CYBERSECURITY IN SAN DIEGO

AN ECONOMIC IMPACT AND INDUSTRY ASSESSMENT

MARCH 2014

SPONSORED BY

SENTEK GLOBAL

Bank of America Merrill Lynch

PRODUCED BY

SAN DIEGO REGIONAL EDC

Cybersecurity in San Diego: An Economic Impact and Industry Assessment

National University System Institute for Policy Research
BW Research, Inc.
SANDAG Service Bureau

[bw] RESEARCH PARTNERSHIP

servicebureau

SANDAG

EXECUTIVE SUMMARY

- At least 6,640 San Diegans work in the core of the cybersecurity industry in San Diego County. We define this industry as firms that provide cybersecurity products and services largely to customers external to their organization or firm.
- A key component of San Diego's cybersecurity industry is the United States Navy Space and Naval Warfare Systems Command (SPAWAR). Employing an estimated 3,095 cybersecurity professionals and tasked with administering hundreds of millions of dollars in cyber contracts, SPAWAR has a profound impact on San Diego's cyber industry.
- The total economic impact of cybersecurity industry workers in 2013 was $1.515 billion, and the industry supports an additional 6,600-plus indirect and induced jobs. This impact is equivalent to hosting 3.3 Super Bowls or 8.5 Comic-Cons each year.
- The cybersecurity industry in San Diego County is closely tied to the federal government, with more than 50 percent of companies surveyed indicating that the federal government is one of their principal customers. Conversely, very few cybersecurity firms in San Diego focus on the consumer market. For the long term, San Diego needs to think of ways to ensure that an industry largely focused on the federal government's needs is able to diversify and satisfy the needs of private businesses.
- The industry is positive about its expectations for short-term growth, with employment projections significantly exceeding overall area employment forecasts. In part, this optimism reflects the robust growth the industry has experienced during the past three years.
- Proximity to customers and the presence of entrepreneurial talent are key advantages for San Diego's cybersecurity industry. Key challenges include the difficulty in finding an adequate supply of trained workers and the bifurcation in the skill sets these workers need. While information-technology generalists who support workers throughout an organization need soft skills, our survey suggests these skills are somewhat less important for cybersecurity specialists.

Cyberspace has become ever present in modern life. According to the Information Technology Innovation Foundation, the commercial Internet annually accounts for $1.5 trillion in global economic activity.[1] Information technology (IT) has radically transformed entire industries and increasingly it constitutes the nervous system of the modern economy. SRI Consulting Business Intelligence, writing for the National Intelligence Council in 2008, predicted a world where Internet-enabled devices would become embedded in everyday objects ranging

1. Robert D. Atkinson et al., *The Internet Economy 25 Years after .com*, Information Technology & Innovation Foundation, March 15, 2010, http://www.itif.org/publications/internet-economy-25-years-after-com.

from home dishwashers to paper documents.[2] In many ways, that day has arrived. For example, we have Internet-enabled thermostats controlling the flow of energy to everyday appliances, which themselves are interconnected and networked. Everyday life has become increasingly wired to the point that Internet connectivity has become a necessity for many individuals and businesses.

As IT's pervasiveness has grown, so too have the threats to these networks and the spending to defend them. Cyber threats range from the work of malicious single hackers to coordinated efforts at security and economic espionage carried out by nation-states. Privacy concerns and the need for different networks to communicate have increased both the complexity of cybersecurity and its vulnerability. Indeed, cyber threats have been recognized as a danger to national security, and millions of businesses and billions of people every day are at financial and personal risk from compromised systems. In an ever-escalating dynamic of threat and response, PricewaterhouseCoopers estimated that $60 billion would be spent globally on cybersecurity products in 2011 and that such spending would increase annually by at least 10 percent over the next three to five years.[3]

This trend has created significant economic opportunities. San Diego is especially well positioned to benefit from them, with both a critical mass of firms and a solid economic foundation on which to grow. The region is already home to large market leaders in cybersecurity solutions such as ESET and Sentek Global. For more than two decades, the region has been a leader in data analytics and encryption technologies.[4]

San Diego also has a strong cyber workforce and a strong workforce pipeline. The region is home to 40,000-plus IT workers. The San Diego Supercomputer Center located on the UCSD campus is one of the nation's leading academic centers involved in high-performance computing, large dataset analysis, and understanding and studying the structure of the Internet. The region's universities and colleges each year teach several thousand computer scientists, computer engineers, and other IT workers the skills to enhance cybersecurity.

There is a robust demand for cybersecurity solutions. The U.S. military has significant cybersecurity assets in San Diego, and the Department of Defense (DoD) recently proposed a five-year cybersecurity budget of more than $23 billion.[5] Firms such as Sempra Energy and Qualcomm have made significant investments in cybersecurity not only to protect critical firm assets but also to serve their customers' requirements for more security technology. A local effort, Securing Our eCity, has drawn attention to the ubiquitous nature of cyber threats and the importance of every individual and business taking action to protect themselves.[6]

---

2. *Disruptive Civil Technologies: Six Technologies with Potential Impacts on US Interests out to 2025*, SRI, Inc., April 2008, http://www.fas.org/irp/nic/disruptive.pdf.
3. *Cyber Security M&A: Decoding Deals in the Global Cyber Security Industry*, PricewaterhouseCoopers, 2011, http://www.pwc.com/gx/en/aerospace-defence-and-security/publications/cyber-security-mergers-and-acquisitions.jhtml.
4. Bruce V. Bigelow, *San Diego Serves as a Hot-bed for Analytics Tech Cluster*, November 13, 2009, Xconomy.com, http://www.idanalytics.com/assets/pdf/Xconomy-San-Diego-Serves-as-a-Hotbed-for-Analytics-Tech-Cluster-11-13-09.pdf.
5. Tony Capaccio, "Pentagon Five-Year Cybersecurity Plan Seeks $23 Billion," Bloomberg.com, June 10, 2013, http://www.bloomberg.com/news/2013-06-10/pentagon-five-year-cybersecurity-plan-seeks-23-billion.html.
6. Securing Our eCity Foundation, http://securingourecity.org/.

This report seeks to catalog San Diego's strengths and assets as a region poised to benefit from the increase in cybersecurity investment. It also seeks to answer the following questions:

1) How big is the cybersecurity industry in San Diego County (how many firms, how many jobs) and what is its overall economic impact on the region? (Part 1)
2) What is the industry outlook, and what are the perceived challenges and perceived benefits of doing business in San Diego? (Part 2)
3) What economic development strategies could the region adopt to grow this industry? (Part 3)

PART I: Measuring the Size and Economic Impact of Cybersecurity in San Diego County

This report defines San Diego's cybersecurity industry as comprising 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 and that sell their products and services to customers external to the immediate organization. The firms may be exclusively focused on cybersecurity, or that function may be one business line that they offer. Services include specific software solutions, system-monitoring services, hardware solutions that complement a customer's IT infrastructure, and cybersecurity consulting services.[7] The customers these firms serve are located all over the world, and when they sell products and services to customers outside of San Diego, cybersecurity firms bring new dollars into the region, fueling regional economic growth and activity.

There are at least two other key parts of the San Diego cybersecurity ecosystem that bear mentioning but that are not part of this study. First, there are several thousand IT workers who have an understanding of cyber threats and cybersecurity and who use this understanding and knowledge as **part** of their overall support for internal and external customers. These workers range from generalists supporting the IT needs of nontechnology firms to highly specialized software engineers who need to understand cyber threats and cybersecurity to adequately design and deliver solutions.

Table 1 shows occupations and employment in the San Diego metro area that are related to IT and that could have job responsibilities that entail understanding cybersecurity threats and solutions.

7. The principal exceptions to this definition are a handful of public-sector entities, such as the Navy's Space and Naval Warfare Systems Command, that provide cybersecurity services to internal customers within the Navy. We have decided to include these entities in our definition and data because of their relatively large size in San Diego and when the cyber professionals they employ are concentrated in a distinct and definable entity like SPAWAR rather than diffusely spread throughout an organization or IT department.

Table 1. Selected Occupational Data for Certain Information-Technology Professions, San Diego–Carlsbad Metropolitan Statistical Area

Occupation (Standard Occupational Code)	**Employment, May 2012**	**Annual mean wage ($)**
Computer and Information Systems Managers (113021)	3,790	136,280
Computer and Information Research Scientists (151111)	930	94,150
Computer Systems Analysts (151121)	4,450	84,850
Information Security Analysts (151122)	610	91,990
Computer Programmers (151131)	4,190	77,290
Software Developers, Applications (151132)	7,410	96,610
Software Developers, Systems Software (151133)	7,150	109,900
Web Developers (151134)	1,420	57,710
Database Administrators (151141)	930	83,160
Network and Computer Systems Administrators (151142)	4,030	78,340
Computer Network Architects (151143)	1,130	107,940
Computer User Support Specialists (151151)	5,370	47,820
Computer Network Support Specialists (151152)	1,320	63,220
Computer Occupations, All Other (151199)	2,200	87,050
Total	44,930	88,850

As table 1 shows, San Diego has a significant IT workforce that constitutes roughly 4 percent of the region's private-sector workforce and that earns wages far above the overall private-sector annual mean wage in 2012 of $52,800. We chose, however, to exclude from our analysis the IT workers that do not specialize in cybersecurity. It would be data intensive to try to survey a representative sample of these workers to accurately measure what proportion of their time is spent on cybersecurity activities and to determine how this proportion varied across job titles and industry groupings. Given the rapid changes occurring in the field, any such data would be quickly outdated and require frequent updating using the same labor-intensive survey methodology. Instead, readers of this report should understand that the 40,000-plus IT workers in the region provide additional assets to cybersecurity firms in the region through both depth of skills and breadth of industry experience.

