CYBERSECURITY SKILLS SHORTAGE

Cybersecurity Shortage by the Numbers

1.8 million jobs unfilled worldwide projected by **2022**

35,000 job openings in California, April 2017–March 2018

Cybersecurity job postings have **grown 3x** as fast as IT jobs

$75,000–$100,000 median cybersecurity salary

75% of organizations report understaffed security teams

There are typically not enough workers to fill cybersecurity job openings and these positions often take longer to fill than jobs in other industries.[19] In addition, the workforce gap is expected to worsen in coming years. The results from the 2017 Global Information Security Workforce Study (GISWS) by Frost & Sullivan estimates 1.8 million unfilled cybersecurity jobs globally by 2022, a 20% increase over the forecast made in 2015. The study found that two-thirds of businesses globally do not have enough cybersecurity workers in their organizations to meet the challenges they currently face.[20]

According to an article in Security Magazine, while security budgets are increasing, 59% of information security professionals report unfilled cyber/information security positions within their organizations.[21] As reported by Dark Reading, a separate study found that 75% of organizations report having understaffed security teams and experience difficulty in recruiting qualified job candidates; and nearly the same proportion report that AI and machine learning tools and services have exacerbated their staffing problems because more highly skilled workers are needed.[22]

A 2016 international report by McAfee and the Center for Strategic and International Studies found that the cybersecurity skills shortage does direct and measurable damage, according to 71% of respondents surveyed. According to the report, one in three respondents said a shortage of skills makes their organizations more desirable hacking targets, and one in four reported that "insufficient cybersecurity staff strength damaged their organization's reputation and led directly to the loss of proprietary data through cyberattack."[23]

Finding qualified workers to fill cybersecurity positions is a widespread challenge facing many employers across all industries.

[19] "Hack the Gap: Close the cybersecurity talent gap with interactive tools and data," CyberSeek, accessed May 18, 2018, https://www.cyberseek.org/index.html#about.

[20] "2017 Global Information Security Workforce Study," The Center for Cyber Safety and Education and Frost & Sullivan, 2017, https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf.

[21] "Security Budgets Increasing, But Qualified Cybertalent Remains Hard to Find," Security Magazine, April 23, 2018, accessed May 18, 2017, https://www.securitymagazine.com/articles/88940-security-budgets-increasing-but-qualified-cybertalent-remains-hard-to-find.

[22] Erica Chickowski, "Automation exacerbates cybersecurity skills gap," Dark Reading, May 2, 2018, accessed May 18, 2018, https://www.darkreading.com/careers-and-people/automation-exacerbates-cybersecurity-skills-gap/d/d-id/1331697.

[23] "Hacking the Skills Shortage: A Study of the International Shortage in Cybersecurity Skills," McAfee and the Center for Strategic and International Studies, 2016, accessed May 18, 2018, p. 4, https://www.mcafee.com/uk/resources/reports/rp-hacking-skills-shortage.pdf.

