CYBERSECURITY

in Augusta, Georgia

AN IMPACT ASSESSMENT AND WORKFORCE STUDY

JANUARY 2022

PREPARED FOR

AEDA
Augusta Economic Development Authority

AUGUSTA UNIVERSITY

PRODUCED BY

TheMettsGroup

Table of Contents

Advisory Committee

Our appreciation to the Advisory Committee and organizations whose insights made this study possible.

Sam Anderson	Softact Solutions
Todd Boudreau	Liaison of the U.S. Army Cyber Center of Excellence, Fort Gordon
Dave Brendza	ADP
Brian Rhodes	TaxSlayer
Michael Shaffer	Augusta University
Kevin Wade	IntelliSystems
Cal Wray	Augusta Economic Development Authority

Executive Summary

This impact assessment analyzes the current landscape of the cybersecurity industry in Augusta and is intended to provide community leaders a baseline to track growth and support industry needs. It catalogs the region's strengths and assets demonstrating Augusta is an area poised to benefit from the increase in cybersecurity investment.

Cybersecurity is a function of all industries and firms in most every vertical, from banks to healthcare to telecom. Because cybersecurity is so pervasive in nature and spans many industries, this study defines and quantifies the industry's role in a broader network.

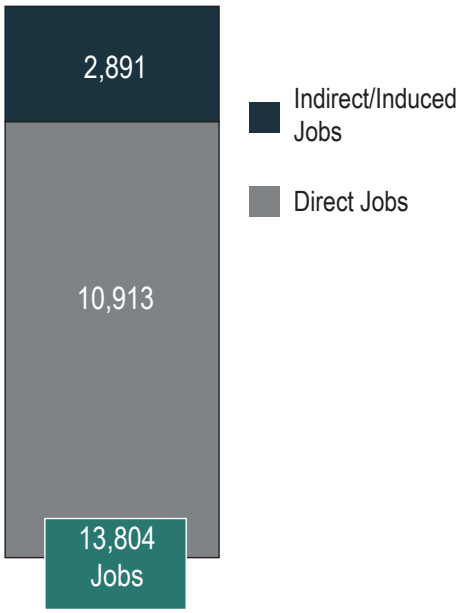
Augusta-Richmond County, GA-SC MSA

The Augusta MSA is prime for cybersecurity firms to do business. Regional partners and industry leaders have done a tremendous job building the ecosystem that currently supports a successful and thriving cybersecurity industry, including building talent pipelines, education and training, facilities, and business support.

As a mid-size city, Augusta stands out as a cybersecurity hub with resources in place and where businesses prosper. Cybersecurity businesses within the identified taxonomy, both private and government, generate approximately $1.9B in total economic impact and contribute $1.4B (directly and indirectly) to Richmond County's overall GDP, over 10% of the County's total GDP.

With an estimated 10,900 employees working directly in the cyber-related industry, Augusta has a substantial cybersecurity workforce for a city of its size. The region has shown significant growth in the cybersecurity industry cluster, growing at an annual rate of 6.1% compared to only 3.7% nationally.

Augusta has created a cybersecurity ecosystem that has proven to be a region for cyber firms to call home.



Introduction

As technology, remote working, and business operations increasingly moved to the cloud; information and network security has become a global issue. Every industry requires some level of cybersecurity to protect its assets as global demand increases. Based on IBM's latest report, the average cost of a global data breach is $3.86 million in 2020. The U.S. has the highest average cost at $8.64 million. This creates strong demand for quality technology solutions. With more ambitious digital initiatives, businesses are changing cyber strategy and investing more.

Georgia is one of the nation's elite cybersecurity hubs, ranking No. 3 in the U.S. for Information Security, according to a recent Technology Association of Georgia report. With many of the state's assets residing in Augusta, it makes the region a prime location for future growth opportunities.

This report analyzes the current landscape of the cybersecurity industry in Augusta and is intended to provide community leaders a baseline to track growth and support industry needs. It catalogs the region's strengths and assets demonstrating Augusta is an area poised to benefit from the increase in cybersecurity investment. It also seeks to answer the following questions:

- How big is the cybersecurity industry and what is its overall economic impact in Richmond County?
- What is the industry outlook in the region, and what are the perceived challenges and perceived benefits of doing business in Augusta?
- What are the primary drivers for attraction and growth of cybersecurity companies?

Methodology

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. Cybersecurity is a function of all industries and firms in almost every vertical, from banks to healthcare to telecom. Because cybersecurity is so pervasive in nature and spans many industries, this study defines and quantifies the industry's role in a broader network.

Therefore, throughout this report, we refer to a taxonomy—a classification of industries—that best defines the cybersecurity industry based on other cyber-rich Metropolitan Statistical Areas (MSA) and defined by the U.S. Census' North American Product Classification System. To measure Richmond County's cybersecurity size and impact, this study uses this taxonomy to quantify the overall impact cybersecurity activity generates across Richmond County and,

Augusta-Richmond County, GA-SC MSA

Methodology Cont'd

ultimately, identifying the supply, demand, and assets of the Augusta MSA (the Augusta-Richmond County, GA-SC). The Augusta MSA is the second-largest metro area in Georgia and includes Richmond, Columbia, Burke, Lincoln, and McDuffie counties in Georgia and Aiken and Edgefield Counties in South Carolina. The taxonomy is listed below in Table 1 and Appendix A of this report.

Table 1: Cybersecurity Taxonomy (industries analyzed in this study)

Computer and Computer Peripheral Equipment and Software Merchant Wholesalers	Administrative Management and General Management Consulting Services
Software Publishers	Other Computer Related Services
Wired Telecommunications Carriers	Marketing Consulting Services
Data Processing, Hosting, and Related Services	Process, Physical Distribution, and Logistics Consulting Services
Custom Computer Programming Services	Other Management Consulting Services
Computer Systems Design Services	Computer and Office Machine Repair and Maintenance
Computer Facilities Management Services	All other Professional, Scientific, and Technical Services
	Investigation and Security Services

A survey was conducted November 2020 - January 2021 and sent to 36 businesses in the Augusta MSA known for their cybersecurity expertise. This was a small sampling of companies that perform cyber-related activities, future surveys will be important to capture such functions and continue to benchmark the industry. The survey examined occupations that their primary functions are in cyber-related activities. Results from the survey provided insights into employer's training needs, where growth will occur, and what the region needs to develop and support cybersecurity needs for Augusta area businesses. Of those surveyed, 42% responded. Highlights from the survey results are summarized in Appendix B and the full results of the survey is provided in Appendix C. Telephone interviews were also conducted to provide context and ground-truth the data presented.

The economic impact analysis of Richmond County for the cybersecurity taxonomy presented in this report was generated by IMPLAN, an economic model that depicts the relationships between industries and firms and their employees. These models are built upon expenditure patterns that are reported to the U.S. Bureau of Labor Statistics, the U.S. Census Bureau, and the U.S. Bureau of Economic Analysis. Data is regionalized so that it reflects and incorporates local conditions such as average wages, expenditure patterns, and resource availability and costs.

This report is intended to serve as a benchmark for future reports and will be used to monitor trends as this report is updated. The research conducted only touches the surface and a deeper dive will be required to better understand how firms relate to the cybersecurity industry.