We also chose to exclude a second group from this study: firms and organizations that are engaged in business pursuits very different than software development or cybersecurity services but that employ cybersecurity professionals because of how important dealing with cyber threats is to their functionality. It is true that this group of workers is of significant size. The growing scope and danger from cyber threats means that companies involved in activities far removed from cybersecurity have to pay an increasing amount of attention to cyber threats.

For example, Sempra places an extremely high priority on cybersecurity as part of its overall commitment to ensuring reliable and safe utility service to the region.[8]

In some cases, cybersecurity is foundational to the entity's basic ability to carry out business. It would be impossible for Intuit, one of San Diego's leading software employers, to provide tax-preparation services and software to customers if its networks were not secure and customers' personal financial information could be easily compromised. And Qualcomm's processors must be resilient to cyber threats and disruptions to be of use to its customers in the wireless industry. Every single one of San Diego's defense contractors has to invest significantly in cybersecurity to protect sensitive information and to ensure the operability of various systems and components. Indeed, throughout San Diego's economy, there are myriad firms whose principle product is in a non-cybersecurity area but whose ability to remain in business demands an extremely vigilant approach toward cyber threats.

Yet, while this "embedded" workforce is an important component of San Diego's cybersecurity economy, measuring its size would be extremely difficult. We know of no research that has attempted to ascertain how cybersecurity activities and investments vary across different industry categories. Even if such an estimate were possible, there remains the task of determining whether the firm is carrying out its cybersecurity work in-house or seeking outside vendors to provide these services. Measuring this aspect of a cybereconomy would require researchers to carry out surveys involving hundreds, if not thousands, of different companies, with the additional difficulty of reaching the right manager within these firms to discuss specific issues related to cybersecurity. Because of these limitations, we have decided, for the most part, to exclude "embedded" cybersecurity workers from this study and to focus on those firms that sell cybersecurity solutions to external customers. We make exceptions for a handful of firms where cybersecurity is so embedded in the core deliverable that it is meaningless to try to disaggregate the two and where the firm is relatively large (100-plus employees).[9]

A. Measuring the Size of the Cybersecurity Industry in San Diego County

In this study, we estimated the size of the industry by a census of known cybersecurity firms.[10] We began by compiling numerous databases and directories of firms in San Diego

8 . See, for example, *Sempra Energy Utilities Response, NIST RFI – Cyber Security Framework*, April 8, 2013, http://csrc.nist.gov/cyberframework/rfi_comments/040813_sempra_energy.pdf.

9. For example, and as noted later, we chose to include a significant portion of ViaSat's employment in our cybersecurity employment. That firm develops secure satellite communication networks. See http://www.viasat.com/company/about/about-viasat.

10. Many studies of regional economies make use of a system of classifying businesses called the North American Industry Classification System (NAICS). Numerous types of information, such as employment, sales, wages, and the composition of an industry's workforce, are gathered and collated based upon these categories. First introduced in 1997, the system employs a six-digit code at its most detailed level. So, for example, NAICS code 541511 refers to the custom computer programming services industry. One serious limitation of the NAICS, and one encountered in this study, is that many industries cut across NAICS categories. While some cybersecurity firms would be classified under code 541511, many firms classified with that code are not cybersecurity enterprises. Likewise, while many cyberfirms use code 541511, many are classified under other codes.

County that had been previously identified as engaging in cybersecurity activities. For example, the CyberMaryland Map contains information about approximately 40 San Diego companies that have opted into this database of self-identified cybersecurity firms.[11] We also added to the database of cybersecurity firms from San Diego State University's Center for Commercialization of Advanced Technology.[12] In addition, we examined several directories of participants at some of the major trade shows, including the 2010 through 2013 attendees to the RSA North America conference and the 2012 and 2013 trade shows of the Information Systems Security Association (ISSA). We also consulted membership directories for ISSA along with past exhibitors catalogued on The Security Network's Web site.

After assembling this database and purging duplicate records, we then conducted Web searches to obtain additional information about firms, including whether they had a physical mailing address in San Diego County and whether they provided cybersecurity products and/or services. We found a number of instances in which firms were actually located in Orange or Riverside counties and a few situations in which the firm was more of a service provider to cybersecurity firms (e.g., recruiters, specialized law firms, public relations agencies) than directly engaged in carrying out cybersecurity work. In some instances, when it was not clear that the Web page had been recently updated or when there was no recent business news about the firm, we made up to three telephone calls to the business to verify that they remained in business and to obtain updated information.

We then used two sources to estimate employment at these firms. The first method relied upon two third-party databases: Dun & Bradstreet and Reference USA. Both of these databases canvass employers on a regular basis to obtain information such as the number of employees that work at a firm and the contact information of key C-level executives. In cases where there was a wide discrepancy among data sources, we called the firm directly to confirm employment information. In cases where the variance was less than 50 percent, we took the average between the two numbers. We also directly called some firms to obtain up-to-date information about the number of employees at their San Diego locations. For firms with a wide variety of products and services, we asked them to provide information about just the employees who spend a majority of their time supporting cybersecurity product lines and services.

We also utilized confirmed data from the San Diego Association of Governments using undisclosed California state Employment Development Department information derived from employers' unemployment insurance filings. This dataset allowed us to confirm our estimates and ensure overall accuracy.

As we have likely overlooked some firms, our estimate should be considered a floor for cybersecurity employment in the region. Employment is likely to be somewhat higher, though we are confident that we identified most of the largest firms meeting the definition of a

---

Because of such limitations, an NAICS-based approach would be of limited utility in measuring the size of the San Diego cybersecurity industry. We would either cast too wide or too narrow a net.

11. The CyberMaryland Map, http://www.cybermarylandmap.com/map.

12. Center for Commercialization of Advanced Technology

cybersecurity enterprise. **A census of known cybersecurity firms in San Diego County yielded an estimated employment of 3,550 workers at 102 firms in the region.**

In addition to these civilian workers, another important part of the cybersecurity landscape for San Diego resides at United States Navy Space and Naval Warfare Systems Command (SPAWAR). SPAWAR is a command within the Navy that provides advanced IT and cybersecurity solutions to the fleet. A large part of the organization's responsibility is detecting and combating cyber threats, which is of vital importance to fleet readiness and war-fighting effectiveness. Presently, SPAWAR employs 4,588 individuals (4,302 Government Civilians, 286 Active Duty Military) in San Diego County, and SPAWAR estimates that 67 percent of its headcount is directly or indirectly engaged in cybersecurity activities. Table 2 shows our estimate of San Diego's total cybersecurity employment for 2012.

Table 2. San Diego Cybersecurity Employment, 2012

Sector	Employment
Private Sector	3,550
SPAWAR	3,095
TOTAL	**6,645**

Table 2 should be understood as setting an absolute floor for cyber employment in the region. As noted previously, our study does not include cybersecurity employees embedded within private-sector firms selling non-cybersecurity products and services. It does not include public-sector entities other than SPAWAR. Finally, given the methodology used, it is likely that we missed a handful of small enterprises that are not well known or that are so new as to not be included in the data sources we consulted.

One limitation of this approach is that it makes comparisons to other regions problematic. Some regions do not have robust intraindustry networks and hence they do not have databases as well developed as San Diego's. Our approach is also time consuming, requiring hundreds of phone calls to firms to obtain information.

B. The Overall Economic Impact of Cybersecurity in San Diego

The cybersecurity industry's impact is greater than its direct employment. As cybersecurity firms buy supplies and services from other firms in the region and as their employees spend wages, these firms have an indirect, positive economic impact on the region.

Economists can estimate these impacts using what are referred to as "input-output models." By using known data about the kinds of services and supplies businesses procure as well as information about consumer spending, it is possible to estimate how an initial input impacts an economy. In this project, we used IMPLAN, one of the most widely used input-output models for studying regional economic impacts. One of IMPLAN's biggest advantages is that by tailoring the model to region-specific data, researchers can obtain a more accurate

understanding of the rate at which economic activity "leaks" out of a region and how differences in wages and salaries between different regions have varying economic impact.

Using the estimated private-sector employment of 3,550, we modeled cyber employment by using three of IMPLAN's industry codes: other computer and related services (code 373); management, scientific, and technical consulting services (code 374), and scientific, research and development services (code 376). We also estimated the economic impact of the 3,095 cyber security employees that work for SPAWAR. In making these estimates, we used updated payroll information to more finely calibrate the IMPLAN model. Table 3 shows our findings.

Table 3. Impact Summary: San Diego Cybersecurity Industry's Economic Impact

Impact Type	Employment	Value Added ($ millions)
Private Sector:		
Direct Effect	3,550	$502.1
Indirect/Induced Effect	3,539	307.4
Total Effect	7,089	809.5
Multiplier	2.00	1.61
SPAWAR:		
Direct Effect	3,095	$437.8
Indirect/Induced Effect	3,085	268.0
Total Effect	6,180	705.8
Multiplier	2.00	1.61

Source: IMPLAN; National University System Institute for Policy Research

This total economic impact of greater than 13,200 jobs is significant. It is equivalent to 3.3 times the economic impact of hosting a Super Bowl and 8.5 times greater than the estimated annual economic impact of Comic-Con.

