CyberSN

Cyber Workforce Risk Management (CWRM)

Retain, Develop, and Optimize your Cyber Teams

Compliance | Defense | Offense | Management | Product Security | IT Security | Response | Sales

NICE

Find us at NIST NICE Cybersecurity Career Pathway Resources

SECURE DIVERSITY

In partnership with Secure Diversity

> This is one call I get to go to that is about caring for me and our team.

Kirk Davis
VP, Chief Information Security Officer
ECU Health

The Problem

Challenges in Cyber Workforce Management

Workforce Optimization:

Organizations often struggle to optimize their cyber workforce, creating inefficiencies and capabilities gaps. Proper alignment and management are crucial for maximizing productivity, achieving strategic goals, and creating appropriate budgets.

Misalignment with Cyber Strategy:

There are often gaps between the activities of the cyber team and the strategic objectives set by leadership. This misalignment results in conflicting priorities and failure to achieve key strategic goals.

Inconsistent Role Definitions:

Generic job titles fail to accurately reflect the specific responsibilities and expertise required in cybersecurity roles. This lack of clarity leads to job dissatisfaction, hinder career progression, and impact overall team performance.

Employee Retention:

The stressful and taxing nature of cyber work leads to burnout and high turnover rates. Effective strategies are essential for fostering a positive culture, promoting growth, and retaining top talent.

Cyber Workforce Risk Management (CWRM) Solution

Empowering Your Cyber Workforce for Optimal Performance and Security

Our Cyber Workforce Risk Management (CWRM) solution is designed to provide comprehensive insights and strategies to enhance and optimize your cyber workforce. Through a structured approach of workshops, in-depth analyses, and tailored recommendations, we help organizations:

- **Understand** their cyber workforce's current capabilities and maturity.
- **Align** job roles, compensation, and titles for optimal clarity and motivation.
- **Boost** employee satisfaction and engagement through targeted insights.
- **Develop** a strategic roadmap for continuous growth and development.

Our Approach

Discovery

We start by conducting thorough workshops with your security leadership and key leadership to gather critical insights into your cyber workforce.

Our approach includes:

Cyber Strategy Intake: Understand the strategic vision and priorities for your security department.

Cyber Workforce Insight: Engage with the cyber organization to document current responsibilities based on tasks and projects.

CyberSN Taxonomy Job Descriptions: Build job descriptions based on what employees are doing day-to-day.

Talent Happiness: Gauge the satisfaction of the work that each employee is doing currently.

In-depth Analysis

Using the discovery, we perform a series of detailed analyses to **understand your organization's gaps** and provide recommendations improvement:

Data-Driven Analysis: Leverage quantitative data to identify trends and insights.

Cyber Fusion Model Analysis: Assess the integration and effectiveness of your cyber organization capabilities.

Organizational Structure Analysis: Evaluate the current structure and propose enhancements.

Strategy and Maturity Analysis: Determine the maturity of your cyber strategies and identify gaps.

Happiness and Training Analysis: Correlate employee satisfaction with training needs and opportunities.

Our Recommendations

Strategic Deliverables

Based on our analyses, we develop tailored recommendations to optimize your cyber workforce:

Executive Summary: Concise overview of findings and recommendations for your leadership team.

Cyber Workforce Happiness Insights: Actionable insights to boost workforce morale and engagement.

Comprehensive Job Descriptions: Detailed and aligned job descriptions using the CyberSN taxonomy.

Cyber Capabilities Insights: In-depth look at your organization's cyber capabilities and potential gaps.

Organizational Capabilities and Gaps: Identify strengths and areas needing improvement.

1-Year, 3-Year or 5-year Insights: Strategic roadmap to guide your organization’s growth and development.

Cyber Strategy Insights: Detailed analysis and recommendations to refine your cyber strategy.

Training and Career Development Recommendations: Personalized training paths and career development plans.

Capabilities Gap Recommendations: Strategies to bridge the gaps in your cyber capabilities.

CWRM Project Outline

This final report is based on workshops with all members of the leadership and technical technical teams. CyberSN platform is used to develop all job descriptions, cyber organizational structure, cyber capabilities.

