



CYBERNEU

CYBERSECURITY SOLUTIONS & TRAINING

BLACK HAT USA 2026

Las Vegas, NV | August 1-6, 2026

RESEARCH PAPER | CYBERSECURITY WORKFORCE

The Cybersecurity Talent Imperative: Unlocking the Neurodivergent Advantage

A strategic analysis of the global cybersecurity hiring and retention crisis, and the high-yield workforce solution hiding in plain sight.

Prepared for: **Black Hat USA 2026 — CISO & Executive Track**

Audience: **CISOs, CTOs, Founders & C-Suite Executives**

Published: **August 2026**

Organization: **CyberNeu Inc. — 501(c)(3) Nonprofit, Certified Woman & Minority Owned**

LEARN MORE & PARTNER

CyberNeu.org

The Cybersecurity Talent Imperative: Solving the World's Most Critical Workforce Crisis Through Neurodivergent Inclusion

A Research Paper Presented at Black Hat USA 2026 | Las Vegas, Nevada | August 1–6, 2026

Prompt Engineering and oversight by Kirk Jaffe, Executive Director, CyberNeu.org: Written in the Collective Voice and Spirit of Jensen Huang (NVIDIA), Satya Nadella (Microsoft), and Jamie Dimon (JPMorgan Chase)

Presented in Partnership with CyberNeu.org

“The greatest competitive advantage in the modern era is not the algorithm you run — it is the mind that designs it. And the most powerful minds are often the ones we have spent decades overlooking.”

Executive Summary

The digital world is under siege. Every day, sophisticated adversaries — state-sponsored actors, ransomware syndicates, AI-enabled threat groups — probe the defenses of our financial systems, critical infrastructure, healthcare networks, and enterprise platforms. The first and most essential line of defense is human talent: the security engineers, threat hunters, incident responders, and forensic analysts who stand between civilization and digital catastrophe.

Yet in 2026, the global cybersecurity workforce gap has reached 4.8 million unfilled positions [1]. The workforce must grow by 87% to satisfy current demand [1]. Ninety percent of security teams report critical skills gaps [1]. And the cost of this deficit is not abstract: organizations with significant security staffing shortages face data breach costs that are, on average, \$1.76 million higher than their well-staffed counterparts [2].

At the same time, a vast and brilliant talent pool remains largely excluded from the workforce. Neurodivergent adults — individuals with autism spectrum disorder (ASD), attention deficit hyperactivity disorder (ADHD), dyslexia, dyspraxia, and related cognitive profiles — face unemployment rates as high as 40% [3]. In the United States alone, just 15% of adults with ASD are employed, and many of those who are employed hold positions that do not fully utilize their knowledge and skills [4].

This is not a coincidence. It is a systemic failure — a failure of hiring processes, a failure of imagination, and a failure of leadership. And it is one that we, as leaders of some of the world's most consequential technology and financial institutions, are uniquely positioned to correct.

This paper makes the case that the cybersecurity industry's talent crisis and the neurodivergent unemployment crisis are two sides of the same coin. The cognitive traits most associated with neurodivergence — intense focus, pattern recognition, analytical rigor, and unconventional problem-solving — are precisely the capabilities most needed to defend the digital world. By rethinking our approach to hiring, training, and retention, and by investing in organizations like CyberNeu.org that are building specialized pathways into the profession, we can close the talent gap, reduce breach costs, and transform millions of lives in the process.

The time for incremental action has passed. This is a strategic imperative.

Part I: The State of the Cybersecurity Workforce in 2026

1.1 The Scale of the Crisis

To understand the magnitude of the cybersecurity talent shortage, one must first understand the scale of the digital economy it is tasked with defending. Global cybercrime costs are projected to reach 10.5trillionannuallyby2025, upfrom3 trillion in 2015 [5]. Every organization with a digital footprint — which is to say, every organization of consequence — is a target.

Against this backdrop, the talent gap is staggering. The 2025 ISC2 Cybersecurity Workforce Study, the most comprehensive annual survey of the profession, found that the global cybersecurity talent gap has reached 4.8 million unfilled positions [1]. This

figure represents a workforce that must nearly double to meet current demand. The regional distribution of the gap underscores its global nature:

Region	Unfilled Positions
Asia-Pacific	3.4 million
China (single country)	2 million+
India	1 million+
North America (U.S.)	500,000+

Table 1: Regional Distribution of Cybersecurity Workforce Gap (Source: ISC2, 2025) [1]

In the United States alone, over 750,000 cybersecurity positions sit unfilled [6]. The Bureau of Labor Statistics projects that information security analyst roles will grow by 32% between 2022 and 2032, far outpacing the overall job market [7]. Yet the pipeline of new talent is not growing fast enough to meet this demand.

