FOR SAN DIEGO, BY SAN DIEGO

2025 Cybersecurity Industry Economic Impact and Workforce Study

CCOE

Research produced by San Diego Regional EDC
October 2025

FOR SAN DIEGO, BY SAN DIEGO

2025 Cybersecurity Industry Economic Impact and Workforce Study

TABLE OF CONTENTS

CCOE

EXECUTIVE SUMMARY

In today's hyperconnected, internet-first economy, cybersecurity is no longer optional. Whether in manufacturing, finance, healthcare, energy, or government, a single breach can inflict cascading operational, reputational, and financial consequences. IBM's 2025 report found that the average cost of a data breach in the United States is at an all-time high of $10.2 million, the highest in the world. Now, more than ever, cybersecurity is essential to the stability and competitiveness of every industry.

> IBM's 2025 report found that the average cost of a data breach in the United States is at an **all-time high of $10.2 million**, the highest in the world.

Authored by San Diego Regional EDC, together with Cyber Center of Excellence (CCOE), in October 2025, this biennial report explores the economic footprint of the San Diego region's cybersecurity cluster. The following sections will quantify the size and economic impact of the cyber cluster, profile its firms and technologies, examine workforce and talent trends, and highlight business sentiments and local initiatives that are shaping the region's cyber ecosystem. These findings are complemented by insights gathered from a survey of the region's cybersecurity firms and interviews with industry leaders and experts.

$4.3B
Total economic impact – greater than hosting **26 Comic-Cons** each year!

1,350
Cybersecurity companies and NAVWAR call San Diego home

29,040
Total jobs impacted and **14,857 cybersecurity roles**

50,432
San Diego cybersecurity-related talent – with **60% diversity** compared to only 25% in the global workforce

4,244
Cyber-related degrees conferred annually by local academic institutions – **51% increase** in 5 years

KEY TAKEAWAYS

San Diego's cybersecurity cluster continues to expand, adding jobs, firms, and economic impact, even as the broader technology industry contracts. There are 14,875 jobs across 1,350 establishments within the cybersecurity cluster in San Diego, up 11 percent and 33 percent over the last two years, respectively. Together, this amounts to $4.3 billion regional economic impact and 29,040 jobs impacted.

The cybersecurity talent pool continues to grow but has been slowing down since 2022. Despite the increased need for cybersecurity professionals, the pace the talent pool grows every year is declining. This trend parallels a similar slowdown in advertised demand, as job postings for cybersecurity workers have declined and remain 60 percent lower than pre-pandemic levels.

San Diego continues to expand cyber skills, particularly in certificate obtainment, which outpaces all of San Diego's peer metros. Overall degree and certificate obtainment in San Diego continues to grow, expanding 51 percent since 2019. Certificates, which are obtained both in and outside of traditional degree programs, have grown 78 percent from 2019 to 2023.

Business sentiment has softened. Survey results show that perceptions of San Diego's business environment have declined relative to 2023, including access to talent, vendors, customers, and capital. Only research and development remained at the same level compared to 2023.

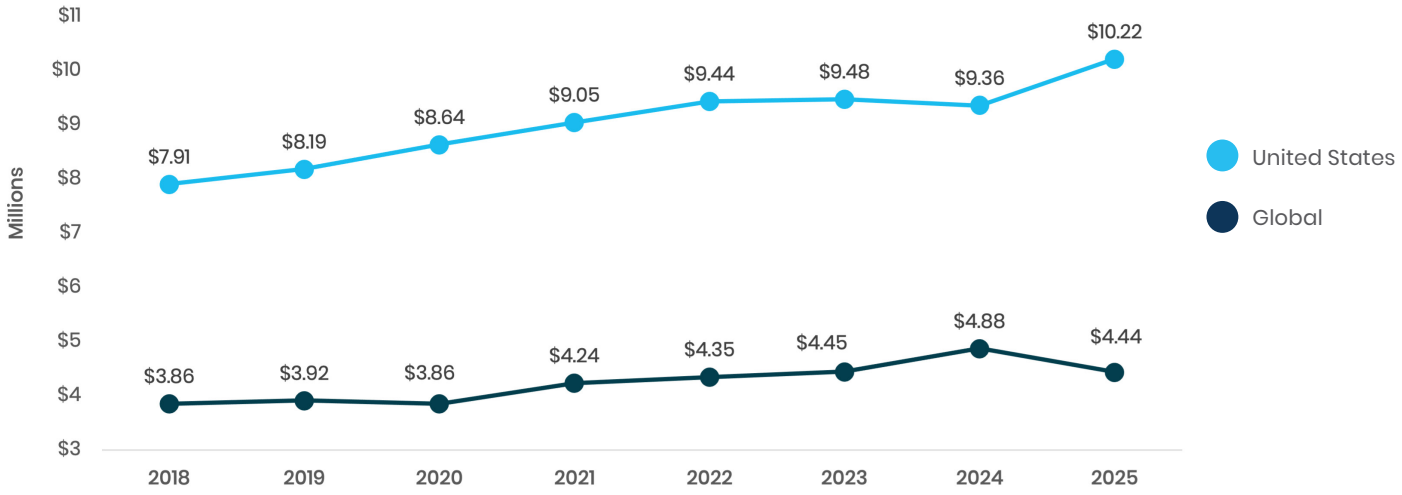
INTRODUCTION

While the U.S. faces record-high costs from data breaches, the picture is not entirely bleak. Technological innovation, particularly in artificial intelligence (AI) and automation, is helping companies become more cyber secure. AI and automation are accelerating detection and containment, which has led to a nine percent decline in average breach costs globally to $4.4 million since 2024, according to IBM.

In contrast, the U.S. average cost of a data breach has climbed to $10.2 million, diverging from global trends. This rise reflects higher regulatory fines, as well as mounting costs related to detection and escalation. The widening gap highlights the critical need for continued investment in cybersecurity capabilities and technologies.

AVERAGE COST OF DATA BREACH

Despite declines globally, the U.S. average cost of data breach is at an all-time high



However, these same technological advancements that help cyber teams detect and contain threats more efficiently present a double-edged sword. Rapid adoption of AI and automation, as well as the increasing interconnectedness of devices all expand an organization's attack surface, creating new opportunities for attackers, even as defenses improve. As the threat landscape changes, the importance of the cybersecurity cluster, including the workforce and firms that sustain it, has grown considerably.

As the threat landscape changes, the importance of the cybersecurity cluster, including the workforce and firms that sustain it, has grown considerably.

CYBERSECURITY CLUSTER & FIRMS

Cybersecurity in San Diego has a **$4.3 billion** economic impact, equivalent to **26 Comic-Cons**

Cluster Overview

More than a decade ago, the cybersecurity cluster in San Diego was a nascent industry, with fewer than 100 companies focused on cyber work. Now, there are 1,350 establishments in the region that are either dedicated to developing cyber products and services or have cyber teams working to thwart attacks. Since 2023, **the region has seen a 33 percent increase in the number of cyber firms**, marking the largest growth observed between reporting periods since tracking began in 2014.