PART II: Opportunities and Challenges for San Diego's Cybersecurity Industry

A. Methodology and Surveys

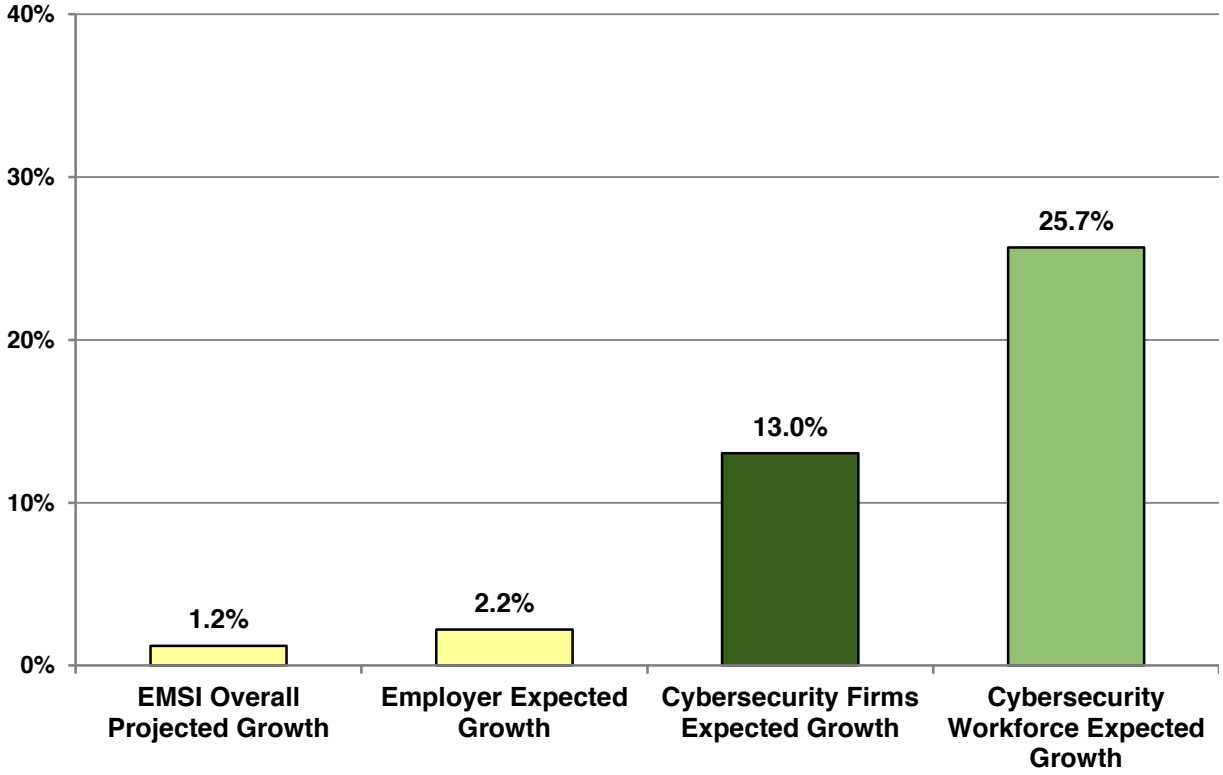
To understand the strengths and weaknesses of the industry, the research team first conducted a survey of both known and unknown cybersecurity firms. This survey instrument (see appendix A) had multiple objectives, including (1) identifying the region's core economic development strengths and weaknesses as they relate to this industry, (2) measuring the size of the cybersecurity workforce, (3) cataloging the workforce skills required by San Diego's cybersecurity firms, and (4) forecasting the likelihood that the industry would contract or grow in the short term.

Two groups of firms constituted our "universe." First, we used the census discussed in the prior section to assemble a set of "known" cybersecurity firms. From November 2013 through January 2014, we placed several calls to these firms, making an extra effort to collect information and opinions from them, as we believed they were the region's largest. We had a success rate of approximately 26 percent in reaching these firms. Second, we surveyed a broader universe of firms. We identified these in a two-step process. First, we used BLS data to identify by North American Industry Classification System (NAICS) code the industries with the greatest concentration of information security analysts (Standard Occupational Code 15-1179). We selected three NAICS codes: 5415 (computer system design and related services), 5416 (management, scientific and technical consulting services) and 5417 (scientific research and development services). We called a stratified sample of large and small firms in this group with a screening question (see appendix A) used to identify cybersecurity firms from other IT providers. We contacted a total of 390 firms, with approximately 3.3 percent being cybersecurity firms not previously identified in our efforts at building a database of known cybersecurity firms.

B. Change in Employment and Forecasted Growth

One of the most important findings is that San Diego County's cybersecurity employers expect to see **considerable growth** in employment over the next 12 months, even while potential issues related to government funding and general economic uncertainty pervade the industry. Figure 1 shows the robust growth expectations by cyber employers for the cyber workforce in comparison to the overall employment-growth expectations in San Diego County.

Figure 1. Employment-Growth Expectations and Projections for the Next 12 Months in San Diego County[13]

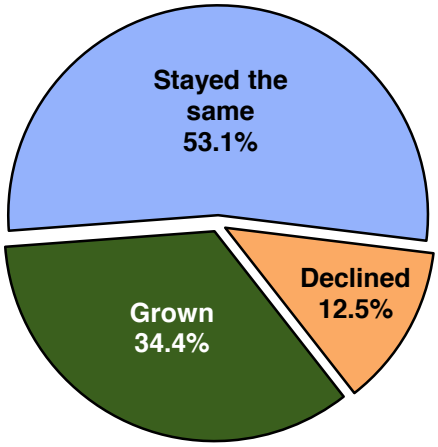


Projected cybersecurity job growth greatly exceeds overall forecasted growth in the San Diego region. While an Economic Modeling Specialists International projection of the San Diego County economy expects to see overall employment growth of just over 1 percent in 2014, NUSIPR forecasts a slightly more robust growth rate of 1.6 percent. A recent survey of San Diego County employers across industries indicated that they expected to grow at just over 2 percent over the second half of 2013 and the first half of 2014.[14] Conversely, cybersecurity employers expect to see their total employment (all employees) grow by over 10 percent and their cybersecurity workforce grow by over 25 percent in a similar time period.[15]

This positive outlook likely reflects the industry's growth over the past three years. When asked about their growth since 2010, as figure 2 shows, cybersecurity businesses surveyed were more than twice as likely to indicate that they had grown in terms of permanent employment (34 percent) rather than declined (13 percent), and they generally were more positive about future growth than about growth in the recent past.

13. We used conservative estimates for cybersecurity growth, with outliers removed from the estimate.
14. BW Research Partnership, *In-Demand Jobs: A Study of the Occupational Outlook in San Diego*, August 2013, http://workforce.org/sites/default/files/pdfs/reports/industry/in-demand_jobs_-_sdwp_-_august_2013_0.pdf.
15. The cybersecurity workforce is defined as those permanent employees that are focused on work related to cybersecurity.

Figure 2. Permanent Employment for the Last Three Years for Cybersecurity Employers



C. Primary Industries and Additional Profile Information

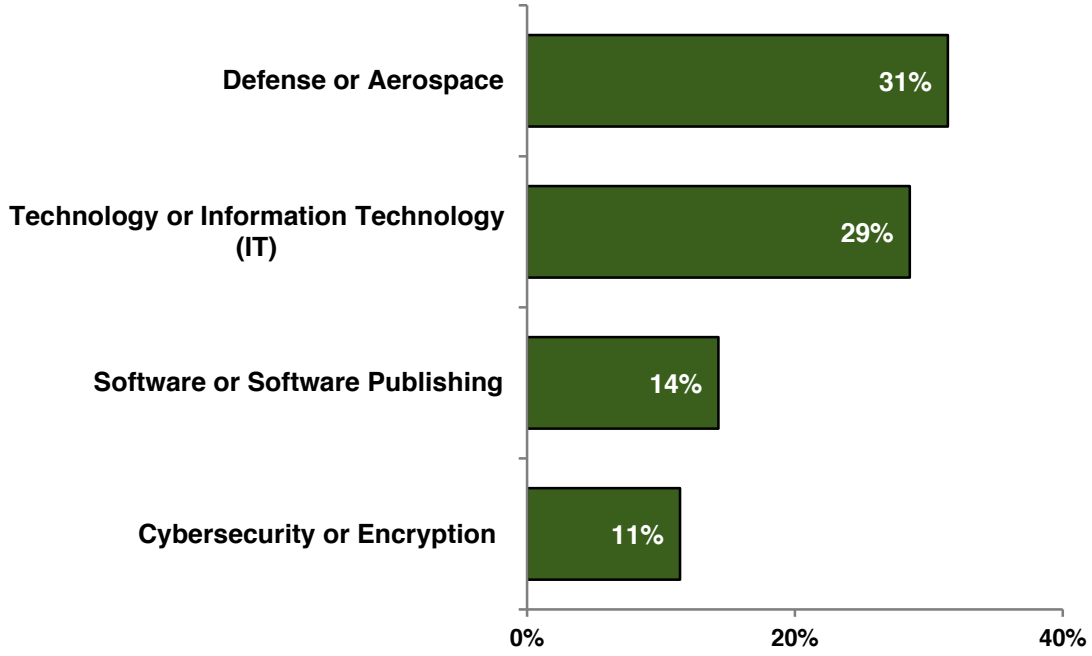
Unlike telecommunications or healthcare firms, cyber employers do not identify themselves consistently within one or even two primary industries. As noted earlier, the current NAICS or Standard Industry Classification (SIC) structures do not have specific industry strata that represent businesses in the cybersecurity industry. Instead, cybersecurity businesses are scattered across traditional industry classifications. In our survey of known firms, most cybersecurity firms in San Diego County fell into the following categories:

- 3341: Computer and electronic product manufacturing
- 3342: Communications equipment manufacturing
- 3364: Aerospace product and parts manufacturing
- 5112: Software publishers
- 5415: Computer systems design and related services
- 5416: Management, scientific and technical consulting services
- 5417: Scientific research and development services

As part of the research process, we analyzed and surveyed businesses in specific industries to find the greatest concentration of cyber employers. We estimate that approximately 7 percent of computer systems design and related services firms (NAICS: 5415) were cyber employers, followed by management, scientific and technical consulting services (NAICS: 5416), with about 3 percent being cyber firms.