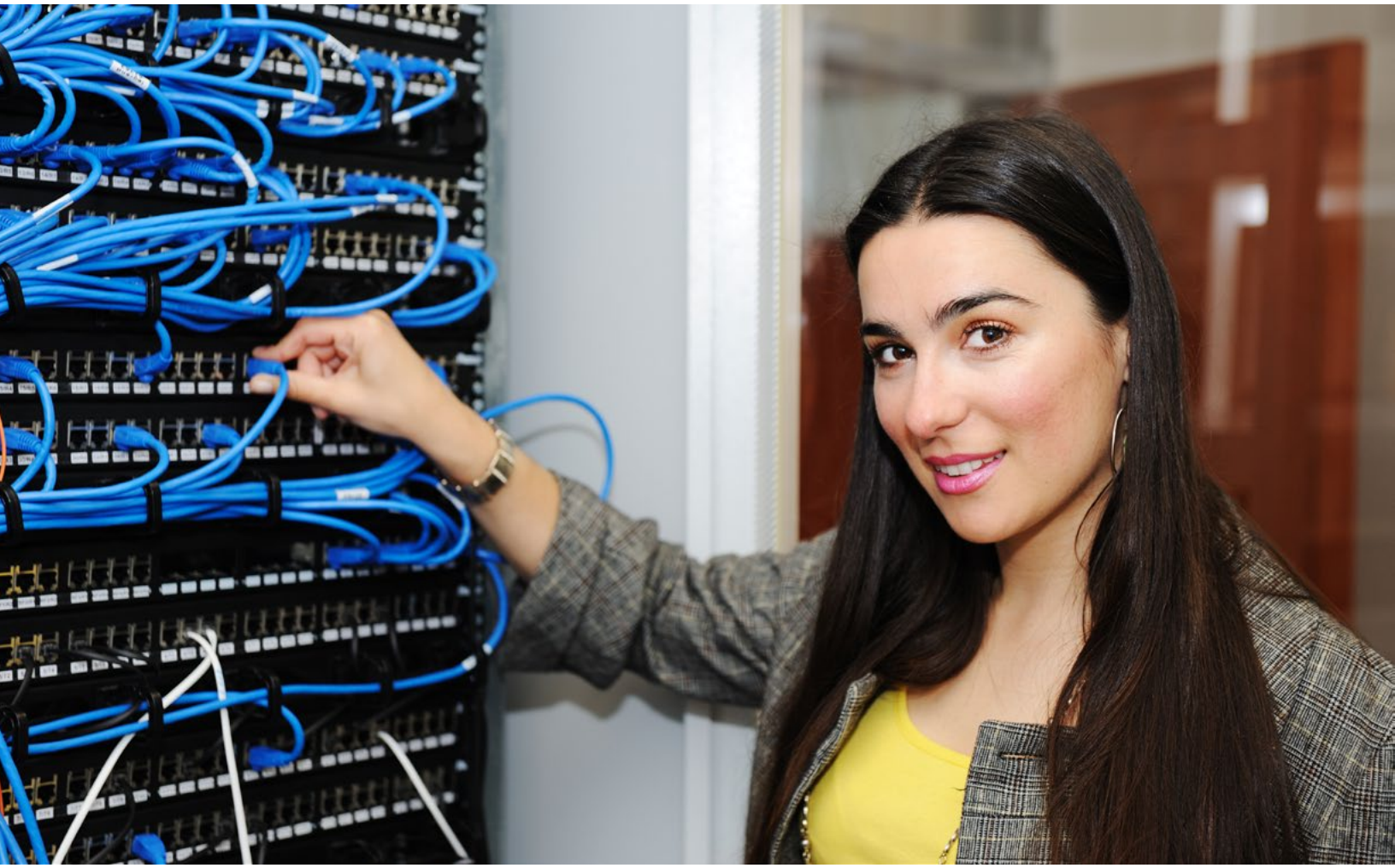
ECONOMIC IMPLICATIONS

According to a study by PwC, investors view cyber threats as the No. 1 threat to business, and think cybersecurity should be a top priority for building trust with customers.[24]

In addition, cyber threats to e-commerce are particularly a concern. Small businesses are big contributors to the economy, but many rely on e-commerce to generate revenue. Perhaps, most alarmingly, CNBC reported in July 2017 that roughly half of the 28 million small businesses in the United States had been breached by hackers, but only 2 percent of small-business owners surveyed viewed cyberattacks as their most critical issue.[25]

The magnitude of the international cybersecurity crisis was captured in this year's World Economic Forum's Global Risks Report. Cyber vulnerabilities ranked fourth in the list of the top five global risks. The soaring number of cyberattacks, particularly those resulting from WannaCry, as well as the number of businesses and institutions affected worldwide and the extreme cost of these attacks contributed to the ranking.

Most significantly, the larger implication of these attacks catapulted cyber vulnerabilities to the top of the list of world risks due the "growing trend of using cyberattacks to target critical infrastructures and strategic industrial sectors, raising fears that, in a worst-case scenario, attackers could trigger a breakdown in the systems that keep societies functioning."[26]



[24] "2018 Global Investor Survey: Anxious Optimism in a Complex World," PwC International Limited, p. 11 and p. 22, https://www.pwc.com/gx/en/ceo-survey/2018/deep-dives/pwc-global-investor-survey-2018.pdf.

[25] Chris Morris, "14 million businesses are at risk of a hacker threat," CNBC, July 25, 2017, accessed May 18, 2018, https://www.cnbc.com/2017/07/25/14-million-us-businesses-are-at-risk-of-a-hacker-threat.html.

[26] Ibid.

CYBERSECURITY WORKFORCE PREPARATION

Because the field of cybersecurity is new and still evolving, there is no standard curriculum nor consensus on standards for training. Cybersecurity studies and training can be included in basic computer courses, and can include specific training in topics such as computer and digital forensics, system vulnerability/penetration testing, system hardening, instruction detection and prevention, reverse malware engineering, and more.