Kick Off	Strategy & Maturity Discovery	Job Descriptions & Happiness	Cyber Organization Capabilities	Final Report

Meetings & Calls

CyberSN conduct workshops collecting cyber workforce insight

- CISO and key leadership strategy and maturity
- Building job descriptions using the CyberSN taxonomy
- Happiness survey
- CISO cyber strategy deep dive
- Compensation and title alignment

Supporting Efforts & Research

- Data driven analysis
- Cyber fusion model analysis
- Organizational structure analysis
- Strategy and maturity analysis
- Happiness and training analysis
- Recommendations development

Final Report

- Executive summary
- Cyber workforce happiness insights
- Comprehensive job descriptions
- Cyber capabilities insights
- Cyber organization capabilities and gaps
- Cyber organization 1-year and 3-year insight
- Cyber strategy insights
- Training and career development recommendations
- Capabilities cap recommendations

Examples of CWRM Deliverables and Results

Driven by the CyberSN Platform

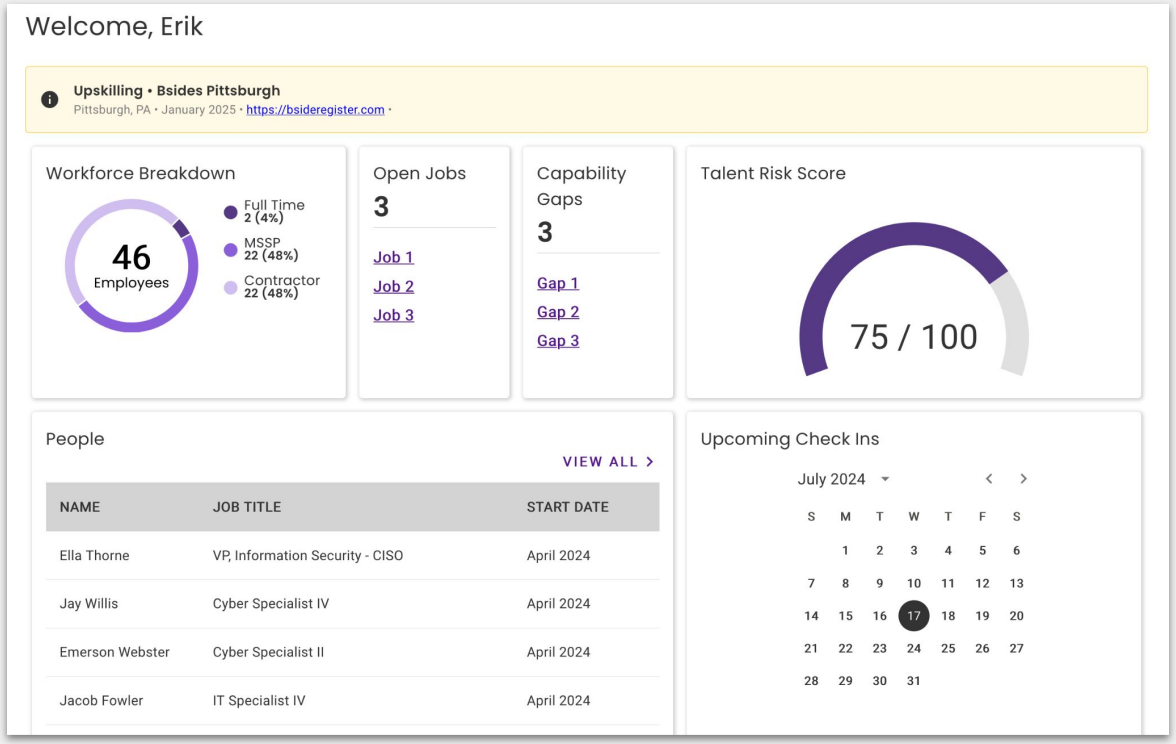
Cyber Workforce Risk Management Solution

Executed and Delivered by our Advanced SaaS Platform

Our Cyber Workforce Risk Management (CWRM) Solution is seamlessly executed and delivered through our cutting-edge SaaS platform. This platform ensures precise data collection, robust analysis, and actionable insights, all while providing an intuitive and user-friendly experience. Clients will have access to the platform through a software licensing agreement, ensuring continuous support and updates.

Key Features of Our SaaS Platform:

- **Comprehensive Data Discovery**:
  - Utilizes the CyberSN taxonomy for accurate categorization of job roles, tasks, and responsibilities.
  - Gathers extensive data through workshops, surveys, and real-time feedback from your cyber workforce.
- **Advanced Analytics**:
  - Performs in-depth analysis using data-driven methodologies to identify gaps, opportunities, and strategic alignments.
  - Leverages the NICE Framework to ensure standardized role definitions and competency assessments.
- **Insightful Reporting**:
  - Generates detailed visualizations to provide clear, actionable insights into your cyber workforce.
  - Offers role clarity to enhance workforce optimization, retention, and alignment with strategic goals.
- **User-Friendly Interface**:
  - Provides an intuitive platform that is easy to navigate for all users, from executives to team managers.