When San Diego County cyber employers were asked what industry or industries were most important to their firms, their responses were as varied as their industry classifications. As figure 3 details, defense and/or aerospace was the most cited industry, followed by technology or IT, software, and cybersecurity or encryption. San Diego County's cyber employers can be found in a variety of industries, are differently sized, have been around from one year to over 20 years, and range in size from small start-ups (those with fewer than five employees) to massive multinational corporations (20,000-plus employees).

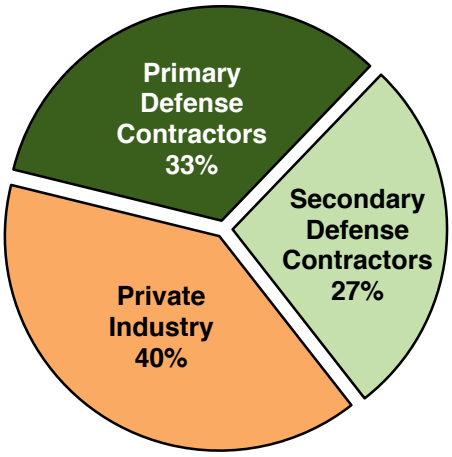
Figure 3. Industries Most Important to San Diego County's Cyber employers



D. Customer Profile

While the types of cybersecurity businesses in San Diego may be varied, the types of customers are not quite as diverse. Over half of all cyber businesses indicated that the federal government, including the DoD, was a customer of their cybersecurity work. Of the 40 percent of San Diego County cyber employers that did not have the federal government as a customer of their cybersecurity work, most (71 percent) were focused on serving private-sector businesses (B2B) or a combination of businesses and consumers (21 percent). Only a small percentage of firms considered consumers their key customers, as figure 4 shows.

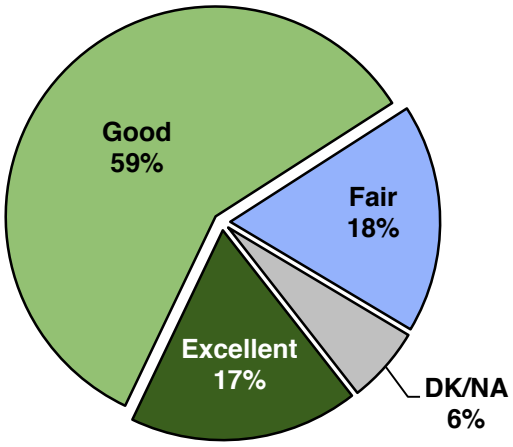
Figure 4. Cyber business Customer Profile



E. Employer's Assessment of San Diego County's Cybersecurity Economy

San Diego's cyber employers generally give the county a good but not excellent rating as a place for cybersecurity firms to do business. As figure 5 shows, no cyber employers surveyed indicated that the county was an overall poor or very poor place to do business. There were as many cyber firms that indicated that the business climate in the county was fair as indicated excellent.

Figure 5. San Diego County Business Climate for Cybersecurity Firms

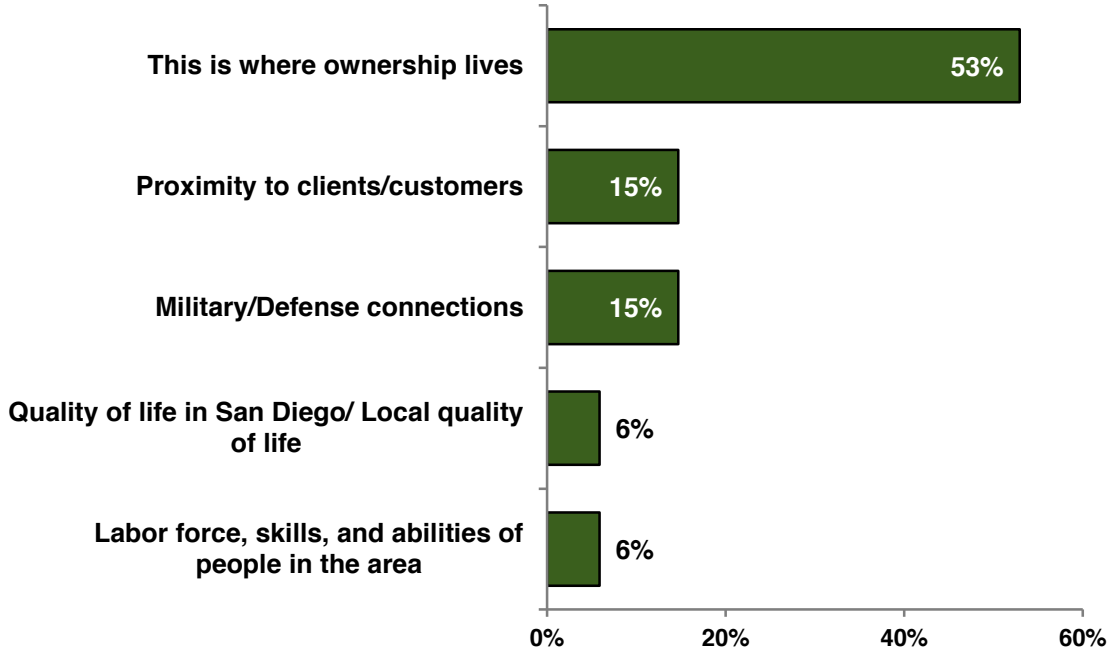


An analysis of cyber employer subgroups reveals that start-ups are generally less positive about the county's business climate for the cyber industry than larger firms are. The analysis of cybersecurity employer subgroups also indicated that those firms whose primary customer was the federal government were generally more positive about the county's business climate than those businesses that either only served the private sector or who saw the federal government as a secondary customer.

F. Primary Reasons for Locating in San Diego County

San Diego County's ability to draw skilled and entrepreneurial individuals, largely driven by its quality of life and considerable military presence, has contributed to the development of cyber employers within the county. As figure 6 displays, having those key entrepreneurs and business owners living in the county, combined with the proximity to customers (including the military), accounts for a large portion of why cyber employers located in the county.

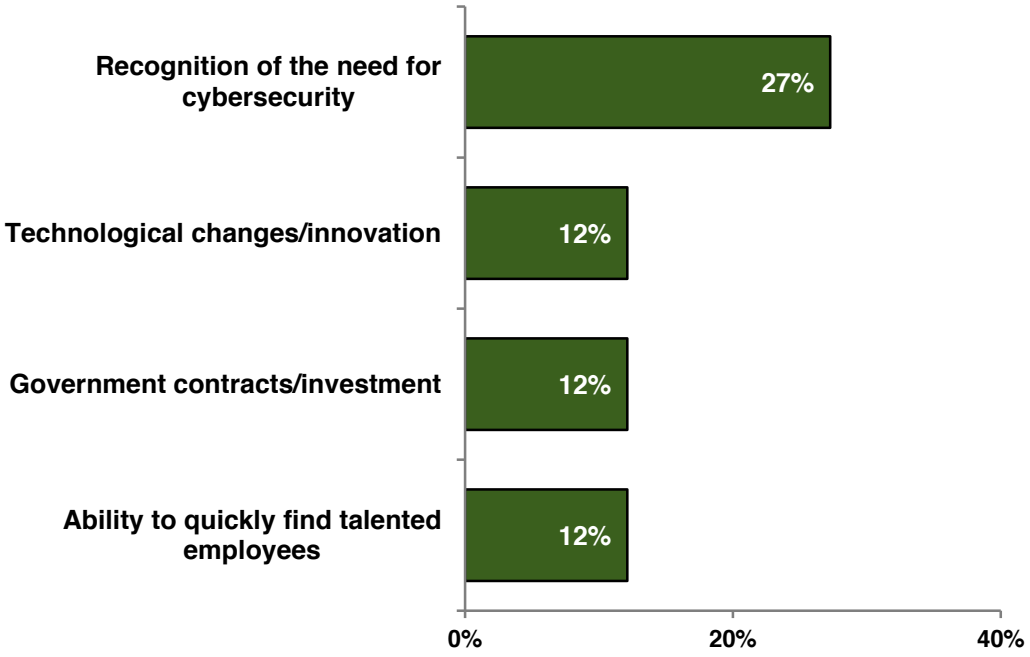
Figure 6. Primary Reasons for Locating in San Diego County