33% increase in the number of regional cyber firms

More firms mean more jobs. **There are 14,875 cyber professionals in San Diego County, 24 percent of which are employed by Naval Information Warfare Systems Command (NAVWAR), the U.S. Navy's cybersecurity hub. The number of cyber jobs in the region represents an 11 percent increase since 2023.** These jobs are also relatively high paying, with median annual wages between $77,400 and $159,200 depending on the specific role.

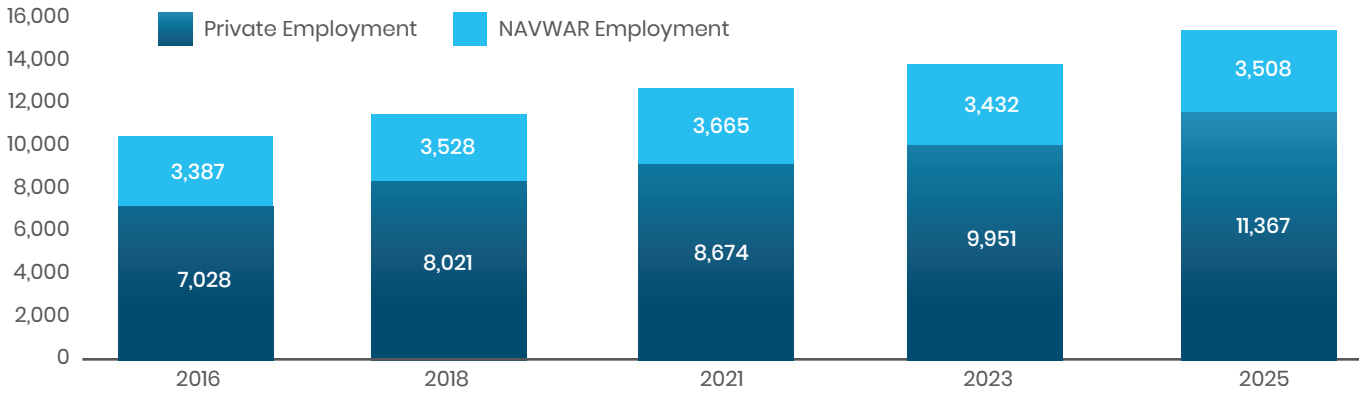
Cyber Employment in San Diego Continues to Grow

The cybersecurity cluster in San Diego, accounting for supply chain interactions and increase in consumer spending, has a total economic impact of $4.3 billion to the regional economy—equivalent to 26 Comic-Cons, the largest convention in the region.

Additionally, the 14,875 jobs directly tied to the cyber cluster support another 14,165 jobs elsewhere in the region, as a result of indirect and induced effects. **Put another way, one job in the cyber cluster supports nearly another job elsewhere in the regional economy.**

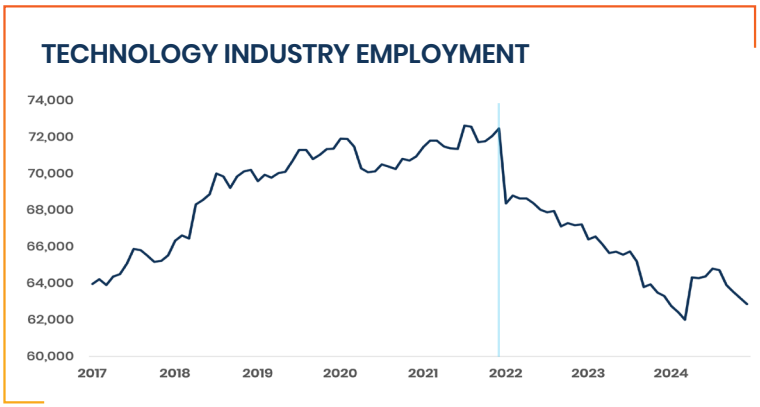
One cyber job supports nearly **one additional job**

More cyber firms mean more cyber jobs with relatively high median annual wages.



Technology Employment Trends

Cyber employment has been on the rise, meanwhile the broader technology industry has been on a downward trend since late 2021 due to post-pandemic correction and high inflationary environment. Cybersecurity has remained an engine for growth, with employment rising steadily between 2021 and 2025. The resilience through this post-pandemic period reflects, in part, the rising importance of cybersecurity across industries, as companies face more costly cyber attacks. As part of this research, a survey of the region's cybersecurity cluster revealed that San Diego cyber firms continue to be involved in a variety of industries. Aside from the expected cybersecurity and technology/IT involvement, cybersecurity firms in the region are also doing work in industries such as defense, education, and healthcare.



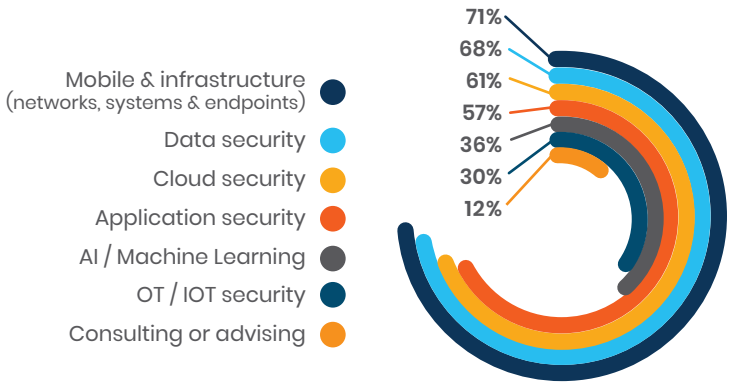
A Look Into Cyber Firms

Cyber firms are also diverse in the type of work they do. From the survey, a large majority of firms (71 percent) are involved in mobile and infrastructure work, protecting the devices, hardware, and digital connections that companies rely on. On top of that, most companies also do work in securing organizations' data, cloud, and applications (68 percent, 61 percent, and 57 percent, respectively). AI and machine learning (ML) has become more prevalent in work streams, leading to more than one-third of firms being involved in this space. With informational and operational technologies now converged, more than 30 percent of companies surveyed are focused on protecting hardware and infrastructure that are now interconnected.

