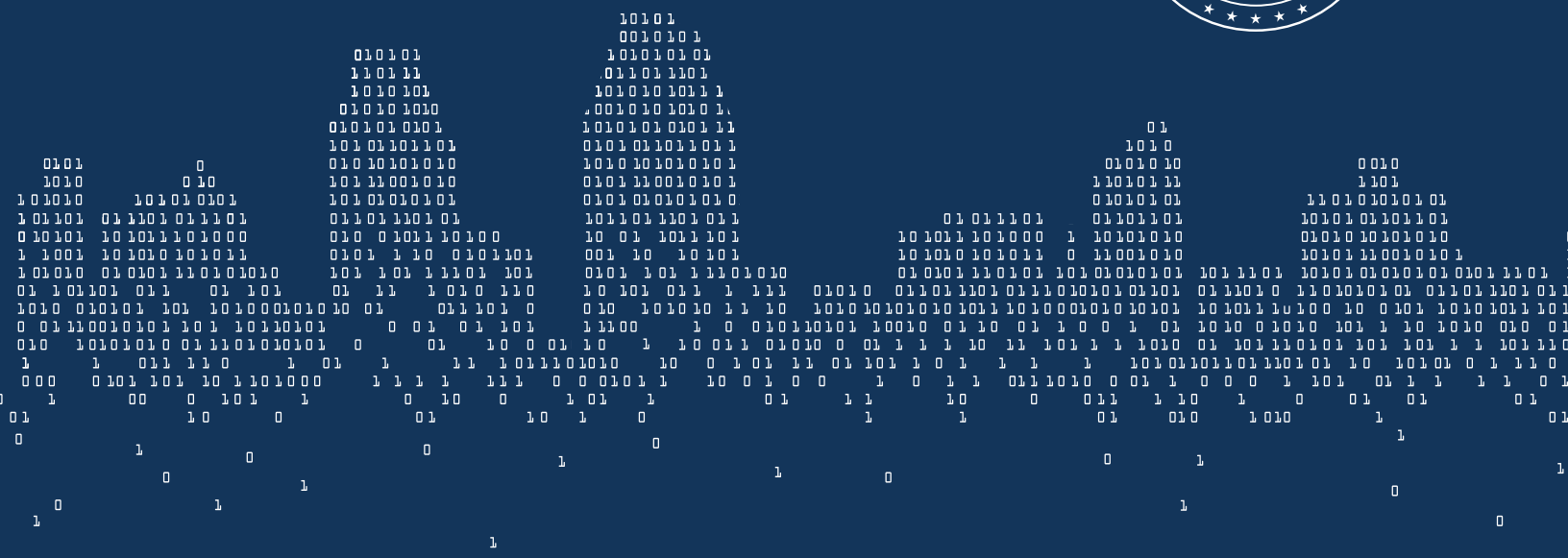
AN ECONOMIC IMPACT ANALYSIS
AND WORKFORCE STUDY

Accelerating the Cyber Innovation Economy
Cyber Center CCoE of Excellence



# SAN DIEGO'S CYBERSECURITY INDUSTRY

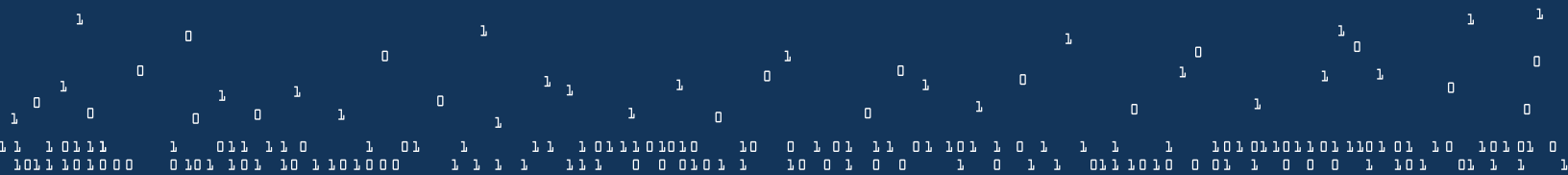
## Executive Summary

Sponsored by

Bank of America

eset

SENTEK GLOBAL



# *SAN DIEGO'S CYBER ECONOMY*

## A unique convergence of assets that exist nowhere else

**The San Diego region is ideally positioned to capitalize on the ever-growing global demand for cybersecurity products and services.**

### *A VIBRANT INNOVATION ECONOMY*

San Diego's entrepreneurial environment has fostered startups to multinational companies in cybersecurity, software development, information technology, communications and defense. The ecosystem includes incubators, financiers, experienced service providers and non-profits that support more than **100** firms focused exclusively on cybersecurity. In addition, the proximity of research and development facilities to Northern Mexico's manufacturing hubs allows for the development of quick-to-market products. Industry leaders, Qualcomm, ESET, ViaSat, iboss and Northrop Grumman are proud to call San Diego home.

### *EDUCATION AND RESEARCH*

San Diego's universities and colleges annually graduate **3,000** students in the computer science and engineering fields and recently launched two new cybersecurity masters programs at University of San Diego and California State University San Marcos. They also support cutting-edge research through resources like the Super Computing Center at UC San Diego and the Advanced Computing Environments Laboratory at San Diego State University. San Diego's universities annually receive **$1 billion** in philanthropic and federal funding for research and development projects.

### *DEPARTMENT OF DEFENSE PRESENCE*

San Diego is home to the Navy's Space & Naval Warfare Systems Command (SPAWAR). SPAWAR directly employs nearly half of all the cybersecurity jobs in San Diego **(3,400)** and its presence in San Diego is a huge contributing factor for many cyber companies to remain located in San Diego. SPAWAR's total budget in FY15 was $6.8 billion, with $5 billion (74%) going to private industry contracts, with the San Diego region receiving over **$1.1 billion**.

# BY THE NUMBERS

## RISING JOB GROWTH AND ECONOMIC IMPACT

**7,620**
Direct Jobs
14.7% increase*

**16,580**
Total Jobs Impacted
25% increase*

**4,230**
Direct Private Sector Jobs
19.2% increase*

**3,390**
Direct SPAWAR Jobs
9.5% increase*

**13%**
Projected Cyber Employment Growth
in the next 12 months compared to 2% overall regional job growth

**$1.9 BILLION**
Total Economic Impact
26.4% increase*

*Impact is greater than hosting 4 Super Bowls or 14 Comic-Cons each year.*

*Since 2014 EDC San Diego Cybersecurity Economic Impact Study

## DIVERSE CONSUMERS

*43%*
National

*37%*
International

*47%*
Exclusively Commercial

*13%*
Exclusively Federal Government

*40%*
Work with Both

**Access to clients, customers, vendors and suppliers are seen as San Diego's greatest strengths among cyber employers.**

# SAN DIEGO'S TECHNOLOGY WORKFORCE

## ROBUST TALENT POOL

**51,000** technology specialists in San Diego

- Developers/Programmers 21,600
- Support 9,340
- Managers 9,120
- Analysts/Researchers 7,830
- Network Specialists 3,150

## CYBER PAYS

**50% HIGHER PAY**

than the average occupation for network support specialist jobs averaging $75,000/year, which generally do not require a bachelor's degree

**$116,000**

average annual salary for analysts, computer scientists and software developers

## AND THE TALENT DEMAND KEEPS GROWING…

**18.8%** tech professionals growth

from 2011-2015 – 3x the average occupation in San Diego

**Network Architects and Research/Security Analysts were among the fastest growing subsets.**

*Produced by* Cyber Center CCoE of Excellence

*Research by* CBRE, San Diego Regional EDC, [bw] Research Partnership

www.sdccoe.org
info@sdccoe.org
@sdccoe

# *ACKNOWLEDGMENTS*


## STUDY ADVISORS

| | |
|---|---|
| **SHIRLEY ADAMS** | CyberTECH |
| **ERIC BASU** | Sentek Global |
| **RICK BELLIOTTI** | San Diego Regional Airport Authority |
| **TREVOR BOHN** | Salem Partners |
| **TOM CLANCY** | Tao Ventures |
| **LIZ FRAUMANN** | Securing Our e-City |
| **GREG GEISEN** | SPAWAR |
| **MATT GRIESBACH** | Bank of America |
| **GARY HAYSLIP** | City of San Diego |
| **PETER MARTINI** | iboss |
| **CHAD NELLEY** | ESET North America |
| **BRUCE ROBERTS** | Cyber Security Institute of San Diego |

## COMMISSIONERS

| | |
|---|---|
| **LISA EASTERLY** | San Diego Cyber Center of Excellence |
| **RADM (RET) KENNETH SLAGHT** | San Diego Cyber Center of Excellence |

## AUTHORS/RESEARCHERS

| | |
|---|---|
| **MICHAEL COMBS** | CBRE |
| **JESSE GIPE** | San Diego Regional EDC |
| **JOSH WILLIAMS** | BW Research |
| **RYAN YOUNG** | BW Research |

## SPONSORED BY

**BANK OF AMERICA**
**ESET**
**SENTEK GLOBAL**

## RESEARCH BY

**CBRE**
**SAN DIEGO REGIONAL EDC**
**BW RESEARCH**

## DESIGN BY

**DISENO COMMUNICATIONS**

## PRODUCED BY

**SAN DIEGO CYBER CENTER OF EXCELLENCE**

# *TABLE OF CONTENTS*

# *INTRODUCTION*

As global connectivity continues to rise, so does the cost and complexity of securing personal, enterprise and government data. According to research and advisory company Cybersecurity Ventures, global spending on cybersecurity reached $77 billion in 2015, and is expected to reach $170 billion by 2020[1]. McAfee estimated that the cost of cyber crime annually was projected to be between $375 and $575 billion[2]. In more recent reports, including one from Juniper Research, the estimated global impact of cyber crime is projected to reach over $2 trillion by 2019[3]. The rising diversity and sophistication of cyber criminals across the world juxtaposed against the explosion in connected devices has created a rapidly growing market that is ripe for innovation.

President Barack Obama rolled out his administration's Cybersecurity National Action Plan in February 2016[4]. Included in that plan is the recommendation for the establishment of a $3.1 billion Information Modernization Fund and increased investment in cybersecurity. In total, over $19 billion for cybersecurity was included in the President's fiscal year (FY) 2017 budget[5]. This represents a more than 35 percent increase from FY 2016 in overall federal resources for cybersecurity, a necessary investment to secure the nation in the future.

In San Diego, the economy is driven by major high tech industries, such as the military and defense, telecommunications, genomics and biotech. The stakes are high for companies in these industries that handle incredibly sensitive data. In particular, those working on matters of national security in the region have fostered the growth of a diverse cybersecurity talent base. With industry, government and education working together under the leadership of San Diego's Cyber Center of Excellence (CCOE) and other leading organizations in the region, San Diego is ideally positioned to capitalize on the ever-growing global demand for cybersecurity products and services.

## OBJECTIVES

The goal of this study is to provide the data, analysis and recommendations to policymakers, educational institutions, businesses, talent and key non-profits that will enable them to foster the growth of this rapidly evolving industry. To achieve this goal, this study focuses on five key objectives:

- **Define the role of cybersecurity in the tech ecosystem**: Because cybersecurity is so pervasive in nature, this study defines and quantifies the industry's role in the broader information and communication technologies (ICT) ecosystem.
- **Quantify the economic impact**: With the use of impact modeling software (IMPLAN), this study analyzes the broader indirect and induced impacts of cybersecurity on jobs, wages and gross domestic product (GDP) in San Diego.

1 http://cybersecurityventures.com/cybersecurity-market-report/
2 http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf
3 http://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion
4 https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan
5 https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

- **Understand employer sentiment**: Through surveys and interviews, this study provides perspective on the advantages and challenges facing cybersecurity businesses in San Diego.
- **Analyze growth and changes since 2014**: This study updates the baseline indicators—employment, economic impacts, employer attitudes, etc.—and forms comparisons on the progress made in the industry in the San Diego region since 2014.
- **Dive deeper into workforce needs**: This study more deeply analyzes the workforce and talent challenges identified by employers in 2014 to more precisely identify the skills and certifications needed by employers.

## 2014 STUDY

In 2014, researchers from National University System Institute for Policy Research (NUSIPR), BW Research, San Diego Association of Governments (SANDAG) and San Diego Regional EDC worked with leaders from industry, government and education to publish an economic impact analysis of the region's cybersecurity ecosystem[6]. That study was the first of its kind in the San Diego region.

The inaugural cybersecurity study in San Diego set many key baseline facts and figures for understanding the impacts, advantages and challenges facing San Diego's cybersecurity industry. The research showed that San Diego's cyber economy was strong and growing. Key facts included:

- More than 100 cybersecurity firms in San Diego employed more than 3,500 private sector employees;
- SPAWAR's cyber employment was over 3,000 people;
- Cybersecurity activities in San Diego generated an economic impact of $1.5 billion—the equivalent of hosting more than three Super Bowls;
- Cybersecurity firms expected to grow by 13 percent in the following year.