G. Challenges and Drivers of Cybersecurity Business

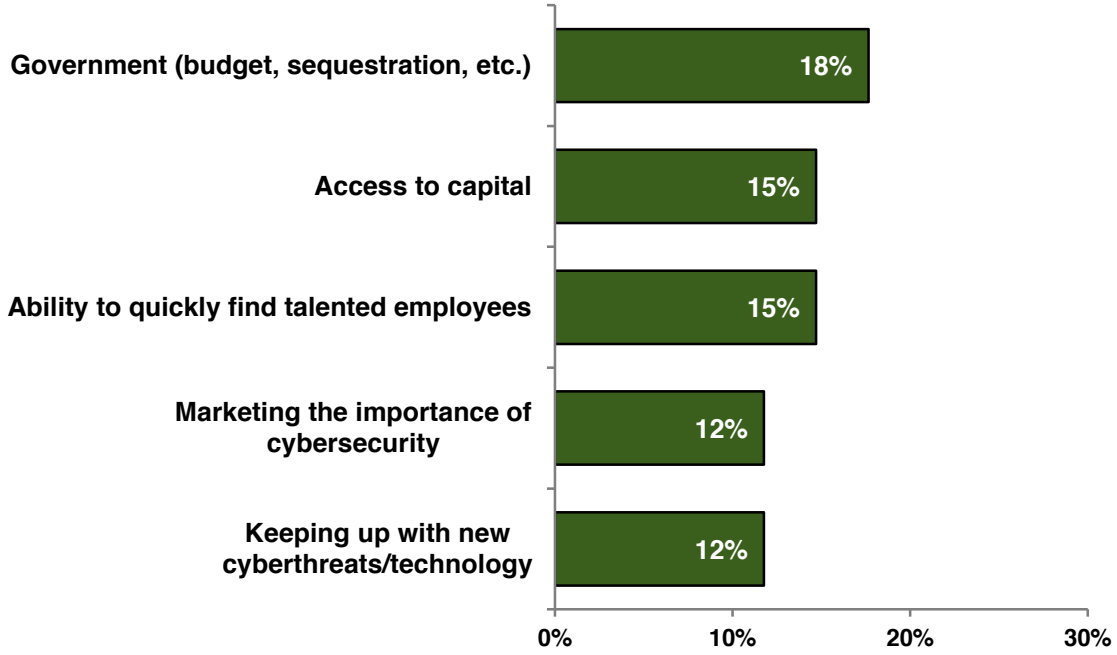
When employers were asked about the key drivers of growth for the cyberindustry, more than 10 percent of respondents identified four issues in response to an open-ended question, as figure 7 illustrates.

Figure 7. Key Drivers of Growth for Cybersecurity



Employers' concerns regarding the cyber industry, also discussed in an open-ended format, varied more. Government funding, access to capital, and talent were the top three concerns of San Diego County's cyber employers. Yet, they still expected to increase total employment by over 10 percent and cyber focused employment by over 25 percent.

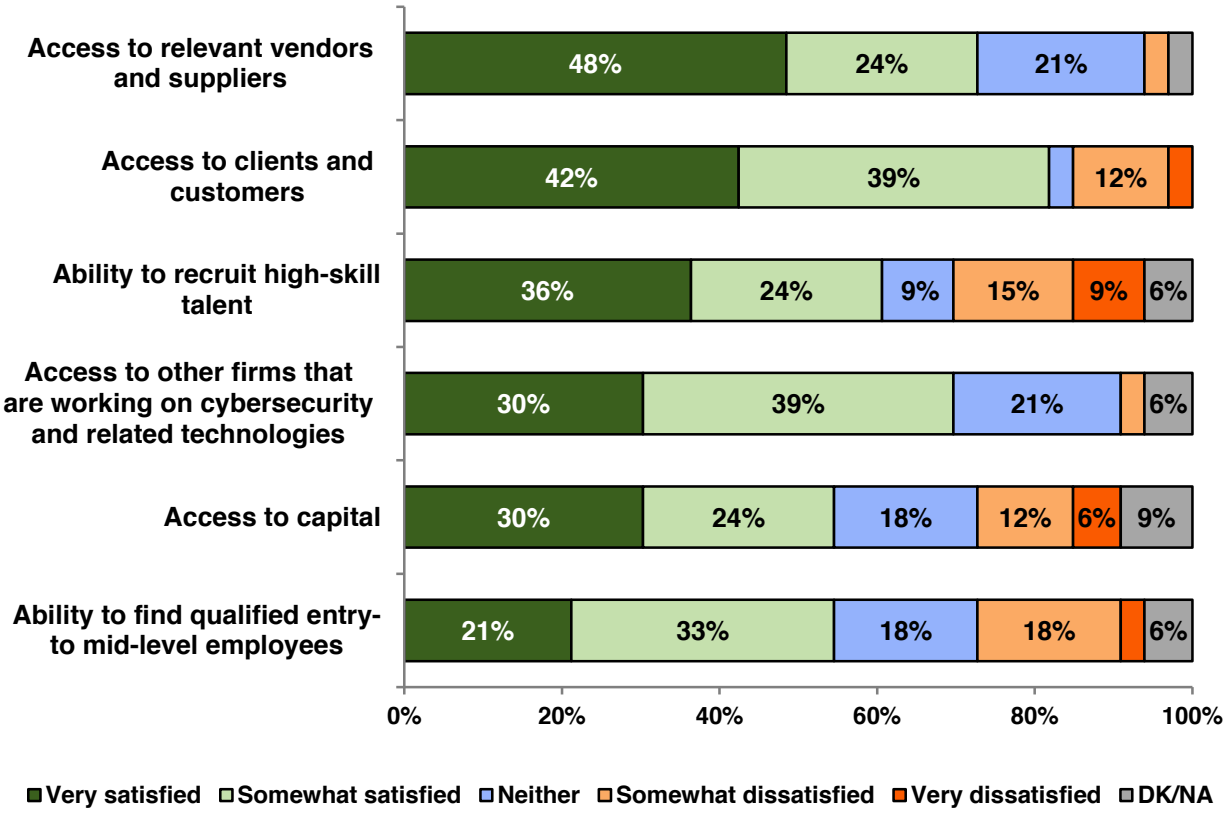
Figure 8. Challenges Facing the Growth of Cybersecurity



H. Key Challenges for San Diego County's Cybersecurity Community

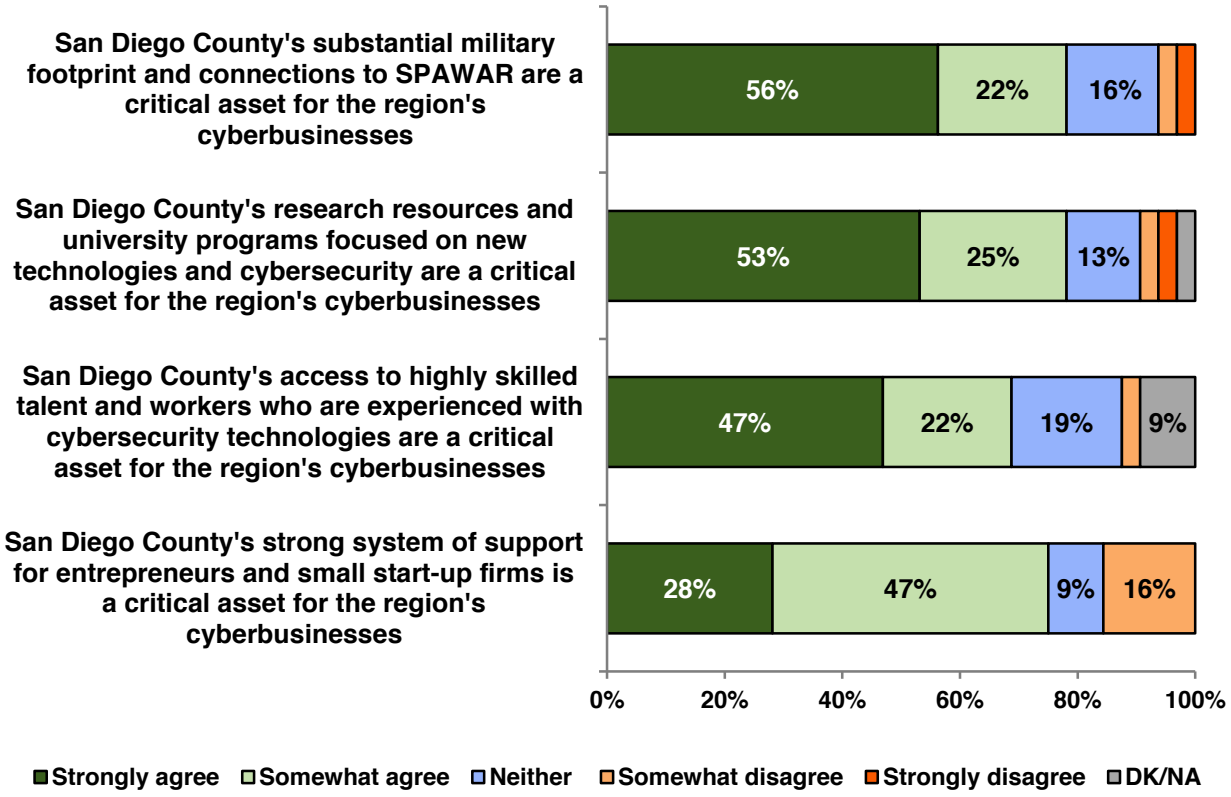
Cyber employers in San Diego County were largely satisfied with their access to vendors and suppliers. They also indicated general satisfaction with access to clients and customers. On issues related to talent and the available workforce, cyber employers were less satisfied, with 60 percent expressing satisfaction with the ability to recruit high-skill talent and just over half (54 percent) satisfied with the ability to find qualified entry to mid-level employees. The relatively low level of satisfaction with the ability to recruit qualified entry to mid-level employees is noteworthy, because in most industry surveys, employers are more likely to be satisfied with their ability to find entry or mid-level employees compared to their ability to recruit highly skilled talent. Figure 9 displays our findings.