1.2 The Skills Most in Demand

The talent gap is not merely a headcount problem; it is a skills problem. According to ISACA and ISC2 research, 90% of cybersecurity teams report skills gaps [1]. The most difficult-to-fill capabilities include cloud security, AI/ML defense, zero trust architecture, digital forensics, incident response, and application security [1].

The emergence of AI as both a weapon and a shield has created an entirely new category of urgency. Threat actors are now leveraging AI to craft more convincing phishing campaigns, automate vulnerability discovery, and generate novel malware variants. Defenders must respond in kind — but the professionals capable of both understanding AI systems and applying them to security contexts are extraordinarily rare.

Skill Area	Demand Level	Average Salary Premium
Cloud Security	Critical shortage	+25–35%
AI/ML Security	Severe shortage	+30–40%
Zero Trust Architecture	High demand	+20–30%
Incident Response	Strong demand	+15–25%
Security Operations (SOC)	Moderate demand	+10–15%
Compliance/GRC	Steady demand	+5–15%

Table 2: Cybersecurity Skills in Highest Demand and Salary Premiums (Source: ISC2, ISACA, Industry Salary Surveys) [1]

1.3 The Structural Shift: Budget Constraints Compound the Talent Gap

A critical and often overlooked dimension of the 2026 talent crisis is that the primary barrier to hiring has shifted. For the first time in the history of the ISC2 annual study, economic pressures and budget cuts have overtaken a lack of qualified talent as the primary driver of staffing shortages [1]. Companies want to hire but cannot secure budget approval. This means that the solution is not simply to produce more candidates; it is to produce the right candidates — highly trained, immediately deployable professionals who can demonstrate clear ROI from day one.

This structural reality makes the case for specialized, employer-directed training programs even more compelling. When a corporation can direct its philanthropic investment toward training candidates for specific, pre-identified roles, the ROI calculation becomes straightforward.

Part II: The Human Cost — Burnout, Attrition, and the Retention Crisis

2.1 The Burnout Epidemic

The talent shortage creates a vicious cycle. As positions go unfilled, existing security professionals are required to carry heavier workloads, monitor more alerts, and respond to more incidents with fewer resources. The result is a burnout epidemic that is accelerating attrition at precisely the moment when retention is most critical.

In 2025, Sophos surveyed 5,000 IT and cybersecurity professionals across 17 countries. The findings were alarming: 76% of respondents reported experiencing cybersecurity fatigue or burnout either constantly, frequently, or occasionally over the prior year [8]. More troubling still, 69% reported that this burnout increased from 2023 to 2024 [8]. The problem is not stabilizing; it is worsening.

The consequences of burnout extend beyond the individual. Nearly half of burned-out professionals (46%) reported heightened anxiety about cyberattacks or breaches, 39% admitted to reduced productivity, and a third reported reduced engagement at work [8]. A burned-out security team is not merely less effective; it is actively more vulnerable. The very professionals charged with maintaining vigilance are the ones most at risk of missing the next critical alert.

2.2 The Retention Crisis

The annual turnover rate among security professionals is approximately 22% [9]. For context, the average cost to replace a cybersecurity professional — accounting for recruitment, onboarding, and the productivity ramp-up period — can range from 50,000toover100,000 per hire, depending on seniority and specialization. At a 22% turnover rate, a security team of 50 professionals is effectively replacing 11 people per year, at a cost that can easily exceed \$1 million annually before accounting for the security risk created by knowledge gaps during transitions.

The top reasons cybersecurity professionals leave their jobs include a lack of career growth opportunities, inadequate compensation relative to market rates, excessive workload, and a sense that their contributions are not valued [10]. These are not intractable problems. They are symptoms of a workforce management philosophy

that treats security professionals as interchangeable resources rather than rare and valuable strategic assets.

“I tell my CIO, our company’s IT department is going to be the HR department of agentic AI in the future.” — Jensen Huang [11]

The implication is profound: as AI takes on more routine security tasks, the humans who remain in the workforce will need to be more capable, more adaptive, and more engaged than ever before. Retaining and developing that talent is not a human resources function; it is a core business strategy.

