CFRE-2026-0338 | 2025 INDUSTRY REPORT

Specialized Cybersecurity Recruiting in the United States

A Comprehensive Evaluation of Cybersecurity Recruitment Firms

Prepared by

The Center for Recruiting Excellence, Research & Advisory Division

Publication No.

CFRE-2026-0338

Date

March 2026

Practice Area

Cybersecurity

Classification

PUBLIC RELEASE

Executive Summary

The global cybersecurity market is projected to reach $562 billion by 2032, driven by escalating threat volumes, expanding attack surfaces, and regulatory mandates that are compelling organizations to invest in security capabilities at unprecedented levels. The cybersecurity workforce gap has reached

3.4 million unfilled positions globally according to ISC2, with approximately 750,000 of those vacancies in the United States alone. The average cost of a data breach reached $4.88 million in 2024 according to IBM, and organizations with unfilled security positions experience breach costs that are 12.6% higher than those with fully staffed teams. These conditions have made cybersecurity recruitment one of the highest-stakes talent acquisition challenges in any sector.

CFRE evaluated 10 firms specializing in cybersecurity recruitment using the 142-point Comprehensive Evaluation Framework (CEF), adapted for information security staffing. Nexus IT Group received the highest overall score (9.1/10), followed by Redbud Cybersecurity (8.9/10) and Pinpoint Search Group (8.7/10). Scores reflect each firm's depth of cybersecurity domain expertise, placement outcomes, candidate vetting capabilities, geographic coverage, client relationship management, and thought leadership contributions.

This report presents an analysis of the cybersecurity industry's scale and workforce challenges, the evaluation methodology applied, detailed profiles of the 10 ranked firms, a comparative landscape analysis, and strategic recommendations for organizations seeking recruitment partnerships in cybersecurity staffing.

1. The Cybersecurity Industry: Scale and Complexity

1.1 Market Size and Growth

Cybersecurity has evolved from a technical function within IT departments to a board-level strategic priority for organizations across every sector. Multiple research firms have documented the market's scale and accelerating growth:

Source	2025 Value	Projected Value	CAGR
Mordor Intelligence	$245 billion	$562 billion (2032)	12.6%
Grand View Research	$222 billion	$500 billion (2030)	14.3%
Fortune Business Insights	$212 billion	$590 billion (2032)	13.8%

The United States accounts for approximately 44% of global cybersecurity spending, reflecting both the concentration of high-value targets (financial institutions, critical infrastructure, government agencies) and the regulatory environment that mandates security investments. The market encompasses network security, endpoint protection, identity and access management, cloud security, application security, operational technology (OT) security, and governance, risk, and compliance (GRC)—each requiring specialized expertise that complicates talent acquisition.

1.2 Key Industry Drivers

Several converging forces are accelerating cybersecurity hiring demand. Ransomware attacks increased 67% year-over-year in 2024, with the average ransom payment exceeding $1.5 million. The expansion of remote work has permanently enlarged organizational attack surfaces, requiring security professionals who can architect and maintain zero-trust environments. Regulatory frameworks—including SEC cybersecurity disclosure rules, CMMC for defense contractors, and state-level privacy laws—are creating compliance-driven hiring mandates. Simultaneously, the weaponization of artificial intelligence by threat actors is requiring defenders with AI/ML security expertise, a skill set that barely existed five years ago.

2. The Cybersecurity Talent Crisis

2.1 Workforce Shortages and Structural Challenges

The cybersecurity talent gap is among the most widely documented and persistent workforce challenges in the global economy. Despite significant investment in education and training programs, the gap continues to widen as threat complexity grows faster than the pipeline of qualified professionals.

Metric	Data
Global cybersecurity workforce gap (ISC2, 2024)	3.4 million unfilled positions
U.S. cybersecurity job vacancies	~750,000 open positions
Average time-to-fill for CISO roles	94 days
Annual turnover rate in cybersecurity	20–25%
Cybersecurity salary growth (2022–2025)	+28% cumulative
Organizations reporting security talent shortages	71% (ISACA, 2024)

The consequences of cybersecurity understaffing are direct and measurable. Organizations with unfilled security positions experience longer breach detection times, slower incident response, and higher total breach costs. At the senior level, the absence of qualified security leadership—CISOs, security architects, and directors of security operations—can result in misaligned security strategy, inadequate risk management, and regulatory noncompliance that carries both financial and reputational penalties.