Despite the many positive findings in the study, employers reported concerns over the ability to find the talent to accommodate their aggressive growth expectations. The San Diego Cyber Center of Excellence (CCOE), a non-profit organization formed to accelerate job and economic growth in the cyber community, took this challenge to task. This organization is driven by a collection of world-class cyber companies who have headquarters or operations in San Diego. Industry leaders including SPAWAR, Qualcomm, FICO, ESET, Sentek Global, Lockton Insurance, Morrison Foerster and San Diego Regional EDC are a few of the founding participants. Under the leadership of CCOE, this 2016 version of the study has dug deeper into those challenges facing cybersecurity employers, with the goal of leveraging the information to improve the workforce pipeline for cybersecurity employers.

## SURVEY NOTE

Many of the findings of this study are based on a survey universe of core cyber firms and additional technology and consulting firms with a possible cyber component in the San Diego region. The results of this survey will be referenced throughout the study. Full survey methods and toplines can be found in the appendix of the study.

6 http://www.sandiegobusiness.org/sites/default/files/Cyber%20Security%20Final%20Report.pdf

# 1 | CYBERSECURITY IN THE TECH ECOSYSTEM

## KEY TAKEAWAYS

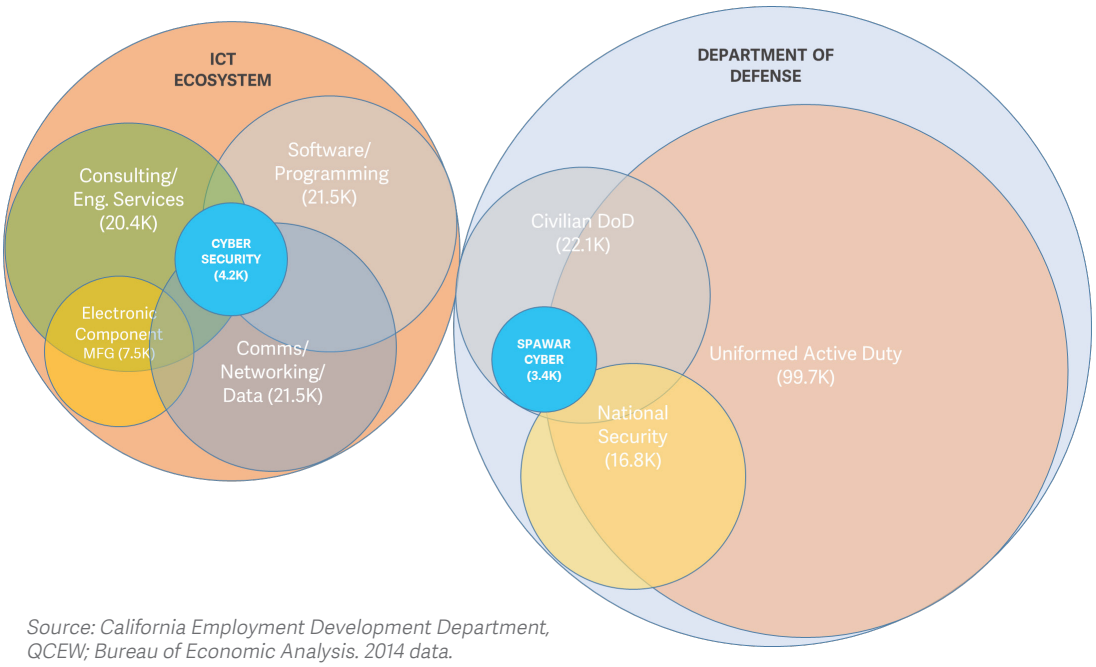
San Diego has more than **104 core cyber firms that employ 4,230 people** in the region and **SPAWAR adds an additional 3,390 employees** to San Diego's cybersecurity industry.

In total, there were **7,620 total jobs** in the known cyber universe, **up 14.7 percent from 2014**.

When including **estimated cybersecurity employment in other tech sectors** beyond the known universe, San Diego is home to approximately **10,420 cybersecurity employees**.

As a relatively new industry, cybersecurity is not cleanly captured in industry classification codes (e.g. NAICS) and other methods typically used to measure the size of a particular industry. Furthermore, cybersecurity permeates many of the region's tech firms and DoD assets. To measure the region's cybersecurity size and impact, this study used the industry definition developed in 2014 to account for the known firms in the San Diego region through a census.[1] When possible, this study mirrored the methods of the 2014 Cybersecurity in San Diego study in order to draw comparisons.

**FIGURE 1.1: CYBERSECURITY WITHIN THE ICT & DEFENSE ECOSYSTEMS**




*Source: California Employment Development Department, QCEW; Bureau of Economic Analysis. 2014 data.*

1 See methodology for more information on the census process.

**DEFINITION** | **Core cyber firms are**: (1) Firms and organizations that provide products and services designed to enhance and protect computers, networks, programs and data from unintended or unauthorized access or destruction; (2) Firms and organizations that sell their products and services to customers external to the immediate organization; (3) The firms may be exclusively focused on cybersecurity or that function may be one business line that they offer.[2]

As shown in figure 1.1, producers of cybersecurity products and services can be challenging to delineate from other companies and organizations within the defense and information and communication technologies (ICT) clusters, even once a definition has been established. To do so, researchers began establishing a census through assembling a database of known cybersecurity firms in the region. This was the same methodology employed in 2014, which provided researchers with a starting point. A full methodology for the census can be found in the appendix.

## PRIVATE

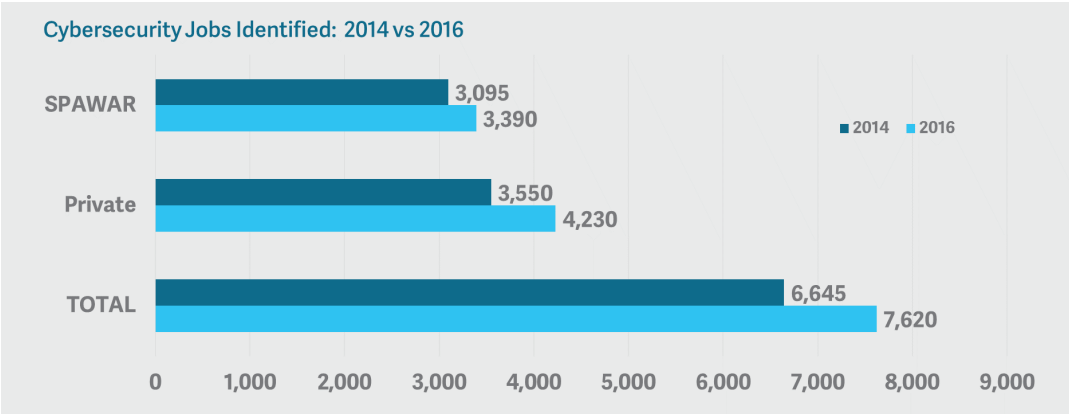
Through the census process, this study identified **104 core cyber firms**, meaning those that fit the definition outlined above. These companies were confirmed through phone calls, e-mails, internet database searches and other methods. These methods also helped confirm or estimate employment counts for these businesses. Through this process, **4,230 employees** were identified within cybersecurity firms or divisions. This includes all employees that work in cybersecurity operations (e.g. sales and management), not just cybersecurity occupations (e.g. analysts and developers). Although the total number of cybersecurity firms grew by less than 5 percent since 2014, private employment count was **19.2 percent higher** than identified in 2014.

## SPAWAR

SPAWAR—the US Navy's Space and Naval Warfare Command—is also a critical component of the region's cybersecurity economy. Through interviews with officials within the agency, this study determined how many employees were specifically dedicated to cybersecurity operations at SPAWAR. In 2016, this figure was reported as **3,390, up 9.5 percent from 2014**.

In total, there were **7,620 total jobs in the known cyber universe, up 14.7 percent from 2014**.

**FIGURE 1.2: CYBERSECURITY JOBS**



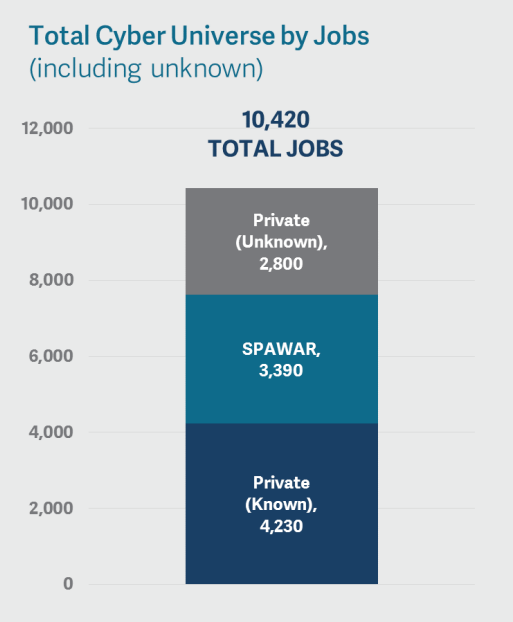

*Source: BW Research; With data from ReferenceUSA*

2 Definition developed by National University System Institute for Policy Research, San Diego Regional EDC and BW Research as part of the 2014 study.

## ESTIMATED UNKNOWN EMPLOYMENT

Despite the intense efforts to identify every cybersecurity employee in the San Diego region, there will inevitably be many cybersecurity operations that are within a company or division that are too small, new or unknown to identify. This study estimated this employment figure by sampling firms within the most common technology and technical consulting-based sectors and estimated that **an additional 549 technology firms employ approximately 2,800 people in cybersecurity occupations or support roles**. Because this figure was not estimated in the 2014 study, this study did not include these figures in the comparative counts of the known cyber universe; however, this estimate demonstrates how pervasive cybersecurity has become in the technology ecosystem when aggregated.

**FIGURE 1.3: TOTAL JOBS IN CYBERSECURITY**




*Source: BW Research*

# 2 | THE ECONOMIC IMPACT OF CYBERSECURITY

## KEY TAKEAWAYS

When accounting for the total **direct**, **indirect** and **induced** impacts, cybersecurity activities **generate more than $1.9 billion in GDP** and **impact 16,580 jobs every year**.

The **total economic impact** of the known cybersecurity universe was roughly the equivalent of **hosting four Super Bowls** or **14 Comic-Cons every year**.

The **private sector impact on GDP increased 41.2 percent** from 2014 to 2016.

If adding in the estimates of the unknown universe, the cybersecurity industry impacts **nearly 22,000 jobs** and **$2.4 billion in GDP** in the region.

To assess the full impacts of cybersecurity on the San Diego region's economy, this study ran the findings from Part 1 through an input/output model known as IMPLAN. This modeling software estimates the effect of cybersecurity employment on the supply chain (indirect), as well as the jobs and impacts generated through increased spending throughout the economy (induced).

## VALUE ADDED (GDP)

Cybersecurity activities generate a significant economic impact on the region's economy. Direct activities in the known cybersecurity universe generated roughly $1 billion in gross domestic product (GDP) in the region in 2016. When accounting for the indirect and induced impacts, cybersecurity activities generated more than $1.9 billion in GDP. The total economic impact of cybersecurity is roughly the equivalent of hosting four Super Bowls[1] or 14 Comic-Cons every year[2].

As the size of the industry has grown, so has its economic impact on the region's economy. The total economic impact of cybersecurity on GDP in 2016 was 26.4 percent higher than in 2014. The private sector increased 41.2 percent over that period and now impacts more than $1.1 billion of the region's GDP.

**FIGURE 2.1: ECONOMIC IMPACT OF KNOWN CYBER UNIVERSE**

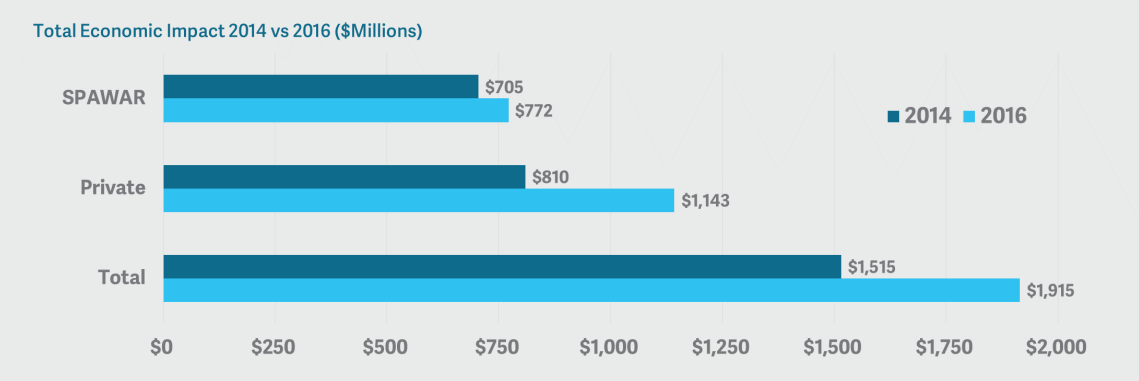
| IMPACT TYPE | EMPLOYMENT | VALUE ADDED ($MILLIONS) |
|---|---|---|
| **PRIVATE SECTOR** | | |
| DIRECT EFFECT | 4,230 | $625.5 |
| INDIRECT/INDUCED | 5,570 | $517.2 |
| **TOTAL EFFECT** | **9,800** | **$1,142.7** |
| MULTIPLIER | 2.3 | 1.8 |
| **SPAWAR** | | |
| DIRECT EFFECT | 3,390 | $479.5 |
| INDIRECT/INDUCED | 3,390 | $292.5 |
| **TOTAL EFFECT** | **6,780** | **$772.0** |
| MULTIPLIER | 2.0 | 1.6 |
| **TOTAL** | | |
| DIRECT EFFECT | 7,620 | $1,105.0 |
| INDIRECT/INDUCED | 8,960 | $809.7 |
| **TOTAL EFFECT** | **16,580** | **$1,914.7** |
| MULTIPLIER | 2.2 | 1.7 |