Cyber firms operate in a variety of industries and are involved in various types of work

- **Cybersecurity** 52%
- **Defense or aerospace** 16%
- **Education & Healthcare** 13%
- **Utility or energy** 6%
- **Networking** 3%
- **Technology or IT** 32%
- **Nonprofit** 13%
- **Software** 10%
- **Telecom** 6%
- **Manufacturing** 3%

*An additional 10% in other industries



NAVWAR's cyber workforce alone has an economic impact of $1.2 billion

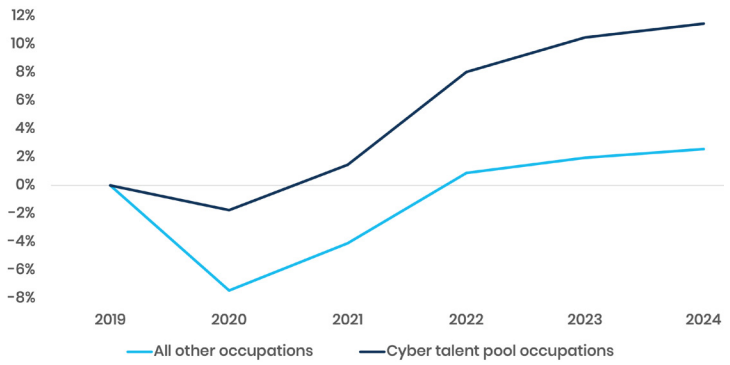
Headquartered in San Diego, NAVWAR's mission is to "identify, develop, deliver and sustain information warfare capabilities and services that enable naval, joint, coalition, and other national missions operating in warfighting domains from seabed to space." Currently, NAVWAR employs 5,311 military and civilian personnel, including a cyber workforce of 3,508. **NAVWAR's cyber workforce alone has an economic impact of $1.2 billion, or just over one-quarter of the total impact of the cyber cluster on the region, making it an anchor of the region's cyber ecosystem.**

TALENT

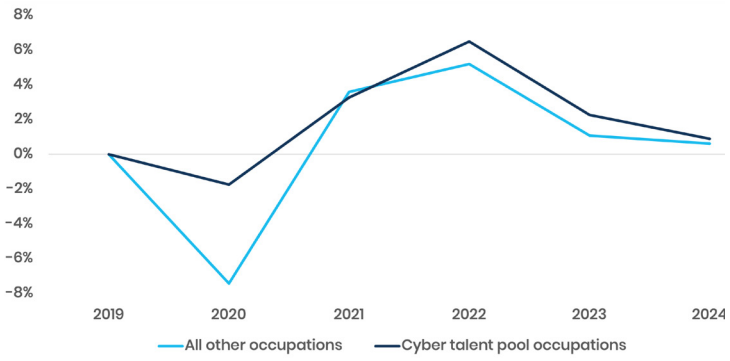
As digital technology becomes increasingly embedded into every aspect of life, extensive and adaptable cybersecurity is essential, which starts with developing and retaining a strong workforce. Globally, cybersecurity is experiencing a talent shortage that, if the trend continues, could reach a shortage of 85 million workers by 2030, according to a 2024 World Economic Forum report.

In San Diego, adequate access to talent appears to be mixed: 44 percent of survey respondents saw access to workforce and talent as a strength, while 28 percent saw this as a weakness. Insights from interviews with local cybersecurity executives suggest that the talent gap is not a straightforward shortage, but rather a complicated intersection of factors such as technological advancement, increasingly diverse industry, and the larger current state of economic uncertainty. As the cyber cluster continues to grow, it is crucial to address the challenges of preparing talent for this rapidly evolving cluster.

SINCE 2019, CYBER TALENT CONTINUES TO EXPAND



THE GROWTH OF THE CYBER TALENT POOL HAS BEEN SLOWING SINCE 2022



Cybersecurity Talent Pool

While there are nearly 15,000 cybersecurity jobs in San Diego, there is a broader talent pool or group of occupations that includes cybersecurity and non-cybersecurity workers who have the skillset desired by cyber employers. Within the cybersecurity talent pool, the median compensation across these occupations is relatively high, paying $145,400, compared to a median of $55,600 across all industries.

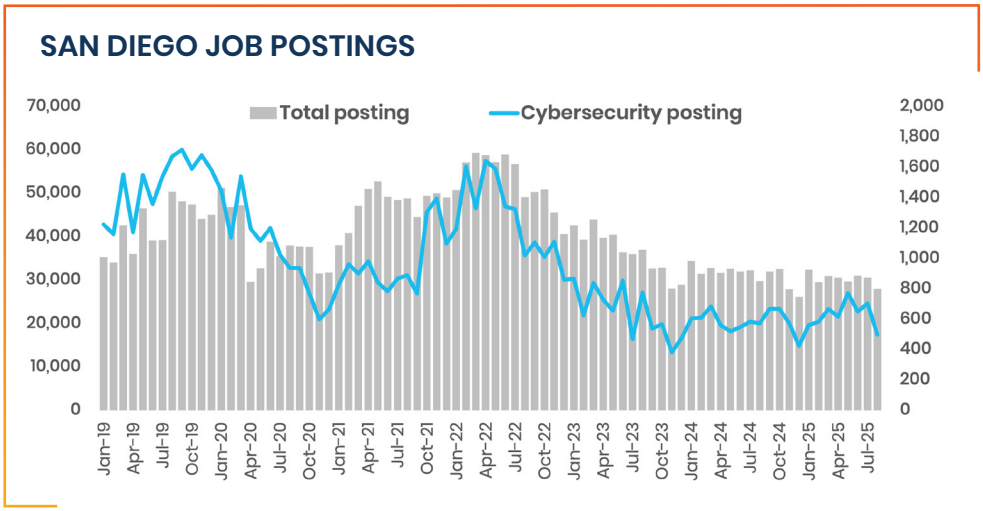
As employment grows, so too does the cybersecurity talent pool. Since 2019, San Diego's cybersecurity talent pool has grown cumulatively 11.5 percent, more than four times greater than all other occupations combined, which have only seen 2.6 percent growth. Through the pandemic, the cyber workforce remained resilient, particularly in comparison to all other occupations. In the post-pandemic period, despite broader labor market corrections, cybersecurity continued to expand, underscoring the cluster's sustained importance.

> San Diego's cybersecurity talent pool has grown cumulatively **11.5 percent**, more than four times greater than all other occupations combined.

While cybersecurity talent continues to grow every year, **the growth rate has been slowing since 2022 despite the increasing need for cybersecurity professionals and the heightened risk of a costly breach due to staff shortages**.

Advertised Demand

The slowing pace of cyber job growth is also reflected in San Diego's advertised demand for cybersecurity workers, which declined in 2022 and now remains at an average monthly posting approximately 60 percent lower than pre-pandemic. The trendline of cybersecurity job postings in San Diego follows a similar pattern to all job postings, reflecting that **cybersecurity is not immune to the impact of economic uncertainty driven by fast-changing federal policy changes and budgetary shifts**, despite its continued growth.

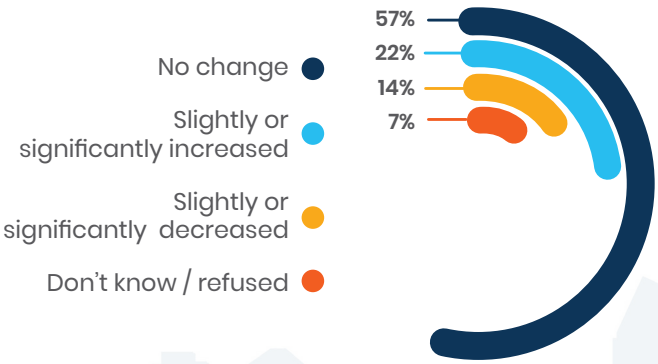


A 2024 ISC2 Cybersecurity Workforce Study highlighted that, unlike in 2023 where an overall lack of talent posed challenges, in 2024, a lack of budget or limited resources to hire and develop talent constrained the ability of firms to grow. In 2025, although cyber employment continues to expand, larger patterns of economic uncertainty may be impacting budgets and limiting hiring, particularly for entry-level talent. One cybersecurity executive explained that firms will often only have budget to hire for one job opening and opt to hire the candidate with more experience and less need for skills training.