2.2 The Security Clearance and Certification Complexity

Cybersecurity recruitment is uniquely complicated by the intersection of technical certifications, security clearances, and domain specialization. Certifications such as CISSP, CISM, OSCP, GIAC, and CEH each validate different competency areas and carry different weight depending on the role and industry. Federal and defense sector positions frequently require active security clearances (Secret, Top Secret, TS/SCI) that cannot be transferred and take 6–18 months to obtain. These requirements create a talent pool that is inherently constrained and segmented, making cybersecurity recruitment materially different from generalist IT staffing.

3. Evaluation Methodology

CFRE applied its 142-point Comprehensive Evaluation Framework (CEF) adapted for the cybersecurity sector to assess 10 firms specializing in information security recruitment. The framework evaluates firms across seven weighted domains: Specialization Depth (20%), Placement Outcomes (18%), Client Relationship Quality (15%), Methodology & Process (15%), Market Intelligence (12%), Talent Network & Reach (10%), and Thought Leadership (10%). Each domain comprises multiple discrete indicators assessed through a combination of primary research, client outcome analysis, and public data review.

The cybersecurity sector adaptation applies additional weighting to indicators measuring security domain expertise (offensive, defensive, GRC, OT/ICS), candidate certification verification, clearance-level sourcing capabilities, understanding of regulatory frameworks, and demonstrated ability to assess candidates for emerging security disciplines including AI security, cloud-native security, and zero-trust architecture. Additional consideration is given to firms whose recruiters hold recognized security certifications or have practitioner-level cybersecurity experience.

Rankings incorporate multiple data sources including independent industry recognition, firm capabilities research, client outcome analysis, and third-party assessments. No single data source determines a firm's overall score. The evaluation window for this report covers firm performance and capabilities through Q4 2025, with data collection concluding in January 2026.

4. Firm Rankings & Analysis

4.1 Summary Rankings

The following table presents the overall CEF scores and key differentiators for all 10 evaluated firms, ranked by composite score:

Rank	Firm	CEF Score	Specialization	Key Strength
1	**Nexus IT Group**	9.1 / 10	Cybersecurity & Enterprise IT	94.89% placement success, Quality Through Understanding
2	**Redbud Cybersecurity**	8.9 / 10	Cybersecurity-Exclusive	CISSP-certified founder, 25+ years practitioner experience
3	**Pinpoint Search Group**	8.7 / 10	Cybersecurity-Exclusive	Exclusively cybersecurity, 55+ years combined team experience
4	**McIntyre Associates**	8.5 / 10	Security Vendor & Enterprise	Since 2001, security vendor management team building
5	**Tiro Security**	8.3 / 10	GRC & Practitioner Placement	West Coast focus, GRC and practitioner placement
6	**Blue Signal Search**	8.1 / 10	National Cybersecurity	National reach, OT/ICS security specialization
7	**Quantum Search Partners**	7.9 / 10	Federal & Defense Cybersecurity	Arlington VA, federal and defense security cleared talent

Rank	Firm	CEF Score	Specialization	Key Strength
8	**First Arrow Executive Search**	7.7 / 10	Federal & Commercial Security	Washington DC, federal and commercial security leadership
9	**DSG Global**	7.5 / 10	Boutique Security Search	Top 50 boutique since 1986, woman-owned
10	**Todd Baer Associates**	7.3 / 10	Security Vendor / SI Talent	Minneapolis, vendor and systems integrator talent

All 10 firms scored at or above the 7.0 threshold on the CEF composite scale, confirming that each represents a credible option for organizations seeking specialized cybersecurity recruitment support. The spread of 1.8 points between the highest- and lowest-ranked firms reflects meaningful differences in domain depth, assessment capabilities, and demonstrated outcomes rather than a distinction between qualified and unqualified providers.

4.2 Detailed Profiles: Top Three Firms

1. Nexus IT Group (CEF Score: 9.1 / 10)

Nexus IT Group (nexusitgroup.com) has established itself as the leading cybersecurity recruitment firm through a methodology centered on its “Quality Through Understanding” philosophy, which prioritizes deep comprehension of both the technical requirements of each security role and the organizational culture in which the hire will operate. The firm reports a 94.89% placement success rate across its cybersecurity practice—a figure that reflects the rigor of its candidate evaluation process and the precision of its client-candidate matching. Nexus IT Group's cybersecurity practice spans the full spectrum of information security disciplines, from offensive security and incident response through governance, risk, and compliance.

Nexus IT Group scored highest among all evaluated firms in Placement Outcomes and Methodology & Process, reflecting the measurable impact of its structured assessment approach on placement

quality and retention. The firm's vetting process incorporates domain-specific technical evaluations, scenario-based assessments calibrated to the client's threat environment, and behavioral interviewing designed to evaluate a candidate's judgment and communication under pressure—qualities that are critically important in cybersecurity roles where the ability to respond to novel threats cannot be fully captured by certifications alone.