Figure 9. Satisfaction with San Diego County's Economic Development Components



San Diego County's cyber employers were asked to rate their level of agreement with four statements regarding the strength of San Diego County's cyber community. A majority of employers agreed either strongly or somewhat with all four statements, but over half strongly agreed with value of the county's military footprint and research resources as critical assets for the region's cyber businesses, while just over a quarter strongly agreed that the county's system of support for entrepreneurs and small start-up businesses was a critical asset for the region's cyber businesses, as figure 10 shows.

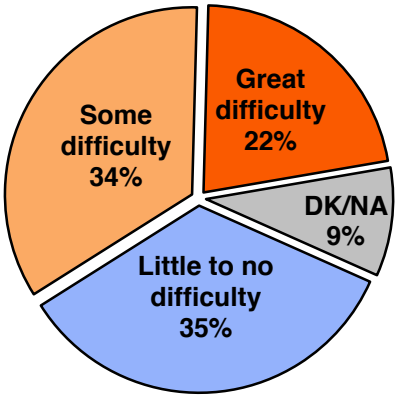
Figure 10. Opinion of San Diego County's Cyber strengths



I. Cybersecurity Workforce Assessment for San Diego County

Over half of cyber employers indicated that they had either some difficulty (34 percent) or great difficulty (22 percent) finding qualified applicants who meet the organization's hiring standards for their cybersecurity positions, as figure 11 shows. An analysis of cyber employer subgroups reveals that medium and large firms (those with five or more employees) were considerably more likely to indicate difficulty finding qualified employees compared to smaller start-ups (those with fewer than five employees). Also, those cyber businesses whose primary customer is the federal government and/or the DoD are having more difficulty finding qualified applicants than those cyber firms that serve the private sector or that have the federal government and/or the DoD as a secondary customer.

Figure 11. Cybersecurity Employers' Difficulties Finding Qualified Employees

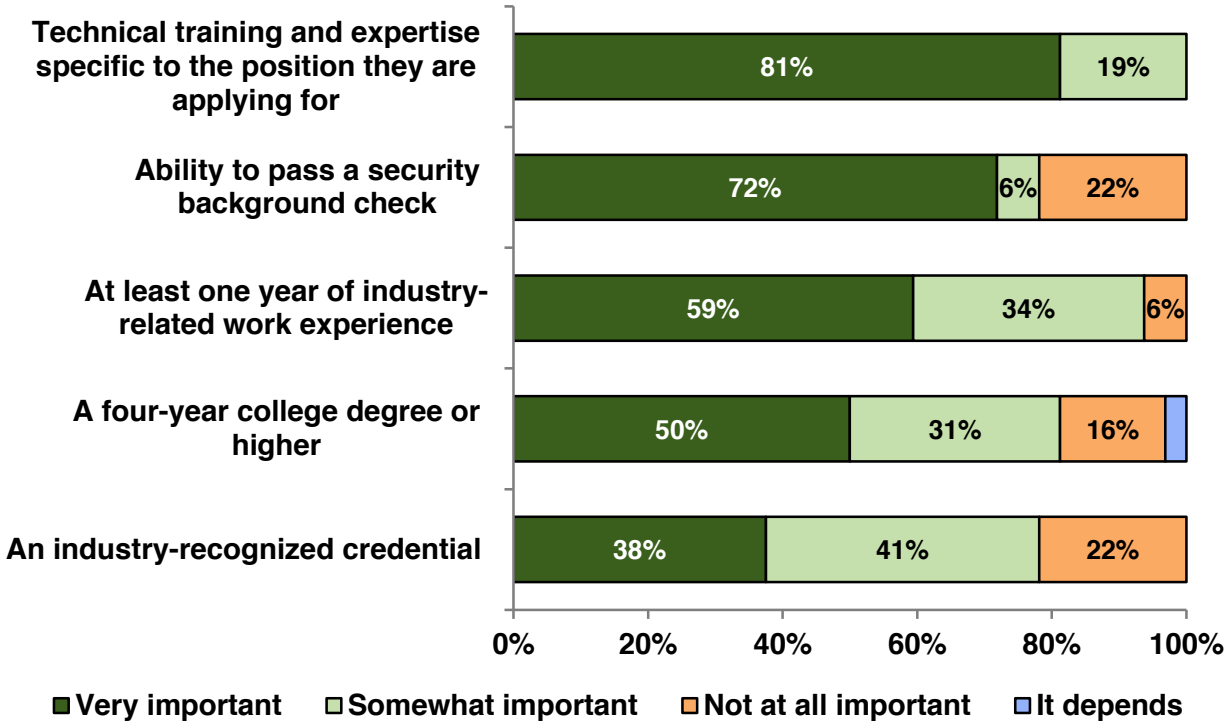


The entry and mid-level cyber positions that San Diego County employers are looking to fill can be categorized into four general groups.

- **Technical developer positions**: These occupations require the ability to program and develop new systems and processes to support the client or employer's data-security objectives. These positions include occupational titles such as information security engineer, software engineer (security and encryption emphasis), and security software developer. These positions typically require at least a four-year degree.
- **Security analyst and quality assurance positions:** These occupations require the ability to evaluate and test systems and processes to ensure they meet regulatory and security requirements. These positions include occupational titles such as information assurance specialist and cybersecurity analyst.
- **Sales and customer service positions**: These occupations require the ability to describe and estimate the abilities and costs of different cybersecurity products and services, as well as the ability to problem-solve for customers. These positions include occupational titles such as sales engineer and customer service representatives at cyber employers.
- **Technical support and cyber implementation positions**: These occupations require the ability to install and maintain cyber products and services within a given network. These positions include occupational titles such as security systems technician and network security engineer.

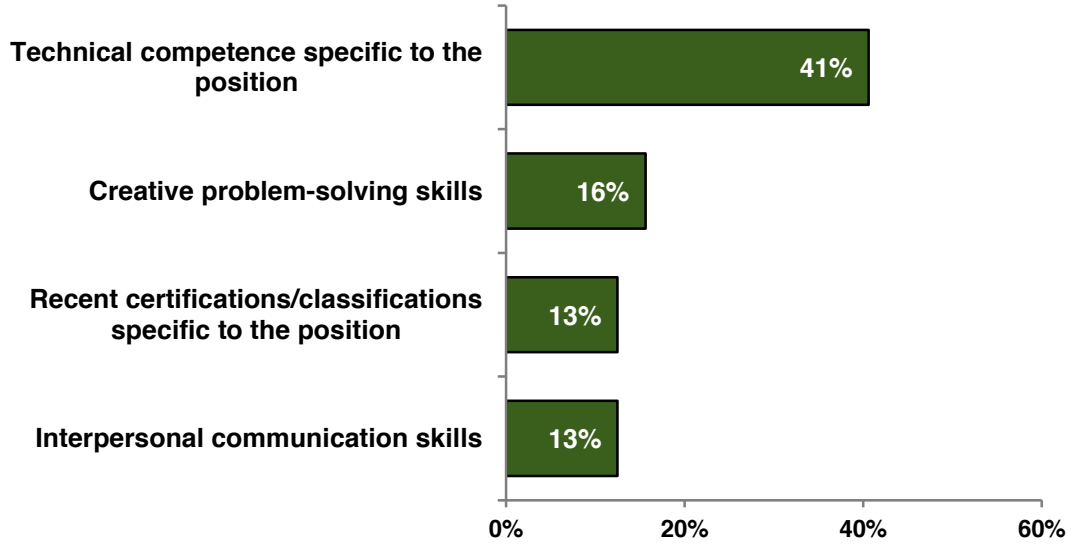
We asked San Diego County's cyber employers about the importance of different attributes for job candidates. Technical training and expertise specific to the position was the most important of the five attributes tested, as figure 12 shows, followed closely by the ability to pass a security background check and industry-related work experience. Even though a four-year degree or higher ranked fourth in importance of the five attributes that were tested, half of employers indicated that a four-year degree or higher was very important and another 31 percent said it was at least somewhat important.

Figure 12. Cybersecurity Workforce Priorities



Unlike other technology-related industries that are emphasizing broader skills beyond technical expertise, cyber employers are keenly focused on technical expertise. Whether this expertise is programming in the relevant computer languages, familiarity with information assurance certifications and accreditation processes, or experience with the DoD's host-based security systems, San Diego cyber employers are looking for employees that have these technical skills first and foremost. Figure 13 shows which skills employers indicated recent hires are lacking.