The Cybersecurity Industry Defined

The cybersecurity industry in Augusta comprises firms and organizations that employ and train cybersecurity professionals. The workforce provides products and services designed to optimize, prevent, recover and protect the internet of things from unintended or unauthorized access or destruction. The industry also enables software applications for predictive and preventative decision-making for response situations. The region's training organizations educate and train cyber professionals in the disciplines of installing, operating, maintaining, and defending the information environment of public, private, and academic domains.

The four domains of cybersecurity include:

1. The physical domain (hardware and software)
2. The information domain (confidentiality, integrity and availability of information)
3. The cognitive domain (how information is perceived and analyzed)
4. The social domain (attention to ethics, social norms and a broad social landscape)

Augusta's Cybersecurity Ecosystem

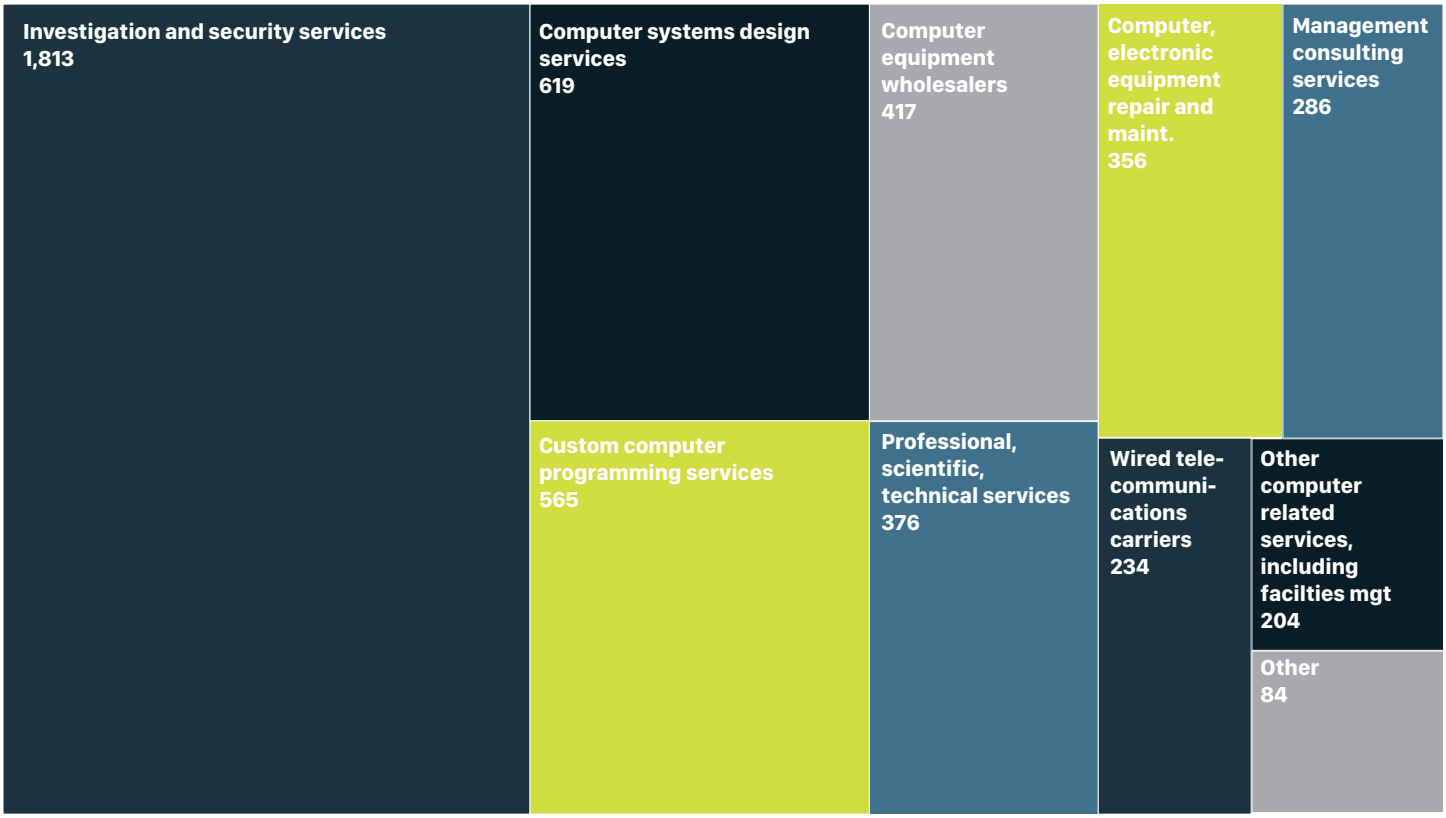
Augusta is prime for cybersecurity firms to do business. Regional partners and industry leaders have done a tremendous job building the ecosystem that currently supports a successful and thriving cybersecurity industry, including building talent pipelines, education and training, facilities, and business support.

Nearly 140 private companies in Richmond County comprise the cybersecurity taxonomy defined for this study, generating an estimated $665 million in output annually. Together, these companies employ nearly 5,000. Figure 1 (page 7) outlines employment by each private industry defined by the cybersecurity taxonomy used as the foundation of this report. The Technology Association of Georgia has 53 confirmed cybersecurity firms in the Augusta MSA that are have been members of the Association. The full list of firms is provided in Appendix D, a few of these companies include:

- Corsica Technologies
- Parsons Corporation
- Cyber Security Solutions, Inc.
- Security Management and Integration
- Assured Information Security (AIS)
- IntelliGenesis, LLC
- RLM Communications
- H2
- Rendition Infosec
- Two Six Labs
- CenCore, LLC
- JANUS Research Group
- Cyber Discovery Group
- Zapata Technology
- the Clubhou.se
- Assured Bridge
- IntelliSystems
- A3 Missions

Augusta's Cybersecurity Ecosystem Cont'd

Figure 1: Private Industry Employment in Cybersecurity (within the taxonomy identified), Richmond County (2020)