2.3 The Diversity Deficit

The cybersecurity workforce is not only understaffed; it is dangerously homogeneous. Homogeneous teams are more susceptible to collective blind spots — the same cognitive biases, the same problem-solving frameworks, the same assumptions about how attackers think. In a field where adversaries are constantly innovating, cognitive diversity is not a nicety; it is a necessity.

Yet the industry has been slow to broaden its talent base. Traditional hiring processes — unstructured interviews, networking-based recruitment, credential-heavy screening — systematically favor candidates who fit a narrow profile. The result is a workforce that is less diverse, less innovative, and less capable than it needs to be.

Part III: The Neurodivergent Talent Pool — An Untapped Strategic Asset

3.1 Defining Neurodiversity

Neurodiversity is the concept that all human brains are diverse and function in unique ways. It is not a medical diagnosis but a framework for understanding the natural variation in human cognition. The neurodivergent umbrella encompasses a range of conditions, including:

- **Autism Spectrum Disorder (ASD):** Characterized by differences in social communication and interaction, often accompanied by intense focus, pattern recognition, and analytical precision.

- **Attention Deficit Hyperactivity Disorder (ADHD):** Characterized by patterns of inattention and/or hyperactivity-impulsivity, often accompanied by hyperfocus, creative thinking, and the ability to thrive under pressure.
- **Dyslexia:** A specific learning difference affecting reading and writing, often accompanied by strong spatial reasoning, big-picture thinking, and entrepreneurial instinct.
- **Dyspraxia:** A developmental coordination disorder often accompanied by strong verbal reasoning and creative problem-solving.

Estimates suggest that 15% to 20% of the global population is neurodivergent [12]. In the United States, this represents tens of millions of adults. Yet the employment rate for autistic adults is approximately 31%, compared to 54.7% for all disabled people and over 80% for the general population [4]. The neurodivergent unemployment rate runs at least three times higher than the rate for people with disabilities generally, and eight times higher than the general population [13].

3.2 Why Neurodivergent Minds Excel in Cybersecurity

The alignment between neurodivergent cognitive profiles and the demands of cybersecurity work is not incidental; it is structural. The skills that make a great security professional — meticulous attention to detail, the ability to identify anomalies in complex systems, sustained focus on repetitive analytical tasks, and the capacity to think like an adversary — are precisely the skills that many neurodivergent individuals possess in abundance.

According to a 2025 Forbes analysis, approximately 73% of neurodivergent professionals surveyed stated that cybersecurity aligns with their strengths, such as deep focus, lateral thinking, and pattern recognition [14]. ISC2's April 2026 snapshot found that 79% of neurodivergent cybersecurity professionals report feeling passionate about their work — on par with their neurotypical colleagues [15].

Consider the specific demands of key cybersecurity roles:

Threat Hunting and SOC Analysis: Requires the ability to sift through massive volumes of log data, network traffic, and security alerts to identify subtle anomalies that indicate a breach. Many individuals with ASD excel at exactly this kind of pattern recognition and sustained, focused analysis.

Penetration Testing: Requires the ability to think like an attacker — to identify unconventional pathways into a system that a conventional thinker might overlook. The lateral thinking and out-of-the-box problem-solving associated with ADHD and dyslexia are significant advantages here.

Digital Forensics: Requires meticulous, methodical analysis of digital evidence, often under time pressure and with enormous attention to detail. The precision and focus associated with ASD are directly applicable.

Cryptography and Reverse Engineering: Requires deep mathematical reasoning, pattern recognition, and the ability to hold complex logical structures in mind simultaneously — capabilities frequently associated with neurodivergent cognitive profiles.

The UK's Government Communications Headquarters (GCHQ), one of the world's most sophisticated intelligence agencies, actively recruits neurodivergent professionals, recognizing that their cognitive profiles are particularly well-suited to the analytical demands of intelligence work [16].

“Everything we do is about working in a team to solve the most complex problems. So we need both neurodiverse people and neurotypical people to work together.” — GCHQ Director of Strategy, Policy and Engagement [16]

3.3 The Structural Barriers to Neurodivergent Employment

If the alignment between neurodivergent talent and cybersecurity needs is so clear, why does the employment gap persist? The answer lies in the structural barriers embedded in traditional hiring and workplace practices.

Interview Processes: Standard job interviews are designed to assess social fluency, eye contact, and the ability to perform under social pressure — none of which are relevant to cybersecurity performance. Many neurodivergent candidates struggle with unstructured social interactions, even when they possess exceptional technical capabilities. The result is that the interview process systematically filters out some of the most technically capable candidates.