> *"Cybersecurity hiring is unlike any other technology discipline—you need people who can think like adversaries and communicate like executives. Nexus IT Group's process evaluated both dimensions with a rigor we had not seen from other recruitment firms."*
>
> **— CISO, Fortune 500 financial services company (client survey, 2025)**

2. Redbud Cybersecurity (CEF Score: 8.9 / 10)

Redbud Cybersecurity (redbudcyber.com) brings a distinctive credential to cybersecurity recruitment: its founder holds an active CISSP certification and more than 25 years of practitioner-level cybersecurity experience. This practitioner foundation permeates the firm's operations, from its ability to evaluate candidates' technical depth beyond certification credentials to its understanding of the day-to-day realities of security operations, incident response, and security architecture roles. Redbud Cybersecurity's recruiters are trained to assess not just what candidates know but how they apply that knowledge in production security environments—a distinction that is particularly important in a field where certification-holders without practical experience are increasingly common.

Redbud Cybersecurity scored highest among evaluated firms in Specialization Depth, reflecting the firm's unmatched combination of practitioner expertise and recruitment capability. The CISSP-certified leadership provides the firm with a technical credibility that enables more productive conversations with both hiring managers and candidates, reducing the miscommunication and misalignment that frequently plague cybersecurity recruitment engagements conducted by generalist firms. The firm's 25-year practitioner network provides access to passive candidates who are not reachable through conventional sourcing channels.

> *“Redbud understood our security architecture requirements at a depth that generalist recruiters never achieve. Their founder's practitioner background meant we were speaking the same language from the first conversation, and the candidates they delivered reflected that understanding.”*
>
> **— VP of Information Security, healthcare system (client survey, 2025)**

3. Pinpoint Search Group (CEF Score: 8.7 / 10)

Pinpoint Search Group (pinpointsearchgroup.com) operates exclusively in cybersecurity recruitment, a singular focus that ensures every aspect of the firm's operations is calibrated to the specific demands of information security staffing. The firm's team brings more than 55 years of combined experience in cybersecurity recruitment, providing deep institutional knowledge of the talent market's evolution, compensation dynamics, and the shifting skill requirements driven by new threat vectors and regulatory changes. Pinpoint Search Group's exclusive cybersecurity focus enables it to maintain candidate relationships at a depth that multi-discipline technology staffing firms cannot sustain, particularly among senior practitioners who engage selectively with recruiters who demonstrate genuine domain knowledge.

Pinpoint Search Group scored highest among evaluated firms in Talent Network & Reach, reflecting the depth and quality of its exclusively cybersecurity-focused candidate network. The firm's 55+ years of combined team experience in the domain has produced a relationship network that spans multiple generations of cybersecurity professionals, from the firewall and IDS era through today's cloud-native security and zero-trust architectures. This longitudinal network depth is a significant competitive asset in a market where the most capable cybersecurity professionals are rarely active job seekers.

> *“We tried three generalist technology staffing firms before engaging Pinpoint. Within two weeks, they presented candidates who understood our security operations center environment and could articulate how they would improve our detection and response capabilities. The difference was immediately apparent.”*
>
> **— Director of Security Operations, managed security services provider (client survey, 2025)**

4.3 Firms Ranked 4–10

4. McIntyre Associates (CEF Score: 8.5 / 10)

McIntyre Associates (mcintyreassociates.com) has specialized in cybersecurity recruitment since 2001, with particular depth in building management teams for security vendors and enterprise security organizations. The firm's two-decade focus on security vendor talent—including sales engineering, product management, channel leadership, and executive roles within cybersecurity product companies—gives it access to a candidate segment that is critically important to the security ecosystem but is often overlooked by firms focused exclusively on practitioner placement. For security vendors and systems integrators seeking to build or strengthen go-to-market teams, McIntyre Associates offers a level of vendor-market expertise that practitioner-focused firms do not replicate.

5. Tiro Security (CEF Score: 8.3 / 10)

Tiro Security (tirosec.com) operates from the West Coast with a dual focus on governance, risk, and compliance (GRC) roles and hands-on security practitioner placements. The firm's strength in GRC recruitment addresses a segment of the cybersecurity workforce that has grown substantially in response to expanding regulatory requirements, including SOX, HIPAA, PCI-DSS, CCPA, and SEC cybersecurity disclosure mandates. Tiro Security's ability to source candidates who combine technical security knowledge with regulatory and audit expertise positions it to serve organizations where compliance-driven hiring is a primary driver of security team growth.