In February 2013, then President Obama signed an executive order calling for a national set of standards, guidelines and practices to help organizations better protect themselves against cyber-attack, and the NICE Framework was developed. Other alternative frameworks are accepted in the field, and there is no consensus or standardization on what constitutes the canon of cybersecurity curriculum or training.

As there is no standardized cybersecurity curriculum, there is also no standard way for a cybersecurity professional to demonstrate qualifications. Various routes include: degrees and certificates issued by postsecondary institutions; industry certifications issued by vendors (e.g., CISCO, CompTIA, Oracle, Juniper/Junos); and other association/organization/governmental/ quasi-governmental sponsored licenses, certifications and credentials. In addition, individuals who win cybersecurity contests are generally considered qualified for employment in the field.

The range in cybersecurity training is vast, from short-term, skills-based credentials to research doctoral degrees and postgraduate certifications. However, industry certifications may have become the de facto standardized measure of cybersecurity skills and competencies as there is no standardized curriculum nor standardized academic credentials. Although there is standardization within industry certification by individual security vendors, there is a lack of standardization across security vendors.

As there is no standardized cybersecurity curriculum, there is also no standard way for a cybersecurity professional to demonstrate qualifications.

According to a study by PwC, **investors view cyber threats as the No. 1 threat to business,** and think cybersecurity should be a top priority for building trust with customers.