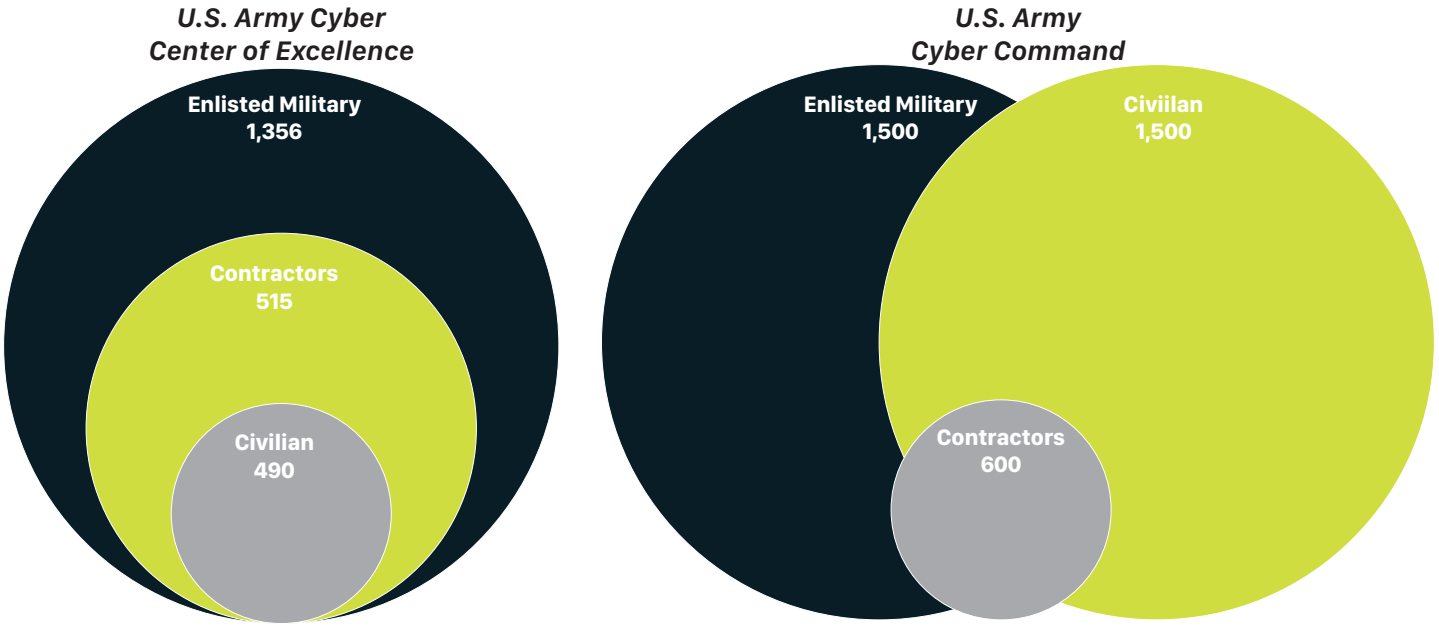


Government facilities are the backbone of Augusta's cybersecurity industry. Augusta is home to the National Security Agency/Central Security Service (NSA/CSS-GA)—one of four U.S. cryptologic centers located outside of the headquarters in Maryland. In 2013, the Pentagon announced that the U.S. Army Cyber Command would relocate from Fort Meade in Maryland to Fort Gordon in Augusta which has fueled cyber talent and industry growth in the region. Over 2,300 people are employed at the U.S. Army Cyber Center of Excellence and another 3,600 are employed with U.S. Army Cyber Command. A breakdown of employment by these two Army units is shown in Figure 2 (page 8).

Augusta's Cybersecurity Ecosystem Cont'd

Figure 2: US Army Employment in Cybersecurity, Fort Gordon (2021)

Source: U.S. Army Cyber School, June 2021



The single largest investment in a cybersecurity facility by a state government is located in Augusta. The $100 million Georgia Cyber Center is a unique public/private partnership involving academia, government, and the private sector.

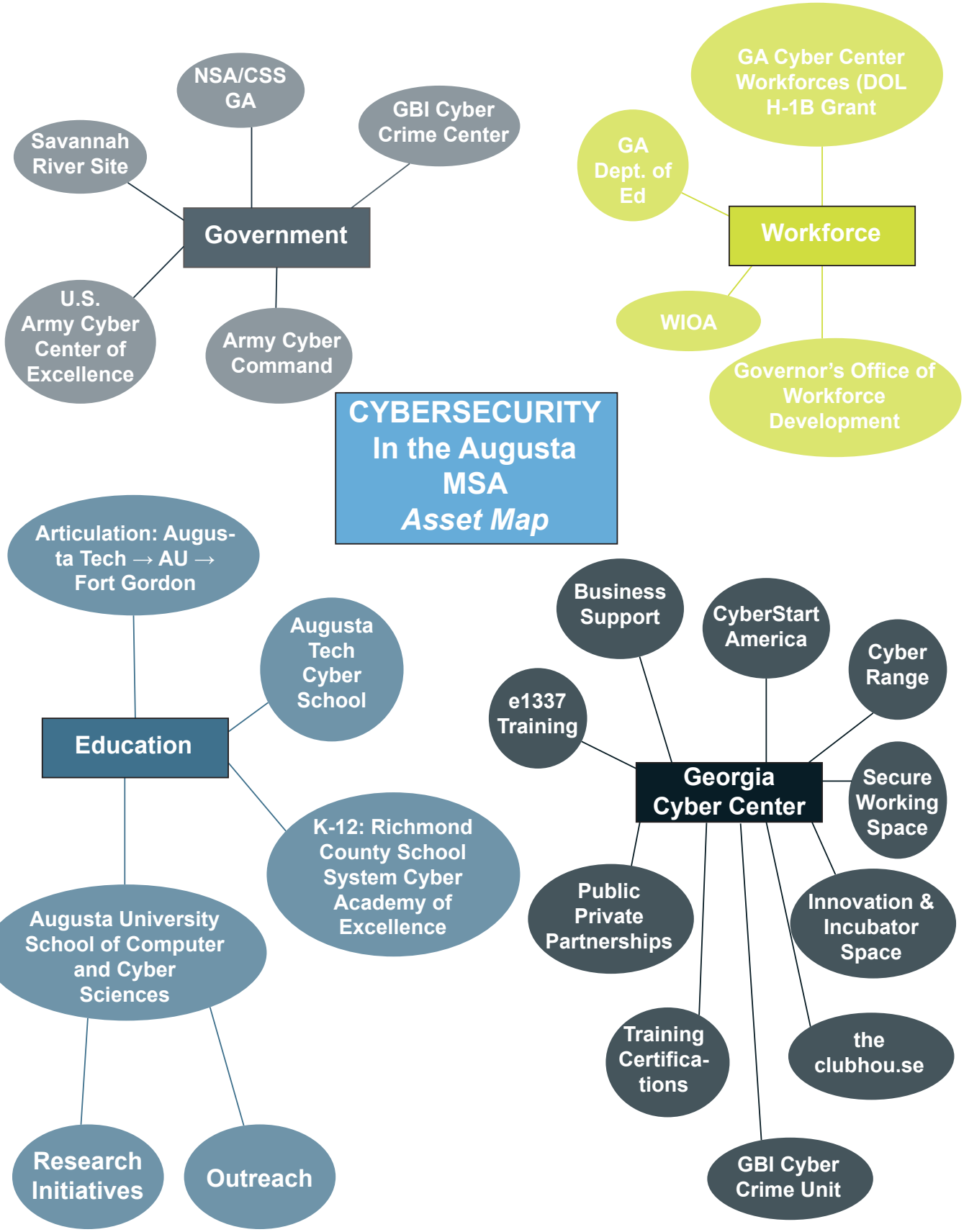
In partnership with Augusta University's School of Computer and Cyber Sciences, regional businesses can grow their talent pipelines locally. The National Security Agency (NSA) and Department of Homeland Security (DHS) designated the School as a Center of Academic Excellence in Cyber Defense (CAE-CD). The School offers degrees at the baccalaureate, master's, and doctoral levels along with a burgeoning research environment. There are a variety of K-12 cyber education efforts, such as the GenCyber summer cybersecurity camp experience for high school students and the CodeHoppers, a Girls Who Code Club for 6th – 12th-grade girls.

Augusta Technical College is the first two-year Technical College System of Georgia institute to be designated a National Center of Academic Excellence in Cyber (CAE2Y) by NSA/DHS. Coursework prepares students for entry-level positions in the cybersecurity workforce and helps students prepare for and pass multiple cyber-related industry certification examinations required by many employers.

The microcosm of assets that exist in Augusta has built the foundation for cybersecurity and will accelerate opportunities for future growth while accentuating economic diversity throughout the region. The following asset map in Figure 3 (page 9) attempts to depict assets that forge the cybersecurity industry in the Augusta MSA.