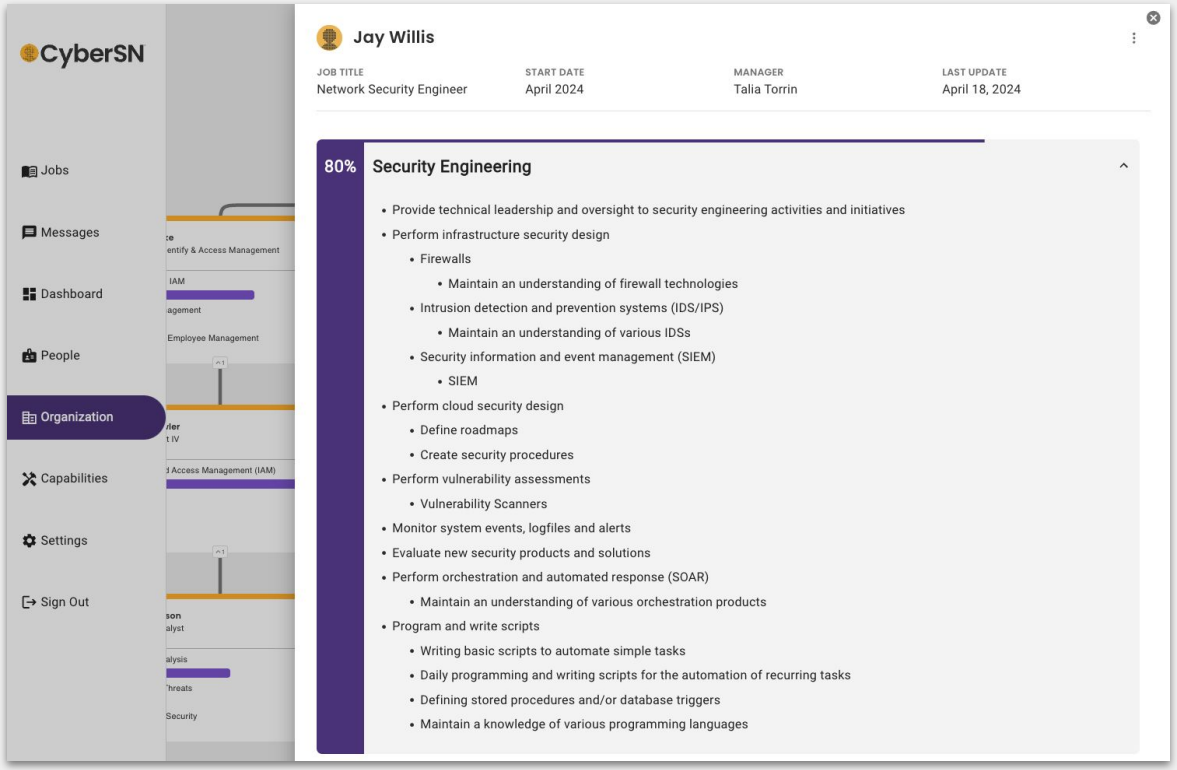


The CyberSN Platform: Empowering Cyber Workforce Insights

Streamlined Data Discovery and Analysis for Effective Workforce Management

Our advanced SaaS platform plays a crucial role in delivering the Cyber Workforce Risk Management (CWRM) Solution by:

- **Utilizing the CyberSN Taxonomy**:
  - **Precision Job Descriptions**: Leverage the comprehensive CyberSN taxonomy to create accurate and effective job descriptions tailored to your organization's needs.
  - **Consistent Role Definitions**: Ensure clarity and consistency in role definitions across your cyber workforce.
- **Efficient Data Gathering**:
  - **Automated Surveys**: Conduct happiness surveys and gather insights seamlessly through the platform.
  - **Real-Time Data Collection**: Capture and store data from workshops, interviews, and leadership sessions in real-time.
- **Insightful Analysis**:
  - **Data-Driven Insights**: Distill collected data into actionable insights using advanced analytical tools.
  - **Customized Reports**: Generate comprehensive reports on cyber workforce capabilities, satisfaction, and development needs.
- **Actionable Recommendations**:
  - **Strategic Alignment**: Align compensation, titles, and training programs with the strategic goals of your organization.
  - **Roadmap Development**: Create a clear path for 1-year and 3-year organizational growth and improvement.