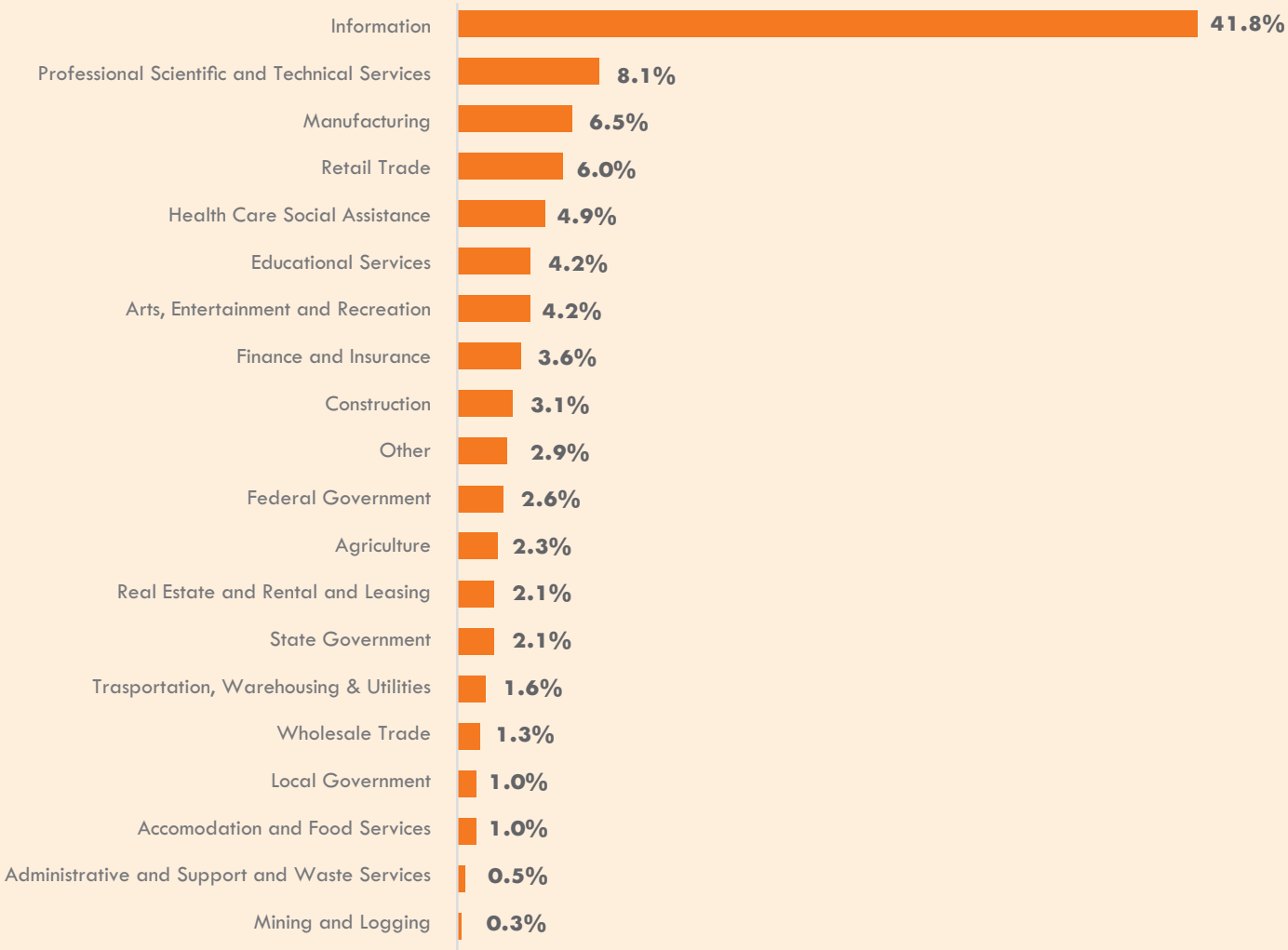
SECTION II: EMPLOYER SURVEY AND WORKFORCE DEMAND ASSESSMENT

SURVEYED EMPLOYER CHARACTERISTICS

Employer survey participants either employ cybersecurity workers or Information Technology/Information Systems (IT/IS) workers who require cybersecurity skills. Overall, there were 385 survey respondents. These survey participants were asked to identify the industry with which their business is most closely associated. About 42% of employers were associated with the information industry (Exhibit 1).

The information industry sector is composed of multiple sub-industries that include information technology, information systems, ISP providers, software publishers, telecommunications and data hosting businesses, all of which have high concentrations of IT/IS workers according to industry staffing patterns.

Exhibit 1. Industries associated with surveyed businesses (n-385)



SURVEYED EMPLOYER CHARACTERISTICS

Exhibit 2 shows the size of the 385 businesses surveyed, based on the number of permanent employees. Nearly 40% of respondents have fewer than 50 employees, while 21% of respondents have 1,000 employees or more, which is consistent with the larger size of businesses found in the information sector.

Exhibit 2. Size of surveyed business by number of employees (n=385)

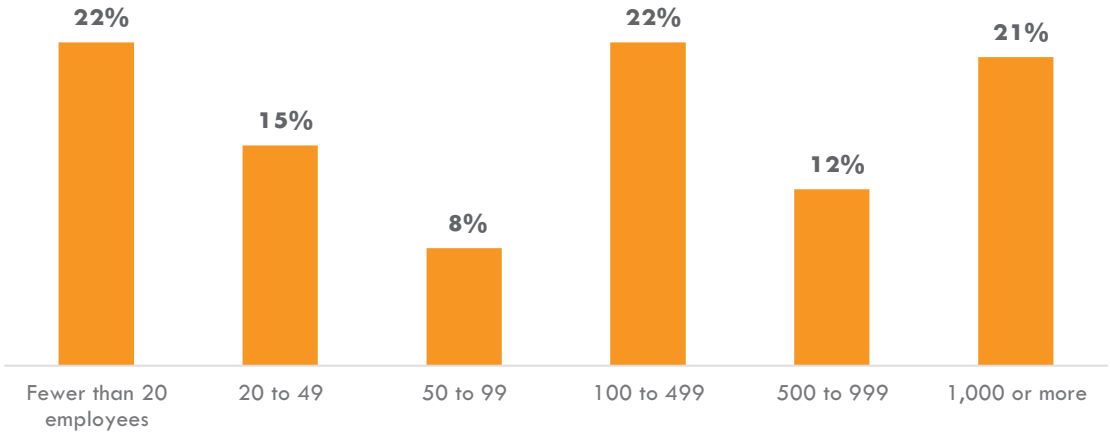
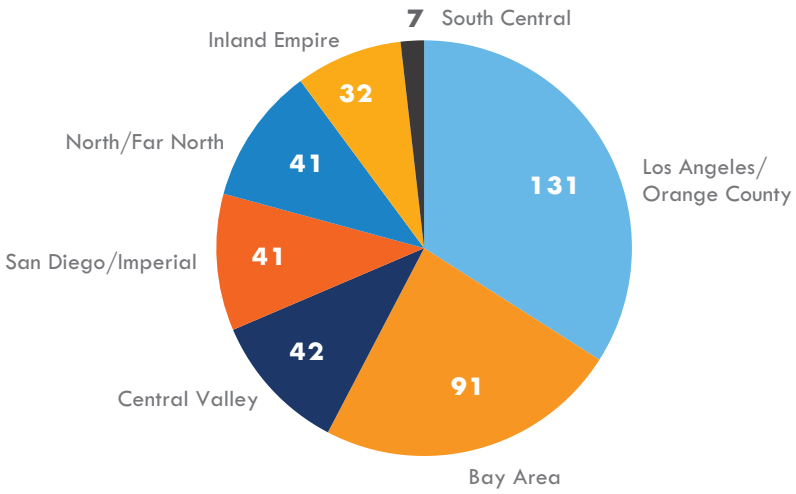