Augusta's Cybersecurity Ecosystem Cont'd

Figure 3: Cybersecurity Assets in the Augusta MSA



The Economic Impact of Cybersecurity

An economic impact analysis quantifies the impact from a given economic event or how some economic activity affects its surroundings—in this case, cybersecurity—on the economy of a specified region. This section highlights how the cybersecurity industry, as defined, contributes economically to Richmond County, Georgia.

The economic activity related to the cybersecurity industry is the millions of dollars of goods and services purchased from local vendors and the wages and benefits paid to local workers. This initial injection of funds circulates to the business owners and employees that supply the goods and services needed to support the industry. These contractors, businesses, and households continue the economic ripple effect by hiring workers and buying goods and services to facilitate their business. Once a cybersecurity firm (or cybersecurity-related activity) is established, commercial activity and new residential households will spend millions of dollars annually in the course of their daily activities. This recirculation of the original expenditures multiplies their impact through these indirect and induced effects.

To further delineate, below are brief definitions of the three typical types of impacts.

Types of Economic Effects

Direct	The shock to the economy caused by the initial spending of money, whether to pay for salaries and wages, purchase goods or services, or cover operating expenses.
Indirect	The business-to-business purchases in the supply chain taking place in the region that stem from the initial industry input purchases. As the industry specified spends their money in the region with their suppliers, this spending is shown through the indirect effect.
Induced	The values stemming from household spending of Labor Income, after removal of taxes, savings, and commuter income. The induced effects are generated by the spending of the employees within the business' supply chain.

What the Impacts Measure

Employment	The total number of jobs impacted in the cybersecurity industry
Labor Income	The total value of all forms of employment income and encompasses employee compensation and proprietor income.
Value Added	Is the measure of the contribution to GDP. This measure encompasses Labor Income, Other Property Income, and Taxes on Production and Imports (sales and excise taxes, property taxes, etc).
Output	The total value of a business' production and is the measure of the value added plus intermediate expenditures.

The Economic Impact of Cybersecurity Cont'd

The extent to which the initial expenditures multiply is estimated using economic models that depict the relationships between industries and firms and their employees. These models are built upon expenditure patterns that are reported to the U.S. Bureau of Labor Statistics, the U.S. Census Bureau, and the Bureau of Economic Analysis. Data is regionalized so that it reflects and incorporates local conditions such as average wages, expenditure patterns, and resource availability and costs.

The multipliers used in this analysis were generated by IMPLAN in coordination with the U.S. Bureau of Economic Analysis' RIMS II multipliers. Where appropriate, conservative estimates were used. Cybersecurity activities generate a significant economic impact on the region's economy. Industries in the private sector and defined within the cybersecurity taxonomy were used to analyze the impacts in this study. Private-sector cybersecurity firms in Richmond County generate $665 million directly in economic impact each year. When accounting for total impacts—direct and those indirectly impacting other sectors of the regional economy—private- sector cybersecurity activities generate more than $923 million each year and impact roughly 6,700 jobs. Total private sector impacts generated by cybersecurity firms in Richmond County are outlined in Figure 4.

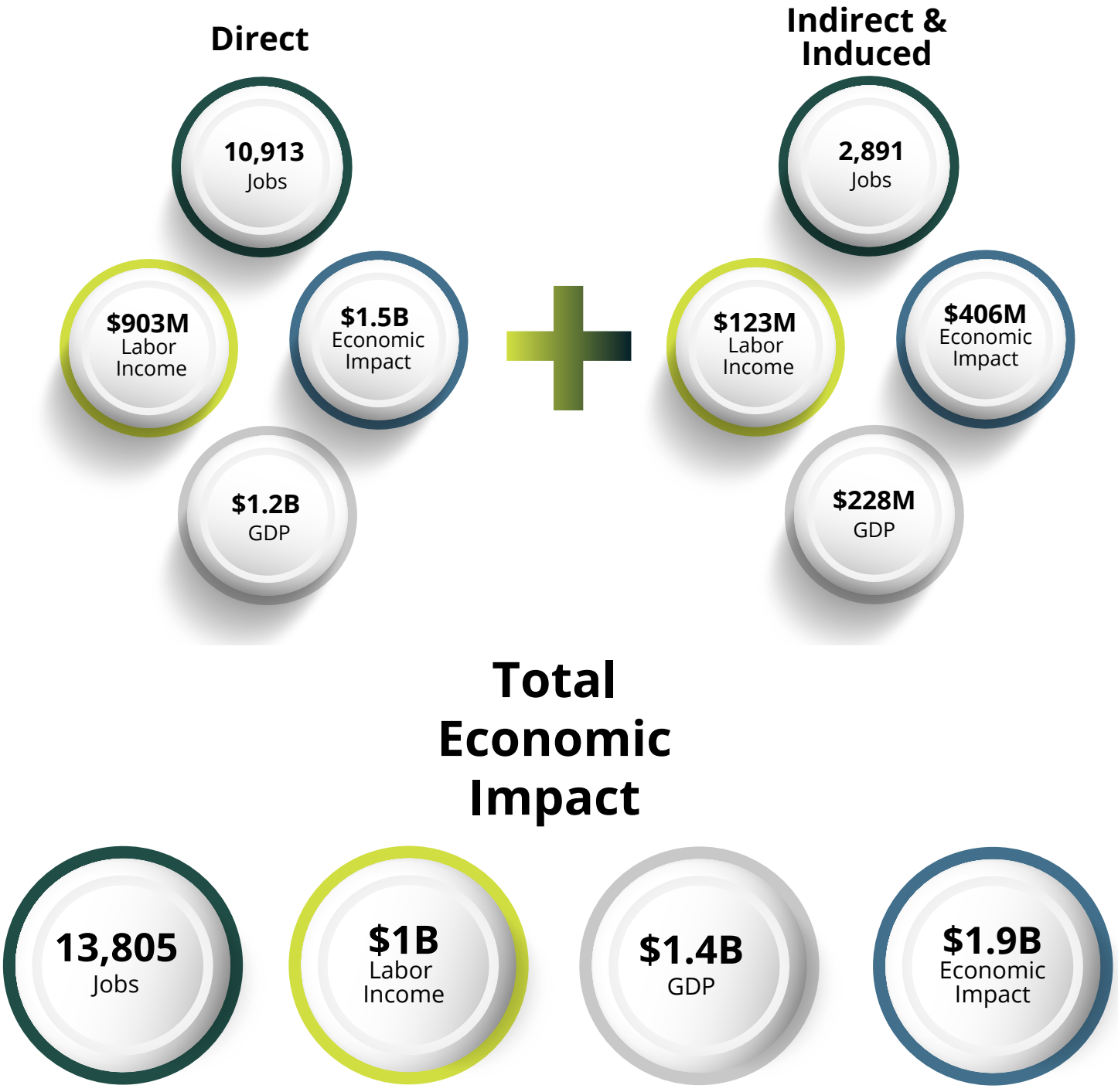
Figure 4: Breakdown of Total Impacts, Richmond County, 2020 (in $2021), CCoE and Army Command (2021) (within the taxonomy identified)

Impact Type	Employment	Labor Income	Value Added (GDP)	Output (Economic Impact
Private Sector				
Direct	4,952	$268,891,000	$371,417,000	$665,425,000
Indirect	1,190	$51,295,000	$89,745,000	$172,566,000
Induced	611	$25,891,000	$49,678,000	$85,030,000
Total Impact	**6,754**	**$346,077,000**	**$510,840,000**	**$923,021,000**
U.S. Army CCoE and Cyber Command				
Direct	5,961	$634,201,000	$830,925,000	$830,925,000
Indirect	$0	$0	$0	$0
Induced	1,090	$46,233,000	$88,414,000	$151,824,000
Total Impact	**7,051**	**$680,434,000**	**$919,339,000**	**$982,749,000**
TOTAL IMPACTS (Private and U.S. Army CCoE and Cyber Command)				
DIRECT	10,913	$903,092,000	$1,202,342,000	$1,496,350,000
INDIRECT	1,190	$51,295,000	$89,745,000	$172,566,000
INDUCED	1,701	$72,124,000	$138,092,000	$236,854,000
TOTAL IMPACT	**13,805**	**$1,026,511,000**	**$1,430,179,000**	**$1,905,770,000**
Richmond County	151,190	$9,202,479,000	$13,913,997,000	$23,795,770,000
% of Total County	9.1%	11.2%	10.3%	8.0%

The Economic Impact of Cybersecurity Cont'd

In total, direct private sector cybersecurity activities within the identified taxonomy contributed roughly $371 million to gross domestic product (GDP), nearly 3% of the County's total GDP in 2020. See graphic summary of impacts in Figure 5.