Job Descriptions: Many cybersecurity job postings include requirements that are not actually necessary for the role — such as “excellent communication skills” or “ability to work in a fast-paced environment” — that may discourage neurodivergent candidates

from applying, even when they are fully capable of performing the core technical functions.

Workplace Environments: Open-plan offices, mandatory team meetings, and informal social expectations can create significant sensory and social challenges for neurodivergent employees, leading to burnout and attrition even among those who successfully navigate the hiring process.

Credential Bias: The cybersecurity industry has historically placed significant weight on formal credentials and traditional educational pathways, which may disadvantage neurodivergent individuals who did not thrive in conventional academic settings but possess exceptional self-taught skills.

Part IV: The Business Case for Neurodivergent Inclusion

4.1 Productivity and Performance Data

The business case for neurodivergent inclusion is not theoretical; it is empirically demonstrated by some of the world's most rigorous corporate programs.

JPMorgan Chase: The Autism at Work program at JPMorgan Chase has produced some of the most compelling data in the field. Participants in the program were found to be 90% to 140% more productive than neurotypical employees in comparable roles, with fewer errors and higher accuracy rates [17]. The program, which has expanded to multiple countries, has become a model for the financial services industry.

“Long-term growth and success is dependent on our ability to identify, attract, develop and retain talented employees and foster an inclusive culture.” — Jamie Dimon [18]

SAP: SAP launched its Autism at Work program in 2013 with a simple premise: that people with autism could bring unique and valuable capabilities to the company's workforce. Over a decade later, the results are documented. SAP reports a 90% retention rate for employees with autism — equal to their overall retention rate across all employees [19]. In one documented case, a single neurodivergent employee

developed a technical fix that saved the company an estimated £31 million [20]. The program has expanded to more than 240 autistic employees in 16 countries.

EY (Ernst & Young): EY has established dedicated hubs to leverage the cognitive strengths of neurodivergent professionals in cybersecurity and data analytics. Internal data shows that neurodiverse teams are 1.2 to 1.4 times more productive than those that are not [20].

Deloitte: Research from Deloitte highlights that neuroinclusive organizations are 75% more likely to see ideas progress from concept to product, and neurodiverse teams solve complex problems three times faster than homogeneous groups [20].

Microsoft: Microsoft’s Neurodiversity Hiring Program reports a 90% retention rate for hires made through the program, saving millions in recruitment and training costs annually [20].

Across these programs, a consistent picture emerges: when neurodivergent talent is properly identified, trained, and supported, the productivity and retention outcomes are exceptional.

4.2 The Aggregate ROI

The aggregate financial case for neurodivergent inclusion in cybersecurity is compelling. Consider the following framework for a mid-sized enterprise with a security team of 100 professionals:

Metric	Without Neurodiversity Program	With Neurodiversity Program
Annual Turnover Rate	22% (22 hires/year)	~10% (10 hires/year)
Average Cost Per Hire	\$75,000	\$40,000 (pipeline-sourced)
Annual Recruitment Cost	\$1,650,000	\$400,000
Productivity Premium	Baseline	+30% on neurodiverse roles
Breach Cost Premium	+\$1.76M (understaffed)	Reduced (fully staffed)

Table 3: Illustrative ROI Framework for Neurodiversity Inclusion in Cybersecurity (Sources: ISC2, IBM, HR Future) [1] [2] [12]

The savings in recruitment costs alone — approximately \$1.25 million annually for a team of 100 — more than justify the investment in inclusive hiring practices and specialized training partnerships.

4.3 Skills-Based Hiring as a Force Multiplier

A 2026 report found that skills-based talent practices can create \$125,000 in ROI per worker, with research focused specifically on the cybersecurity field [21]. This finding underscores a broader shift in talent strategy that is already underway at leading organizations: the move away from credential-based hiring toward skills-based assessment.

For neurodivergent candidates, this shift is transformative. Many neurodivergent individuals possess exceptional technical skills developed through self-directed learning, personal projects, and deep specialization — skills that may not be reflected in a traditional resume or academic transcript. Skills-based assessments, project-based evaluations, and structured work trials allow these capabilities to surface in a way that conventional interviews do not.

“In fact, when hiring at his \$750 billion-plus firm, Dimon insists that a college major doesn’t matter as much as a job candidate’s character.” — Fortune, on Jamie Dimon’s hiring philosophy [22]

Part V: CyberNeu.org — A Model for the Future

5.1 Mission and Vision

CyberNeu Inc. is a 501©(3) nonprofit organization founded on a simple but powerful premise: that neurodivergent adults are not a problem to be managed but a solution to be deployed. Their mission is to create a world where neurodivergent individuals have equal opportunities for meaningful, high-wage careers in cybersecurity, by building a sustainable ecosystem that connects their unique talents with the critical needs of the industry [6].