Exhibit 3 shows where the surveyed businesses are located by major geographic region in California. Of the businesses that participated in the survey, 34% were in Los Angeles and Orange counties, and 24% were in the Bay Area, which is consistent with these two regions having large concentrations of businesses that employ cybersecurity and IT/IS workers.

Exhibit 3. Surveyed businesses by region

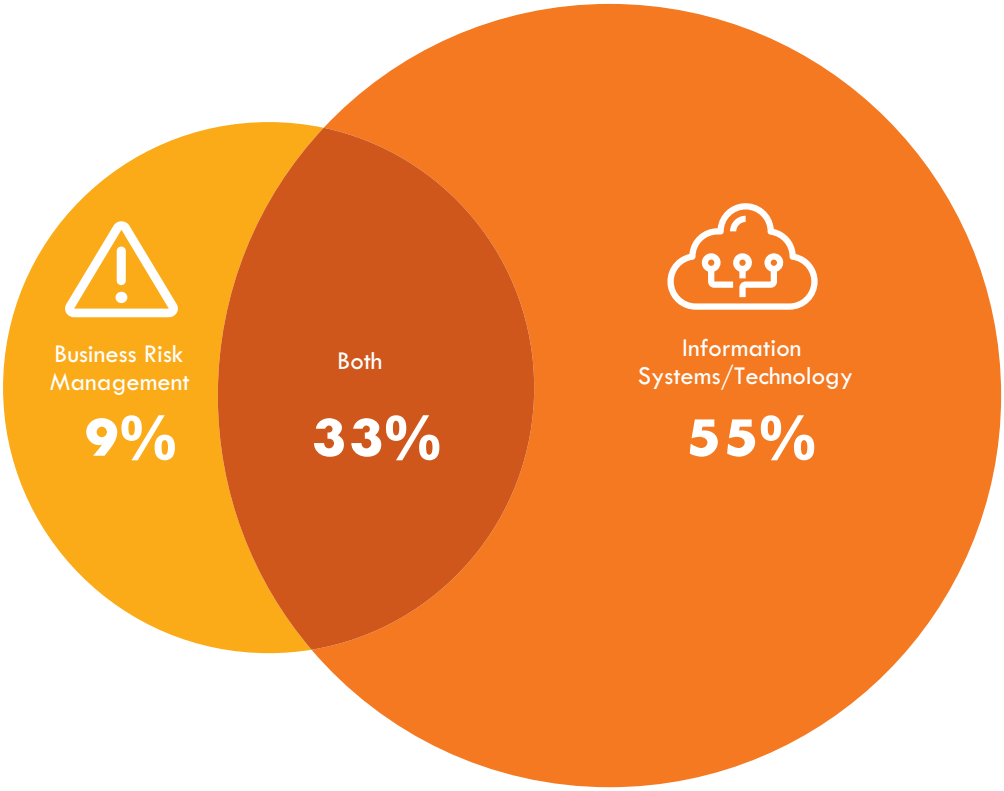


SURVEYED EMPLOYER CHARACTERISTICS

Respondents were asked if their business operates cybersecurity as an information systems or technology function, a business risk management function or both.

As shown in Exhibit 4, 55% of the businesses surveyed indicated they focus on cybersecurity as an information systems/technology function. Just over 33% of businesses operate cybersecurity as both an information systems/technology function and a business risk management function. Only about 9% of businesses operate cybersecurity as a business risk management function.

Exhibit 4. Distribution of surveyed firms in business risk management, IT/IS, or both



There are increasing concerns about whether businesses are sufficiently integrating cybersecurity into all aspects of their operations. To better understand how businesses/organizations are involved with cybersecurity, respondents were asked to indicate if their business is a creator/producer of cybersecurity products; a provider of cybersecurity products and/or services; a user of cybersecurity products and services; or has some other involvement with cybersecurity.