Organizational Structure and Job Descriptions

Building a Robust Cyber Workforce Framework

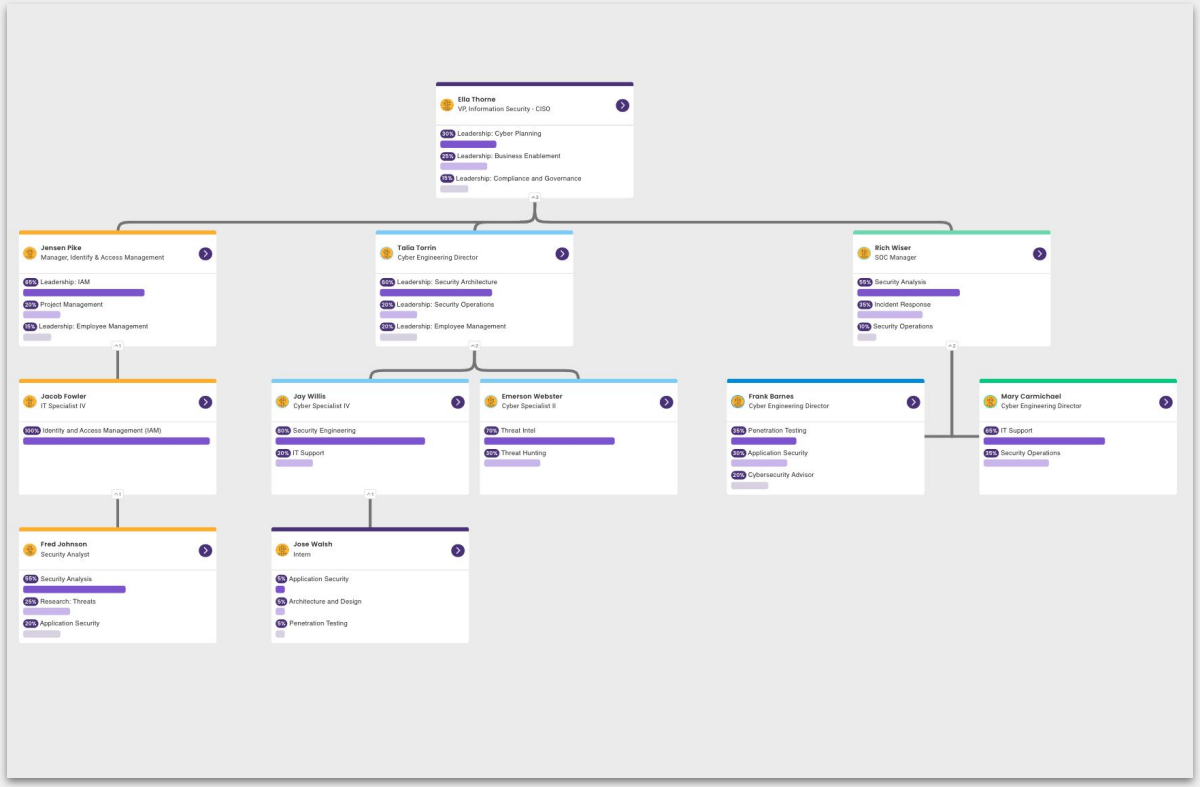
Our SaaS platform is instrumental in constructing a detailed and effective organizational structure, leveraging the CyberSN Taxonomy to ensure precision and alignment. This platform enables us to:

Develop Comprehensive Organizational Structures:

- **Visual Representation**: Display a clear and structured hierarchy of your cyber workforce.
- **Role Clarity**: Define and delineate roles and responsibilities within the organization.

Create Accurate Job Descriptions:

- **CyberSN Taxonomy**: Utilize the CyberSN taxonomy to craft precise job descriptions that align with industry standards.
- **Consistency and Clarity**: Ensure job descriptions are consistent and clearly understood across the organization.