*Source: CBRE; BW Research; IMPLAN Group*

1 Lisa Halverstadt, "Tourism Boosters Are Expecting Less Money from Comic-Con." Voice of San Diego, June 30, 2015. http://www.voiceofsandiego.org/topics/economy/tourism-boosters-are-expectingless-money-from-comic-con/

2 http://blog.gbta.org/2016/01/29/the-super-bowl-winner-the-host-city/

**FIGURE 2.2: ECONOMIC IMPACT**




*Source: CBRE; BW Research; IMPLAN Group*

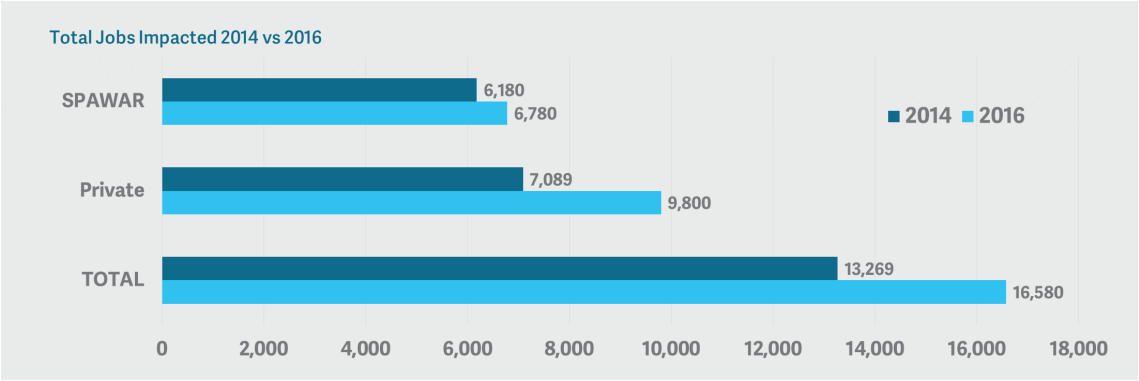
## JOBS

This study estimated that 16,580 total jobs were impacted by the known cybersecurity universe in 2016. The private sector alone impacted 9,800 jobs and cybersecurity activities at SPAWAR impacted an additional 6,780 jobs.

On average, every 100 jobs created in cybersecurity yielded 220 jobs throughout the economy. Many of these jobs paid above average wages. The average job generated through indirect or induced impacts paid about $58,000. The average direct cybersecurity job generated approximately $102,000 in labor income. Overall, the average job impacted by cybersecurity paid about $75,000, creating significant value for the region.

The private sector showed the most growth. Private sector impact on jobs grew by 38.2 percent from 2014 to 2016. SPAWAR's impact on jobs also rose 9.7 percent. In total, the number of jobs impacted by known cybersecurity activities was 25.0 percent higher in 2016 than in 2014.

**FIGURE 2.3: JOBS IMPACT**




*Source: CBRE; BW Research; IMPLAN Group*

## ESTIMATED ADDITIONAL IMPACTS

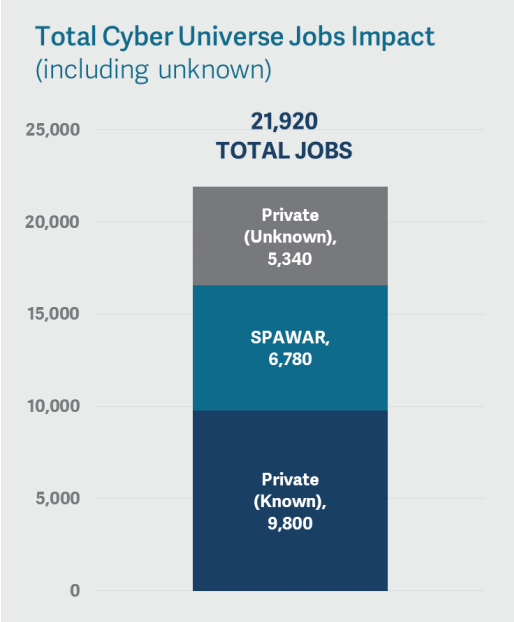
As detailed on page 6, this study also estimated the cybersecurity activities in technology and consulting beyond the known cyber universe used for the census. These activities impact an additional estimated 5,340 jobs and $459 million in GDP. When added to the known universe, this study estimates that the cybersecurity industry impacts nearly 22,000 jobs and $2.4 billion in GDP in the region.

### FIGURE 2.4: ECONOMIC IMPACT OF ESTIMATED CYBER EMPLOYMENT IN TECH

| IMPACT TYPE | EMPLOYMENT | VALUE ADDED ($MILLIONS) |
|---|---|---|
| **ESTIMATED TECH** | | |
| DIRECT EFFECT | 2,800 | $245.3 |
| INDIRECT/INDUCED | 2,540 | $213.8 |
| **TOTAL EFFECT** | **5,340** | **$459.1** |
| MULTIPLIER | 1.9 | 1.9 |

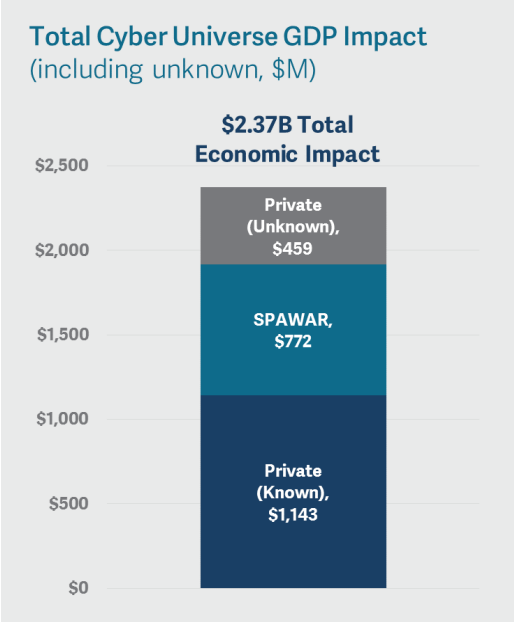
*Source: CBRE; BW Research; IMPLAN Group*

### FIGURE 2.5: TOTAL JOBS IMPACTED




*Source: CBRE; BW Research; IMPLAN Group*

### FIGURE 2.6: TOTAL GDP IMPACTED




*Source: CBRE; BW Research; IMPLAN Group*

# 3 | *TALENT AND WORKFORCE*

## KEY TAKEAWAYS

As of 2015, there were approximately **51,000 technology specialists** in San Diego, working in **a variety of cybersecurity-relevant occupations**.

**Information security analysts grew by 13.9 percent** per year on average from 2013 to 2015 in San Diego—**nearly double the 7.0 percent national average**.

Employers expect their **cybersecurity workforce to grow by 13 percent** in the next year, but concerns over the **ability to acquire skilled talent** may present obstacles.

Talent and workforce are undoubtedly major drivers of any technical industry, especially an industry like cybersecurity, where specialized skills, certifications and security clearances are often required. The Department of Homeland Security's (DHS) National Initiative for Cybersecurity Careers and Studies (NICCS)[1] as well as the National Institute of Standards and Technology's (NIST) National Initiative for Cyber Education (NICE) programs outline many of these skills and certifications needed to be effective in the cybersecurity industry.[2]

As the industry grows, regions aligned to address these workforce challenges will be imperative. According to a report from Peninsula Press that is based on data from Burning Glass and the Bureau of Labor Statistics, cybersecurity jobs grew by 112 percent in San Diego from 2007 to 2013—one of the highest in the US. Burning Glass estimates that cyber jobs grew 3.5 times faster than other IT professions and 12 times faster than overall job growth. The Peninsula Press report also anticipated that cyber professions will grow by 53 percent from 2014 to 2018.

There is a global shortage in tech talent and the need within cybersecurity is even more acute. This is compounded by the fact that employees working with or in the Department of Defense are under increased scrutiny to access security clearances. These restrictions limit the extent to which foreign labor—an important pipeline of talent for other tech sectors—can work within the industry. As demand in the commercial market continues to grow, the ability for a more diverse foreign labor force will evolve; however, there major demand will remain from entities like SPAWAR and other defense contractors in the region that are reliant on US talent to meet their workforce needs.

## EXISTING WORKFORCE

San Diego is well positioned to take advantage of this expected growth, not only because of its premier educational institutions, existing industry base and robust federal assets, but because

1 https://niccs.us-cert.gov/training/national-cybersecurity-workforce-framework
2 http://csrc.nist.gov/nice/workforce.html

it has an existing workforce that is ready or adaptable with training for the needs of cybersecurity employers. As of 2015, there are approximately 51,000 technology specialists in San Diego working in a variety of relevant occupations, such as computer programmers, network architects, information security analysts, and operational research analysts.

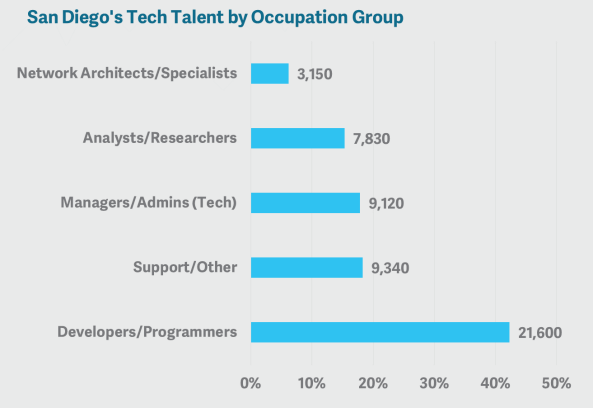
Figure 3.1 illustrates how San Diego's tech talent pool breaks down by occupation group. San Diego's strength is most notably in computer programmers and applications, systems and web developers, who make up more than 40 percent of the tech talent pool.

These jobs tend to pay much higher than average wages. Analysts, computer scientists and software developers on average make $116,000 per year in the San Diego region. Even network support specialists, which often require less than a bachelor's degree, make $75,000 per year on average in the region, which is roughly 50 percent higher than the average job.[3]

## TALENT GROWTH

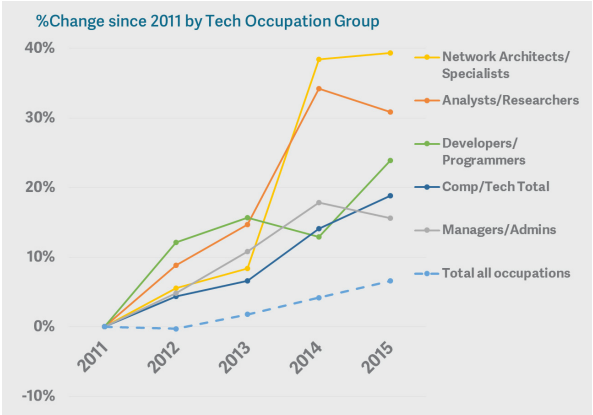
While developers and programmers are the largest occupation group, network architects/specialists and analysts/researchers are the fastest growing in San Diego. From 2011 to 2015, network architects/specialists grew by 9.8 percent annually on average and analysts/researchers grew by 7.7 percent over that same period. Meanwhile, total tech talent grew by 4.7 percent and the overall employment in the region by 1.6 percent.

**FIGURE 3.1: TALENT BREAKDOWN - SAN DIEGO**



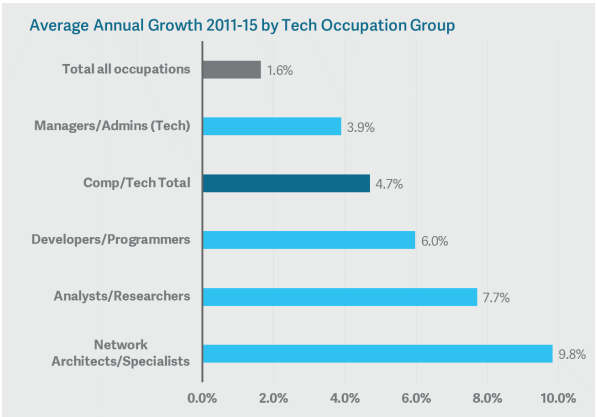

*Source: CBRE; BLS OES, 2015*

**FIGURE 3.2: TALENT GROWTH - SAN DIEGO**




*Source: CBRE; BLS OES, 2015*

**FIGURE 3.3: AVG. ANNUAL GROWTH - SAN DIEGO**




*Source: CBRE; BLS OES, 2015*

3 Bureau of Labor Statistics, Occupation Employment Statistics, 2015

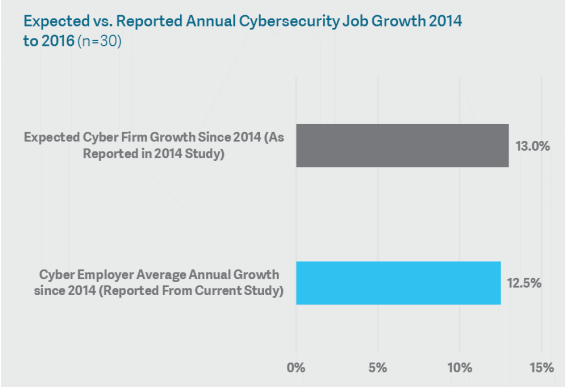
The most notable occupations among these two groups are information security analysts, operations research analysts and computer network architects—three occupations closely related to the cybersecurity industry.

