Procom

The people who power performance.

BUILDING A RESPONSIVE CYBERSECURITY WORKFORCE

SPECIALIZATION INSIGHTS

www.procomservices.com

A practical guide to building a cybersecurity workforce that's aligned with your organization's defense strategy and prepared to mitigate emerging threats.

CONTENT

Understanding **the New Threat Landscape**

The attack surface of cybersecurity threats have expanded, necessitating a stronger cybersecurity workforce to protect sensitive data and infrastructure.

Meanwhile, the cybersecurity industry faces a critical skills shortage due to increasing threats, technological advancements, and lack of comprehensive education programs.

"CYBERSPACE HAS KICKED THE DOORS WIDE OPEN — ANYONE CAN WALK THROUGH, AND MANY ARE. THE PERILS OF WEAPONIZED DIGITAL TECHNOLOGY ARE GROWING, PRESENTING NEW VULNERABILITIES FOR PEOPLE, INSTITUTIONS, AND ENTIRE COUNTRIES."

– ANTÓNIO GUTERRES, SECRETARY-GENERAL OF THE UNITED NATIONS

The following critical and emerging cybersecurity threats demand immediate and proactive attention from organizations worldwide:

- **CLOUD ATTACKS**
- **IDENTITY THREATS**
- **PUBLIC-FACING APP EXPLOITS**
- **RANSOMWARE**
- **ZERO-DAY VULNERABILITIES**

$10.5
TRILLION

Global cybercrime damage costs are expected to reach $10.5 trillion annually by 2025, growing by 15% each year, highlighting the urgency for organizations to invest in specialized cybersecurity talent.

(SOCRadar Cyber Intelligence Inc.)

Trust Nothing, **Verify Everything**

Traditional cybersecurity models are no longer sufficient to protect organizations from emerging threats. The *Zero Trust* model, which asserts "never trust, always verify," has emerged as the backbone of modern cybersecurity strategies. Zero Trust is not just a technology or a set of tools—it's a mindset shift that changes how organizations approach security.

For organizations to truly lead in cybersecurity, they must not only adopt Zero Trust principles but also cultivate a workforce that is aligned with this strategy. Building a team skilled in Zero Trust methodologies ensures that security is embedded in every layer of the organization—from the development of secure applications to the management of sensitive data.

WHY ZERO TRUST MATTERS:

Unprecedented Threat Landscape: As cyberattacks become more sophisticated, the need for greater risk management is needed. Zero Trust helps mitigate risks by assuming every interaction—whether internal or external—could be a potential threat.

Workforce Transformation: As organizations embrace remote work, cloud computing, and digital collaboration, Zero Trust becomes essential in ensuring that access to resources is strictly controlled and continuously verified.

Regulatory Compliance: With increasing regulatory scrutiny, adopting a Zero Trust architecture can help organizations meet stringent compliance requirements while protecting sensitive data.

Align with Established Cybersecurity Frameworks

Building a Strong Cybersecurity Foundation for Your Organization

01

THE CIA TRIAD

A foundational cybersecurity model that ensures Confidentiality, Integrity, and Availability of information, protecting data from unauthorized access, modification, and ensuring it's accessible when needed.

02

NIST FRAMEWORK

A comprehensive guide for organizations, structured around Identify, Protect, Detect, Respond, and Recover functions, helping to manage and reduce cybersecurity risks effectively.

03

ISO/IEC 27001

An internationally recognized standard for information security management, providing a systematic approach to securing sensitive data and ensuring compliance with global regulations.

04

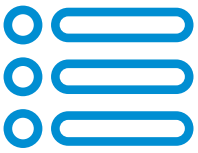
NICE FRAMEWORK

A detailed framework focused on defining and developing a skilled cybersecurity workforce, outlining roles, skills, and training needed to defend against evolving cyber threats. We will focus on this framework primarily.

NICE Cybersecurity Framework Integration

Expanding Your Cybersecurity Workforce: Roles for Emerging Domains

As cyber threats evolve, so too must the roles and skills within your cybersecurity workforce. The NICE Cybersecurity Workforce Framework provides a structured approach to identifying the necessary roles and competencies to address new and emerging cybersecurity domains. The framework can be broken down into five distinct components, but within each of them, lie more sub-elements. Categories, for example, can be broken down into: Oversight and Governance, Design and Development, Implementation and Operation, Protection and Defense, Investigation, Cyberspace Intelligence and Cyberspace Effects. Consulting the NICE Framework will help your organization craft a highly specialized cybersecurity role.



Categories

Broad functional areas that organize cybersecurity work into seven distinct categories, such as *Protect and Defend*, guiding the overall structure of cybersecurity roles.

Specialties

Subdivisions within categories that focus on specific types of cybersecurity tasks, providing detailed classifications of different cybersecurity functions.

Roles

Defined positions within the framework that outline the tasks, knowledge, skills, and abilities needed for specific cybersecurity jobs.

Tasks

Specific activities associated with each work role, detailing the responsibilities and daily actions required to perform the job.

KSAs

Knowledge, skills and abilities. The essential competencies required for each work role, guiding both hiring and professional development in cybersecurity.

Address Threats with Specialized Roles

1

Cyber Defense Analysts

Detects, analyzes, and mitigates cyber threats in real-time.

2

Incident Responders

Manages and coordinates responses to cybersecurity incidents.

3

Vulnerability Assessment Analysts

Identifies and mitigates vulnerabilities in systems before they can be exploited.

4

Secure Software Assessors

Evaluates the security of software throughout the development lifecycle.

5

Cloud Security Specialists

Secures data and infrastructure in cloud environments.