Figure 5: Total Impacts, Richmond County, 2020 ($2021) (within the taxonomy identified)

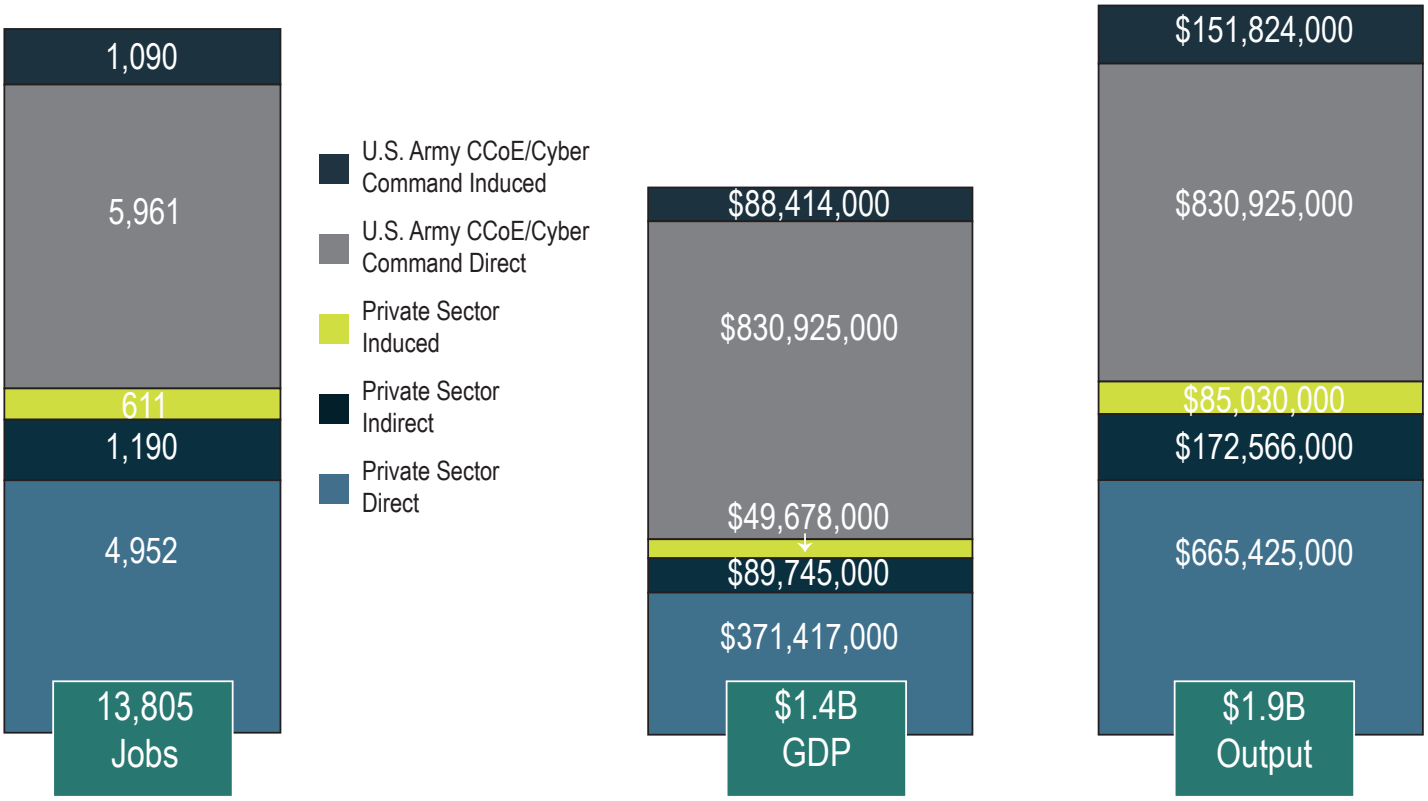


The Economic Impact of Cybersecurity Cont'd

As mentioned earlier, U.S. Army's Cyber Command relocation to Fort Gordon has expanded the region's cybersecurity presence significantly. Together, Army Cyber and the U.S. Army's Cyber Center of Excellence directly contribute 6% of the County's total GDP and add nearly 6,000 cyber jobs (see Figure 6) and another 1,090 in other industries, for a total of roughly 7,050 jobs.

For every ten jobs created in cybersecurity, another eight jobs are established, on average, throughout the economy. Given this ratio, over 10,900 jobs can directly be attributed to the cyber-related industry and another roughly 2,900 are created in other sectors throughout the economy.

Figure 6: Total Impacts, Richmond County, 2020 (within the taxonomy identified) by Private Sector and U.S. Army Units



Talent and Workforce

Workforce talent is critical to technical industries, particularly cybersecurity, where specialized skills, certifications, and security clearances are often required. As threats that exploit vulnerabilities in our cyberinfrastructure grow and evolve, an integrated cybersecurity workforce must be capable of designing, developing, implementing, and maintaining defensive and offensive cyber strategies. An integrated cybersecurity workforce includes technical and nontechnical roles that are staffed with knowledgeable and experienced people.

According to a Workforce Analysis of the Augusta Metro (Garner Economics, July 2020), the Augusta MSA ranks high among all metros across the country in terms of highly skilled cybersecurity talent. These individuals offer businesses with the highest standards in cybersecurity certifications, including CompTIA Security+, CISSP, GIAC Security Essentials, and others. Additionally, many of the workforce in Augusta possess high-security clearances. According to the survey, there is growing demand from regional businesses in machine learning and Artificial Intelligence.

According to Cyberseek.org, there are roughly 1,500 people employed in cyber-related occupations in the Augusta MSA. The region has shown significant growth in the cybersecurity industry cluster, growing at an annual rate of 6.1% compared to only 3.7% nationally. That rate is expected to jump in just the next year— roughly 130 cybersecurity positions are expected to be added over the next year within just those businesses who responded to the Augusta Cybersecurity Survey in late 2020—an 8% increase in cyber employment over the year.

According to the survey, education and training were the most important resources needed, followed by regional industry associations for cybersecurity (Figure 7). The training organization most used to train or upskill their workforce by survey respondents was Augusta University. Augusta University's School of Computer and Cyber Sciences is a testament to its support and dedication to cybersecurity in the region. The School's mission is to provide high-engagement, state-of-the-art technology education and research across its computer science, information technology, and cybersecurity disciplines. Since its inception, Augusta University has committed to this mission and has expanded its computer science, information technology, and cybersecurity programs. The School is headquartered in the Georgia Cyber Center to further partner and expand education, training, and research needs.