Information security analysts grew by 13.9 percent per year on average from 2013 to 2015 in San Diego—nearly double the national average of 7.0 percent. The occupation only began being tracked in 2013 as the cybersecurity industry grew. According to the Bureau of Labor Statistics' (BLS) Occupational Outlook Handbook, "Information security analysts plan and carry out security measures to protect an organization's computer networks and systems. Their responsibilities are continually expanding as the number of cyberattacks increases."[4] Their expected job outlook nationally through 2024 is 2.5 times the average occupation, and the BLS predicts that demand for this occupation will remain high as the costs of security breaches increase.

Operations research analyst is a rapidly growing occupation both locally and nationally. The occupation grew by 15.8 percent per year from 2011 to 2015 in San Diego, nearly 10 times the rate of average job growth. Operations research analysts focus on complex statistical and analytical methods in a wide variety of contexts and they are often hired by the Department of Defense.[5]

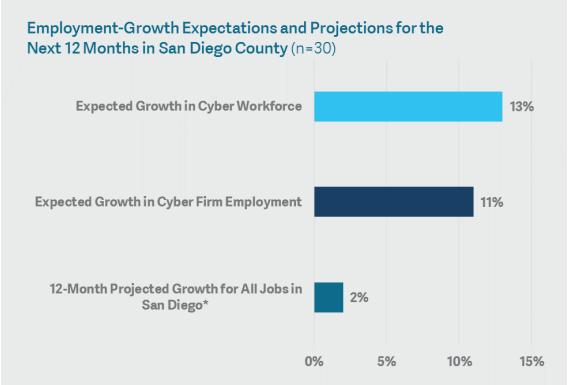
Computer network architects are most relevant for cybersecurity service providers or firms with an in-house networking professional or CTO. They are responsible for setting up networks and more recently essential in developing and securing cloud computing networks.[6]

**FIGURE 3.4: GROWTH SINCE 2014 STUDY**



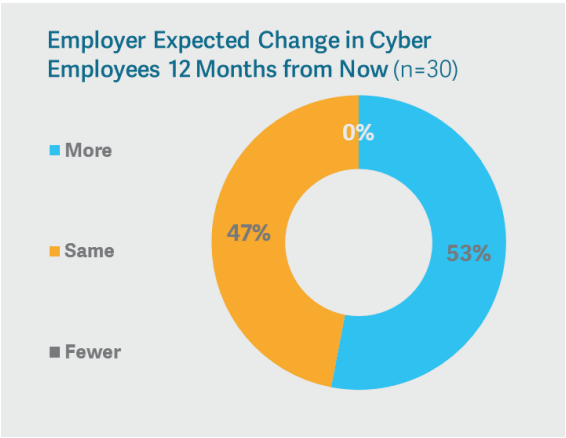

*Source: BW Research; NUSIPR*

**FIGURE 3.5: CYBER-EMPLOYER PROJECTED GROWTH**




*Source: BW Research; *CBRE Econometric Advisors*

**FIGURE 3.6: CYBER-EMPLOYER EXPECTED CHANGE**




*Source: BW Research*

4 http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
5 http://www.bls.gov/ooh/math/operations-research-analysts.htm#tab-1
6 http://www.bls.gov/ooh/math/operations-research-analysts.htm#tab-1

## EMPLOYER-REPORTED GROWTH

In 2014, cybersecurity employers reported that they expected to grow 13.0 percent over the next 12 months. When asked how much cybersecurity firms have grown since that period, employers reported an average growth rate of 12.5 percent employment growth per year, roughly at the expected target in 2014.

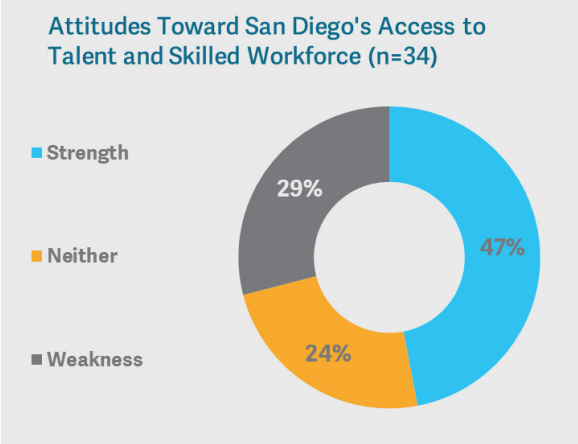
In 2016, employers expect that growth rate to slow, but only slightly to 11 percent. Approximately 53 percent of cybersecurity employers said they expect to grow within the next 12 months, while no employers reported that they expected to downsize. When asked specifically about their cyber workforce, meaning those skilled professionals in cybersecurity occupations, employers expected 13 percent growth. CBRE Econometric Advisors, an independent research firm owned by CBRE, projects employment to grow at about 2 percent over the next 12 months. Therefore, cybersecurity firms and particularly cybersecurity professionals are expected to vastly exceed overall employment growth.

## POTENTIAL OBSTACLES TO GROWTH

While firms were generally optimistic about their growth expectations, one potentially limiting factor will be access to a pipeline of skilled professionals. In 2014, employers reported this as a potential challenge for growth and there were concerns over access to talent. In 2016, those sentiments remained on employers' minds.

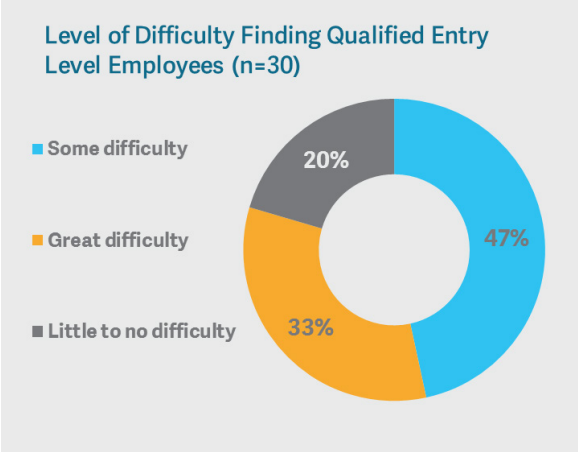
Employers did not overwhelmingly report that talent access was a weakness in San Diego, but just under half of cybersecurity employers reported that it was a strength in the region. There was little difference as to whether or not the positions were entry-level

**FIGURE 3.7: EMPLOYER ATTITUDES**



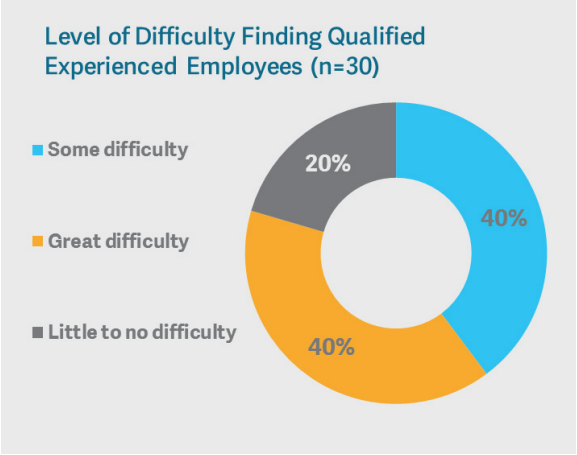

*Source: BW Research*

**FIGURE 3.8: ENTRY LEVEL DIFFICULTY**




*Source: BW Research*

**FIGURE 3.9: EXPERIENCED TALENT DIFFICULTY**



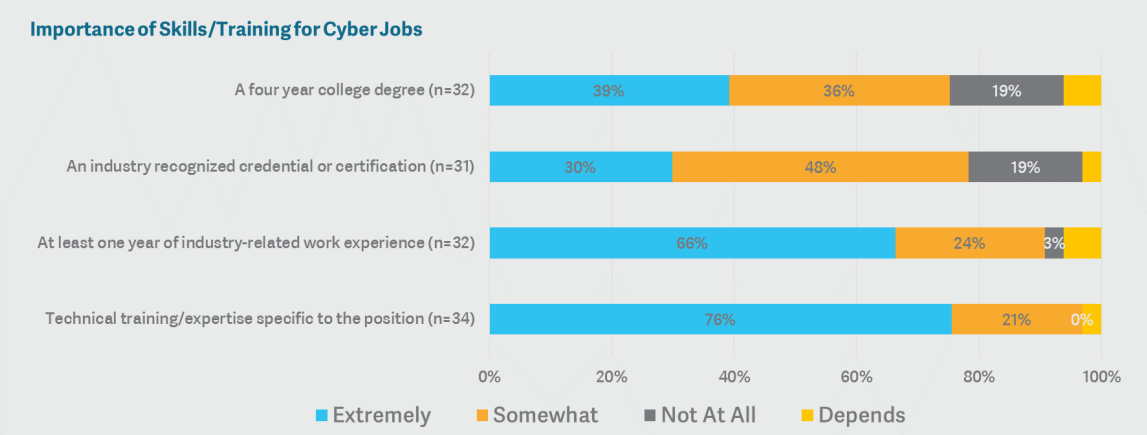

*Source: BW Research*

or experienced. Both questions yielded responses of 80 percent of businesses saying they have had great or some difficulty hiring qualified cybersecurity employees. Employers were more likely to respond that they had "great difficulty" finding qualified experienced employees, but overall the difficulty was roughly the same. Only 20 percent of employers reported little to no difficulty.

Though finding qualified professionals remains a problem for San Diego employers, the problem is global. A 2014 Cisco Annual Security Report estimated the worldwide shortage of information security professionals was at 1 million openings.[7] An analysis by the Peninsula Press and Burning Glass found that more than 209,000 cybersecurity jobs in the US were unfilled as of March 2015.[8]

San Diego has the opportunity to become a leader in educating and training a cyber workforce that will fill the needs of employers. Figures 3.10 and 3.11 highlight the skills and certifications most desired by cybersecurity employers in the San Diego region. While there is clearly a role for a structured four-year university education, experience and technical training are the most important skills for cybersecurity employers. In terms of specific certifications, they range depending on the specific type of employer, though the most common certifications are CCNP, CCNA, ISC2 and Security+.

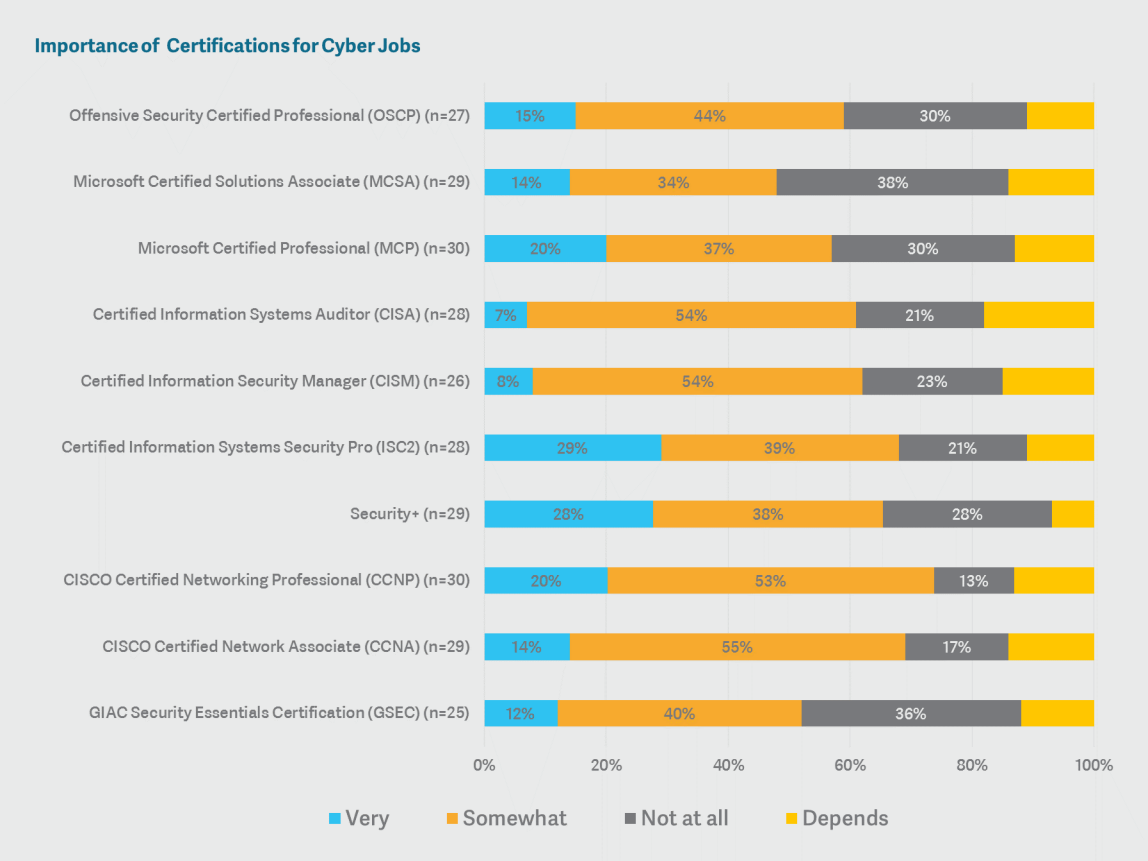
**FIGURE 3.10: IMPORTANCE OF SKILLS**




*Source: BW Research*

7 http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
8 http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/

**FIGURE 3.11: CERTIFICATIONS**




*Source: BW Research*

# 4 | EMPLOYER PROFILE AND FEEDBACK

## KEY TAKEAWAYS

Of the companies surveyed, **43 percent** responded that they have **a national customer base**, while **37 percent** said they have **an international base**.

