updated retention plans.
 5. Hold focus groups on desired training, then release an expanded training calendar based on the feedback.

WORKFLOW AUTOMATION AND IMPROVEMENT SOLUTIONS

Identify opportunities to optimize the workflow, increasing productivity and enhancing work life. Examine processes to identify areas which could be automated or improved with tools for increased efficiencies. Then, identify redundant workflows which create fatigue among teams. Finally, research solutions which reduce burnout while streamlining work. There are various options, including:

- Automating manual data tasks through scripts, bots, and AI.
- Integrate collaboration/productivity tools into workflows in order to standardize processes.
- Removing systems requiring extensive maintenance.
- Accepting and using feedback from users as a method for recognizing pain points and ineffective tools.

WORKLOAD AND BURDEN BALANCING

Investigate workload and responsibility distribution across teams to ensure equitable allocation. Be cautious of tasks assigned to women, minorities and junior members of your team that do not advance their careers—such as recruiting or mentoring tasks without providing opportunities to become leaders or empower themselves as part of an inclusive workplace culture.

CONCLUSION: THE VALUE OF INVESTING IN PEOPLE

Some organizations avoid substantially investing in talent development because of fears that employees will promptly leave after receiving training. But research suggests the opposite is often true—employees felt greater loyalty when organizations actively enabled their success and growth.

Developed talent who remain become invaluable assets for their employers. They mentor newer team members, carry vital institutional knowledge, and strengthen organizational community bonds. Losing tenured professionals means losing these irreplaceable contributions.

A reputation for effectively incubating talent also enhances recruiting efforts, providing access to scarce in-demand professionals who seek growth opportunities. Investing in people ultimately pays dividends across organizational culture, security, operations, and reputation.

Some organizations avoid substantially investing in talent development because of fears that employees will promptly leave after receiving training. But research suggests the opposite is often true.

REDUCED TURNOVER AND RECRUITMENT COSTS

Thoughtful wellness, growth, and engagement initiatives reduce frustrations that drive turnover. Lower attrition saves substantial recruitment and onboarding costs. Losing and replacing employees carries enormous expenses when factoring in productivity loss, training, job posting fees, interviewing, and ramp up time.

STRONGER SECURITY POSTURE

Empowered professionals who feel valued and invested in their organization's mission are better at securing critical systems. In contrast, burned out, underdeveloped staff struggle to implement best practices and respond decisively to incidents.

IMPROVED RISK MANAGEMENT

Lost veteran professionals mean losing years or decades of irreplaceable institutional memory and situational fluency. Retained experts provide continuity and critical insights that new hires cannot immediately replicate. They identify emerging risks and patterns quickly.

HEALTHIER AND MORE COLLABORATIVE CULTURE

Investing in people promotes loyalty, connectivity and mentorship. Employees feel valued and are more inclined to stay when organizations demonstrate care for their welfare and growth. Retention and development creates bonds.

ENHANCED EMPLOYER BRAND AND RECRUITING ADVANTAGE

Commitment to talent development establishes reputations as an employer of choice. In today's competitive hiring climate, top professionals seek environments enabling personal and career success. Being known for nurturing people generates a recruiting edge.

The cybersecurity talent shortage makes recruiting proficient staff more essential than ever. But thoughtful retention and development initiatives focused on existing team members are equally critical.

The cybersecurity talent shortage makes recruiting proficient staff more essential than ever. But thoughtful retention and development initiatives focused on existing team members are equally critical. Burnout and stagnated growth currently drive unacceptable levels of attrition. Prioritizing programs focused on employee wellbeing, continuous learning, and engagement provides the most promising path forward.

While fully addressing the talent crisis requires collective effort across the industry, individual organizations can drive meaningful impact by starting small. With focus and initiative, businesses can implement effective retention initiatives to empower their people and strengthen culture. Nurturing and maintaining top talent must become both a moral and strategic imperative for employers. The cybersecurity workforce is irreplaceable human capital enabling organizational success. Their health, development and satisfaction should be paramount.

The cybersecurity talent shortage makes recruiting proficient staff more essential than ever. But thoughtful retention and development initiatives focused on existing team members are equally critical.

CALL TO ACTION: TURNING RECOMMENDATIONS INTO ACTION

Transforming suggested retention and development initiatives into reality requires planning, resources and sustained commitment. But organizations that proactively invest in empowering their teams will reap the rewards. By systematically following a timeline, organizations can lay a firm foundation for employee retention and empowerment programs, placing them at the forefront of addressing the industry's talent challenges. Here is concise guidance on activating the proposed programs over the next year:

1-YEAR TIMELINE FOR EMPOWERING CYBERSECURITY TALENT

MONTH 1-2:

Perform Current State Assessments: Evaluate current offerings and gather insights through surveys, interviews, and data analysis. Recognize any shortcomings or gaps in current initiatives.

MONTH 3:

Secure Leadership Buy-In: Develop and present the business case. Emphasize the immediate and long-term risks of inaction, aiming to gain strong executive support.

MONTH 4-5:

Develop Implementation Roadmaps: Draft a phased plan for recommended initiatives, considering your organization's capacity, budgetary constraints, and required sequence of actions. Form cross-functional teams to execute these plans.