Impact of AI

Outside of increasing economic uncertainty, the role of AI in the workforce has become top of mind. For cybersecurity professionals, AI is increasingly becoming integrated into the workflow, as interviews with executive professionals highlighted that employers are increasingly asking how candidates integrate AI. At the same time, universities are actively training students and faculty on AI tools to better prepare and expand the talent pool in an increasingly complex threat environment.

Respondents do not see AI impacting overall employment in the last 12 months



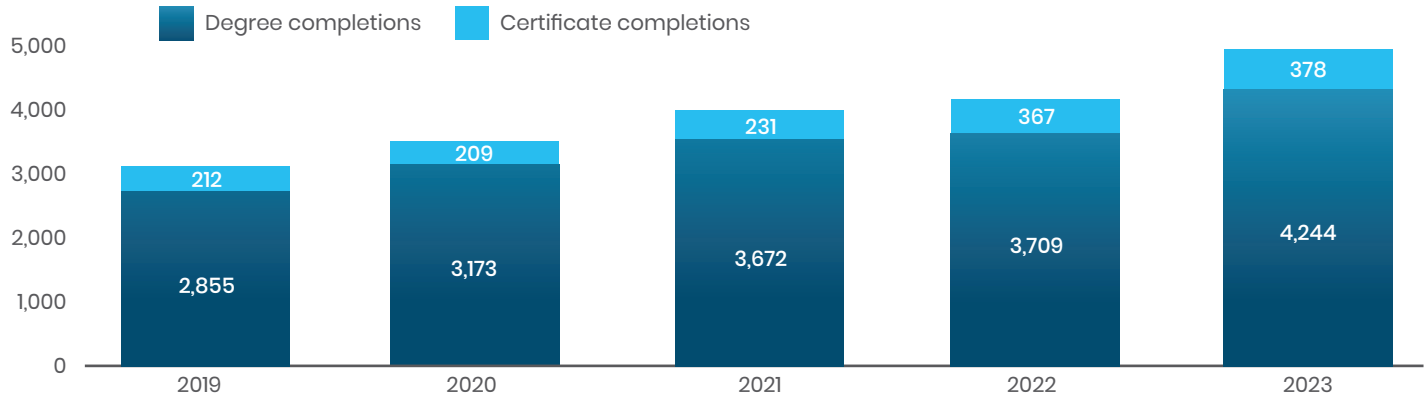
The use of AI is supplementing, not replacing, cybersecurity jobs. Though it has changed the way cybersecurity professionals must operate, AI has not demonstrably impacted hiring practices in the last year. 57 percent of survey respondents said that AI has not changed employment at their business in the last 12 months, and 22 percent said that it increased employment. AI increases the amount and frequency of cyber-related threats, meaning more employees and AI-related skills are needed.

Cybersecurity Educational Pipeline

Economic constraints slowing hiring practices, combined with the rise in cyber threats fueled by rapid technological advancement, simultaneously limits cyber-related opportunities and drives demand for new hires to be highly skilled.

Cybersecurity-related educational attainment in San Diego continues to grow. From **2019 to 2023, cyber-related degree and certificate attainment grew 51 percent, with completions in 2023 totaling 4,244 degrees and 387 certificates**. More individuals are investing their time into obtaining cybersecurity-related skills in San Diego, expanding the expertise of the talent pool.

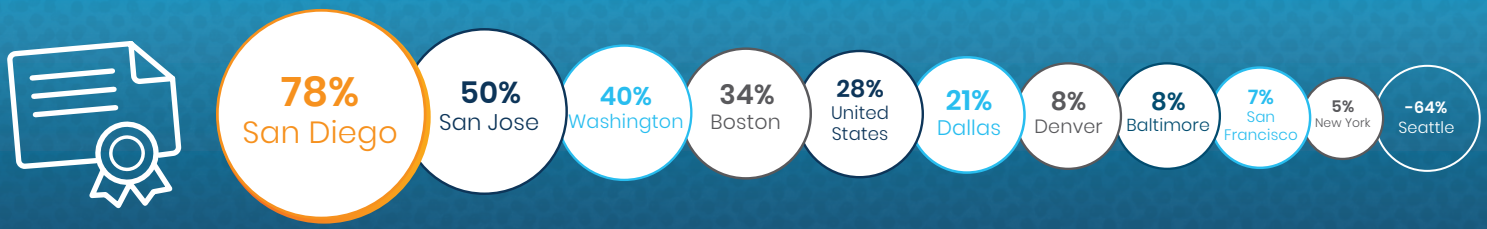
CYBER-RELATED EDUCATION COMPLETIONS



Cybersecurity is a fast-growing, diverse cluster, creating a need for adaptable and often unstandardized skillsets. Interviews with cybersecurity executives affiliated with universities highlighted the challenge of adapting curriculum to the evolving needs of cybersecurity employers, as traditional four-year curriculum cannot move at the same pace.

San Diego, in addressing this challenge, extends training and opportunity beyond a traditional four-year degree. Certificates, both obtained alongside or outside of four-year degrees, reflect an educational emphasis on specialized knowledge, and often provide population-specific support, aimed at meeting the needs of the growing cybersecurity workforce. **San Diego has seen a high growth of certificate obtainment since 2019, growing 78 percent from 2019-2023, a percentage far above its peer metros.**

SAN DIEGO HAS THE HIGHEST GROWTH OF CYBER CERTIFICATE OBTAINMENT SINCE 2019



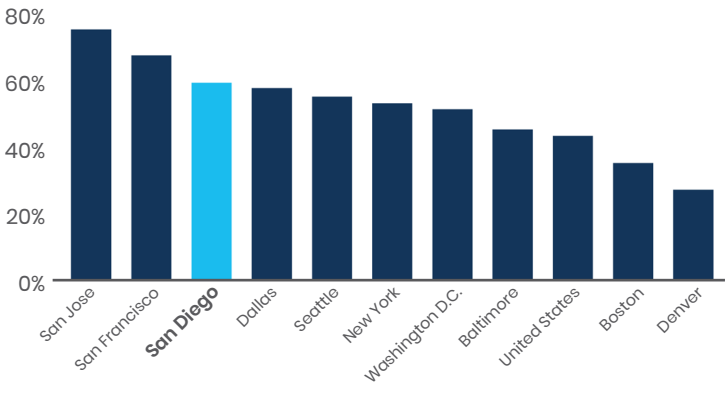
> Educational institutions continue to build on approaches that have served well in recent years. However, cybersecurity is evolving at a pace few sectors can match. The result isn't a lack of talent. It's a reflection of how quickly the field transforms. We're all learning to adapt faster, finding new ways to help students translate foundational knowledge into real-world readiness.
>
> Mansi Thakar, Staff Security Analyst, NVIDIA & Adjunct Professor, National University

Cybersecurity Educational Pipeline (cont.)