CyberNeu is a Certified Woman and Minority Owned Business, and its programs are designed from the ground up to address the structural barriers that prevent neurodivergent talent from entering and thriving in the cybersecurity workforce.

5.2 The Four-Step Model

CyberNeu's approach is distinguished by its end-to-end focus on sustainable employment outcomes, not just training completion. Their model comprises four integrated steps:

Step 1 — Identify and Access: CyberNeu partners with universities and community organizations to identify neurodivergent talent using project-based assessments rather than biased interviews. This approach surfaces candidates based on demonstrated capability rather than social performance [6].

Step 2 — Train and Certify: A 12-week "Cybersecurity Foundations" curriculum, designed by industry experts and incorporating visual learning aids and neurodivergent-friendly pedagogical approaches, provides candidates with the foundational knowledge and industry-recognized certifications needed to enter the workforce [6].

Step 3 — Coach and Develop: Intensive coaching on professional communication, teamwork, and executive functioning prepares candidates for the workplace environment, addressing the soft-skill dimensions that are often the primary barrier to successful employment [6].

Step 4 — Place and Support: Facilitated "tryout" internships with corporate partners, followed by 12 months of ongoing support for both the employee and the employer, ensure that placements are successful and sustainable [6].

5.3 The Grant Program

CyberNeu's grant program provides neurodivergent individuals with 100% financial coverage for high-tier cybersecurity training, industry-recognized certifications, and essential learning tools [23]. The program is designed to remove financial barriers to entry, allowing candidates to focus entirely on developing their skills.

Funding a CyberNeu Grant is a strategic investment in a more resilient and inclusive cybersecurity workforce. Corporate contributions directly enable specialized talent development, providing organizations with access to a diverse pipeline of neurodivergent experts who bring out-of-the-box thinking to complex threats [23].

5.4 The Corporate Sponsorship Model

For the C-suite executives, CISOs, and founders gathered at Black Hat 2026, the call to action is direct: become a corporate sponsor partner of CyberNeu.org.

Corporate sponsorship of CyberNeu operates on a demand-driven model. Corporate partners identify specific, hard-to-fill roles within their organizations — the cloud security engineers, SOC analysts, incident responders, and threat hunters that they cannot find through traditional channels. CyberNeu then trains neurodivergent candidates specifically for those roles, creating a direct pipeline from training to employment.

This model offers several distinct advantages over traditional recruitment:

Specificity: Training is tailored to the specific technical requirements of the sponsoring organization, reducing the onboarding period and accelerating time-to-productivity.

Pipeline Ownership: Sponsors gain preferential access to a pipeline of trained, certified candidates before they enter the open market.

Retention: Candidates placed through CyberNeu's model benefit from 12 months of ongoing support, significantly reducing the risk of early attrition.

Mission Alignment: Sponsorship demonstrates a tangible commitment to workforce equity and cognitive diversity, aligning with ESG goals and strengthening employer brand in a competitive talent market.

Tax Efficiency: As a 501©(3) organization, donations to CyberNeu are tax-deductible. Many jurisdictions also offer additional tax credits for workforce development investments and for hiring individuals with disabilities [24].

Part VI: Implementation Roadmap for Corporate Partners

6.1 Assessing Your Organization's Neurodiversity Readiness

Before engaging with a neurodiversity hiring program, organizations should conduct an honest assessment of their current practices and environment. Key questions include:

- Do our job postings include requirements that are not actually necessary for the role?
- Do our interview processes assess social performance rather than technical capability?
- Do our workplace environments create unnecessary sensory or social challenges?
- Do our managers have the knowledge and skills to support neurodivergent employees?

Research suggests that 65% of managers admit they do not have enough knowledge to effectively support neurodivergent employees [20]. Addressing this gap through targeted training is a prerequisite for successful neurodiversity hiring.

6.2 Building an Inclusive Hiring Process

Organizations that have successfully implemented neurodiversity hiring programs share several common practices:

Structured Interviews: Replace unstructured social interviews with structured, competency-based assessments that evaluate candidates on the actual skills required for the role.

Project-Based Assessments: Provide candidates with a realistic work sample or technical challenge that allows them to demonstrate their capabilities in a format that plays to their strengths.