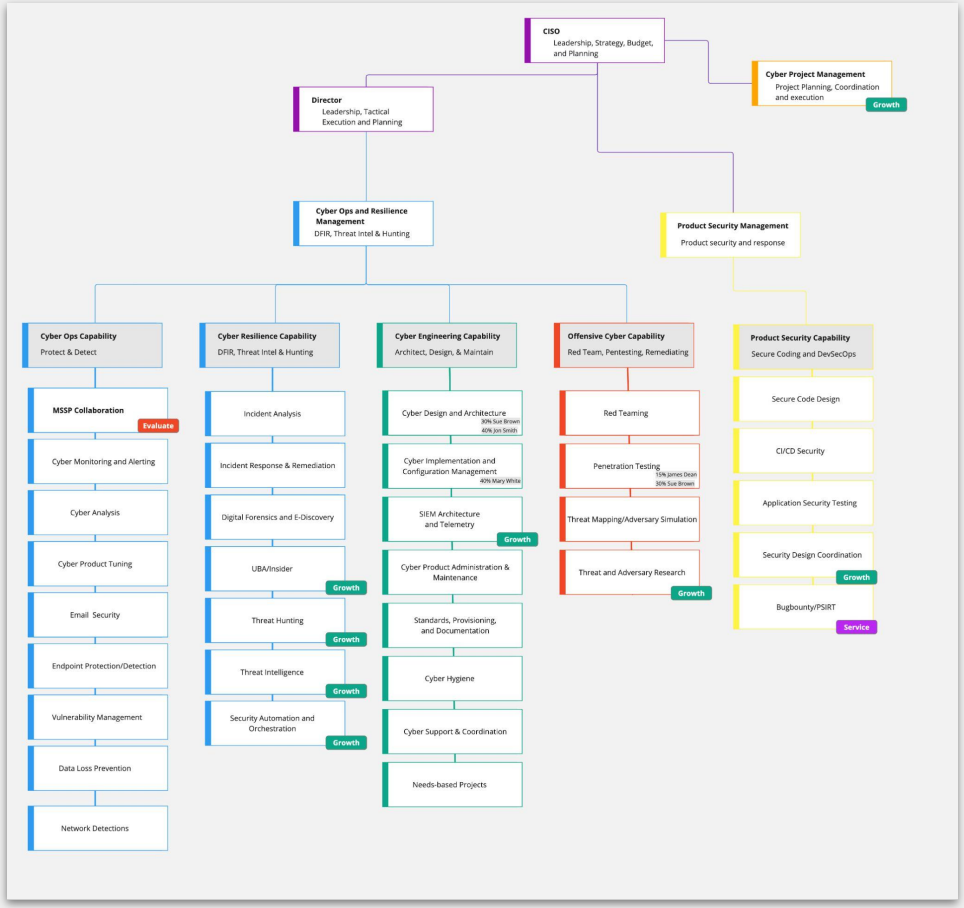


The Cyber Capabilities Model: Enhancing Program Maturity

Assessing, Identifying, and Advancing Your Cybersecurity Program

Our Cyber Workforce Risk Management (CWRM) Solution delivers a comprehensive cyber capabilities model. This model helps your organization:

- **Evaluate Program Maturity**:
  - **Maturity Assessment**: Assess the current maturity level of your cybersecurity program using a detailed cyber risk fusion model.
  - **Benchmarking**: Compare your program's maturity against industry standards and best practices.
- **Identify Capability Gaps**:
  - **Gap Analysis**: Highlight gaps in your current cybersecurity capabilities.
  - **Risk Assessment**: Understand the potential risks associated with these gaps.
- **Develop a Strategic Roadmap**:
  - **Growth Plan**: Provide a clear roadmap for internal growth and capability development.
  - **Outsourcing Opportunities**: Identify areas where outsourcing can enhance program capabilities.
  - **Vendor Utilization**: Recommend strategic vendor partnerships to fill critical gaps.
- **Achieve Program Maturity**:
  - **Strategic Initiatives**: Outline key initiatives to advance your cybersecurity program maturity.
  - **Milestone Setting**: Set achievable milestones for tracking progress and success.
  - **Resource Alignment**: Ensure alignment of resources and efforts with strategic goals.



Data-Driven Insights: Time Allocation Across Cybersecurity Functions

Optimizing Workforce Efficiency and Focus

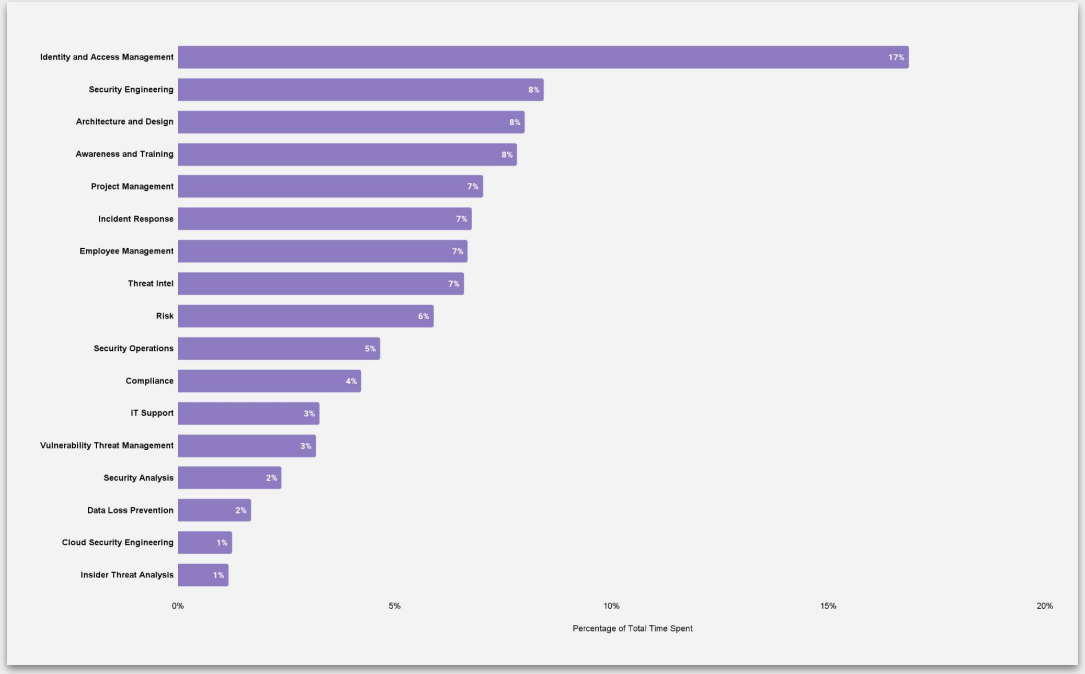
Our detailed analysis provides valuable insights into how your cybersecurity team allocates their time across various functions. By capturing and analyzing this data, we can identify areas of focus and opportunities for improvement. The chart illustrates the time spent across key cybersecurity functions, highlighting that a significant portion of the team's efforts are dedicated to Identity and Access Management (IAM).