Further, San Diego's cyber security ecosystem has also shown a commitment to connecting industry to students. New cybersecurity degree and certificate programs (such as San Diego State University's Cybersecurity Center for Research and Education, CSU San Marcos and City College and UCSD's extended study certificate) all intentionally collaborated between academia, industry, and government when creating curriculum. Additionally, to provide hands-on training the San Diego Cyber Clinic not only offers free services across sectors in San Diego, but in doing so provides students across three universities hands-on training and experience.

As the cyber threat-landscape continues to evolve, it will be critical to continue to invest in pathways that align the region's expanding cyber talent with industry needs. For one interviewed cybersecurity executive, this collaboration was a major strength of San Diego, where a tightly connected cybersecurity ecosystem, with networking between industry, academia, and training providers, drive new opportunities for the cyber cluster. To adapt to challenging circumstances, San Diego's cybersecurity cluster must continue to invest in the skills of early-career talent to build a sustainable workforce prepared for the evolving industry.

San Diego's non-white talent pool ranks high among its peers



San Diego's cybersecurity cluster continues to attract a diverse talent pool, outperforming many peer metros in the ethnic diversity of its workforce. **60 percent of San Diego's cyber talent pool identifies as non-white, which is 16 percentage points higher than that of the United States.**

Yet, the cluster still has an opportunity to attract an even wider pool of talent, as the racial demographic makeup of San Diego's cybersecurity talent pool is not reflective of the region's overall workforce. The racial demographics of cybersecurity-related degree earners closely mirrors the racial composition of the existing cyber workforce, yet neither mirror the demographics of the workforce across all occupations in San Diego. Particularly, 34 percent of San Diego's overall workforce is Hispanic or Latino, while only 19 percent of cyber-related degree earners, and 15 percent of those employed within the cyber talent pool are Hispanic or Latino. While employers are largely drawing from the available degree-earning talent pool, the dissonance between cyber-degrees and San Diego's overall workforce demographics emphasize potential to further grow the cyber talent pool through attention earlier in the pipeline.

Cybersecurity Educational Pipeline (cont.)

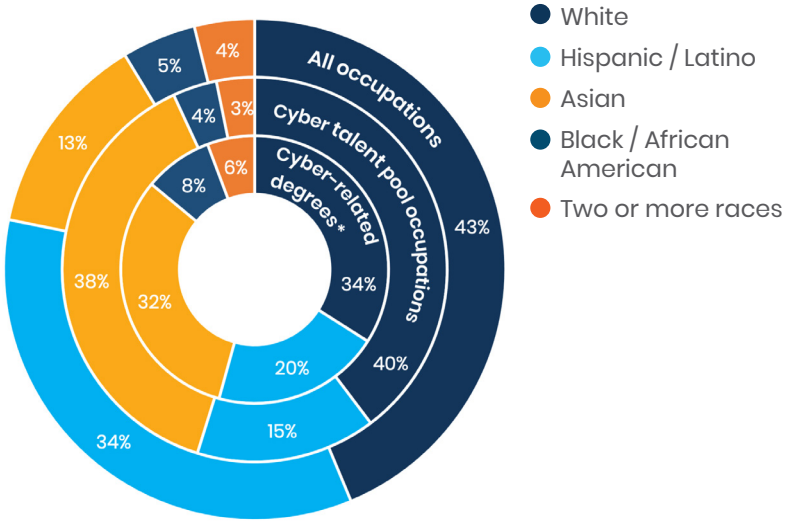
However, not all degree-earning groups are represented in the cyber talent pool workforce. Notably, the representation of the Black population in San Diego cybersecurity-related degrees is higher (at eight percent) than their representation in both the general workforce (at five percent) and the current cybersecurity talent pool (at four percent). This indicates a needed opportunity to better connect and support this skilled group to employment pathways in the field.

There is potential to expand the talent pool, particularly through early and intentional recruitment of underrepresented individuals into cybersecurity-related educational pathways.

Further, across the technology sector, the underrepresentation of women persists, and cybersecurity is no different. Women only make up one-quarter of the cyber talent pool and related degrees. This gender gap reflects disparities in K-12 and college level education that later impacts employment demographics.

SAN DIEGO'S OVERALL WORKFORCE

The cybersecurity talent pool is not reflective of San Diego's overall workforce



There is potential to expand the talent pool, particularly through early and intentional recruitment of underrepresented individuals into cybersecurity related educational pathways. Collaborative programs, like CyberHire, are one way to support inclusive cybersecurity pathways. CyberHire partners with local organizations to create cybersecurity career pathways and educational support for individuals facing employment barriers such as youth, veterans, and individuals with disabilities. Expanding initiatives such as these can play a critical role in broadening the cybersecurity talent pool.

** Cyber-related degrees racial demographics data does not encompass non-US residents, which made up 21% of completions*

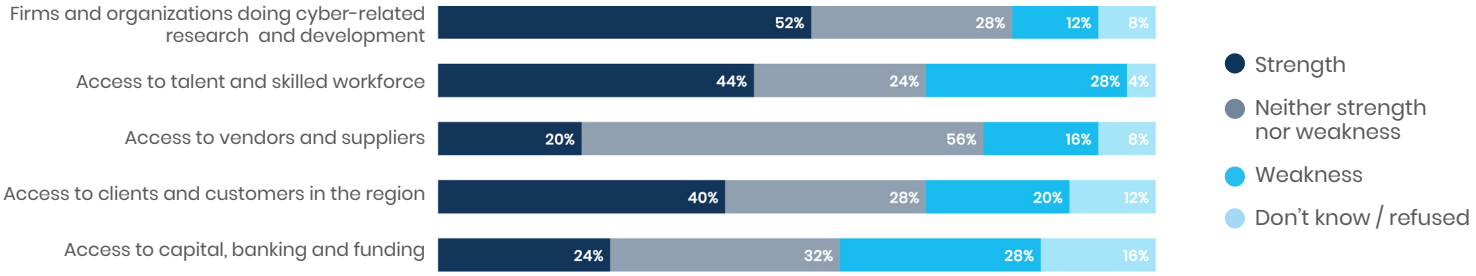
Expanding initiatives, such as supporting inclusive cybersecurity pathways, can play a critical role in broadening the cybersecurity talent pool.

BUSINESS OUTLOOK

The outlook on San Diego's cybersecurity business landscape presents a mix of optimism and ongoing challenges. Survey results show that **satisfaction is highest with the region's research and development capabilities, underscoring San Diego's strength in innovation and collaboration**. Access to talent follows closely behind, reflecting the effective role of local universities and community colleges in supplying cybersecurity professionals. However, more than a quarter of respondents expressed dissatisfaction with the regional talent pool, likely a reflection of the demand of a fast growing cluster. Respondents also viewed access to customers positively, driven by San Diego's diverse industry pool, where cybersecurity needs span sectors from defense and healthcare to biotech and finance. In contrast, access to capital and vendors was relatively less positive compared to other aspects of the region.