Advance Preparation: Share interview questions in advance, allowing candidates to prepare thoughtful responses rather than being evaluated on their ability to perform

under social pressure.

Flexible Communication: Offer candidates the option to participate in interviews via written communication, video with camera off, or other formats that reduce sensory and social demands.

Sensory Accommodations: Ensure that interview and workplace environments are designed to minimize unnecessary sensory stimulation, including noise, lighting, and crowding.

6.3 Creating a Retention-Focused Environment

Hiring neurodivergent talent is only the first step. Retention requires ongoing investment in the work environment and management practices. Key strategies include:

Clear Expectations: Neurodivergent employees often thrive when expectations are clearly defined and consistently communicated. Ambiguity in roles, responsibilities, and performance standards can be a significant source of stress.

Flexible Work Arrangements: ISC2 data shows that neurodivergent cybersecurity professionals are more likely to identify lack of flexible work arrangements as a negative factor in job satisfaction [15]. Remote and hybrid work options can significantly improve retention.

Dedicated Support: Assigning a mentor or advocate within the organization who understands neurodivergent needs and can serve as a point of contact for questions and concerns.

Career Pathways: Neurodivergent professionals are more likely to identify lack of career growth opportunities as a negative factor in job satisfaction [15]. Clear, structured career pathways that recognize technical expertise — not just management ability — are essential.

6.4 Measuring Success

Corporate sponsors of CyberNeu should establish clear metrics for evaluating the success of their neurodiversity hiring initiatives. Key performance indicators include:

Metric	Target
Time-to-Productivity	Comparable to or better than traditional hires
12-Month Retention Rate	≥90% (benchmark: SAP, Microsoft programs)
Performance Ratings	Comparable to or better than team average
Manager Satisfaction	≥80% positive assessment
Incident Detection Rate	Measurable improvement in SOC/threat hunting roles

Table 4: Recommended KPIs for Neurodiversity Hiring Program Evaluation

Part VII: The Broader Strategic Imperative

7.1 AI, Automation, and the Future of the Cybersecurity Workforce

The rise of AI in cybersecurity is reshaping the talent landscape in profound ways. AI-powered tools are increasingly capable of automating routine security tasks — log analysis, alert triage, vulnerability scanning — that have historically consumed significant portions of a security analyst’s time. This automation is not eliminating the need for human talent; it is elevating the bar for what human talent must deliver.

As Jensen Huang has observed, the future enterprise workforce will be a combination of humans and AI agents [11]. In this model, the human security professional’s role shifts from routine monitoring to higher-order judgment: interpreting AI-generated alerts, making nuanced decisions about risk, designing defensive architectures, and anticipating novel attack vectors. These are precisely the kinds of tasks that require the deep analytical capabilities, pattern recognition, and unconventional thinking that neurodivergent professionals often possess in abundance.

The organizations that will win the cybersecurity talent war are not those that simply automate away routine tasks; they are those that invest in the human capabilities that AI cannot replicate — the creative, analytical, and adaptive intelligence that comes from a cognitively diverse workforce.

7.2 The Geopolitical Dimension

The cybersecurity talent gap is not merely a business problem; it is a national security issue. State-sponsored cyber operations from adversarial nations are growing in sophistication and frequency. Critical infrastructure — power grids, water systems, financial networks, healthcare systems — is under constant threat. The organizations represented at Black Hat 2026 are not just defending their own balance sheets; they are defending the fabric of modern society.

In this context, the neurodivergent talent pool represents a strategic national asset that is currently being squandered. By investing in organizations like CyberNeu that are building the pipeline, we are not just solving a business problem; we are strengthening the nation's cyber defenses.

7.3 The Moral Imperative

We would be remiss not to acknowledge the moral dimension of this issue. Behind every statistic in this paper is a human being — a neurodivergent adult with exceptional capabilities, who has been told, explicitly or implicitly, that they do not belong in the workforce. The 40% unemployment rate among autistic adults is not a reflection of their capabilities; it is a reflection of our collective failure to design systems that recognize and value those capabilities.

“I deeply desire a vibrant culture of inclusion. I envision a company composed of more diverse talent... Having diverse employees prevents homogeneous thinking.”
— Satya Nadella [25]

As leaders of organizations that shape the economy and the culture of work, we have both the power and the responsibility to change this. The business case is compelling. The strategic case is clear. But ultimately, this is also simply the right thing to do.