MONTH 6-7:

Focus on User Experience: Begin the development of employee-centric programs, emphasizing simplicity and relevance. Conduct user tests to ensure alignment with employee needs and preferences.

MONTH 8-9:

Collect Ongoing Feedback: Launch pilot versions of your initiatives. Establish and track metrics related to participation, satisfaction, and impact. Begin collecting preliminary feedback to inform future refinements.

MONTH 10:

Reinforce Strategy Through Communications: Introduce the overarching strategy to the broader organization. Share the reasoning behind the initiatives and highlight early successes, positioning employees as invaluable strategic assets.

MONTH 11-12:

Refinement & Expansion: Using the feedback gathered, refine the initiatives and expand their reach. Celebrate milestones and continuously promote the value of the programs to the organization.



GET INSPIRED

SAMPLE CYBER PROFESSIONAL DEVELOPMENT AND RETENTION PROGRAMS

ORGANIZATION: CYBER THREAT ALLIANCE

Type of Organization

Non-profit

Name of Retention/ Development Program

Informal Development

Program Type

Both retention and development

Program Mission and Description

Encourages its staff to participate in webinars, write papers for publication, or submit presentations to speak at cybersecurity related conferences. Such work supports both the organization's mission of raising the level of cybersecurity across the digital ecosystem and our employee's development. Although the number of employees is very small (less than 10 employees at any given time), this program is important to staff based on their feedback.

Workforce Focus Areas

Mid-Level

DEIA-focused

No

Program Duration

Indefinite

Program Modality

Hybrid

Employee Eligibility/Criteria

All CTA employees are eligible.

Selection / Admission Process

CTA employees propose the activity they would like to engage in to the CEO for approval.

Benefits of Program to Employee

Increases personal knowledge and skills, expands the network of colleagues, and allows the exploration of new areas.

Benefits of Program to Organization

It provides exposure for CTA to relevant audiences as well as allowing us to retain employees for longer periods of time.

Incentives for Participation

No official incentives.

Number of Participants Selected

2

Participant Duties:

No official duties.

Mechanism for Employee Feedback:

Yes

Cost of implementation

\$

Effect on Organization

Experience is limited due to a small employee base, but CTA staff has provided positive feedback. Several have indicated that previous employers did not allow this sort of activity and they appreciated the freedom to pursue talks or serve on panels.

Timeline to Impact/Value

Immediate

Type of Organization

Private corporation

**Name of Retention/
Development Program**

Cyber TechStarter (Cohort)

Program Type

Both retention and development

Program Mission and Description:

Cyber TechStarter is designed to provide a flexible, self-paced learning environment for increasing employees' beginner and fundamental knowledge of cyber. We leverage the 70-20-10 or 3E development framework. It consists 70% of learning from on-the-job challenges—experiences, 20% from other people—exposure, and 10% from coursework—education. Cyber TechStarter is designed to provide a blend of experiences and exposure with education that is part of our participants' ongoing development.

Workforce Focus Areas

Introductory / Entry-Level

DEIA-focused

Yes

Program Duration

3 months

Program Modality

Online

Employee Eligibility/Criteria

Enterprise wide; Beginner-level knowledge of cyber; No formal education or training.

Selection / Admission Process

HR and Engineering teams nominate individuals from their organization to participate. Employees can also express interest in the cohort and these names are considered for nomination.

Benefits of Program to Employee

Expands cross-sector & network connections; Receives guidance from NG

SMEs; Gains insights from technical & functional leaders; Applies acquired skills to potential future roles; Understands career & follow-on development opportunities; Completes beginner & fundamental courses; Prepares for the CompTIA Security+ (SYO-601) exam.

Benefits of Program to Organization

An increase of employees moving into cyber-related jobs at NG, an increase in diversity at our higher technical job grades, a strong network across our company's cyber community, and strong retention metrics within this community.

Incentives for Participation

No financial incentive provided.

Number of Participants Selected

< 100

Participant Duties

Participants are required to complete all coursework and 2 CompTIA Security+ practice exams, attend all sessions, meet with their mentor, and complete / present their final project.

Mechanism for Employee Feedback

Yes

Cost of implementation

\$\$

Effect on Organization

Business results are currently being evaluated. Program aims to increase diverse representation at higher technical levels and increase the number of employees with cyber knowledge.

Timeline to Impact/Value

Participants are able to immediately apply what they learn back to their current job or to a future role. Application and business results are currently being evaluated 6 months after program completion and beyond.

Type of Organization

Private corporation

**Name of Retention/
Development Program**

Cyber TDP (On-demand)

Program Type

Both retention and development

Program Mission and Description

The Cyber Technical Development Path (TDP) communicates critical competencies and provides a roadmap of resources from beginner to advanced. From Cyber Architect to Systems Security Engineer to Test Engineer and Threat Analyst, for those seeking to enhance their cyber skillset and proficiency, the resources have been curated by cross-sector subject matter experts at Northrop Grumman. The Cyber TDP works in conjunction with the professional certifications channel—where featured prep resources are available on-demand, for key industry certifications, from providers such as CompTIA, Microsoft, Cisco and more.