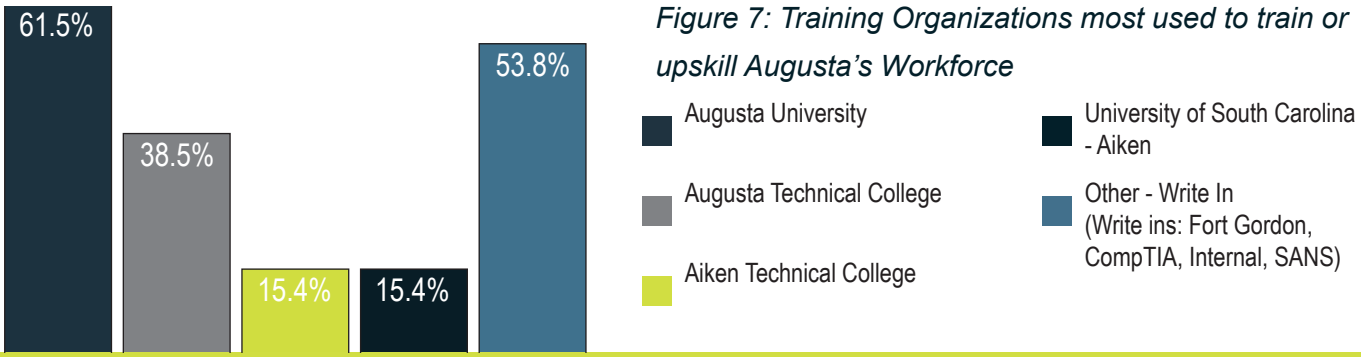


Figure 7: Training Organizations most used to train or upskill Augusta's Workforce

SWOT Analysis

A SWOT analysis was not part of this project, however, throughout the project trends were formulated and conclusions were based largely on asset strengths already possessed by the cybersecurity industry and asset weaknesses that were not present or were at low levels. After these factors were considered, existing and emerging trends were reviewed for opportunities and threats primarily from other locations such as a list of competitive regions with large concentrations of cyber-related activity and declining trends that will reduce the value of existing assets.

Figure 8 is a summary of findings through the survey and interviews coupled with data and desktop research.

Figure 8: Summary of Strengthes, Weaknesses, Opportunities, and Threats in Cybersecurity Industry

Competing Regions

The new national economy—sometimes referred to as the "digital economy"—driven by innovation and technology, is projected to create large numbers of jobs across the U.S. with median incomes of approximately 180% of local median incomes for all employment. The digital economy is believed to be less susceptible to recession, quicker to recover, and more sustainable over the long term. For communities with robust infrastructure and technology assets to be competitive, the new digital economy is becoming the top economic development strategy.

Cybersecurity is a very high-value niche within the digital economy. The primary drivers for attraction and growth of cybersecurity companies by MSA are:

1. Current availability of qualified workers and an expanding talent pipeline.
2. Proximity to federal government facilities, military bases, and major infrastructure, such as power plants.
3. A strong customer presence.
4. An established or emerging cybersecurity ecosystem.

However, the number of highly-competitive cybersecurity MSAs across the country is much smaller than for manufacturing and technology sectors in general. Areas lacking even one of the top factors listed above would likely have difficulty scaling up an effective campaign to win competitive cyber project locations or launch and retain a significant number of small companies.

The highest concentrations of cybersecurity companies and employment are in some of the nation's largest metropolitan areas like the San Francisco-San Jose MSA, Washington, D.C., New York City, and states like Virginia, Texas, Florida, and Maryland. Few mid-size cities can compete across the board but may have a subsector in which they are strong, such as cybersecurity applied to medical technology.

Augusta stands out as a mid-size city with exceptional potential, due to having the U.S. Cyber Command at Fort Gordon, Cyber Center of Excellence, the Georgia Cyber Center, NSA/CSS-GA, several large technology and cyber-related companies, and a nuclear power plant about 30 miles away. Additionally, with an estimated 1,500 employees in cybersecurity and roughly 1,200 job postings (according to Cyberseek), Augusta has a substantial cybersecurity workforce for a city of its size.

With these competitive advantages, Augusta's only limitation might be the size of the metro area and future population growth (compared to its competitors). Augusta has the opportunity to create a "preferred future" strategy to maintain and improve the quality of life and evolving ecosystem.

Competing Regions Cont'd

Major Locations

Major cyber hubs across the country include places like Sunnyvale, Detroit, Pittsburgh, Huntsville, and Waterloo (Ontario) which are all leading the way in automotive cybersecurity. Other cyber cities such as San Diego, San Jose, Washington DC, Clearwater, Orlando, Boston, Houston, Tulsa, and New York City are all staking their claims. A comprehensive list of top cybersecurity firms with head-quarter locations is summarized in Appendix E and a list of top consulting firms working in this realm is in Appendix F.

The following table (Table 2) details the MSAs with large concentrations of cybersecurity employment, indicated by a location quotient (LQ) above 1.0 (national average), and GDP in the U.S. The data includes only private sector employment which may include contractors working with the government but not government employees directly. For comparison purposes, only metro areas were used when analyzing competing regions, therefore, Richmond County is included as part of the Augusta metro but not stand alone in this analysis.

Los Alamos and Idaho Falls are both small areas with national labs located nearby. Although the numbers do not include those workers directly payrolled by the federal government, they do include contract workers.

Table 2: Competing MSAs for Cybersecurity (within taxonomy identified)

MSA Name	2015 Jobs	2020 Jobs	2015-2020 % Change	Location Quotient	Payrolled Business Locations	GDP
Los Alamos, NM	10,052	12,212	21%	10.65	82	$1,731,562,391
San Jose-Sunnyvale-Santa Clara, CA	313,561	374,057	19%	4.72	9,952	$193,102,591,494
Boulder, CO	36,841	42,308	15%	3.11	3,795	$10,801,597,748
California-Lexington Park, MD	8,702	9,817	13%	2.96	316	$1,435,952,916
Huntsville, AL	35,668	43,668	22%	2.69	1,545	$7,074,912,798
San Francisco-Oakland-Berkeley, CA	330,393	419,075	27%	2.38	19,814	$168,859,868,781
Washington-Arlington-Alexandria, DC-VA-MD-WV	465,456	501,770	8%	2.24	34,992	$106,785,749,111
Austin-Round Rock-Georgetown, TX	121,140	152,145	26%	2.01	9,422	$36,432,296,070
Boston-Cambridge-Newton, MA-NH	323,085	378,144	17%	2.01	18,789	$101,253,241,602
Durham-Chapel Hill, NC	36,653	45,681	25%	1.99	2,454	$10,205,193,147
Raleigh-Cary, NC	70,518	85,689	22%	1.92	6,829	$19,370,476,357
Palm Bay-Melbourne-Titusville, FL	23,766	30,181	27%	1.91	1,724	$6,209,805,794
Manchester-Nashua, NH	23,736	26,357	11%	1.87	1,238	$7,054,506,557
Seattle-Tacoma-Bellevue, WA	214,765	275,167	28%	1.87	15,373	$117,431,329,666