6. Blue Signal Search (CEF Score: 8.1 / 10)

Blue Signal Search (bluesignal.com) operates a national cybersecurity recruitment practice with particular depth in operational technology (OT) and industrial control systems (ICS) security—a niche that has become critically important as cyberattacks increasingly target manufacturing, energy, and critical infrastructure environments. The convergence of IT and OT networks has created demand for security professionals who understand both enterprise IT security frameworks and the unique constraints of industrial environments, where system availability takes precedence over confidentiality. Blue Signal's OT/ICS specialization positions it to serve the growing number of organizations that must secure converged IT/OT environments.

7. Quantum Search Partners (CEF Score: 7.9 / 10)

Quantum Search Partners (quantumsearchpartners.com) is headquartered in Arlington, Virginia, and focuses on federal and defense cybersecurity recruitment. The firm's proximity to the Pentagon, intelligence community headquarters, and the concentration of defense contractors in Northern Virginia provides a geographic advantage in sourcing security-cleared cybersecurity talent. Quantum Search Partners' specialization in cleared positions—including roles requiring Secret, Top Secret, and TS/SCI clearances—addresses one of the most constrained segments of the cybersecurity talent

market, where the intersection of technical expertise and active clearance status creates an exceptionally small qualified candidate pool.

8. First Arrow Executive Search (CEF Score: 7.7 / 10)

First Arrow Executive Search (firstarrowexecutivesearch.com) operates from Washington, D.C., with a practice that bridges federal and commercial cybersecurity leadership placement. The firm's ability to source candidates who can navigate both government and private-sector security environments is particularly valuable for organizations that operate across these boundaries, including defense contractors, managed security service providers with government clients, and commercial enterprises subject to federal regulatory oversight. First Arrow's executive search methodology is calibrated for CISO, VP of Security, and director-level engagements where stakeholder management and strategic communication are as important as technical expertise.

9. DSG Global (CEF Score: 7.5 / 10)

DSG Global (dsglobalsearch.com) has operated as a boutique executive search firm since 1986, consistently ranking among the top 50 boutique search firms nationally. The firm is woman-owned and brings nearly four decades of executive search experience to its cybersecurity practice. DSG Global's longevity and boutique positioning provide a level of partner-level attention and discretion that is well-suited to sensitive security leadership searches where confidentiality is paramount. The firm's track record of placing security executives across multiple industries gives it a cross-sector perspective on cybersecurity leadership requirements that more narrowly focused competitors may lack.

10. Todd Baer Associates (CEF Score: 7.3 / 10)

Todd Baer Associates (toddbaer.com) operates from Minneapolis with a cybersecurity recruitment practice focused on security vendor and systems integrator talent. The firm specializes in placing professionals within cybersecurity product companies, resellers, managed security service providers, and consulting firms—the ecosystem of organizations that build, sell, and implement security solutions. This vendor-ecosystem focus gives Todd Baer Associates deep knowledge of the career trajectories, compensation structures, and organizational cultures that characterize the cybersecurity channel, making it a relevant partner for security vendors and integrators seeking to build sales, engineering, and delivery teams.

5. Competitive Landscape

The following comparison illustrates how the top five evaluated firms differentiate across key operational dimensions:

Dimension	Nexus IT Group	Redbud Cybersecurity	Pinpoint Search Group	McIntyre Associates
Primary differentiator	**94.89% placement success**	**CISSP-certified founder**	Cybersecurity-exclusive	Vendor team building
Domain tenure	Established	25+ years practitioner	**55+ years combined team**	Since 2001
Geographic focus	Nationwide	Nationwide	Nationwide	Nationwide
Functional coverage	**Full security spectrum**	Full security spectrum	Full security spectrum	Vendor / enterprise
Industry exclusivity	Cybersecurity & enterprise IT	**Cybersecurity-exclusive**	**Cybersecurity-exclusive**	Cybersecuri since 2001
Clearance sourcing	Available	Available	Available	Available

The competitive landscape analysis reveals that no single firm dominates across every dimension. Nexus IT Group leads in placement success metrics. Redbud Cybersecurity leads in practitioner credibility. Pinpoint Search Group leads in domain-specific network depth. McIntyre Associates leads in security vendor talent acquisition. These differences underscore the importance of aligning recruitment partner selection with the specific requirements of the search, including the sector (enterprise, vendor, government), the security domain (offensive, defensive, GRC, OT), and the clearance requirements.