The industry has moved **toward more private sector customers**, as the share of firms who **focus primarily on the private sector has grown** substantially to **47 percent**.

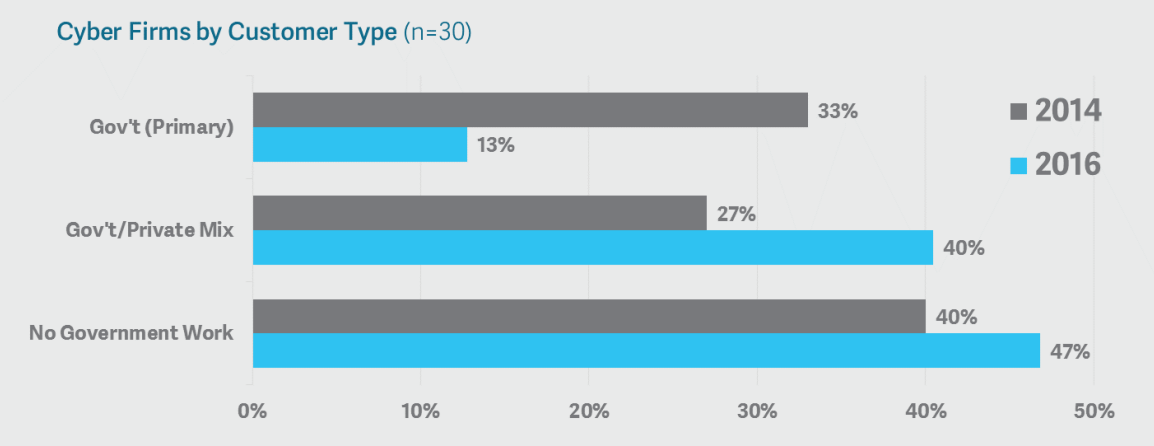
**Access to clients**, **customers**, **vendors** and **suppliers** are seen as San Diego's **greatest strengths** among cyber employers.

To understand the nuances of the cybersecurity industry in San Diego, BW Research conducted telephone and web surveys of core cybersecurity firms and industries with a high concentration of cyber employment in San Diego County. BW's efforts resulted in participation from more than 100 firms who provided answers to questions about the size and nature of their business, the role of cybersecurity, their customers and their sentiments about doing business in San Diego.

## EVOLVING CUSTOMER BASE

Cybersecurity employers in San Diego work with a broad base of customers and provide a diverse mix of services and products. In 2014, survey respondents were more exclusively focused on government contracting as their primary line of business; 33 percent said government was their primary customer, compared to only 13 percent in 2016. Respondents were far more likely to report a mix of consumers between government and private in 2016 than 2014, an indication that the industry is moving toward more private customers as their needs become more apparent.

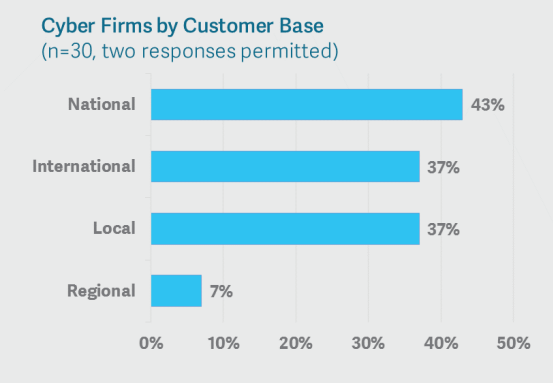
**FIGURE 4.1: CUSTOMER TYPE**




*Source: BW Research*

Of the companies surveyed, 43 percent responded that they have a national customer base, while 37 percent said they have an international base[1]. Selling products and services to firms outside of the region brings additional money into San Diego, deepening the economic impact. More than a third of firms have a local customer base, and firms rated access to clients and customers in the region as a strength of doing business in San Diego.

**FIGURE 4.2: CUSTOMER LOCATION**

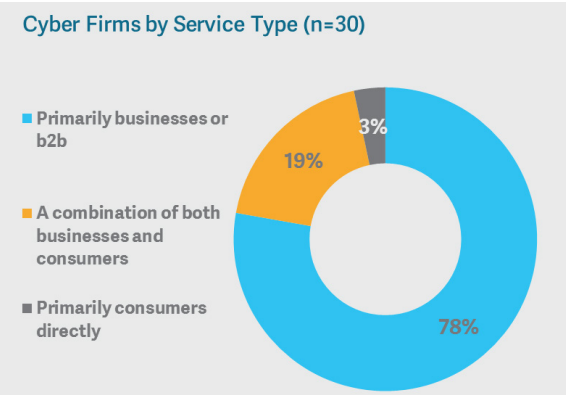



*Source: BW Research*

## INDUSTRY AND TYPE OF WORK

Cybersecurity employers in San Diego are largely service providers, assisting organizations in their cybersecurity needs. Most commonly, these companies are providing solutions to businesses (b2b); 78 percent of respondents said they are primarily b2b, while 22 percent said they were either exclusively consumer oriented or a mix of both b2b and b2c.

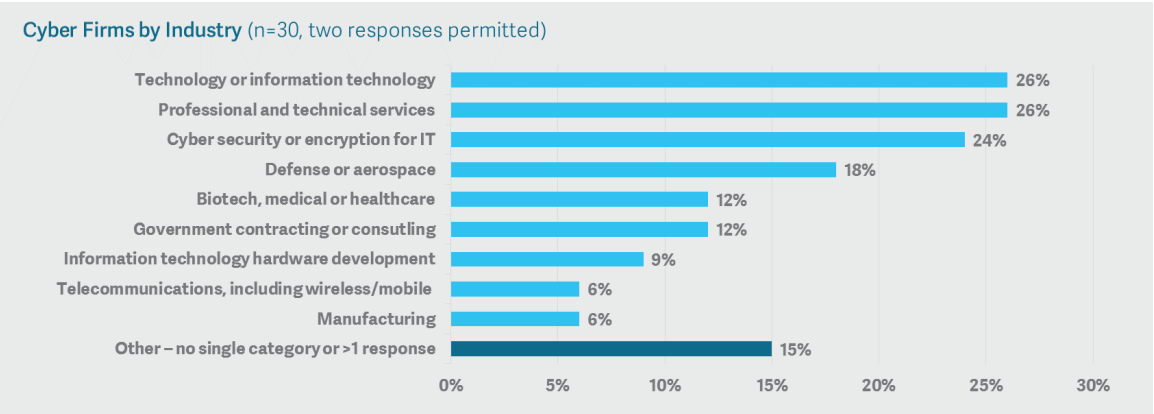
**FIGURE 4.3: TYPE OF WORK**




*Source: BW Research*

Employers were asked (unprompted) to self-identify which industry or industries best represent their business. Employers largely reported that they are in industries like IT, professional and technical services, followed by the encryption and defense spaces. Twelve percent of employers reported that they work in biotech, medical or healthcare industries—the fifth most reported—which demonstrates the increasing need for the securing of systems beyond those in government and defense.

**FIGURE 4.4: FIRMS BY INDUSTRY**




*Source: BW Research*

1 Note: more than one response allowed; therefore, some firms can be engaged in both national and international markets.

## FIRM SIZE AND CYBER FOCUS

Cybersecurity employers in San Diego are a mix of small, medium and large businesses. Approximately two-fifths of cybersecurity employers have more than 50 employees, while about one-fifth have fewer than five. The remaining two fifths of employers fall within the 5 to 49 range.

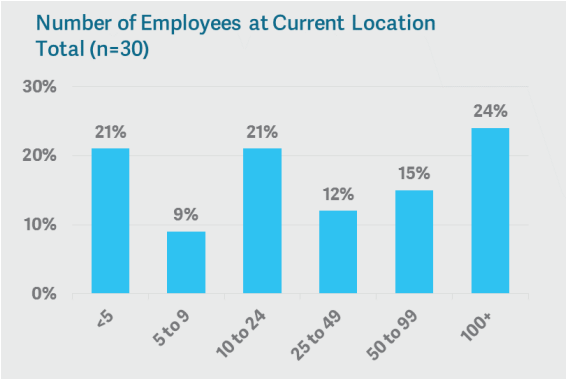
When looking specifically at the number of employees focused on cybersecurity projects, about three-quarters of businesses said they had 10 or fewer. When asked what portion of work was focused on cybersecurity, nearly half (47 percent) said that it was a minor part of what they do, meaning they spend less than 25 percent of their operations on cybersecurity[2]. Thirty-nine percent of employers reported that it was the primary focus of their work, with the remaining 15 percent reporting that it was a secondary focus.

## SENTIMENTS ABOUT THE REGION

Cybersecurity employers generally have positive views on San Diego as a place for their business. Nearly three-fourths (73 percent) reported that San Diego was either a good or excellent place for their business, with 27 percent reporting it as fair. No respondents reported that the region was either poor or very poor for their business.

When asked specifically about the region's strengths and weaknesses, access to clients, customers, vendors and suppliers are seen as San Diego's greatest strengths. None of the prompts were rated as overwhelming weaknesses, but access to capital/funding was seen more as a weakness than a strength in the region. Access to talent and a skilled workforce was largely rated as a strength, but a sizable share (29 percent) also rated it as a weakness.

**FIGURE 4.5: TOTAL EMPLOYMENT BY SIZE**

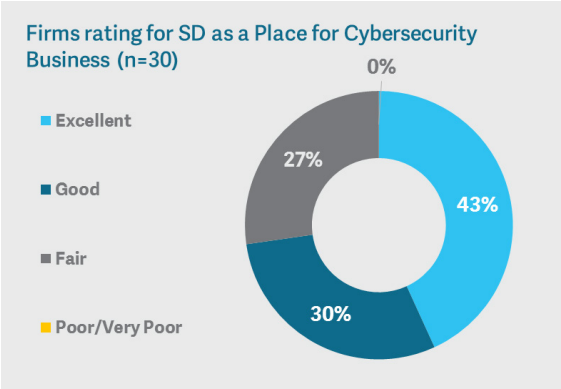



*Source: BW Research*

**FIGURE 4.6: CYBER EMPLOYER FOCUS**


*Source: BW Research*

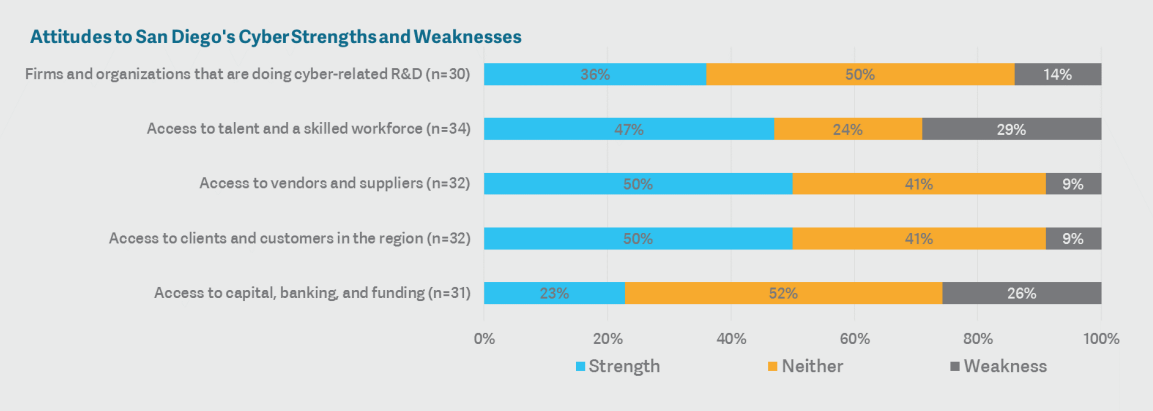
**FIGURE 4.7: CYBER EMPLOYMENT BY SIZE**




*Source: BW Research*

2 Note: this does not indicate that the company has a small cybersecurity team. For instance, a defense contractor with 1,000 employees could have a cyber division of 200 employees, which is sizeable, but still only makes up 20 percent of operations.

**FIGURE 4.8: EMPLOYER SENTIMENTS**




*Source: BW Research*

# 5 | *REGIONAL ASSETS*

## KEY TAKEAWAYS

Companies in the San Diego region received **more than $1.1 billion in contracts** from **SPAWAR** in 2015.

San Diego's **universities** and **colleges** confer more than **3,000 degrees in computer science** and **engineering** every year.

The San Diego region has **more than 20 incubators and accelerators**, as well as programs designed **specifically for cybersecurity** startups.