REGIONAL TALENT POOL SATISFACTION

Research and development satisfaction underscores the region's innovation and collaboration



The relatively lower satisfaction around access to vendors may reflect growing challenges tied to stricter cybersecurity compliance and procurement standards, particularly as **supply chain compromises** have become the second most common cause of breaches, per IBM. As organizations, government agencies, defense contractors, and education institutions adopt cybersecurity frameworks, many firms struggle to qualify as a vendor or subcontractor.

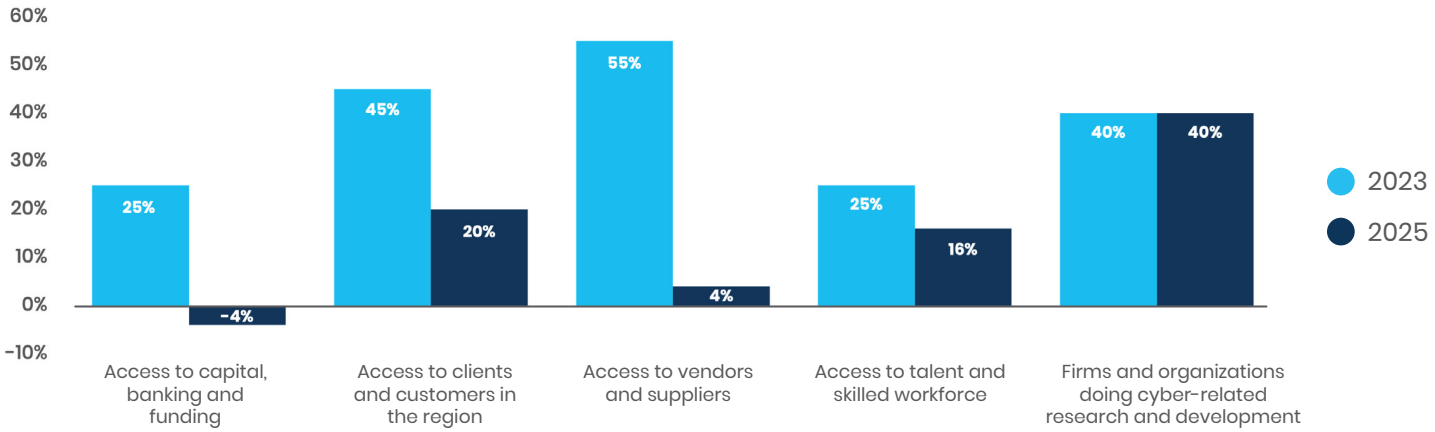
Executive interviewees mentioned that this barrier may be especially difficult for small businesses, which make up 99 percent of San Diego County's economy and often lack the resources to meet the standards. This issue is exacerbated when a business may be navigating business with multiple big buyers which all have different cyber standards. Moreover, meeting regulatory checklists, although important to have a framework, does not always equate to true cyber resilience. Helping small businesses navigate, achieve, and sustain compliance, while focusing on practical cybersecurity readiness, will continue to be critical to strengthening the region's supply chain.

> "Cyber compliance is essential but uneven. Larger organizations may have the resources to comply, while small businesses shoulder a disproportionate burden from varying client standards."
>
> Ricardo Fitipaldi, CISO
> San Diego State University

Overall Perceptions of San Diego's Business Environment

Compared to 2023, overall perceptions of San Diego's business environment have worsened, with several dimensions showing substantial declines. Looking at net rating—the difference between the share of respondents identifying a category as a regional strength versus a weakness—only research and development maintained its previous standing. All other dimensions, including access to talent, capital, and customers, were viewed less favorably than in 2023, suggesting that while the region's innovation engine remains strong, broader macroeconomic trends may have caused strain for cybersecurity firms in the region.

BUSINESS ENVIRONMENT PERCEPTIONS



This decline in sentiment may reflect broader uncertainty linked to federal policy and budgetary shifts that are affecting every industry, including cybersecurity. As a region with significant ties to the federal government due to the heavy military presence and research funding, San Diego is particularly sensitive to changes at the federal level, and unfortunately the cyber cluster is not immune. For example, the recent uncertainty surrounding the U.S. government's Common Vulnerabilities and Exposures program, a core database for tracking cybersecurity vulnerabilities, illustrated how even temporary ambiguity in federal priorities can create ripple effects across the cybersecurity ecosystem. These shifting dynamics may be contributing to a more cautious business outlook, even as the cluster continues to demonstrate strong innovation and growth.

> "While the policy landscape continues to shift, we're seeing organizations use this moment to strengthen their foundations, focusing on resilience, visibility, and readiness for what's next."
>
> Rob Johnson
> Vice President of Cybersecurity Sales, Thales

CONCLUSION

San Diego's cybersecurity cluster continues to stand as one of the region's most resilient industries, growing even as the broader technology industry contracts. **Now supporting a total of 29,000 jobs and contributing $4.3 billion to the regional economy**, the cluster's resilience underscores the importance of cybersecurity across every sector of the economy, especially due to the ever-increasing consequences of incurring a breach.

Despite strong growth, San Diego's cybersecurity cluster faces headwinds. Talent shortages remain a persistent issue, not due to a lack of local capability, but because of the accelerating pace of technological change and the nature of the rapidly evolving cyber field. Additionally, procurement standards and compliance continue to impose barriers, especially for small businesses that struggle to meet the various and complex cybersecurity requirements. At the same time, federal policy and budget shifts have created uncertainty among the general business community that even cyber cluster is susceptible to.

To ensure continued growth of the cybersecurity cluster, the San Diego region must lean on its collaborative ecosystem and regional assets. Continuing to develop and strengthen locally developed programs, initiatives, and networks can help the cyber cluster sustain its growth.

Now supporting a total of 29,000 jobs and contributing $4.3 billion to the regional economy

Research produced by

SAN DIEGO REGIONAL EDC

Title sponsor

THALES
Building a future we can all trust

Advisory sponsors

Deloitte.

eset

Small business sponsors

LEVITZACKS
CERTIFIED PUBLIC ACCOUNTANTS

NDIA
San Diego Chapter

In partnership with CCOE, the report was authored by San Diego Regional EDC in October 2025.

To learn more, visit sdccoe.org and sandiegobusiness.org/about-the-region.

ADVISORY COMMITTEE

Many Thanks to Our Industry Advisory Committee

Adam Bolio, Managing Director, Deloitte

Mark Compton, CISO, NAVWAR

Brendan Daly, CISO, City of San Diego

Ricardo Fitipaldi, CISO, SDSU

Ryan Grant, Country Manager, ESET

Andy Haass, Principal, Booz Allen Hamilton & CCOE Co-Chairman of the Board

Rob Johnson, Vice President of Sales, Thales

Vidya Murthy, COO, MedCrypt

Francisco Perez, CISO, San Diego Water Authority

Mansi Thakar, Staff Security Analyst, NVIDIA & Adjunct Professor, National University

Kris Virtue, Vice President, Qualcomm & CCOE Co-Chairman of the Board

APPENDIX

Local Organizations and Programs

Local organizations and programs are essential to sustaining the growth of the cyber cluster here in San Diego. The following support systems strengthen the region's cyber ecosystem:

CCOE: A San Diego-based nonprofit celebrating more than 10 years of mobilizing industry, academia, and government to grow the regional cyber economy and create a more secure digital community for all.