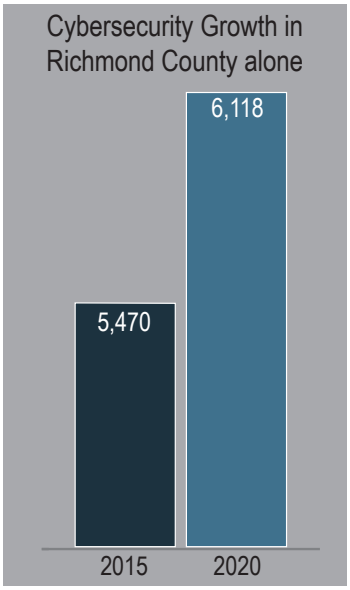
Competing Regions Cont'd

Table 2 Cont'd: Competing MSAs for Cybersecurity (within taxonomy identified)

MSA Name	2015 Jobs	2020 Jobs	2015-2020 % Change	Location Quotient	Payrolled Business Locations	GDP
Provo-Orem, UT	25,665	33,842	32%	1.76	2,485	$6,435,793,102
Idaho Falls, ID	8,112	8,546	5%	1.73	307	$1,259,343,815
Denver-Aurora-Lakewood, CO	142,045	169,249	19%	1.59	17,895	$37,757,729,520
Cedar Rapids, IA	14,751	15,510	5%	1.58	718	$3,952,274,750
San Diego-Chula Vista-Carlsbad, CA	152,280	174,861	15%	1.57	11,203	$42,455,311,372
Albuquerque, NM	35,614	38,280	7%	1.4	2,190	$6,602,340,478
Burlington-South Burlington, VT	11,852	12,083	2%	1.39	1,239	$2,078,880,378
Ann Arbor, MI	18,716	21,346	14%	1.37	1,223	$4,314,245,004
Madison, WI	32,732	37,608	15%	1.37	1,853	$8,420,395,366
Portland-Vancouver-Hillsboro, OR-WA	104,513	115,788	11%	1.37	10,104	$26,511,421,951
Baltimore-Columbia-Towson, MD	117,535	128,007	9%	1.34	7,911	$27,789,784,737
Detroit-Warren-Dearborn, MI	176,380	172,459	-2%	1.34	8,484	$28,160,765,743
Atlanta-Sandy Springs-Alpharetta, GA	206,765	230,178	11%	1.22	16,049	$56,961,017,348
San Antonio-New Braunfels, TX	51,290	59,547	16%	0.79	3,865	$9,379,984,900
Augusta MSA, GA-SC	9,218	8,290	-10%	0.48	622	$1,165,481,440

The Augusta MSA shows a decline in employment within those private industries included in the cybersecurity taxonomy. The large drop was due, in-part, to about a 2,500 loss in Professional Services (NAICS 54) employment in the private sector. The same sector in Richmond County, however, increased by 300 jobs during the same time (see graph to right).

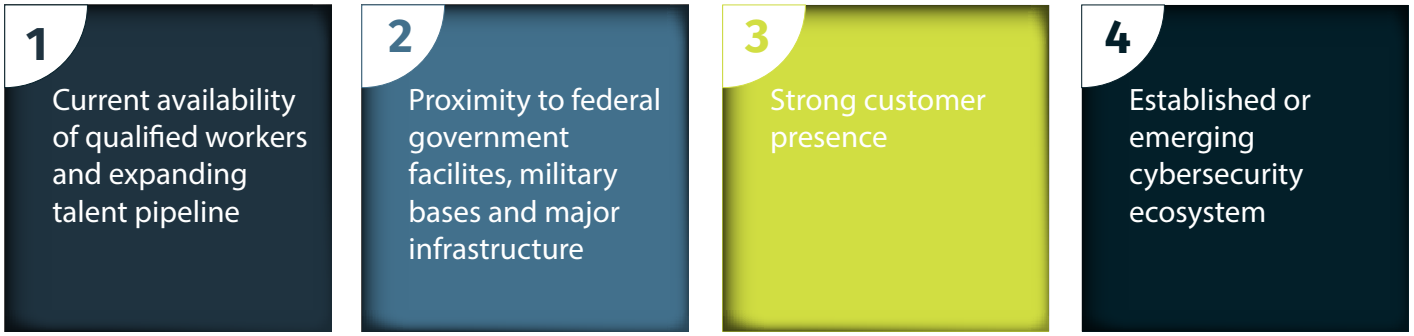
Overall, all industries that comprise the Cybersecurity cluster grew by nearly 650 jobs in Richmond County alone.



Competing Regions Cont'd

Business Attraction

The primary drivers for attraction and growth of cybersecurity companies are:



The Top 15+ locations in the U.S. for cybersecurity have dedicated branding, marketing channels, and economic development resources to grow and attract companies. As the cybersecurity industry evolves, it is proving to be even more highly dependent than many other industries – including other technology sectors - on having a high concentration of potential customers and trained/experienced workers in the region.

Federal facilities, especially DoD and Homeland Security, government and industry research centers, and major university partners seem to be almost as important as the size of the customer base and workforce. It appears the colocation of as many aspects of the cybersecurity industry as possible in a given MSA is what drives location decisions for cybersecurity product developers and service providers.

The need to have a robust and collaborative ecosystem appears to affect economic development strategies and incentives. Tax breaks and traditional workforce development strategies alone cannot overcome the need to congregate. There is a long history of technology clustering to illustrate that research and technology need a much denser ecosystem than, say, manufacturing industries.

Many states have invested heavily in new resources for schools and post-secondary educational institutions, including community colleges, technical institutes, and nontraditional sources for training and certifications, in an effort to increase regional talent pipelines. Several national and international trade associations and 3rd-party vendors (like CompTIA) test and certify employment-ready skills for the cybersecurity community.

Large concentrations of cybersecurity companies and workers frequently overlay a dense cluster of high-technology and innovation activities in an MSA. Having a vibrant startup ecosystem is critically important to help attract talent to the industry, introduce new products and services, and fuel an innovation culture locally. The Georgia Cyber Center has played an integral role in building the cyber ecosystem in Augusta, helping make it a more competitive place for cyber-related activity and firms to locate.

Competing Regions Cont'd

Business Attraction Cont'd

Since it takes time to expand a local workforce, Augusta should consider leveraging its advantages for growth in cybersecurity, especially in the short run, by promoting hard-to-fill or slow-to-fill job opportunities to qualified workers across the country. While economic development practice has generally held that bricks and mortar and local job creation are the measures of success, remote workers who enable a company to grow faster and more sustainably have intrinsic worth. In a highly competitive global market for cybersecurity professionals, a strategy to connect qualified remote workers in the U.S. to area jobs could become a critical success factor by helping local employers even-out peaks and valleys in employment demand.

As the cybersecurity industry evolves, it is proving to be even more highly dependent than many other industries—including on other technology sectors—on having a high concentration of potential customers and trained/experienced workers in the region.

Many more cyber professionals are needed. What can a community do? Augusta is already incorporating some of these initiatives into their ecosystem, therefore, it can be just a reminder of how important they are and what has proven successful in other areas across the country. Talent can be developed through universities and technical colleges, but there is a substantial lag.

Talent development efforts could include:

- Younger people are attracted to cyber work.
- Supplement with focused certification programs.
- Digitally connect students and cyber professionals.
- Engage early education and develop internship programs in high school.
- People on the autistic spectrum make good candidates for cyber work.