San Diego is uniquely positioned to continue to grow its cybersecurity industry and address the cybersecurity workforce needs of employers in the region. The region has a diverse mix of cybersecurity firms who work with an array of customers both locally and around the world. The region is also home to unparalleled education and research assets. San Diego has the largest military presence in the US and the US Navy's Space and Naval Warfare command—a major cyber employer and generator of R&D. Finally, the region is home to cutting-edge industry trade associations and cyber-specific incubators that support existing businesses and entrepreneurs.

## DEPARTMENT OF DEFENSE PRESENCE

In San Diego, SPAWAR is the anchor of the cybersecurity industry. This unique asset not only drives significant talent attraction, but also feeds a much larger defense cyber ecosystem. While exclusively commercial focused companies are growing, the federal government remains a major customer for San Diego cybersecurity employers. Fifty-three percent of employers said the government was a customer, while 13 percent said it was their only customer. San Diego is home to the Navy's Space & Naval Warfare Systems Command (SPAWAR). SPAWAR directly employs nearly half of all the cybersecurity jobs in San Diego and its presence in San Diego is a major contributing factor for many cyber companies to remain located in San Diego. SPAWAR's total budget in FY15 was $6.8 billion, with $5 billion (74 percent) going to private industry contracts, with the San Diego region receiving over $1.1 billion.[1]

**FIGURE 5.1: SPAWAR CAMPUS IN SAN DIEGO**

*Source: SPAWAR*

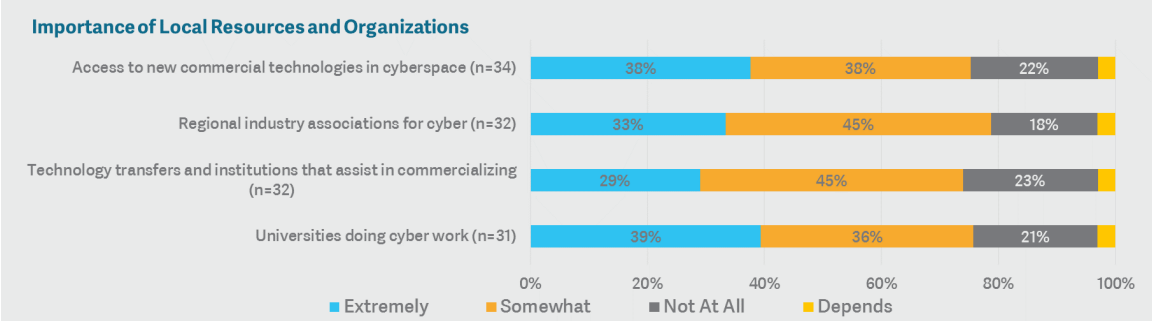
1 SPAWAR

## EDUCATION AND RESEARCH

San Diego's robust academic resources have been actively working with cybersecurity trade organizations and businesses across the region to create a curriculum that can remain agile enough to meet the demands of this rapidly evolving industry. San Diego's universities and colleges confer more than 3,000 degrees in computer science and engineering every year.[2] University of San Diego[3] and California State University San Marcos[4] recently launched two new cybersecurity masters programs specifically aimed at training professionals for the evolving demand of employers. In 2014, UC San Diego launched a unique masters program in data science and engineering[5]. The program is a partnership between the San Diego Supercomputer Center and the Jacobs School of Engineering and it is aimed at working professionals in the region. National University has a cybersecurity program that is recognized by the National Security Agency and the Department of Homeland Security as Center of Academic Excellence in Information Assurance and Cyber Security[6]. In addition to programs offered at San Diego's four-year colleges and universities, associate, bachelor's and master's certificates for cybersecurity programs have been established at University of Phoenix[7].

The legacy of research excellence across institutions opens the door for industry-research institution partnerships, especially as the federal government continues to increase funding for IT modernization and cybersecurity products. Employers surveyed for this study noted that access to new commercial technologies, institutions assisting in commercialization, and universities doing cyber work were overwhelmingly important. The region is home to resources like the San Diego Supercomputing Center at UC San Diego[8] and the Advanced Computing Environments Laboratory at San Diego State University[9], both of which are responsible for cutting-edge research in the field. San Diego's universities annually receive $1 billion in philanthropic and federal funding for research and development projects, making it a hotbed for innovation in the industry.[10]

**FIGURE 5.2: IMPORTANCE OF LOCAL ASSETS**




*Source: BW Research*

2 National Center for Education Statistics (NCES)
3 https://onlinedegrees.sandiego.edu/programs/master-of-science-in-cyber-security-operations-and-leadership/
4 http://www.csusm.edu/el/degreeprograms/psmcybersecurity/
5 http://jacobsschool.ucsd.edu/mas/dse/
6 http://www.nu.edu/OurPrograms/SchoolOfEngineeringAndTechnology/ComputerScienceAndInformationSystems/Programs/Master-of-Science-in-Cyber-Security-and-Information-Assuranc.html
7 http://www.phoenix.edu/colleges_divisions/technology/cyber-security-degrees.html
8 http://www.sdsc.edu/
9 http://www.cs.sdsu.edu/laboratories/
10 http://www.sandiegobusiness.org/sites/default/files/Research_Institutions_EIS_2015_EDC.pdf

## TRADE ORGANIZATIONS AND INCUBATORS

San Diego has a collection of incubators and trade organizations that serve diverse purposes. These organizations are aligned to focus on growing companies in San Diego and ensuring those companies have access to the talent, capital and other resources needed to compete globally. The San Diego region has more than 20 incubators and accelerators, as well as programs designed specifically for cybersecurity startups.[11]

### TRADE ORGANIZATIONS

- **Cyber Center of Excellence (CCOE)**
  CCOE is comprised of some of San Diego largest most established cybersecurity firms. CCOE's mission is to draw together the collective resources of regional academia, the military, and private industry to ensure that San Diego is able to take full advantage of the economic opportunities that cybersecurity represent.[12]

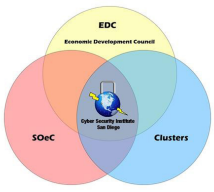
- **Securing Our eCity Foundation (SOeC)**
  SOeC assists businesses, families and the community to be better prepared for a safer cyber experience. They provide awareness of potential issues and offer free cybersecurity information and education, ensuring that the community understands the risks associated with the connected world.[13]

- **Tech San Diego**
  Tech San Diego is a non-profit organization supporting the regional small and mid-size technology community, including many cybersecurity firms. Tech San Diego has a robust peer executive development platform for C-level executives and promotes increasing the regional technical talent through its University Talent Initiative.[14]

- **CONNECT**
  CONNECT is one of the first formal accelerator programs in the country, dating back to the mid-1980s. The organization runs several programs, including Spring Board and Capital Match that help college students and entrepreneurs build and fund great companies. CONNECT 3.0 is the next iteration of programming to support thriving companies throughout their entire life cycle.[15]

- **CyberTECH**
  Based in San Diego, CyberTECH is a global cybersecurity and Internet of Things (IoT) network ecosystem providing cybersecurity and IoT resources, strategic programs and thought leadership events across the nation. In partnership with national and local organizations, the CyberTECH mission is to stimulate innovation and advance the adoption of cyber and IoT technologies for the economic and social benefit of the nation.[16]

- **Cyber Security Institute of San Diego (CSI-SD)**
  CSI-SD was formed in October 2011 by individuals associated with the National University Cyber Security and Information Assurance Program to facilitate the establishment and sustainment of a world class research and development capability in the San Diego region. The CSI-SD focuses on enabling public, private and academic institutions in the region to cooperate in a synergistic environment.[17]




11 San Diego Venture Group; San Diego Regional EDC; City of San Diego
12 http://sdccoe.org/about/
13 http://securingourecity.org/about
14 http://techsandiego.org/about
15 http://www.connect.org/about-connect
16 http://cybertechnetwork.org/aboutcybertech/
17 http://csi-sd.org/about.html

## INCUBATORS AND ACCELERATORS

- **EvoNexus**
  Since 2010, EvoNexus has helped 134 companies by providing mentorship, space and access to capital, helping their companies raise more nearly a billion dollars in capital. As of 2016, EvoNexus has more than 47 companies being incubated, making it the most active incubator in San Diego.[18]

- **CyberHive**
  CyberHive is a unique, innovative shared workspace and incubator program that is part of the CyberTECH network. CyberHive delivers business and technical support to early stage companies providing cybersecurity and high tech related products and services. CyberHive members receive business support services from CyberHive's experienced and highly skilled services team, robust and redundant data connectivity, and access to shared reception areas and conference rooms. [19]

- **iHive**
  Powered by CyberTECH, iHive is a shared workspace and incubator program dedicated to the Internet of Things. iHive delivers business and technical support to early stage companies providing Internet of Things related products and services.[20]

- **xHive**
  Also part of the CyberTECH network, xHive is a sustainable non-profit shared workspace and incubator community focused in the areas advanced new technologies including devices powering the IoT, software and app development, robotics, 3D printing and drones.[21]

- **NEST**
  Perched with amazing views overlooking downtown and the San Diego Bay, NEST is 5,000 square feet of full service co working space with a full kitchen, gym, showers, a meditation and relaxation room, and many work options. NEST was launched in February 2016 as part of the CyberTECH network.[22]

18 http://evonexus.org/about/
19 http://cybertechnetwork.org/aboutcyberhive/
20 http://cybertechnetwork.org/aboutihive/
21 http://cybertechnetwork.org/xhive/
22 http://cybertechnetwork.org/nest/

# 6 | *ACTION ITEMS AND NEXT STEPS*



In order to capitalize on the momentum in the industry and address the challenges facing employers in the region, leaders from industry, education and government should focus on the following action items and next steps:

## RETAIN LOCAL UNIVERSITY GRADUATES

San Diego's universities are tremendous assets to the region, but graduates with relevant skills or degrees are often heavily recruited to leave the area well before their graduation. Students who participate in local internships programs, however, are often easier to recruit and retain within the region. Through internships, students not only gain valuable work experience, but internships have often proven to be an effective way for employers to build loyalty with an increasingly transient workforce[1]. Local leadership should establish partnerships between universities and industry that will increase student exposure to internships and local opportunities.

## SUPPORT PROGRAMS TO TRAIN MORE QUALIFIED ENTRY-LEVEL TALENT

Employers identified that while a degree is important by far the most important skill was job experience and technical training; therefore, competition is fierce for talent with security certificates and experience. With more than 21,000 software developers working in San Diego across the economy, there is enough talent to meet demand if qualified workers can acquire the necessary skills and experience for employment in cybersecurity. By increasing visibility and access to certificate programs, it is possible to begin to alleviate some of the pressure on employers seeking experienced talent. San Diego code academies have been growing rapidly and they are helping retool the workforce through accelerated training programs aimed at finding careers in tech. These academies, as well as certificate programs at community colleges and university extensions, are a useful tool for increasing the talent pipeline.

## ENHANCE NATIONAL REPUTATION

Shaping a national reputation that highlights San Diego's unique cybersecurity strengths and established employers will over time support the recruitment of top experienced talent from across the US. San Diego's political leadership should work with local industry and trade organizations on a unified communications strategy that will increase the visibility for the region and make talent attraction easier. Leaders should also ensure that San Diego's cybersecurity companies are showcased at existing local and national programs and events that highlight the region, such as San Diego Startup Week and the various local and national hackathons.

1 http://www.wsj.com/articles/SB10354066434669069 51

## STRENGTHEN THE REGION'S CYBERSECURITY FOUNDATION

SPAWAR remains the single most valuable resource to San Diego's cyber ecosystem, but one issue area for SPAWAR is the regulatory structure that governs how they can recruit and retain talent. The sensitive nature of their work creates limitations on who and how they might be able to recruit from universities. San Diego has thousands of veterans exiting the service every year. Local leadership should work with Navy and Marine Corps partners across the region to identify technical talent that would be interested in working in cybersecurity and leverage existing programs to provide the adequate career and technical training.

## GROW LOCAL OPPORTUNITIES AND INTER-INDUSTRY RELATIONSHIPS

As the global commercial demand for cybersecurity grows, San Diego businesses have the potential to capture new markets. San Diego's cybersecurity employers are already going global, but there are increasingly new programs being established within the region to help streamline global expansion interests of local businesses. By working with partners like World Trade Center on programs like the Metro Connect Prize, companies can identify and expand into new and growing commercial markets around the globe.

While global expansion will be important for the growth of the industry, there remain many untapped opportunities for partnerships within the region. Through regional branding and partnership with local elected officials and organizations like SoEC, it is possible to help build visibility for solutions that will create new business for San Diego companies and will enhance the security of the region. If San Diego can cement itself as a business environment that is actively working to enhance the security of all businesses, this will help drive opportunities in particular for smaller cyber startups who often are more reliant on local work.

Strategic partnerships should also be explored with key growth industries that have highly sensitive data requirements. San Diego's growing genomics, medical devices and robotics clusters could find great mutual benefit in partnership with local cyber leadership to develop technical solutions to protect sensitive information.  Successful partnerships would become a talking point of national interest, which in turn would highlight San Diego as a cyber hub.