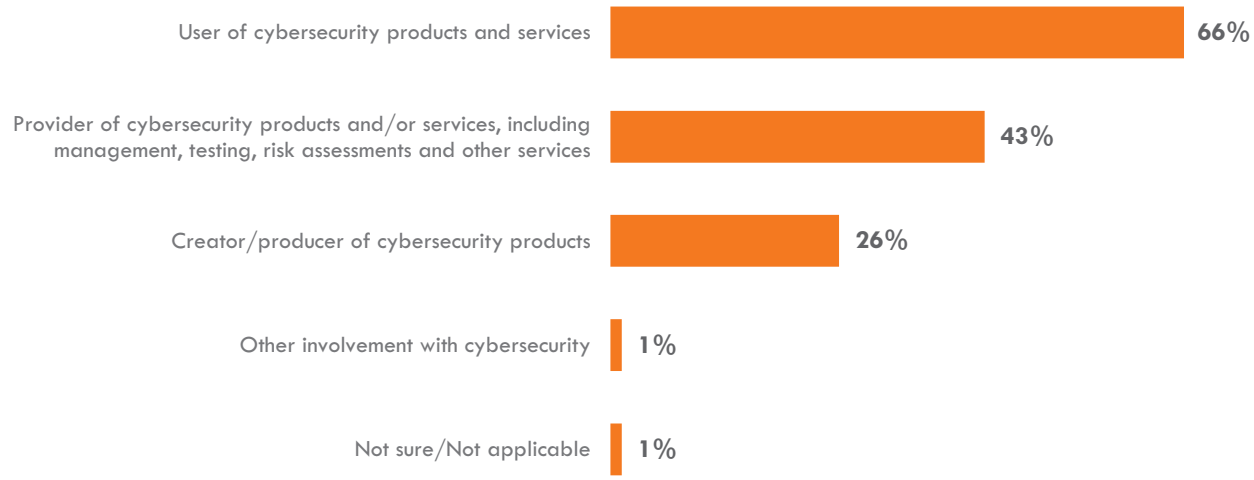
For this question, employers could choose more than one category, which resulted in a total of 530 responses for this question. As shown in Exhibit 5:

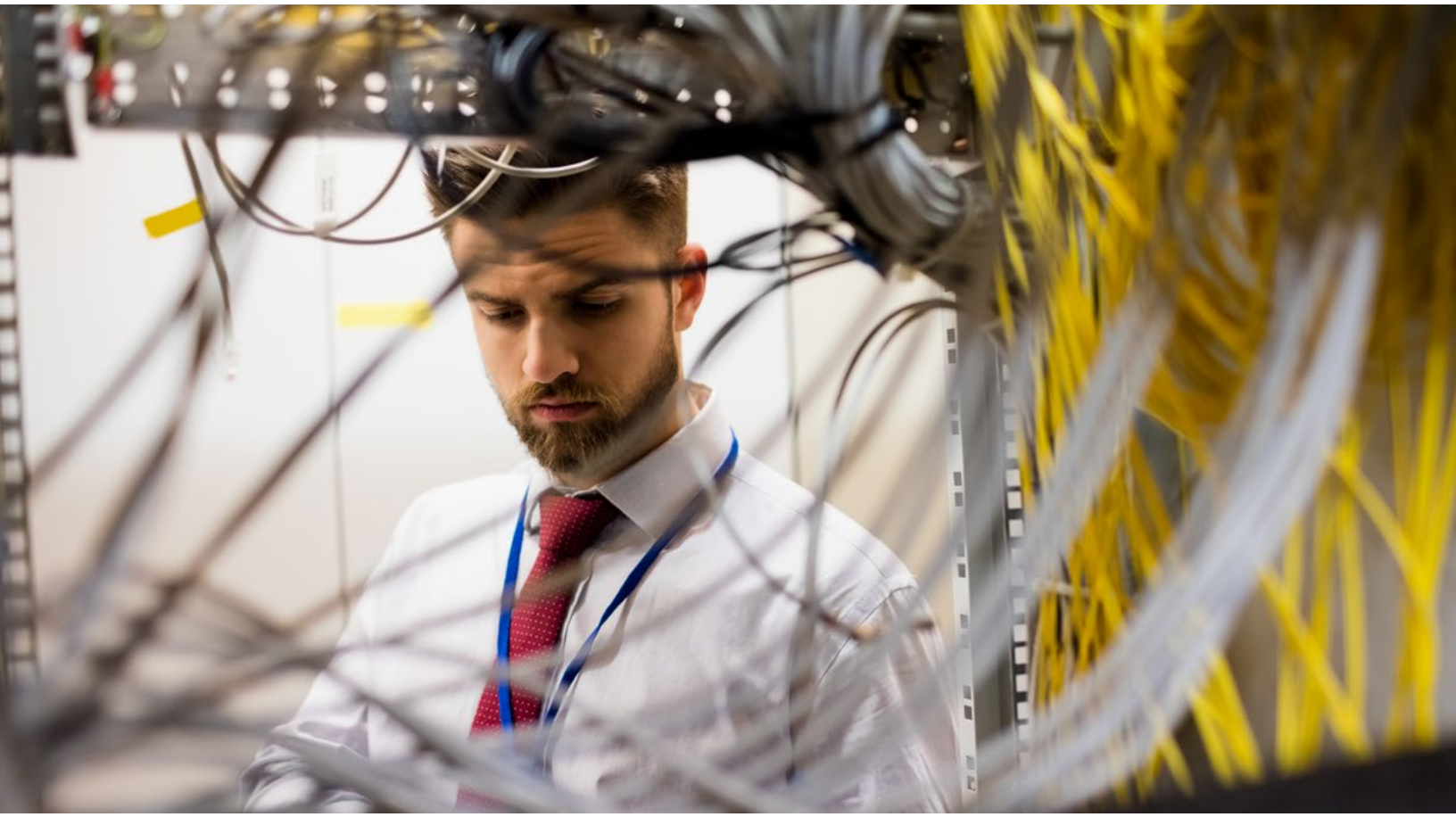
- 66% of respondents indicated they are a user of cybersecurity products and services.
- 43% of respondents indicated they are a provider of cybersecurity products and/or services (including management, testing, risk assessments and other services), and of this group 50% indicated that over half of their business focuses on this.
- 26% indicated they are a creator/producer of cybersecurity products, and of this group 57% indicated that over half of their business focuses on this.

SURVEYED EMPLOYER CHARACTERISTICS

To fulfill an important objective of this study, respondents were asked if their business is a defense contractor (including first, second, third, or fourth tier subcontractor) and 49% of businesses indicated they are a defense contractor. (Data for this sub-group of respondents is included in the next section of the report.) In addition, 43% of respondents indicated their business provides cybersecurity products and/or services to the defense industry (Exhibit 5).

Exhibit 5. How surveyed businesses are involved in cybersecurity (n=385)





WORKFORCE DEMAND FOR NINE WORK ROLES

Specialized Cybersecurity Work Roles

- Systems Security Analyst
- Cyber Defense Analyst
- Cyber Defense Infrastructure Support Specialist
- Vulnerability Assessment Analyst
- Cyber Defense Forensics Analyst

IT/IS Work Roles Requiring Cybersecurity Skills

- Technical Support Specialist
- Network Operations Specialist
- System Administrator
- Software Developer

This section of the report provides survey findings for the nine cybersecurity work roles selected for this study. The work roles include five specialized cybersecurity positions and four IT/IS positions that require cybersecurity skills.

Employers answered a series of questions about the nine work roles, providing information about a number of workforce-related issues and challenges.

Employers completed the survey for the work roles they employ at their business and for no more than three work roles, which kept the survey to a reasonable length of time. (Appendix D: Work Role Profiles contains detailed survey results for each work role.)