Key Insights:

- **Identity and Access Management (IAM)**: A large portion of the cyber team's time is devoted to IAM, indicating a critical focus area for the organization.
- **Awareness and Training**: Time spent on training and awareness showcases the proactive measures taken to educate the workforce increase the organization's security posture.
- **Compliance**: Compliance activities are a necessary part of ensuring regulatory adherence and risk management and are currently underserved.

Benefits of Understanding Time Allocation:

- **Resource Optimization**: Identify areas where time can be reallocated for greater efficiency.
- **Strategic Focus**: Ensure critical functions receive appropriate attention and resources.
- **Skill Development**: Target training and development efforts based on where the team spends the most time.
- **Balanced Workload**: Address any imbalances in workload distribution to prevent burnout and improve productivity.



Data-Driven Insights: Percentage of Time Managers Spend on Employee Management

Cultivating a Positive Culture and Enhancing Employee Development

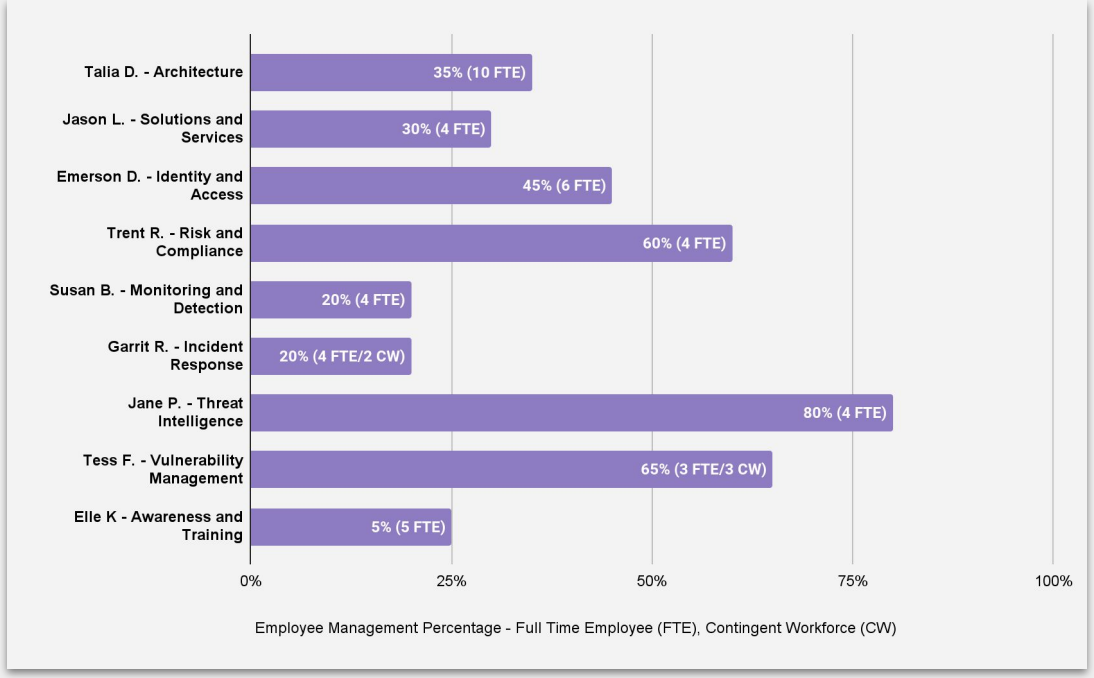
Our analysis provides valuable insights into how much time each manager allocates to employee management. This is crucial for fostering a positive culture, promoting employee development, and enhancing overall retention.

Key Insights:

- **Inconsistent Employee Management Across Teams**:
  - **Observation**: There is a notable inconsistency in the amount of time managers spend on employee management across different teams.
  - **Range**: The time allocation varies significantly, with some managers dedicating as little as 5% and others as much as 80%.