## BE ACTIVE IN SHAPING POLICY

California's Cyber Security Taskforce is a vehicle for San Diego leaders to make an impact on statewide policies. Several prominent members of San Diego's cybersecurity industry are actively involved in different committees on the task force. These individuals can help ensure that state policy is intelligently crafted, while continuing to position San Diego as a leader on cybersecurity policy. There is also growing pressure on the federal government to enact sweeping cybersecurity regulations. San Diego needs its industry groups and cybersecurity employers to remain active in this policy process to ensure these regulations are effective for local employers.

# A | *SURVEY, QUANTIFICATION & ECONOMIC IMPACT METHODOLOGY*

The following methodology is a description of the secondary data, business survey and extrapolation research done by BW Research in support of the 2016 study on San Diego County's cybersecurity business and employers. The outcome of this research became the basis for the economic impact analysis that was performed using the IMPLAN modeling software from MIG.

## SURVEY DESIGN

The following table provides a brief overview of the methodology utilized for the survey research component of the study.

**TABLE A.1: OVERVIEW OF SURVEY METHODOLOGY**

| | |
|---|---|
| **Method** | Telephone and Web Survey of Core Cybersecurity Firms and Industries with a High Concentration of Cyber Employment in San Diego County |
| **Number of Survey Participants** | 34 Firms that were either Core Cybersecurity or had Cybersecurity Employment in San Diego County Completed the Full Survey<br><br>87 Additional Firms Counted as Short Completes (answered "no" to cyber employment – used for extrapolating unknown employment) |
| **Survey Field Dates** | Web & Telephone Survey: February 22 – April 8, 2016. |
| **Survey Universe** | 140 Core Cyber Firms in San Diego County<br><br>5,740 Additional Businesses from the Unknown Universe |

Through an iterative process, BW Research worked closely with the San Diego Regional Economic Development Corporation (SDREDC) and the San Diego Cyber Center of Excellence (CCOE) to develop a survey instrument that met the research objectives of the study. In developing the survey instrument, BW Research utilized techniques to overcome known biases in survey research and minimize potential sources of measurement error within the survey.

### Sampling Method

BW Research with the assistance of SDREDC, CCOE and the cyber advisory group developed a database of known core cybersecurity firms in San Diego County. These known core cyber firms were delineated into primary (those firms who primarily develop cyber technology products and services) and proportional (those firms who develop cyber products and services, but it is less than the primary focus of their firm) firms. There were 140 firms identified in the known core cybersecurity database in San Diego County.

As part of the research, BW Research, also examined firms from the NAICS industries 5415 (Computer Systems Design & Related Services) and 5416 (Management, Scientific, and Technical Consulting Services) to determine unknown cyber employment. A total 5,470 firms[1] in these two industries were identified as the basis for the unknown employment research.

**Data Collection**

Prior to beginning data collection, BW Research tested the online survey and conducted interviewer training to ensure that all words and questions were easily understood by the respondents. The data collection period was February 22 through April 8, 2016.

**Cybersecurity Employment Estimation**

Cybersecurity employment in San Diego County was derived from a multiple method approach that is broken into the three phases listed below.

**Phase 1**: Develop, classify, and analyze a database of "known" Core Cybersecurity firms in San Diego County. Duplicates were removed based on identifying factors such as phone number, company name, and address. Next, BW Research conducted a census on this list to determine overall Cybersecurity employment at these locations. The phase was conducted through online and phone surveys. Employment at these known firms is identified as primary Cyber employment as these firms are considered to conduct work primarily in Cybersecurity.

**Phase 2**: BW Research developed a sample of "unknown' firms in San Diego County within industries previously identified to have a high incidence of Cybersecurity employment. These industries were identified at the 4-digit NAICS level and included;

- NAICS 5415 – Computer Systems Design & Related Services
- NAICS 5416 – Management, Scientific, and Technical Consulting Services

A random sample of businesses was generated and these firms were called as part of the survey effort. Each record that was called was assigned a disposition that could be used in calculating industry churn and Cyber employment incidence. A total of 493 firms were called in the "unknown" database, with 99 firms participating in the survey effort. Incidence of Cyber employment was then applied to QCEW[2] establishment totals for the County (1,878 total establishments in Computer Systems Design & Related Services, and 3,904 total establishments in Management, Scientific, and Technical Consulting Services) to determine "unknown" Cyber employment establishments. The following numbers were generated;

- NAICS 5415 – 366 Cyber employing establishments, 1,868 Cyber employees
- NAICS 5416 – 183 Cyber employing establishment, 932 Cyber employees

1 Firms in the known database of core cybersecurity firms were removed from the unknown database.
2 http://www.bls.gov/cew/

These establishments are not considered Core Cyber establishments, therefore, the Cyber employment that is calculated is considered secondary to the focus of "unknown" firms in San Diego County.

**Phase 3**: The final phase compared the employment collected from "known" respondents in the 2016 survey to the survey conducted at the end of 2013. This was done to identify potentially misreported information and outliers. For the remaining Core Cyber firms on the list, an extensive collection of secondary data was undertaken to estimate Cyber employment. This was done by searching internet databases, including InfoUSA[3], for employment numbers and deriving proportional Cyber employment from a search of the company online or comparing to the share of Cyber employment at firms as reported in the 2014 Cybersecurity study.

## IMPLAN METHODOLOGY

The research team used MIG IMPLAN, a widely accepted tool for economic impact assessment, to asses the indirect and induced impacts on employment, value added (gross regional product) and labor income (wages). Indirect impacts are the effects of local industries buying goods and services from other industries. For instance, management consultants, law firms, market research, and other establishments generate local impacts through their buying and selling activities with cybersecurity firms or divisions. Induced impacts are a result of employees at cybersecurity firms spending their dollars in the local economy, usually on food services, medical services, housing, and leisure.

The inputs for the model came from the results of the census and survey outlined above. Firms were assigned a NAICS code based on their response to questions or their records in InfoUSA. For some firms, the NAICS code needed to be reasonably refined based on the nature of the work performed. The team used the total employment for each NAICS code and converted these to IMPLAN codes using the built-in code bridge in the IMPLAN software. Given the nature of the work and the type of employees needed, the team used a standard "tech employee" wage for non-tech industries, based off of the average wages of workers in tech industries like computer systems design and technical consulting services. For employees in the aforementioned sectors, the team used the IMPLAN model income estimate.

To estimate the impacts of SPAWAR, the team used the factors from the 2014 study for consistency. Given that the nature of work at SPAWAR is largely similar to 2014, changing the model assumptions would dramatically change the impact figures.[4]

The final results were rounded for reporting purposes.

3 www.salesgenie.com
4 http://www.sandiegobusiness.org/sites/default/files/Cyber%20Security%20Final%20Report.pdf

## IMPLAN MODEL INPUTS

| IMPLAN CODE | NAICS CODE | NAICS DESCRIPTION | EMPLOYMENT INPUT |
|---|---|---|---|
| **PRIVATE KNOWN UNIVERSE** | | | |
| 305 | 3342 | COMMUNICATIONS EQUIPMENT MANUFACTURING | 388 |
| 315 | 3345 | NAVIGATIONAL, MEASURING, ELECTROMEDICAL, AND CONTROL INSTRUMENTS MFG | 499 |
| 363 | 3366 | SHIP AND BOAT BUILDING | 111 |
| 422 | 5112 | SOFTWARE PUBLISHERS | 678 |
| 429 | 5179 | OTHER TELECOMMUNICATIONS | 166 |
| 430 | 5182 | DATA PROCESSING, HOSTING, AND RELATED SERVICES | 422 |
| 438 | 5242 | AGENCIES, BROKERAGES AND OTHER INSURANCE RELATED ACTIVITIES | 2 |
| 449 | 5413 | ARCHITECTURAL, ENGINEERING, AND RELATED SERVICES | 246 |
| 450 | 5414 | SPECIALIZED DESIGN SERVICES | 3 |
| 452 | 5415 | COMPUTER SYSTEMS DESIGN AND RELATED SERVICES | 508 |
| 453 | 5416 | MANAGEMENT, SCIENTIFIC, AND TECHNICAL CONSULTING SERVICES | 644 |
| 460 | 5419 | OTHER PROFESSIONAL, SCIENTIFIC, AND TECHNICAL SERVICES | 33 |
| 466 | 5615 | TRAVEL ARRANGEMENT AND RESERVATION SERVICES | 2 |
| 467 | 5616 | INVESTIGATION AND SECURITY SERVICES | 115 |
| 470 | 5619 | OTHER SUPPORT SERVICES | 404 |
| 506 | 8112 | ELECTRONIC AND PRECISION EQUIPMENT REPAIR AND MAINTENANCE | 7 |
| **SPAWAR** | | | |
| - | - | SPAWAR (USED 2014 FACTOR) | 3,390 |
| **PRIVATE UNKNOWN / ESTIMATED** | | | |
| 452 | 5415 | COMPUTER SYSTEMS DESIGN AND RELATED SERVICES | 1,868 |
| 453 | 5416 | MANAGEMENT, SCIENTIFIC, AND TECHNICAL CONSULTING SERVICES | 932 |

# B | *SURVEY TOPLINES*



[SEE ATTACHED WORKSHEET]

**SDREDC – Cyber**
**San Diego County**
**April 2016**
**Preliminary Toplines 1.1**

## Cyber Firms (n=34)

### Introduction:

[FOR A FIRM OF 20 OR MORE PEOPLE]
Hello, my name is _____. May I please speak to someone who is involved or leading the strategic planning, hiring or location decisions at your firm?

[FOR A FIRM OF 19 OR LESS PEOPLE]
Hello, my name is _____. May I please speak to a manager or someone in charge of hiring decisions at your firm?

Hello, my name is _____ and I'm calling on behalf of the **San Diego Cyber Center of Excellence (SDCCOE) and the San Diego Regional Economic Development Corporation (SDREDC)** who would value your participation in a brief survey about San Diego County's economic needs and opportunities.

**(If needed):** This survey has been commissioned by the San Diego Regional Economic Development Corporation, which is committed to supporting the businesses in the County.

**(If needed):** The survey is being conducted by BW Research, an independent research organization, and should take approximately ten minutes of your time.

**(If needed):** Your individual responses will **not** be published; only aggregate information will be used in the reporting of the survey results.

### Screener Questions

A. How many business locations does your company or organization have in San Diego County?

**79% One location in San Diego County**
**21% Two or more locations in San Diego County**

B. For this survey only answer for your current San Diego County business location. If your firm has more than one location, please do not include their information. What is the zip of your current location?

_____ I am answer for my business location in zip:
999 Not sure [TERMINATE]

## PART 1 – BUSINESS PROFILE

1. Including all full-time and part-time employees, how many **permanent** employees work at or from your current location?

| | |
|---|---|
| **21%** | **Less than 5** |
| **9%** | **Between 5 and 9** |
| **21%** | **Between 10 and 24** |
| **12%** | **Between 25 and 49** |
| **15%** | **Between 50 and 99** |
| **24%** | **100 or more** |

2. If you currently have [TAKE Q1 #] full-time and part-time **permanent** employees at your current location, how many more or less employees do you expect to have 12 months from now?

**Breakdown:**

| | |
|---|---|
| **65%** | **More** |
| **0%** | **Fewer** |
| **32%** | **Same number of permanent employees** |
| **3%** | **(DON'T READ) DK/NA** |

**Expected Permanent Employment in 12 months *outliers removed**
(Calculated by only examining businesses with both current and projected data)

| | Current | 12 months |
|---|---|---|
| n | 25 | 25 |
| Mean | 28.84 | 32.00 |
| Median | 14.00 | 20.00 |
| Total Employees | 721 | 800 |
| Change | | 79 |
| % Growth | | **11%** |

[If amount differs by 10% or more in either direction, ask: ]
Just to confirm, you currently have ____ permanent employees and you expect to have _____ (more/less) employees, for a total of ____ employees 12 months from now.

Next I would like to ask about the industries that are most important to your firm.

3. What industry or industries best describes the work that your firm is involved in and connected to? (DO NOT READ, ALLOW MORE THAN ONE RESPONSE) (Multiple responses permitted, percentages may sum to more than 100%)

**26% Technology or information technology**
**26% Professional and technical services**
**24% Cyber security or encryption for IT**
**18% Defense or aerospace**
**12% Biotech, medical or healthcare**
**12% Government contracting or consutling**
**9% Information technology hardware development**
**6% Telecommunications, including wireless communication (include mobile devices)**
**6% Manufacturing**
**15% Other – *no single category more than one response***

4. Over the last three years, has your company grown, declined or stayed about the same in terms of permanent employment at your location? [If it has grown or declined, ask] By about how many people?

**Breakdown:**

**59% Grown**
**29% Stayed the same**
**12% Declined**
**0% (DON'T READ) DK/NA**

**Growth in Permanent Employment over Last 3 Years *outliers removed**
(Calculated by only examining businesses with both current and past data)

| | Current | 12 months |
|---|---|---|
| n | 26 | 26 |
| Mean | 24.54 | 30.69 |
| Median | 13.50 | 16.50 |
| Total Employees | 638 | 798 |
| Change | | 160 |
| % Growth | | **25%** |

**PART 2 – CYBER & CUSTOMER PROFILE**

Next I want you to think about the work that your firm does at your current location in cyber security or information technology security which can be defined as ***products or services designed to protect computers, networks, programs and data from unintended or unauthorized access or destruction.*** [REMIND AND REPEAT CYBER DEFINITION AS NEEDED].