Build a Resilient Cybersecurity Workforce

Today's threat landscape is complex, and threat actors are targeting organizations globally. Building a resilient cybersecurity workforce involves not just the ability to defend against current threats but also to anticipate, adapt, and respond to new challenges as they emerge. To achieve this, organizations must prioritize the continuous development of technical skills, foster a multidisciplinary approach, and implement strategic recruitment and retention practices that align with the NICE Cybersecurity Workforce Framework.

PRIORITIZE CONTINUOUS SKILL DEVELOPMENT AMIDST EVOLVING THREATS

Focus: Ongoing training is vital, as 62% of companies report a lack of skilled cybersecurity staff as a key challenge in managing their security posture.

Implementation: As cyber threats evolve, it's essential to keep your team's skills sharp. Invest in regular training and certifications such as CISSP and OSCP, which are crucial for roles requiring deep technical expertise in areas like penetration testing, incident response, and threat intelligence. Continuous learning is necessary to combat advanced threats like ransomware, which saw a 105% increase in attacks globally in 2021 alone.

LEVERAGE DATA-DRIVEN RECRUITMENT TO CLOSE THE WORKFORCE GAP

Focus: Leverage recruitment strategies that target the skills most in demand, such as cloud security and threat analysis.

Implementation: With LinkedIn reporting a 30% increase in demand for cybersecurity professionals year-over-year, it's critical to use data-driven recruitment tools. Focus on hiring for roles identified by the NICE Framework, such as Cyber Defense Analysts and Cloud Security Engineers, to ensure your organization is equipped to handle modern cyber threats. The right recruitment strategies are essential to addressing the global shortfall in cybersecurity talent.

FOSTER CROSS-FUNCTIONAL EXPERTISE TO MITIGATE RISK

Focus: Organizations with cross-functional cybersecurity teams are 2.5 times more likely to have a strong security posture.

Implementation: Integrate cybersecurity professionals with legal, compliance, and business operations teams. This collaboration ensures that cybersecurity strategies are aligned with broader business goals and regulatory requirements. For example, teams can work together to address the growing regulatory challenges posed by frameworks like GDPR and CCPA, where non-compliance fines reached over $1 billion in Europe in 2021 alone.

A CONTINGENT WORKFORCE CAN SUPPLEMENT INTERNAL TEAMS

Focus: The cybersecurity skills gap is driving organizations to increasingly rely on a contingent workforce to meet their security needs.

Implementation: Establish relationships with a specialized contingent workforce provider to fill critical gaps in your cybersecurity team. This approach enables you to access top talent on an as-needed basis, especially for highly specialized tasks like forensic analysis, advanced threat hunting, or incident response. According to a Deloitte survey, 41% of organizations are now using contingent workers for critical cybersecurity roles, allowing them to remain agile and responsive to evolving threats.

Strengthen Security Posture and Readiness

Proactive Security Posture: The Key to Cost Savings

A proactive approach to cybersecurity is essential. Organizations that focus on proactive measures, such as continuous monitoring and real-time threat intelligence, experience a reduction in breach recovery costs. Utilizing tools like Security Information and Event Management (SIEM) systems, which are implemented by 80% of large enterprises, helps detect and mitigate threats before they escalate.

The Importance of Regular Security Assessments

Regular security audits and penetration tests are crucial for identifying and addressing vulnerabilities. A Deloitte study shows that companies conducting these assessments quarterly are 40% less likely to experience significant breaches. Penetration testing simulates real-world attacks, offering valuable insights that allow organizations to strengthen their defenses proactively.

Strategic Incident Response Planning

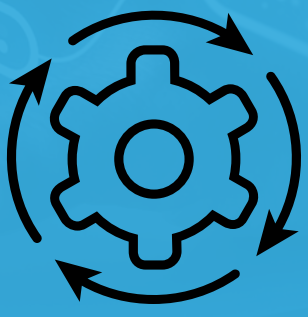
A comprehensive incident response plan (IRP) is vital for minimizing the impact of cyber incidents. IBM's research indicates that having a well-prepared IRP can reduce breach costs by an average of $2.66 million. Regular training and simulations ensure that your team can respond swiftly and effectively when an incident occurs.

Cultivating a Culture of Cybersecurity Awareness

Human error remains a leading cause of data breaches, responsible for 85% of incidents, according to Verizon's Data Breach Investigations Report. Organizations that invest in regular phishing simulations and cybersecurity training reduce the likelihood of successful phishing attacks by 70%. Building a culture where every employee is aware of cybersecurity best practices is essential for protecting your organization's assets.

Regular and Engaging Training Programs

Leadership Involvement and Commitment



Integrate Cybersecurity Into Daily Operations

Procom

The people who power performance.

Procom can help you find specialized cybersecurity talent.

1	**RIGHTFIT™ RECRUITMENT PROCESS:** Each cybersecurity IT candidate we submit to you has gone through our proven 5-step ISO-certified process to ensure they have the necessary skills and are the right fit for your organization and project.
2	**MARKET RATE INTELLIGENCE:** As one of North America's largest IT staffing firms, Procom has over 28,000 data points a month on current rates across all verticals/industries in North America.
3	**DEDICATED CLIENT PORTAL** Access and manage your Procom talent all from one dashboard. Gain visibility over your candidates' recruitment lifecycle, collaborate and communicate more easily to make better hiring decisions faster.
4	**PROVEN TRACK RECORD:** Procom's cybersecurity IT talent recruitment experts have over 45 years of experience recruiting in the cybersecurity industry.
5	**LOCATIONS SERVED:** Procom is one of North America's largest IT staffing and contingent workforce management firms with 20+ locations across North America.