Actionable Recommendations:

- **Empower Managers**:
  - **Ownership and Decision-Making**: Encourage managers to take ownership of their teams, make informed decisions, and lead effectively.
  - **Leadership Training**: Provide leadership development programs to equip managers with the skills needed for effective team management.
- **Leverage Strong Technical Expertise**:
  - **Dual Roles**: Recognize that managers are balancing technical contributions with employee management responsibilities.
  - **Support Systems**: Implement support systems to help managers balance these dual roles effectively.



Data-Driven Insight: Alignment with Cyber Strategy

Ensuring Strategic Cohesion and Identifying Opportunities for Improvement

Our analysis provides a comprehensive view of how well your cyber team's activities align with the overarching cyber strategy set by leadership. By capturing detailed information from our intake meetings and comparing it against the provided cyber strategy, we identify gaps and highlight opportunities for improvement.

Identifying Gaps:

- **Current Activities vs. Strategic Goals**: Highlight specific areas where the cyber team's current activities do not align with the strategic goals.
- **Resource Allocation**: Identify gaps in resource allocation that may be hindering strategic alignment.

Highlighting Opportunities for Improvement:

- **Strategic Focus**: Recommend adjustments to ensure that the cyber team's efforts are focused on strategic priorities.
- **Process Enhancements**: Suggest process improvements to bridge the gaps between current activities and strategic objectives.
- **Training and Development**: Propose targeted training programs to align team skills with strategic needs.

Cyber Strategy Objective	Alignment
Advance adoption of a defined and measurable cybersecurity framework Informal and undocumented environment impacting progress in this practice.	People, Process, Technology, Metrics
Reduce project risk with upfront cybersecurity design requirements Security solutions team is focused on implementations and operations and informal practices.	People, Process, Technology, Metrics
Seamless and robust cybersecurity risk assessment for centralized documentation Lacking a comprehensive awareness compliance of all applicable compliance frameworks (SOC2, FedRAMP, HIPAA) across teams.	People, Process, Technology, Metrics
Drive a "culture of security" into everyday processes across the company Informal metrics measuring cyber operations and resilience ROI.	People, Process, Technology, Metrics

Aligning Roles with Industry Standards for Career Growth

Aligning Roles with Industry Standards for Enhanced Career Growth

Our Cyber Workforce Risk Management (CWRM) Solution goes beyond generic job titles to provide meaningful, industry-aligned titles that accurately reflect the responsibilities and expertise of your workforce. This approach fosters job satisfaction and illustrates clear career progression.

Here's how we do it:

- **Capture and Analyze Responsibilities**:
  - **Detailed Assessment**: Conduct thorough surveys and analyses of employees' responsibilities and daily tasks.
  - **Insight Gathering**: Understand the scope and impact of each role within the organization.
- **Provide Industry-Aligned Job Title Suggestions**:
  - **Cybersecurity Industry Standards**: Align job titles with recognized industry standards to ensure clarity and relevance.
  - **Role-Specific Titles**: Move away from generic hierarchical titles such as "Security Analyst IV" to more precise titles like "Cloud Security Engineer".
- **Enhance Job Satisfaction and Career Progression**:
  - **Clear Role Definitions**: Provide employees with job titles that accurately reflect their contributions and expertise.
  - **Career Path Clarity**: Illustrate clear career progression paths, enhancing motivation and retention.
  - **Teammate Engagement**: Increase teammate engagement and satisfaction by recognizing their specific skills and roles.

CURRENT TITLE	→	RECOMMENDED TITLE
Security Analyst 2	→	Security Engineer
Security Analyst 2	→	GCR Analyst
RISC Privacy Lead	→	Privacy Lead
Security Analyst 1	→	DevSecOps Engineer
Security Analyst 2	→	Security Engineer
Unit Supervisor	→	Security Program Manager
Security Analyst 1	→	Security Analyst

Salary and Compensation Assessments

Leveraging Industry Data for Competitive Compensation Packages

As a leader in cyber staff augmentation, our Cyber Workforce Risk Management (CWRM) Solution includes comprehensive salary and compensation assessments. Utilizing our extensive database and knowledge of current trends, we ensure your organization offers competitive and fair compensation packages. Here's how we achieve this:

- **Extensive Job Data Analysis**:
  - **Comprehensive Database**: Leverage our extensive database of cybersecurity job roles and compensation information.
  - **Data-Driven Insights**: Utilize data from a wide range of industry sources to inform our assessments.
- **Current Trends in Cyber Staff Augmentation**:
  - **Trend Awareness**: Stay abreast of the latest trends in cyber staff augmentation to provide relevant and up-to-date compensation advice.
  - **Market Benchmarking**: Compare your organization's compensation packages against current market standards.
- **Tailored Compensation Recommendations**:
  - **Role-Specific Assessments**: Provide salary and compensation assessments tailored to specific roles and responsibilities.
  - **Competitive Packages**: Ensure your compensation packages are competitive to attract and retain top talent.
  - **Salary Needed to Replace**: Assess the salary required to replace key positions, ensuring continuity and minimizing disruption.
- **Alignment with Industry Standards**:
  - **Strategic Alignment**: Align compensation packages with your organization's strategic goals and financial capabilities.