5. What portion of the work done from this location is focused on cyber security? (ACCEPT FIRST RESPONSE)

   [REPEAT CATEGORIES AS NEEDED]

   **24% All of it - it is the only thing we focus on at this location (100%)**
   **15% It is the primary focus of this location (50% to 99%)**
   **15% It is a secondary focus of this location (25% to 49%)**
   **47% It is a minor part of what we do at this location (1% to 24%)**
   **0% [DON'T READ] Do not do any of it from this location TERMINATE**
   **0% [DON'T READ] DK/NA**

6. If you currently have [TAKE Q1 #] full-time and part-time **permanent** employees at your San Diego County location(s), how many of these employees are focused on work related to cyber security work?

   **29% 1 or 2**
   **21% Between 3 and 5**
   **24% Between 6 and 10**
   **9% Between 11 and 49**
   **18% 50 or more**

7. If you currently have [TAKE Q6 #] full-time and part-time **permanent** employees at your San Diego County location(s) who are focused on work related to cyber security, how many more or less cyber security employees do you expect to have 12 months from now?

**Breakdown:**

| | |
|---|---|
| **53%** | **More** |
| **0%** | **Fewer** |
| **47%** | **Same number of permanent employees** |
| **0%** | **(DON'T READ) DK/NA** |

**Expected Permanent Cyber Security Employment in 12 months *outliers removed**
(Calculated by only examining businesses with both current and projected data)

| | Current | 12 months |
|---|---|---|
| n | 30 | 30 |
| Mean | 15.57 | 17.63 |
| Median | 5.00 | 7.00 |
| Total Employees | 467 | 529 |
| Change | | 62 |
| % Growth | | **13%** |

8. Which of the following categories best describes the type of work you do in the cyber security realm?

| | |
|---|---|
| **56%** | **Support and technically assist organizations in their cyber security needs** |
| **24%** | **Provide cyber or IT security solutions and/or software to your customers** |
| **9%** | **Develop or support the development of new cyber security products or software** |
| **9%** | **Other** |
| **3%** | **(DON'T READ) DK/NA** |

9. Does your firm do cyber security work directly or indirectly for the Federal government, including the Department of Defense. If yes, is the cyber security work you do for the federal government the primary focus of your firm's cyber security work?

| | |
|---|---|
| **12%** | **Yes, and it is the primary focus of our firm** |
| **38%** | **Yes, but it is not the primary focus of our firm** |
| **44%** | **No** |
| **6%** | **(DON'T READ) DK/NA** |

SKIP TO Q12 IF Q9="Yes, and it is the primary focus of our firm"

10. Next, as your think about your firm's cyber security work is your firm primarily focused on serving other businesses – a b2b focus, or primarily focused on serving consumers directly, or a combination of both b2b and consumers? (n=30)

| | |
|---|---|
| **70%** | **Primarily businesses or b2b** |
| **3%** | **Primarily consumers directly** |
| **17%** | **A combination of both businesses and consumers** |
| **10%** | **(DON'T READ) DK/NA** |

11. Are your customers primarily local - within San Diego County, regional - within Southern California, Statewide – within California, national – within the Country, or international - outside the Country? [UP TO 2 RESPONSES PERMITTED] (Multiple responses permitted, percentages may sum to more than 100%) (n=30)

| | |
|---|---|
| **37%** | **Local - San Diego County** |
| **7%** | **Regional – Within Southern California** |
| **0%** | **Statewide – Within California** |
| **43%** | **National – Within the United States** |
| **37%** | **International – Outside the United States** |

**[PART 3 – CYBER LOCATION QUESTION]**

12. Now thinking about San Diego County, how would you rate ***San Diego County*** as a place for cyber security firms to do business?

| | |
|---|---|
| **38%** | **Excellent** |
| **26%** | **Good** |
| **24%** | **Fair** |
| **0%** | **Poor** |
| **0%** | **Very poor** |
| **12%** | **(DON'T READ) DK/NA** |

**[RANDOMIZE ORDER OF Q13 AND Q14 – ONLINE ONLY]**

13. What do you see as the biggest advantages of doing business in San Diego County as a cyber-security firm?

***Verbatim responses to be provided***

14. What do you see as the biggest challenges of doing business in San Diego County as a cyber-security firm?

***Verbatim responses to be provided***

Next, I want to ask a few quick questions about the resources and business opportunities in San Diego County

15. Please tell me if you think the following resources in San Diego County are a strength of the region or if they are a weakness, in comparison to other regions your business could be located.

    Are San Diego County's_____ a strength, a weakness or neither a strength nor weakness, when compared to other regions?

**RANDOMIZE**

| | Strength | Neither strength nor weakness | Weakness | (DON'T READ) DK/NA |
|---|---|---|---|---|
| **A. Access to capital, banking, and funding** | **21%** | **47%** | **24%** | **9%** |
| **B. Access to clients and customers in the region** | **47%** | **38%** | **9%** | **6%** |
| **C. Access to vendors and suppliers** | **47%** | **38%** | **9%** | **6%** |
| **D. Access to talent and a skilled workforce** | **47%** | **24%** | **29%** | **0%** |
| **E. Firms and organizations that are doing cyber-related research development** | **31%** | **44%** | **13%** | **13%** |

**Q15 with DK/NA removed**

| | Strength | Neither strength nor weakness | Weakness |
|---|---|---|---|
| **A. Access to capital, banking, and funding (n=31)** | **23%** | **52%** | **26%** |
| **B. Access to clients and customers in the region (n=32)** | **50%** | **41%** | **9%** |
| **C. Access to vendors and suppliers (n=32)** | **50%** | **41%** | **9%** |
| **D. Access to talent and a skilled workforce (n=34)** | **47%** | **24%** | **29%** |
| **E. Firms and organizations that are doing cyber-related research development (n=30)** | **36%** | **50%** | **14%** |

16. Please tell me how important the following resources and organizations are to your firm and its work related to cyber and Information security.

**RANDOMIZE**

| | Extremely important | Somewhat important | Not at all important | (DON'T READ) It depends | (DON'T READ) DK/NA |
|---|---|---|---|---|---|
| **A. Universities doing cyber work** | **38%** | **35%** | **21%** | **3%** | **3%** |
| **B. Technology transfers and institutions looking to assist in commercializing new cyber products** | **26%** | **41%** | **21%** | **3%** | **9%** |
| **C. Regional industry associations for cyber** | **32%** | **44%** | **18%** | **3%** | **3%** |
| **D. Access to new commercial technologies in cyberspace** | **35%** | **35%** | **21%** | **3%** | **6%** |

**Q16 with DK/NA removed**

| | Extremely important | Somewhat important | Not at all important | (DON'T READ) It depends |
|---|---|---|---|---|
| **A. Universities doing cyberwork (n=33)** | **39%** | **36%** | **21%** | **3%** |
| **B. Technology transfers and institutions looking to assist in commercializing new cyber products (n=31)** | **29%** | **45%** | **23%** | **3%** |
| **C. Regional industry associations for cyber (n=33)** | **33%** | **45%** | **18%** | **3%** |
| **D. Access to new commercial technologies in cyberspace (n=32)** | **38%** | **38%** | **22%** | **3%** |

**[PART 4 – CYBER WORKFORCE QUESTION]**

Lastly, I would like to ask about your organization's need for new employees, in particular those that are working in cyber or information security

17. Thinking about the ***positions related to cyber*** you hire at your San Diego County location(s), how much difficulty does your company have finding **qualified entry to mid-level applicants** who meet the organization's hiring standards?

**18%** **Little to no difficulty**

**41%** **Some difficulty**

**29%** **Great difficulty**

**12%** **(DON'T READ) DK/NA**

18. Thinking about the ***positions related to cyber*** you hire at your San Diego County location(s), how much difficulty does your company have finding qualified ***experienced industry professionals*** who meet the organization's hiring standards?

| | |
|---|---|
| **18%** | **Little to no difficulty** |
| **35%** | **Some difficulty** |
| **35%** | **Great difficulty** |
| **12%** | **(DON'T READ) DK/NA** |

19. Please tell me how important the following items are when considering candidates for available cyber security positions at your firm: very important, somewhat important, or not at all important.

**RANDOMIZE**

| | Very important | Somewhat important | Not at all important | (DON'T READ) It depends | (DON'T READ) DK/NA |
|---|---|---|---|---|---|
| **A. An industry recognized credential or certification** | **29%** | **47%** | **18%** | **3%** | **3%** |
| **B. At least one year of industry-related work experience** | **65%** | **24%** | **3%** | **6%** | **3%** |
| **C. A four-year college degree or higher** | **38%** | **35%** | **18%** | **6%** | **3%** |
| **D. Technical training and expertise specific to the position they are applying for** | **74%** | **21%** | **0%** | **3%** | **3%** |

20. Please tell me how important the following certification are when considering candidates for available cyber or information security positions at your firm: very important, somewhat important, or not at all important.

**RANDOMIZE**

| | Very important | Somewhat important | Not at all important | (DON'T READ) It depends | (DON'T READ) DK/NA |
|---|---|---|---|---|---|
| **A. GIAC Security Essentials Certification (GSEC)** | **9%** | **29%** | **26%** | **9%** | **26%** |
| **B. CISCO Certified Network Associate (CCNA)** | **12%** | **47%** | **15%** | **12%** | **15%** |
| **C. CISCO Certified Networking Professional (CCNP)** | **18%** | **47%** | **12%** | **12%** | **12%** |
| **D. Security+** | **24%** | **32%** | **24%** | **6%** | **15%** |
| **E. Certified Information Systems Security Pro (ISC2)** | **24%** | **32%** | **18%** | **9%** | **18%** |
| **F. Certified Information Security Manager (CISM)** | **6%** | **41%** | **18%** | **12%** | **24%** |
| **G. Certified Information Systems Auditor (CISA)** | **6%** | **44%** | **18%** | **15%** | **18%** |
| **H. Microsoft Certified Professional (MCP)** | **18%** | **32%** | **26%** | **12%** | **12%** |
| **I. Microsoft Certified Solutions Associate (MCSA)** | **12%** | **29%** | **32%** | **12%** | **15%** |
| **J. Offensive Security Certified Professional (OSCP)** | **12%** | **35%** | **24%** | **9%** | **21%** |

**Q20 with DK/NA removed**

| | Very important | Somewhat important | Not at all important | (DON'T READ) It depends |
|---|---|---|---|---|
| **A. GIAC Security Essentials Certification (GSEC) (n=25)** | **12%** | **40%** | **36%** | **12%** |
| **B. CISCO Certified Network Associate (CCNA) (n=29)** | **14%** | **55%** | **17%** | **14%** |
| **C. CISCO Certified Networking Professional (CCNP) (n=30)** | **20%** | **53%** | **13%** | **13%** |
| **D. Security+ (n=29)** | **28%** | **38%** | **28%** | **7%** |
| **E. Certified Information Systems Security Pro (ISC2) (n=28)** | **29%** | **39%** | **21%** | **11%** |
| **F. Certified Information Security Manager (CISM) (n=26)** | **8%** | **54%** | **23%** | **15%** |
| **G. Certified Information Systems Auditor (CISA) (n=28)** | **7%** | **54%** | **21%** | **18%** |
| **H. Microsoft Certified Professional (MCP) (n=30)** | **20%** | **37%** | **30%** | **13%** |
| **I. Microsoft Certified Solutions Associate (MCSA) (n=29)** | **14%** | **34%** | **38%** | **14%** |
| **J. Offensive Security Certified Professional (OSCP) (n=27)** | **15%** | **44%** | **30%** | **11%** |

21. Are there specific technical (DEFINE) skills or types of experience you are looking for, when hiring cyber professionals?

***Verbatim responses to be provided***

22. What city is your firm headquartered in?

***Verbatim responses to be provided***

23. Would you be willing to be contacted by researchers and/or educators who are developing new strategies and regional plans to support the San Diego County's cyber businesses?

**56% Yes**
**38% No**
**6% (DON'T READ) DK/NA**

**Since it sometimes becomes necessary for the project manager to call back and confirm responses to certain questions, I would like to verify your contact information.**

A. First and Last Name_____

B. Position_____

C. Phone_____

D. Email _____

E. Company Name_____

**Those are all of the questions I have for you.**
**Thank you very much for participating!**

F. Company Name _____

G. Company location_____

H. Date and time of Interview_____

I. Name of Interviewer _____

J. PRIMARY NAICS CODE (ACCORDING TO DATA FILE)_____

K. SECONDARY NAICS CODE (ACCORDING TO DATA FILE)_____

L. NUMBER OF EMPLOYEES (ACCORDING TO DATA FILE)_____

M. Gender (VOICE)

1 Male
2 Female

**SAN DIEGO'S CYBERSECURITY INDUSTRY** AN ECONOMIC IMPACT ANALYSIS AND WORKFORCE STUDY

*Sponsored by*

Bank of America

eset

SENTEK GLOBAL

*Produced by*

Cyber Center CCoE of Excellence

*Research by*

CBRE

SAN DIEGO REGIONAL EDC

[bw] RESEARCH PARTNERSHIP

www.sdccoe.org
info@sdccoe.org
@sdccoe