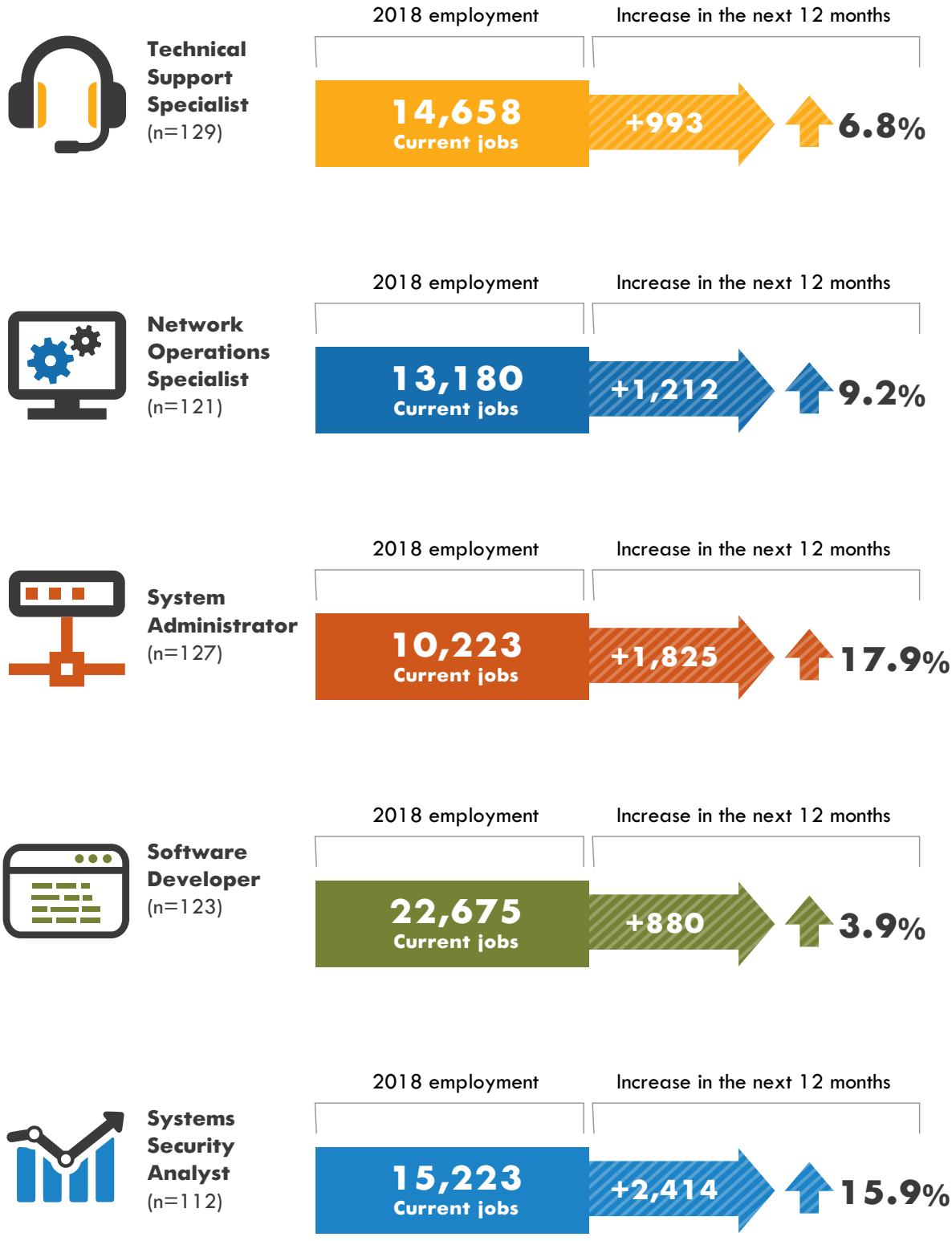
Exhibit 6 shows the current levels of combined permanent and temporary employment and the projected increase in permanent and temporary employment in 12 months, for each of the nine work roles. Notable findings include:

- **Software developer** is the largest work role, with current permanent and temporary employment totaling 22,675 positions.
- **Cyber defense forensic analyst** is the second largest work role with 21,293 positions.
- **System security analyst** is the work role projected to increase employment by the largest amount over the next 12 months, with an increase of 2,414 positions.
- **Cyber defense forensic analyst** is projected to have the second largest increase in the next 12 months, with 2,336 positions.
- **Cyber defense infrastructure support analyst** will have the largest percentage increase in permanent and temporary employment in 12 months, growing by 21.3% and adding 2,146 positions.
- **Systems administrator** is projected to increase employment by 17.9% in 12 months, adding 1,825 positions.

Across the nine work roles, when comparing defense contractors as a sub-group of all employers surveyed, the percentage increase in employment in 12 months is slightly higher. The range is 1% to 2% higher, depending on the work role.

WORKFORCE DEMAND FOR NINE WORK ROLES

Exhibit 6. Current employment and projected occupational demand in 12 months for the nine work roles identified



WORKFORCE DEMAND FOR NINE WORK ROLES

Exhibit 6. Current employment and projected occupational demand in 12 months for the nine work roles identified (continued)