Workforce Focus Areas

All

DEIA-focused

No

Program Duration

Varies by discipline (some >20 hours)

Program Modality

Online

Employee Eligibility/Criteria

Enterprise wide; Beginner to Advanced-level knowledge of cyber.

Selection/Admission Process

Through development planning, employees and managers can identify capabilities to build and develop resources to use, for both longer-term growth and nearer-term performance support.

Benefits of Program to Employee

Skill progression clarity and on-demand access to developmental resources can fuel professional growth, mastery, and credentialing (when formal certification is pursued).

Benefits of Program to Organization

Expertise and critical skill proficiency in key technical capability areas sustain our business and drive our innovation. Equipped talent are vital for program execution and winning new business.

Incentives for Participation

No financial incentive provided.

Number of Participants Selected

1,000s

Participant Duties

Learners must allot time and focus to glean from these development resources--and ultimately apply skills learned to their particular program/domain.

Mechanism for Employee Feedback

Yes

Cost of implementation

\$

Effect on Organization

Common, enterprise development paths capture valued and transferable skills from sector to sector—that can also be efficiently leveraged in design of technical development programs, like TechStarter.

Timeline to Impact/Value

Used as performance support or learning in the flow of work, returned value to the business can be immediate; longer-term acquisition of skills, including certifications can satisfy future contract requirements.

**ORGANIZATION:
TARGET**

Type of Organization

Private corporation

**Name of Retention/
Development Program**

eMIP

Program Type

Both retention and development

Program Mission and Description

eMIP: To prepare female and under-represented talent for leadership roles across tech. You can join the program as an existing team member or as a newly hired team member directly into the program. You will work with a cohort of peers and focus on building leadership skills through a variety of trainings and experiences.

Workforce Focus Areas

Senior

DEIA-focused

Yes

Program Duration

1 year

Program Modality

Hybrid

Employee Eligibility/Criteria

Already have the baseline technical skills needed to perform at a high-level individual contributor.

Selection/Admission Process

A variety of technical and soft skills screening process with the eMIP oversight committee.

Benefits of Program to Employee

They are better prepared for a leadership role and have not only the program support, but the support of a mentor and sponsor to help advocate for them and eventually help place them into a leadership role.

Benefits of Program to Organization

Brings more diverse leadership into the organization.

Incentives for Participation

Career growth.

Number of Participants Selected

5–10 per cohort

Participant Duties

Split their time between their day job as an individual contributor and their development program. Over time they take on more leadership duties within their team.

Mechanism for Employee Feedback

Yes

Cost of implementation

\$

Effect on Organization

Increased the number of female and under-represented front-line leaders.

Timeline to Impact/Value

12–24 months

Type of Organization

Private corporation

**Name of Retention/
Development Program**

Employee Engagement Teams

Program Type

Both retention and development

Program Mission and Description

Employee engagement teams are employee led groups with an executive sponsor that have the mission to drive cyber employee engagement with three primary goals. Goals include 1) fostering a sense of community across our cyber professionals, 2) strengthening cross functional team knowledge & connections by host internal learning opportunities for our cyber professionals, and 3) curating volunteer opportunities to serve our communities. Each goal is led by one of the three committees: Cyber Social, Cyber Learning & Connections, Cyber Citizens.

Workforce Focus Areas

Mid-Level

DEIA-focused

Yes

Program Duration

Ongoing annually

Program Modality

Online

Employee Eligibility/Criteria

Committees are run by volunteer cyber employees (all levels). Participation is for all Cyber employees (all levels).

Selection/Admission Process

Committees are refreshed annually and limited to 15–20 employees each. Employees volunteer for a one year commitment.

Benefits of Program to Employee

Drives employee engagement. Fosters community and contacts across the cyber organization to enable career growth opportunities. Provides sharing of best practices (skills, tools, processes and automation) to minimize department silos and allows employees to work horizontally.

Benefits of Program to Organization

Drives employee engagement and retention. Fosters community and contacts across the cyber organization. Provides sharing of best practices (skills, tools, processes and automation) across Cyber and promotes engagement by working together to serve local and virtual communities.

Incentives for Participation

Engagement with cyber professionals in other parts of the organization and engagement with cyber leadership. No financial incentives.

Number of Participants Selected

50–60

Participant Duties

2–3 hours per month commitment fulfilling the responsibilities of the cyber employee engagement committees.

Mechanism for Employee Feedback

Yes

Cost of implementation

\$

Timeline to Impact/Value

< 6 months

COPYRIGHT © 2024 BY THE ASPEN INSTITUTE

This work is licensed under the Creative Commons Attribution Noncommercial 4.0 International License.

To view a copy of this license, visit: <https://creativecommons.org/licenses/by-nc/4.0/>

Individuals are encouraged to cite this report and its contents. In doing so, please include the following attribution:

"Bits, Bytes, and Loyalty." Aspen Digital, a program of the Aspen Institute, Mar. 2024. CC BY-NC. <https://www.aspendigital.org/report/bits-bytes-loyalty/>