Example Assessment: Salary needed to replace individual

- **Current Role**: Cloud Security Engineer
- **Recommended Salary Range**: $120,000 - $140,000 (based on your total compensation)

Individual Upskilling Plans for Career Advancement

Fostering Deep, Transferable Skills for Long-Term Success

Our Cyber Workforce Risk Management (CWRM) Solution includes personalized upskilling plans for each teammate designed to advance careers and develop deep, transferable skills. We leverage existing training curriculums within your organization and recommend supplemental training to ensure comprehensive development. Here's how we approach it:

- **Customized Upskilling Plans**:
  - **Personalized Pathways**: Develop individualized plans tailored to each employee's career goals and current skill set.
  - **Utilize Existing Resources**: Maximize the use of existing training curriculums available within your organization.
- **Supplemental Recommendations**:
  - **Partnered Institutes**: Collaborate with top training institutes to provide additional learning opportunities.
  - **Focused Upskilling**: Ensure efforts focus on mastering concepts and building skills beyond merely operating specific tools or applications.
- **Philosophy**:
  - **Focus on Mastery, Not Machinery**: Emphasize deep understanding and proficiency over simply learning to use particular products.
  - **Build Skills Beyond Tools**: Develop skills that are transferable and valuable across various contexts and roles.

Example Upskilling Plan:

- **Current Role**: Security Analyst
- **Upskilling Focus**: Advanced Threat Detection
- **Recommended Courses**:

Internal: Cybersecurity Threat Detection (Existing **Curriculum**)

  - **Supplemental**: Advanced Threat Detection Techniques (Partnered Institute)

Alignment with the NICE Framework

Enhancing Standardization and Consistency in Cyber Workforce Management

Our Cyber Workforce Risk Management (CWRM) Solution is supported by the CyberSN taxonomy, which enables precise categorization of job roles, tasks, and responsibilities. By aligning with the National Initiative for Cybersecurity Education (NICE) Workforce Framework, we ensure that our services promote standardization across the cybersecurity industry. (NIST CyberSN)

Key Aspects of Our Alignment:

- **Comprehensive Role Definitions**:
  - The NICE Framework provides a common language and structure for defining and categorizing cybersecurity roles, tasks, and skills, ensuring clarity and consistency across the industry (NICCS) (CISA).
- **Data-Driven Insights**:
  - Using the CyberSN taxonomy, which extends the NICE Framework, we capture detailed data on workforce activities and align them with strategic cybersecurity objectives, facilitating informed decision-making and strategic alignment (NIST CSRC).
- **Career Development and Training**:
  - The NICE Framework's detailed competency areas and work roles guide the development of tailored training programs and career pathways, helping to bridge skill gaps and enhance employee development (NIST) (NIST).
- **Enhanced Recruitment and Retention**:
  - Standardized job descriptions and clear role definitions based on the NICE Framework make it easier to recruit qualified candidates and retain top talent by providing clear career progression paths (CISA).

Benefits of NICE Framework Alignment:

- **Improved Communication**: Establishes a common language for describing cybersecurity work, improving communication within and across organizations.

Strategic Workforce Planning: Helps organizations align their **workforce** with cybersecurity goals and strategic objectives.

- **Industry Standardization**: Promotes consistency in job roles and skills, making it easier to compare and align with industry standards.

Unlock the Full Potential of your Workforce

Benefits of CyberSN's Cyber Workforce Risk Management

Expertise:

Our team of experts brings unparalleled knowledge and experience in cyber workforce management.

Tailored Solutions:

We customize our approach to meet the unique needs of your organization.

Actionable Insights:

Receive clear, data-driven recommendations that are easy to implement.

Holistic View:

Our comprehensive service covers all aspects of your cyber workforce, from strategy to satisfaction.

Workforce Optimization:

Optimize your cyber workforce to enhance efficiency, satisfaction, and overall performance.

CyberSN

Lower your risk profile

Empower, engage, and retain your cybersecurity professionals.

> A cybersecurity budget that doesn't include talent planning, talent development, and talent retention is not a cybersecurity budget that any Security Leader, CEO, or Board can rely on for accurate risk calculations.

Deidre Diamond
Founder & CEO, CyberSN
Founder, Secure Diversity