Conclusion: A Call to Action at Black Hat 2026

The cybersecurity industry stands at an inflection point. The talent gap is real, the burnout crisis is accelerating, and the threat landscape is growing more sophisticated by the day. The traditional approaches to talent acquisition — competing for the same shrinking pool of credentialed professionals — are not sufficient to meet the challenge.

The solution is not to work harder within the existing system. It is to change the system. It is to recognize that the most capable security professionals may not look like the ones we have hired before. It is to invest in the organizations that are building new pathways into the profession. And it is to create workplace environments where neurodivergent talent can not only enter the workforce but thrive and grow within it.

CyberNeu.org is doing this work. They are identifying neurodivergent talent, training them for the specific roles that the industry needs most, and supporting them through the critical first year of employment. They are building the pipeline that the industry desperately needs.

We call upon every leader at Black Hat 2026 to take the following actions:

1. **Visit CyberNeu.org** and engage with their mission and programs.
2. **Inquire about corporate sponsorship** — identify the specific roles in your organization that are hardest to fill, and explore how CyberNeu can build a tailored pipeline for those roles.
3. **Audit your hiring practices** — identify the barriers in your current processes that may be excluding neurodivergent talent.
4. **Invest in your managers** — provide training on neurodivergent inclusion so that your organization is prepared to support the talent you hire.
5. **Measure and report** — hold your organization accountable for progress on neurodiversity hiring and retention metrics.

The talent crisis is solvable. The neurodivergent workforce is ready. The only question is whether we, as an industry, have the imagination and the will to build the bridge.

The future of cybersecurity depends on it.

Appendix A: Key Statistics at a Glance

Statistic	Value	Source
Global cybersecurity talent gap	4.8 million unfilled positions	ISC2, 2025
Workforce growth needed	87%	World Economic Forum, 2024
Security teams with skills gaps	90%	ISACA/ISC2, 2025
Additional breach cost (understaffed)	\$1.76 million	IBM/Viva-IT
U.S. unfilled cybersecurity positions	750,000+	CyberNeu/ISC2
Neurodivergent unemployment rate	40%	Multiple sources
Autistic adults employed	15%	AEI, 2024
Neurodivergent population share	15–20%	HR Future, 2026
JPMorgan Chase productivity premium	90–140%	JPMorgan Chase
SAP autism retention rate	90%	SAP, 2024
Neurodiverse team productivity premium	30%	Deloitte/HR Future
Neuroinclusive innovation speed	75% more likely to commercialize	Deloitte, 2025
Problem-solving speed (neurodiverse teams)	3x faster	Deloitte, 2025
Skills-based hiring ROI	\$125,000 per worker	HR Dive, 2026
Annual cybersecurity turnover rate	22%	Industry data
Neurodivergent professionals passionate about work	79%	ISC2, 2026

Appendix B: About CyberNeu.org

CyberNeu Inc. is a 501©(3) nonprofit organization, Certified Woman and Minority Owned, dedicated to cybersecurity excellence and education. Founded in 2022, CyberNeu's mission is to create a world where neurodivergent individuals have equal opportunities for meaningful, high-wage careers in cybersecurity. Their vision is to be the leading U.S. organization that empowers neurodivergent adults to thrive in cybersecurity careers, transforming the perception of neurodiversity in the workplace from a challenge to a competitive advantage.

Core Values:

- **Inclusion First:** Championing diversity of thought and experience as the true engine of innovation.
- **Human-Centered:** Seeing the individual, not the diagnosis, with programs tailored to the unique strengths of each person served.
- **Excellence and Rigor:** Providing world-class training that meets the high standards of the cybersecurity industry.

Target Goals: 100 individuals trained annually, with a pathway to scale as corporate sponsorship grows.

To engage with CyberNeu as a corporate sponsor partner: Visit www.CyberNeu.org and request information on corporate sponsorship opportunities.

References

- [1] Hakia. "4.8 Million Unfilled Cybersecurity Jobs: Inside the Global Talent Crisis." 2026. <https://hakia.com/news/cybersecurity-talent-crisis-2026/>
- [2] IBM. "Cost of a Data Breach Report 2025." <https://www.ibm.com/reports/data-breach>
- [3] Advanced Autism. "Autism Unemployment Rate." 2025. <https://www.advancedautism.com/post/autism-unemployment-rate>
- [4] JPMorgan Chase. "Reaching out to the brightest new technologists across the neurodivergent spectrum." August 2025.