Figure 13. Skill Deficiencies among Recent Hires



PART III. Conclusions and Recommendations for San Diego's Cybersecurity Economy

San Diego is poised to benefit from a probable explosion in demand for cybersecurity solutions. The region already is home to several thousand employees in the industry and serves one of the most important procurers (and developers) of solutions: the federal government. San Diego has a critical mass of existing firms, and some of the issues that have hampered growth in other areas of the IT sector (such as access to capital, support for entrepreneurs, and access to key customers) seem less of an issue in cybersecurity than in some other technology-oriented industries.

That said, our survey data and our analysis of the industry's composition revealed key issues that should interest economic development leaders.

ISSUE 1. Cybersecurity professionals which are embedded in information technology versus those who are specialized.

There is a focus on developing increased cyber literacy among all IT developers as cybersecurity becomes more of an embedded product in an increasingly wired world. IT workers cannot ignore these issues nor fail to be conversant in key cybersecurity issues. However, because of the significant role that the DoD's cyber demands play in the region, there is also a need for very specialized cybersecurity developers. These two needs are not in conflict, but they are not necessarily complementary. To grow the industry, there may be a need for two tracks of training, one that is embedded within a broader set of IT training efforts and one that is increasingly specialized.

ISSUE 2. Success and growth of cybersecurity are largely tied to the federal government.

Our survey showed just how critical the DoD is to the local cybersecurity industry. Unlike the San Francisco Bay Area, cybersecurity in San Diego is generally not focused on the consumer or business-to-business market. Specifically, the U.S. Navy Space and Naval Warfare Systems Command directly employs nearly half of all the cyber security jobs in San Diego and its presence in San Diego is a contributing factor for many cyber companies to remain located in San Diego. This fact presents both promise and peril to the industry. On the one hand, the DoD appreciates the role that cyber threats and cybersecurity play in the modern world and has made addressing these threats a key priority. Even in the face of tremendous budget pressures and sequestration, the FY15 President's Budget listed cyber security as one of the largest growth areas. San Diego is well positioned to benefit from that emphasis, and the rosy outlook by many firms in the industry seems to reflect a similar estimation. Yet, political challenges abound in Washington along with longer-term financial constraints and challenges

ISSUE 3. Talent is a key ingredient and potential obstacle for growth.

Cybersecurity employers identified the importance of talent in growing their businesses, but also indicated difficulty in finding qualified candidates, particularly at the entry and mid-level positions. This situation is somewhat different from that of many San Diego technology industries, which often express optimism about finding entry-level talent but anxiety about finding higher-level talent. Difficulties in finding entry and mid-level talent raise important questions for future research about educational capacity, recruitment strategies, and any unique considerations regarding immigration and security clearances given the importance of defense work for so many of the region's cybersecurity firms.

ISSUE 4. Technical expertise is critical to employees looking to work for firms that primarily have the federal government and the DoD as their customers.

The greater information- and communications-technology employer community has recently expressed the need for a workforce with broader nontechnical skills such as communication skills, the ability to work in a team, and the ability to innovate and grow with a firm.[16] San Diego County's cyber employers have largely bucked that trend and are focused on the technical skills associated with the positions they are hiring for. Employers are looking for individuals that have specific experience with particular software applications and programming languages and also want experienced professionals who have used the systems that are often required when doing work for the DoD.

We believe the emphasis on technical skills is largely driven by the reality that three out of five San Diego County cyber businesses have the DoD as either a primary or secondary customer, and the DoD's requirements are technically demanding and specific. SPAWAR's presence in San Diego is the driving factor in this highly technical employment requirement. The unique environment of operating securely across the globe, in space, above, on and below the world's oceans requires a highly developed and specialized skill set. The emphasis on technical skills is also likely a function of the evolving nature of cybersecurity and the demands to constantly remain one step ahead of hackers and cybercriminals. As San Diego County's cyber businesses expand and see a larger proportion of non-DoD-related customers, the need for workers with a broader nontechnical skill set is likely to follow.

16. See NOVA Workforce Board and BW Research Partnership, *Silicon Valley in Transition: Economic and Workforce Implications in the Age of iPads, Android Apps, and the Social Web*, July 2011, http://www.work2future.biz/images/documents/TechStudyFullReport_03.pdf.

APPENDIX A
SURVEY AND TOP LINES

SDREDC, NUSIPR & SANDAG

Cyber Security Employer Survey (n=35)

December 2013
Preliminary Toplines

[bw] RESEARCH PARTNERSHIP

2725 JEFFERSON STREET, SUITE 13, CARLSBAD CA 92008
50 MILL POND DRIVE, WRENTHAM, MA 02093
T (760) 730-9325 F (888) 457-9598

bwresearch.com
twitter.com/BW_Research
facebook.com/bwresearch

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 **San Diego Regional Economic Development Corporation** who would value your participation in a brief survey about San Diego County's economic needs and opportunities.

(If needed): The survey should take approximately ten minutes of your time. By answering this survey, you can help us better serve San Diego's technology businesses.

(If needed): The surveys are being conducted by BW Research, an independent research organization.

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

Screener Questions

SCREENER A

For this survey, please 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 code of your current location? (If needed: This is the location where you are physically located).

100%	I am answering for my business location in zip: _____
0%	(DON'T READ) Refused [TERMINATE]

[PHONE – CHECK DATABASE OF COMPLETES AND END SURVEY IF ALREADY HAVE ONE FOR THAT SAME COMPANY IN THE ZIP CODE GIVEN]

SECTION 1 - Organization-Related Questions

Q1

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

[IF UNABLE TO PROVIDE NUMBER, OFFER INTERVALS]

Total Employees	Mean	Median
389	11.11	4.00

Breakdown:

51%	Fewer than 5
14%	Between 5 and 9
23%	Between 10 and 24
6%	Between 25 and 49
6%	Between 50 and 99

Q2 If you currently have [TAKE Q1 #] full-time and part-time permanent employees at your location, how many more or less employees do you expect to have at your location 12 months from now?

Breakdown:

69%	More
3%	Fewer
20%	Same number of permanent employees
9%	Don't know/ Refused

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

	Current	12 months
n	32	32
Mean	10.38	12.63
Median	4.00	8.00
Total Employees	332	404
Change		72
% Growth		**22%**

w/outliers removed*	Current	12 months
n	29	29
Mean	11.10	12.55
Median	4.00	6.00
Total Employees	322	364
Change		42
% Growth		**13%**

***removes three firms that expected to grow by 10 permanent employees (keeps firm expecting to lose 20 employees)**

[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.

SECTION 2 – Industry, Technology and Work Profile

Q3 Now I would like to ask about the industries that are most important to your firm.

What industry or industries best describe the work that your firm is most connected to? (DO NOT READ, ALLOW MORE THAN ONE RESPONSE)

31%	Defense or Aerospace
29%	Technology or Information Technology (IT)
14%	Software or Non-Cyber Security Software Publishing
11%	Cyber Security or Security or Encryption for Information
9%	Professional and Technical Services
9%	Life Sciences
6%	Utility or Energy
3%	Telecommunications or Telecom, including Wireless Communication
3%	Information Technology Hardware Development
9%	Other – *No single category over three percent*
0%	Don't know/ Refused

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].

Q4 What portion of the work done from this location is focused on cyber security? (ACCEPT FIRST RESPONSE)

[REPEAT CATEGORIES AS NEEDED]

17%	All of it - it is the only thing we focus on at this location (100%)
31%	It is the primary focus of this location (50% to 99%)
17%	It is a secondary focus of this location (25% to 49%)
26%	It is a minor part of what we do at this location (1% to 24%)
6%	Do not do any of it from this location
3%	(DON'T READ) DK/NA

[IF Q4="All of it" THEN SKIP TO Q7]

Q5 If you currently have [TAKE Q1 #] full-time and part-time permanent employees at your location, how many of these employees are focused on work related to cyber security work? (n=28)

[IF UNABLE TO PROVIDE NUMBER OFFER INTERVALS]

Percentages among the 28 respondents that said cyber security was not the only focus at their current location

Total Employees	Mean	Median
147	5.25	2.00

Breakdown:

41%	1 or 2
24%	Between 3 and 10
10%	Between 11 and 24
7%	Between 25 and 99
14%	No permanent cyber security employees
3%	(DON'T READ) DK/NA

Q6 If you currently have [TAKE Q5 #] full-time and part-time permanent employees at your location who are focused on work related to cyber security, how many more or less cyber security employees do you expect to have at your location 12 months from now? (n=34)

Breakdown:

50%	More
0%	Fewer
43%	Same number of permanent employees
7%	Don't know/ Refused

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

	Current	12 months
n	26	26
Mean	4.46	5.96
Median	1.50	2.50
Total Employees	116	155
Change		39
% Growth		**34%**

w/outliers removed*	Current	12 months
n	25	25
Mean	4.52	5.68
Median	1.00	2.00
Total Employees	113	142
Change		42
% Growth		**26%**

***removes one firm that expected to grow by 10 permanent cyber security employees**

Q7a Does your firm do cyber security work directly or indirectly for the Federal government, including the Department of Defense.