San Diego Cyber Clinic: CCOE, CSU San Marcos, National University, and San Diego State University established the San Diego Cyber Clinic, which provides free cybersecurity services across public and private sectors. The clinic offers students hands-on training, growing the skills needed for an increasingly demanding cybersecurity workforce.

San Diego Regional Cyber Lab: The Cyber Lab was created to increase cyber awareness throughout San Diego through access to tools and resources as well as a physical lab space—the cyber hub—where IT professionals can develop their cybersecurity skills with practice scenarios. Recently, AI chatbot **My eCISO** was developed to provide custom cybersecurity evaluations and helps users identify blind spots in their cyber security practices.

CyberHire: A collaborative effort between the San Diego Workforce Partnership, EDC, and CCOE, CyberHire is a program designed to address the region's growing demand for cybersecurity talent by providing cyber career pathways to individuals that typically face employment barriers. Partnering with trusted community organizations such as National Foundation for Autism Research, Able-Disabled Advocacy, and San Diego Futures Foundation, CyberHire delivers needed trainings, access to work-based learning opportunities, and matches individuals with local employers.

InfraGard: InfraGard is an FBI-affiliated nonprofit founded in 2005 with the goal to safeguard the region's critical infrastructure and people by reducing malicious activities by criminals and terrorists. Collaboration and communication between leaders from the private sector, government, academia, and first responders allows the region to quickly respond to threats to critical infrastructure.

APPENDIX

Local Organizations and Programs (cont.)

Professional development networks:

- **BSides:** BSides is a community information security conference that provide a space of education, collaboration, and debate, for IT security professionals.
- **CSA:** The Could Security Alliance (CSA) is an organization centered around the future of cloud cybersecurity, providing webinars, membership, skills, and tools to mitigate risks.
- **ISACA:** The San Diego chapter of the global Information Systems Audit and Control Association (ISACA) provides education, workshops, and regular meetings to elevate information security audit, control, and security in the region.
- **Information Systems Security Association (ISSA):** ISSA is a global organization that advances cybersecurity knowledge through educational forums, publications, and peer-interaction opportunities.
- **Open Worldwide Application Security Project (OWASP):** OWASP is one of the largest chapters worldwide, and provides monthly meetings and networking opportunities to promote a network dedicated to application security.

Peer groups:

- San Diego's Chief Information Security Officers Roundtable: Meeting quarterly, this group aims to share current threats, intel, and concerns within the San Diego cybersecurity ecosystem.
- Women in Cyber Security (WICyS) San Diego: WICyS is a global nonprofit, with a San Diego chapter, dedicated to recruiting, retaining, and advancing women in cybersecurity through professional development opportunities and by providing a support network.
- Raìces Cyber San Diego: Through mentorship, educational programs, and career development resources, Raìces aims to develop an inclusive workforce by focusing on underrepresented communities.
- DEFCON 858/619: San Diego's DEFCON chapter provides a gathering space for people interested in cybersecurity and technology to connect and share information.

METHODOLOGY

Cybersecurity Employment and Firms

Known Universe

BW Research, with assistance from San Diego Regional EDC and CCOE, created the known universe of the cybersecurity cluster, which refers to a set of companies that are known to be doing cybersecurity work in San Diego County. There were 183 firms identified in the known universe of the cybersecurity cluster and through surveys of those companies by BW Research, total employment was found to be 6,942.

Unknown universe

The unknown universe of the cybersecurity cluster refers to companies in San Diego County doing cybersecurity work but are not captured by the known universe. The unknown universe was identified by using four-digit North American Industrial Classification System (NAICS) codes:

NAICS	INDUSTRY
3342	Communications Equipment Manufacturing
3345	Navigational, Measuring, Electromedical, and Control Instruments Manufacturing
3366	Ship and Boat Building
4431	Electronics and Appliance Stores
5112	Software Publishers
5179	Other Telecommunications
5182	Data Processing, Hosting, and Related Services
5191	Other Information Services
5242	Agencies, Brokerages, and Other Insurance-Related Activities
5413	Architectural, Engineering, and Related Services
5414	Specialized Design Services
5415	Computer Systems Design and Related Services
5416	Management, Scientific, and Technical Consulting Services
5419	Other Professional, Scientific, and Technical Services
5615	Travel Arrangement and Reservation Services
5616	Investigation and Security Services
5619	Other Support Services
8112	Electronic and Precision Equipment Repair and Maintenance

METHODOLOGY

Cybersecurity Employment and Firms (cont.)

These NAICS codes were used because they were found to be employing a high concentration of cybersecurity-related occupations. These occupations were defined using **Standard Occupational Classification (SOC)** codes:

SOC CODES	OCCUPATION DESCRIPTION
11-3021	Computer and Information Systems Managers
15-1252	Software Developers
15-1211	Computer and Systems Analysts
15-1212	Information Systems Analysts
15-1231	Computer Network Support Specialists
15-1241	Computer Network Architects
15-1244	Network and Computer Systems Administrators
15-1299	Computer Occupations, all other

A random sample of unknown firms in San Diego County was generated using the four-digit NAICS codes above. Each business in the sample was surveyed by BW Research and a subset of the sample participated. Incidence of cybersecurity employment among participants were applied to firm and establishment totals which yielded 1,167 firms and 4,425 employees in the unknown universe of the cybersecurity cluster.

Naval Information Warfare Systems Command (NAVWAR)

NAVWAR's employment number was sourced directly from the organization itself. As of September 2025, there are a total of 3,508 cybersecurity workers at NAVWAR, with 3,232 being civilian and 276 being military personnel.

Economic Impact

The economic impact of the cybersecurity cluster on San Diego County's economy is estimated using software from **IMPLAN**. The software requires employment numbers portioned out by IMPLAN codes to estimate economic activity. IMPLAN codes are similar to NAICS codes but are not exactly the same. The following IMPLAN codes were used as a proxy for the four-digit NAICS codes:

NAICS	IMPLAN CODE AND DESCRIPTION
3342	302 - Broadcast and Wireless Communications Equipment Manufacturing
3345	312 - Search, Detection, and Navigation Instruments Manufacturing
3366	360 - Ship Building and Repairing

METHODOLOGY

Economic Impact (cont.)