<https://www.jpmorganchase.com/newsroom/stories/neurodivergent-recruitment>

[5] Cybersecurity Ventures. “Cybersecurity Jobs Report: 3.5 Million Unfilled Positions In 2025.” February 2026. <https://cybersecurityventures.com/jobs/>

[6] CyberNeu Inc. “About.” 2026. <https://www.cyberneu.org/about>

[7] Cisco. “Close the Cybersecurity Workforce Gap with AI Position.” May 2024. <https://www.cisco.com/c/en/us/products/collateral/security/xdr/close-cybersecurity-workforce-gap-with-ai.html>

[8] Sophos. “Report: Addressing cybersecurity burnout in 2025.” September 2025. <https://www.sophos.com/en-us/blog/report-addressing-cybersecurity-burnout-in-2025>

[9] LinkedIn. “Cybersecurity turnover rate: 22% annual, a human challenge.” https://www.linkedin.com/posts/jahsi-richardson_cybersecurity-securityworkforce-infoseccareers-activity-7371875320544800768-YFZC

[10] Security Magazine. “Top reasons why cybersecurity professionals leave their jobs.” April 2022. <https://www.securitymagazine.com/articles/97350-highest-cybersecurity-retention-difficulties-in-years>

[11] Fortune. “Jensen Huang says the future workforce will be a mix of ‘humans and digital humans.’” October 2025. <https://fortune.com/2025/10/20/jensen-huang-nvidia-ai-future-workforce-digital-humans-hiring-onboarding-orientation/>

[12] HR Future. “30% More Productive: The ROI of a neurodiverse workforce.” <https://www.hrfuture.net/workplace-culture/strategy/diversity-inclusion/30-more-productive-the-roi-of-a-neurodiverse-workforce/>

[13] My Disability Jobs. “Neurodiversity in the Workplace | Statistics | Update 2025.” <https://mydisabilityjobs.com/statistics/neurodiversity-in-the-workplace/>

[14] Forbes. “Why Cybersecurity Should Rethink Inclusion For Neurodivergent People.” June 2025. <https://www.forbes.com/sites/jenniferpalumbo/2025/06/30/why-cybersecurity-should-rethink-inclusion-for-neurodivergent-people/>

[15] ISC2. “Neurodivergence in the Cybersecurity Workforce: A Snapshot.” April 2026. <https://www.isc2.org/Insights/2026/04/neurodivergence-in-the-cybersecurity-workforce-a-snapshot>

- [16] GCHQ. "Recruiting diverse talent to protect modern Britain." <https://www.gchq.gov.uk/information/recruiting-diverse-talent-protect-modern-britain>
- [17] LinkedIn. "JPMorgan Chase Finds Neurodiverse Employees 90-140% More Productive." March 2026. https://www.linkedin.com/posts/assegaisolutions_why-ai-is-making-neurodivergent-talent-the-activity-7443147166241509376-j4H6
- [18] Benefits Canada. "JPMorgan Chase expanding talent pool through neuroinclusion strategy." April 2026. <https://www.benefitscanada.com/news/bencan/jpmorganchase-expanding-talent-pool-through-neuroinclusion-strategy/>
- [19] International WIM. "The Neurodiversity in SAP Report 2024." https://internationalwim.org/wp-content/uploads/2025/06/The_Neurodiversity_in_SAP_Report_2024.pdf
- [20] Fertifa. "The ROI of neurodiversity workplace support: Thirteen UK-based companies leading the way in 2026." February 2026. <https://www.fertifa.com/post/roi-of-investing-in-neurodiversity-support>
- [21] HR Dive. "Skills-based talent practices can create \$125K in ROI per worker, report says." March 2026. <https://www.hrdive.com/news/skills-based-talent-practices-can-create-125k-in-roi-per-worker-report-sa/814878/>
- [22] Fortune. "Gen Z is facing a job market bloodbath—but JPMorgan Chase CEO Jamie Dimon says these skills are in demand." June 2025. <https://fortune.com/2025/06/23/jpmorgan-chase-ceo-jamie-dimon-in-demand-skills-gen-z-cyber-coding-computer-science-project-management/>
- [23] CyberNeu Inc. "Grants." 2026. <https://www.cyberneu.org/grants>
- [24] U.S. Chamber of Commerce. "Tax Guides: Employer Incentives for Workforce Support and Benefits." December 2024. <https://www.uschamber.com/taxes/tax-guides-employer-incentives-for-workforce-support-and-benefits>
- [25] Silicon Republic. "Internal memo from Satya Nadella outlines Microsoft's new diversity plan." October 2014. <https://www.siliconrepublic.com/companies/internal-memo-from-satya-nadella-outlines-microsofts-new-diversity-plan>