59%	Yes
38%	No
3%	Don't know/ Refused

Q7b Is the cyber security work you do for the federal government the primary focus of your firm's cyber security work?. (n=20)

55%	Yes
45%	No

[SKIP TO Q9 IF Q7="Yes and it is the primary focus of our firm"]

Q8 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=14)

Percentages among the 14 respondents that indicated that work for the Federal government, including the Department of Defense, was not the primary focus of their firm (Small sample size – caution generalizing the results)

71%	Primarily businesses or B2B
0%	Primarily consumers directly
21%	A combination of both businesses and consumers
7%	(DON'T READ) DK/NA

PART 3 - Location and Overall Rating for Economic Development

Q9 Next I want to ask about your location in San Diego County.

How long has your company been located in San Diego County? (n=34)

6%	Less than 3 years
35%	Between 3 and 5 years
21%	Between 6 and 10 years
38%	More than 10 years

[IF Q9>"3 years" ASK Q10, OTHERWISE SKIP TO Q11]

Q10 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? (n=32)

Percentages among the 32 respondents that indicated their company had been located in San Diego County for three years or more

34%	Grown
53%	Stayed the same
13%	Declined

Q11 Now thinking about San Diego County, how would you rate San Diego County as a place for cyber security firms to do business? (n=34)

18%	Excellent
59%	Good
18%	Fair
0%	Poor
0%	Very poor
6%	(DON'T READ) DK/NA

Q12 [For each "Poor" or "Very Poor" ask:] What are your biggest frustrations with doing business in San Diego County as a cyber-security firm?

N/A

Q13 Thinking big picture, what were the primary reasons your firm located in San Diego County? [DO NOT READ: ALLOW MULTIPLE RESPONSE]

53%	This is where ownership lives
15%	Military/Defense connections
15%	Proximity to clients/customers
6%	Labor force, skills and abilities of people in the area
6%	Quality of life in San Diego / local quality of life
3%	Near Customers
12%	Other – *No single category over three percent*
3%	(DON'T READ) DK/NA

Q14 What are the biggest challenges for the growth of your firm in cyber security? [DO NOT READ: ALLOW MULTIPLE RESPONSE] (n=34)

18%	Government (budget, sequestration, etc.)
15%	Speed and ability to find talented people - talent
15%	Access to capital
12%	Keeping up with new cyber threats/technology
12%	Marketing the inportance of cyber security
9%	Domestic competition
9%	International competition
3%	Regulations and requirements
12%	Other – *No single category over three percent*
12%	(DON'T READ) DK/NA

Q15 What are the key drivers of growth for your firm in cyber security? [DO NOT READ: ALLOW MULTIPLE RESPONSE] (n=33)

27%	Recognition of the need for cyber security
12%	Speed and ability to find talented people
12%	Government contracts/investment
12%	Technological changes/innovation
6%	The economy
6%	Increased threats to cyber security
3%	Strong quality of life
3%	Proximity to clients/customers
3%	Close to large markets in a small town feel
15%	Other – *No single category over three percent*
9%	(DON'T READ) DK/NA

Please tell me how satisfied your company is with the following issues and attributes regarding the business climate in San Diego County.

Q16 Is your company satisfied, dissatisfied, or neither satisfied nor dissatisfied with San Diego's: _____? (GET ANSWER AND THEN ASK:) Would that be very (satisfied/dissatisfied) or somewhat (satisfied/dissatisfied)? (n=33)

RANDOMIZE

	Very satisfied	Somewhat satisfied	Neither sat nor dissat	Somewhat dissat	Very dissat	(DON'T READ) DK/NA
A. Access to capital	30%	24%	18%	12%	6%	9%
B. Access to clients and customers	42%	39%	3%	12%	3%	0%
C. Ability to recruit high skill talent	36%	24%	9%	15%	9%	6%
D. Ability to find qualified entry to mid-level employees	21%	33%	18%	18%	3%	6%
E. Access to relevant vendors and suppliers	48%	24%	21%	3%	0%	3%
F. Access to other firms that are working on cyber security and related technologies	30%	39%	21%	3%	0%	6%

Now I'm going to read a list of statements that describe attitudes or opinions regarding San Diego County as a place to do business for the cyber-security business.

Q17 Here is the (fist/next) one: _____ Do you generally agree, disagree, or neither agree nor disagree with the statement? (GET ANSWER IF AGREE OR DISAGREE ASK:) Would that be strongly (agree/disagree) or somewhat (agree/disagree)? (n=32)

RANDOMIZE

	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree	(DON'T READ) DK/NA
A. San Diego County's research resources and universities programs focused on new technologies and cyber security are a critical asset for the regions cyber businesses	53%	25%	13%	3%	3%	3%
B. San Diego County's substantial military footprint and connections to SPAWAR are a critical asset for the region's cyber businesses	56%	22%	16%	3%	3%	0%
C. San Diego County's strong system of support for entrepreneurs and small start-up firms are a critical asset for the region's cyber businesses	28%	47%	9%	16%	0%	0%
D. San Diego County's access to high skilled talent and workers who are experienced with cyber security technologies are a critical asset for the region's cyber businesses	47%	22%	19%	3%	0%	9%

SECTION 3 – Workforce Development & Skills Assessment

Now I would like to ask about your organization's need for new employees.

Q18 Thinking about the positions related to cyber security you hire at your location, how much difficulty does your company have finding qualified applicants who meet the organization's hiring standards? (n=32)

34%	Little to no difficulty
34%	Some difficulty
22%	Great difficulty
9%	(DON'T READ) DK/NA

Q19 Please tell me how important the following items are when considering candidates for open positions at your firm: very important, somewhat important, or not at all important. (n=32)

RANDOMIZE

	Very important	Somewhat important	Not at all important	(DON'T READ) It depends	(DON'T READ) DK/NA
A. An industry recognized credential	38%	41%	22%	0%	0%
B. At least one year of industry related work experience	59%	34%	6%	0%	0%
C. Ability to pass a security background check	72%	6%	22%	0%	0%
D. A four year college degree or higher	50%	31%	16%	3%	0%
E. Technical training and expertise specific to the position they are applying for	81%	19%	0%	0%	0%

Q20 Thinking in general about recent hires at your organization, which general skills would you say that recent hires tend to be most deficient in? [DO NOT READ - ACCEPT FIRST TWO RESPONSES] (n=32)

41%	Technical competence specific to the position
16%	Creative problem-solving skills
13%	Interpersonal communication skills
13%	Recent certifications/ classifications specific to the position
6%	Ability to work with different groups or departments
6%	Previous experience related to the position
3%	Have not hired entry-level recently
16%	(DON'T READ) DK/NA

Q21 Are there any cyber security related positions at your firm that you expect to hire for in the next 12 months and if yes, could you identify the position(s)?

Verbatim responses to be provided

Q22 Next, I would like to ask about the different technical credentials and their influence in the hiring process for positions in cyber security.

Here's the (first/next) one _____ (READ ITEM): Did this credential positively influence your hiring decision of any employees in the last 12 months? (n=31)

RANDOMIZE

	Yes	Somewhat	No	DK/NA
A. CISSP	45%	10%	42%	3%
B. SSCP	26%	16%	45%	13%
C. CompTIA Security+ Certification	29%	16%	48%	6%
D. Security +	26%	23%	42%	10%

Q23 Are there any other credentials that we have not asked about that are valuable when considering cyber security applicants and if yes, what are they?

Verbatim responses to be provided

Lastly, I'd like to ask you a couple general questions and verify your contact information.

Q24 **SECTION 4 – Permission Questions**

Does your firm have any locations outside of San Diego County? (n=31)

39% Yes
61% No

[IF Q24="Yes" ASK Q25 OTHERWISE SKIP TO Q26]

Q25 What city is your firm headquartered in?

Verbatim responses to be provided

Q26 Would you be willing to be contacted by researchers and/or educators who are developing new strategies and regional plans to support cyber security businesses in San Diego County? (n=31)

55%	Yes
45%	No

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.

Those are all the questions I have.
Thank you very much for your time.

Note: Four respondents dropped off in the course of taking the survey (one after Q5, one after Q14, one after Q16, and one after Q21). A total of 31 respondents completed the entire survey.

SAN DIEGO REGIONAL ECONOMIC DEVELOPMENT CORPORATION

ADDRESS 530 B Street, 7th Floor
San Diego, CA 92101

PHONE 619.234.8484

WEB sandiegobusiness.org

FOR A COPY OF THE COMPLETE REPORT, PLEASE VISIT SANDIEGOBUSINESS.ORG/RESEARCH

AUTHORED BY

[bw] RESEARCH PARTNERSHIP

National University System Institute For Policy Research

servicebureau SANDAG

INDUSTRY PARTNERS

San Diego CYBERHIVE Create Converge Prosper

SDMAC

Securing Our eCITY Foundation

ADVISORY COUNCIL MEMBERS

Andrew Lee | ESET North America

Brian Proctor | San Diego Gas & Electric

Darin Andersen | CyberHive San Diego/CyberUnited

Eric Basu | Sentek Global

Julian Parra | Bank of America Merrill Lynch

Kevin Carroll | CONNECT

Liz Fraumann | Securing Our eCity Foundation

Lou Kelly | SDSU Research Foundation

Matt Harrigan | Critical Assets

Tom Clancy | Software San Diego/TAO Venture Partners

Tony Nufer | Vector Planning & Services Inc.

MILITARY ADVISOR TO THE COUNCIL

Mr. Pat Sullivan | Space and Naval Warfare Systems Command