NAICS	IMPLAN CODE AND DESCRIPTION
4431	404 - Retail: Electronics and Appliance Stores
5112	428 - Software Publishers
5179	435 - Satellite, Telecommunications Resellers, and All Other Telecommunications
5182	436 - Data Processing, Hosting, and Related Services
5191	438 - Internet Publishing and Broadcasting and Web Search Portals
5242	445 - Insurance Agencies, Brokerages, and Related Activities
5413	457 - Architectural, Engineering, and Related Services
5414	458 - Specialized Design Services
5415	460 - Computer Systems Design Services
5416	462 - Management Consulting Services
5419	468 - Marketing Research and All Other Miscellaneous Professional, Scientific, and Technical Services
5615	474 - Travel Arrangement and Reservation Services
5616	475 - Investigation and Security Services
5619	478 - Other Support Services
8112	514 - Electronic and Precision Equipment Repair and Maintenance
NAVWAR	545 - *Employment and Payroll of Federal Government, Military

The output includes cybersecurity-specific employment, labor income, value added, and output along with the direct, indirect, and induced effects in San Diego County:

Impact	Employment	Labor income	Value added	Output
Direct	14,875.28	$1,346,803,029.17	$2,575,174,121.68	$4,345,200,398.10
Indirect	7,448.42	$539,765,783.32	$835,126,667.26	$1,475,673,260.85
Induced	6,716.28	$429,648,821.23	$840,352,660.13	$1,281,922,156.91
Total	29,039.99	$2,316,217,633.73	$4,250,653,449.06	$7,102,795,815.87

Direct effects refer to the activity resulting directly from the cybersecurity cluster. Indirect effects refer to the business-to-business purchases (supply chain) that arise from the cybersecurity firms in the region. Induced effects refer to spending of labor income by the cybersecurity cluster and its supply chain on personal items such as healthcare or food. To learn more about direct, indirect, and induced effects, **click here**.

METHODOLOGY

Quantitative Survey

In addition to the surveys done to estimate employment for the known and unknown universe, BW Research conducted an anonymous quantitative survey of San Diego County cybersecurity companies. Firms had to pass screener questions to be surveyed (located in San Diego County and involved in cybersecurity or information security technology). This survey aimed to learn more about these firms and had questions revolving around the firm profile, employment, hiring, occupational profile, artificial intelligence/machine learning, and outlook on doing business in San Diego County. There was a total of 31 survey respondents (full and partial). The survey period was from July 15 through August 18, 2025.

Cybersecurity Talent Pool

The cybersecurity talent pool is a group of occupations that have skills that are desired by cyber employers. The SOC codes used in the unknown universe were used to define the talent pool. This group of occupations includes both cybersecurity and non-cybersecurity workers. Formulating the group this way allows analysis of the available talent, not just current workers who are in cybersecurity roles.

Data Gathering

Occupational, peer metros, job demand, demographic, and educational data were collected from **Lightcast**. Lightcast data is **sourced** from dozens of government and private sector sources, including but not limited to U.S. Census Bureau, Bureau of Labor Statistics (BLS), and National Center for Education Statistics (NCES).

Peer metros

The list of SOC codes that make up the cybersecurity talent pool was used to compare San Diego to its peer metros. The geographic boundaries used for the analysis are Metropolitan Statistical Areas (MSAs).

Nine metros were identified to investigate San Diego's cybersecurity cluster and how it compares to other markets across the United States. The metros were chosen based on four criteria (2024 data): employment, employment concentration, median annual earnings, and average monthly unique job postings. A database containing all MSAs across the U.S. was analyzed based on those four criteria. Metros that were top 25 among all MSAs across the U.S. in each criterion were identified as peer metros:

METHODOLOGY

Peer metros

New York-Newark-Jersey City, NY-NJ*
Washington-Arlington-Alexandria, DC-VA-MD-WV
Dallas-Fort Worth-Arlington, TX
San Francisco-Oakland-Fremont, CA
San Jose-Sunnyvale-Santa Clara, CA
Seattle-Tacoma-Bellevue, WA
Boston-Cambridge-Newton, MA-NH
Denver-Aurora-Centennial, CO
Baltimore-Columbia-Towson, MD

*New York ranked 38th in employment concentration. However, New York was included because the metro ranked first in employment and there was no other metro that ranked top 25 for every category.

Job demand

Job demand was measured using Lightcast's job posting analytics report, which uses their advanced scraping technology. The technology identifies sites that are a valid source of employment opportunities and scrapes that site for job postings and related information. Currently, more than 50,000 sites are scraped for postings by Lightcast. A deduplication process is used to identify unique job postings from total postings.

Cybersecurity-specific job postings were gathered from Lightcast's job posting analytics report by using keywords: "cybersecurity", "cyber security", "information technology security", and "IT security".

To find the non-cybersecurity job postings, another job analytics report was pulled using the list of SOC codes that make up the cybersecurity talent pool. The nature of the cybersecurity talent pool means that the job postings include both cybersecurity and non-cybersecurity postings. Subtracting out the number of cybersecurity-unique job postings from the report using keywords leaves the non-cybersecurity postings.

All job posting data is from January 2019 to August 2025.

To learn more about Lightcast's job posting analytics methodology, **click here**.

METHODOLOGY

Education pipeline

Educational data was collected from Lightcast using Classification of Instructional Program (CIP) codes developed by the U.S. Department of Education. A **SOC-CIP crosswalk** developed by NCES and BLS was used to obtain CIP codes that are related to cybersecurity. Using the SOC codes that define the cybersecurity talent pool resulted in the following CIP codes:

CIP CODE	TITLE
11.0101	Computer and Information Sciences, General
11.0102	Artificial Intelligence
11.0103	Information Technology
11.0104	Informatics
11.0201	Computer Programming/Programmer, General
11.0202	Computer Programming, Specific Applications
11.0203	Computer Programming, Vendor/Product Certification
11.0204	Computer Game Programming
11.0205	Computer Programming, Specific Platforms
11.0301	Data Processing and Data Processing Technology/Technician
11.0401	Information Science/Studies
11.0501	Computer Systems Analysis/Analyst
11.0701	Computer Science
11.0802	Data Modeling/Warehousing and Database Administration
11.0804	Modeling, Virtual Environments and Simulation
11.0901	Computer Systems Networking and Telecommunications
11.0902	Cloud Computing
11.1001	Network and System Administration/Administrator
11.1002	System, Networking, and LAN/WAN Management/Manager
11.1003	Computer and Information Systems Security/Auditing/Information Assurance
11.1005	Information Technology Project Management
11.1006	Computer Support Specialist
14.0901	Computer Engineering, General
14.0903	Computer Software Engineering
14.0999	Computer Engineering, Other
15.1204	Computer Software Technology/Technician
26.1103	Bioinformatics
26.1104	Computational Biology
30.0801	Mathematics and Computer Science
30.1601	Accounting and Computer Science

METHODOLOGY

Education pipeline (cont.)

CIP CODE	TITLE
30.3001	Computational Science
30.3101	Human Computer Interaction
30.3901	Economics and Computer Science
30.4801	Linguistics and Computer Science
30.7001	Data Science, General
40.0512	Cheminformatics/Chemistry Informatics
43.0403	Cyber/Computer Forensics and Counterterrorism
51.072	Healthcare Information Privacy Assurance and Security
51.2706	Medical Informatics
52.0205	Operations Management and Supervision
52.1201	Management Information Systems, General
52.1206	Information Resources Management
52.1207	Knowledge Management
52.1299	Management Information Systems and Services, Other
52.2101	Telecommunications Management