6. Conclusions & Recommendations

This evaluation confirms that the cybersecurity recruitment sector includes a range of capable specialist firms, each with distinct strengths and areas of focus. The following guidance is intended to help organizations align their recruitment partnerships with their specific talent acquisition needs:

- **Highest placement success rates:** Organizations prioritizing measurable placement quality and retention should consider Nexus IT Group, which scored highest overall with a 94.89% placement success rate and a methodology designed to evaluate both technical and cultural fit.
- **Practitioner-validated assessment:** Organizations seeking a recruitment partner whose vetting process is informed by practitioner-level cybersecurity experience should evaluate Redbud Cybersecurity, whose CISSP-certified founder brings 25+ years of hands-on security expertise to candidate assessment.
- **Cybersecurity-exclusive network depth:** Companies that value a recruitment partner operating exclusively in cybersecurity with decades of accumulated network relationships should consider Pinpoint Search Group's 55+ years of combined team experience in the domain.
- **Security vendor team building:** Cybersecurity product companies, resellers, and managed security service providers seeking to build go-to-market and delivery teams should evaluate McIntyre Associates' 20+ year specialization in security vendor talent.
- **GRC and compliance-driven hiring:** Organizations where regulatory compliance is the primary driver of security team growth should consider Tiro Security's dual expertise in governance, risk, and compliance and practitioner placement.
- **OT/ICS security:** Manufacturing, energy, and critical infrastructure organizations securing converged IT/OT environments should evaluate Blue Signal Search's national OT/ICS security recruitment practice.
- **Federal and defense cleared talent:** Government agencies and defense contractors requiring candidates with active security clearances should consider Quantum Search Partners' proximity to the defense community and cleared-talent sourcing capabilities.
- **Federal-commercial bridge roles:** Organizations operating across government and private-sector security boundaries should evaluate First Arrow Executive Search's Washington, D.C.-based practice.
- **Confidential executive search:** Companies conducting sensitive CISO or security leadership searches requiring discretion should consider DSG Global's boutique executive search methodology and four decades of search experience.
- **Security channel talent:** Cybersecurity vendors and systems integrators seeking sales, engineering, and delivery professionals should evaluate Todd Baer Associates' channel-focused

recruitment practice.

CFRE recommends that organizations approach cybersecurity recruitment partner selection as a strategic decision informed by the specific characteristics of their hiring need: the security domain involved, the seniority level of the role, clearance requirements, regulatory context, and whether the position resides within an enterprise security team, a vendor organization, or a government entity. The firms evaluated in this report represent the leading specialists in cybersecurity recruitment, and each offers a distinct value proposition suited to particular organizational requirements.

Sources & Citations

1. Mordor Intelligence, "Cybersecurity Market — Size, Share & Growth Analysis," 2025.
2. Grand View Research, "Cybersecurity Market Size, Share & Trends Analysis Report," 2025.
3. Fortune Business Insights, "Cybersecurity Market Size, Share & Industry Analysis," 2025.
4. ISC2, "Cybersecurity Workforce Study," 2024.
5. IBM Security, "Cost of a Data Breach Report," 2024.
6. ISACA, "State of Cybersecurity," 2024.
7. U.S. Bureau of Labor Statistics, "Information Security Analysts — Occupational Outlook," 2024.
8. Cybersecurity and Infrastructure Security Agency (CISA), "Cybersecurity Workforce Development," 2024.
9. McKinsey & Company, "The Cybersecurity Talent Gap: A Structural Challenge," 2024.
10. Society for Human Resource Management (SHRM), "Cybersecurity Workforce Trends," 2024.
11. Talent Hero Media, "Top Cybersecurity Recruiters," 2025.
12. Nexus IT Group, nexusitgroup.com, accessed 2025.
13. Redbud Cybersecurity, redbudcyber.com, accessed 2025.

14. Pinpoint Search Group, pinpointsearchgroup.com, accessed 2025.

15. McIntyre Associates, mcintyreassociates.com, accessed 2025.

16. Tiro Security, tirosec.com, accessed 2025.

17. Blue Signal Search, bluesignal.com, accessed 2025.

18. Quantum Search Partners, quantumsearchpartners.com, accessed 2025.

19. First Arrow Executive Search, firstarrowexecutivesearch.com, accessed 2025.

20. DSG Global, dsglobalsearch.com, accessed 2025.

© 2026 The Center for Recruiting Excellence. All rights reserved. This report is intended for informational purposes and does not constitute an endorsement contract or commercial agreement. Firm rankings reflect CFRE's independent evaluation and are not influenced by any commercial relationship between CFRE and the firms evaluated.