Primary drivers for attraction are:

- Co-location
- Proximity to highly advanced DoD and military operations
- Government and industry research centers
- Major university partners
- Leading cyber education programs
- Competitive cost of doing business
- Highly dependent on having a high concentration of potential customers
- Established or emerging cybersecurity ecosystem

Competing Regions Cont'd

Business Attraction Cont'd

Cybersecurity could become one of the top subsectors of technology with some of the highest job creation and employee pay. Cybersecurity companies have become among the most sought-after economic development projects not only in the U.S., but globally. The following best practices depict a few ways to stay competitive as a region in the cybersecurity market. Some of the practices have been implemented in Augusta. However, they are still iterated to illustrate what is occurring in other cyber-rich areas across the country (in no particular order).

Concentration of customers: As the cybersecurity industry evolves, it is proving to be even more highly dependent than many other industries – including other technology sectors - on having a high concentration of potential customers and trained/experienced workers in the region.

Tax incentives: Expanded tax incentives and workforce development programs previously available to multiple industry sectors to include cybersecurity.

Tax exemptions: Capital formation and capital gains tax exemptions that applied to tech businesses, a tax credit specifically for cybersecurity.

Targeted incentives: Incentives to companies that have an office in the "Innovation District" and derive most of their revenue from technology-related companies
Technology zones: Increased technology zones to encourage tech businesses to move operations to the county.

State tax credit programs: Statewide program in effect since 2010 offering capital gains tax exemptions to tech companies, including cybersecurity companies, on income already taxed by the federal government as a long-term capital gain.

Tax incentives for commitments: Maryland's groundbreaking incentive in 2013, targeted specifically to cybersecurity startups already in the state, offered $3-million in tax breaks to be distributed among those startups that agreed to locate [permanently] in Maryland.

Branding, marketing: Top 15+ locations in the U.S. for cybersecurity have dedicated branding, marketing channels and economic development resources to grow and attract companies. San Antonio leaders have staked their claim as Cyber City, USA while investment created a western point-of-presence on what is now known as Louisiana's I-20 Cyber Corridor.

Competing Regions Cont'd

Business Attraction Cont'd

Industry targeted incentives: Focus on cybersecurity to incent technology companies to ramp up products and services quickly to meet government and industry needs.

Federal facilities: The presence of federal facilities, especially DoD and Homeland Security, government and industry research centers, and major university partners seem to be almost as important as the size of the customer base and workforce.

Ecosystem: Co-location of many aspects of the cybersecurity industry as possible in a given area is what drives location decisions for cybersecurity product developers and service providers. Proximity to highly advanced DoD and military operations, including the Air Force Cyber Command and NSA Texas, paired with leading cyber education programs, and a competitive cost of doing business puts San Antonio in a position that other cities cannot duplicate.

Technology clustering: Tax breaks and traditional workforce development strategies alone cannot overcome the need to congregate. There is a long history of technology clustering to illustrate that research and technology need a much denser ecosystem than, say, manufacturing industries.

Certifications: Several national and international trade associations (like CompTIA) and 3rd-party vendors test and certify employment-ready skills for the cybersecurity community.

Leverage high density of high tech: Large concentrations of cybersecurity companies and workers frequently overlay a dense cluster of high-technology and innovation activities in a region.

Develop dedicated Innovation centers: Need to have a way to keep segments of the center "private", for confidential testing and activities, cyber range. A top-down approach—need state- and regional- level buy-in and promotion.

Typical Economic Development programs may not be the right fit: Economic Development programs do not work well in this case, because they have not incentivized knowledge workers. Making incentives worthwhile would prove more successful.

Cater to cyber professionals and startups: Target cyber professionals in the region about what else they need. Look for retirees that still want to work after they end their "career." Provide resources for people wanting to leave their current employer and become a consultant, or develop a new company, yet still work in the area.

Competing Regions Cont'd

Business Attraction Cont'd

Assist remote working: Consider value of remote workers living and working in the region but employed by firms elsewhere. Set up co-working and socializing spaces; high-speed fiber connections; growing clubs in the area to support these remote workers; develop a sense of "cyber-community"; brand the region; highlight cyber activities and related events, meetups, etc.

Dedicated Cyber facilities: In 2017, Governor John Bel Edwards created the Louisiana Cybersecurity Commission to bolster the state's cyber safety and to position Louisiana as a national leader. The Cyber Innovation Center anchors Louisiana's 3,000-acre National Cyber Research Park, where General Dynamics operates an 800-employee Integrated Technology Center and where Louisiana Tech University and Bossier Parish Community College operate a STEM Building aimed at fast-tracking students for cybersecurity and other technology careers. The state invested $57 million and local governments $50 million to build the Cyber Innovation Center in the early 2000s. Similar initiatives linked an 800-job IBM Client Innovation Center with LSU; a 400-job CGI IT Center of Excellence with the University of Louisiana.

San Antonio: Just southwest of San Antonio's urban core is Port San Antonio—a major platform that is growing advanced technologies in the region, including aerospace, cybersecurity, defense and manufacturing with an employment base of more than 13,000 professionals on the campus. The Port's development strategies include Project Tech—a set of state-of-the-art secure office facilities to support the growth of cybersecurity operations in the region.

Partnerships: For years, Louisiana has cracked that code by investing in cyber partnerships at college campuses that embrace the private sector.

High concentration of workers: San Antonio has the highest concentration of cyber and intelligence professionals outside of the national capital region.

Talent pipeline-HS: CAST Tech (San Antonio), the first of three industry driven high schools, works hand-in-hand with industry partners to prepare students for careers in technology.

Talent pipeline—collegiate: San Antonio's six NSA Centers of Excellence specialize in cybersecurity research and education and support a sustainable cybersecurity workforce pipeline. University of Texas at San Antonio boasts the nation's top ranked cybersecurity undergraduate program and recently opened its National Security Collaboration Center (NSCC).

Conclusion

As a mid-size city, Augusta stands out as a cybersecurity hub with resources in place and where businesses prosper. Cybersecurity businesses within the identified taxonomy, both private and government, generate approximately **$1.9B** in total economic impact and contribute $1.4B (directly and indirectly) to Richmond County's overall GDP, over 10% of the County's total GDP.

With an estimated 10,900 employees working in the cyber-related industry, Augusta has a substantial cybersecurity workforce for a city of its size. Talent development is the key to success. K-12, higher education institutions, and economic and workforce development partners have collaborated to prioritize internship development, experiential learning, continuing education, and certifiable credentials to build and support a highly trained cybersecurity workforce.

Augusta has created a cybersecurity ecosystem that has proven to be a region for cyber firms to call home.

Appendix A: Taxonomy

NAICS Code	NAICS Description
423430	Computer and Computer Peripheral Equipment and Software Merchant Wholesalers
511210	Software Publishers
517311	Wired Telecommunications Carriers
518210	Data Processing, Hosting, and Related Services
541511	Custom Computer Programming Services
541512	Computer Systems Design Services
541513	Computer Facilities Management Services
541519	Other Computer Related Services
541611	Administrative Management and General Management Consulting Services
541613	Marketing Consulting Services
541614	Process, Physical Distribution, and Logistics Consulting Services
541618	Other Management Consulting Services
811212	Computer and Office Machine Repair and Maintenance
541990	All other Professional, Scientific, and Technical Services
5616	Investigation and Security Services

Appendix B: Summary Highlights of Survey

925
employees added to payrolls (past three years)

383
of over 3,200 employees focus on cybersecurity work

150
# of employees expected in next 12 months

of the 3,200+ employees, **12%** are focused on work related to cybersecurity

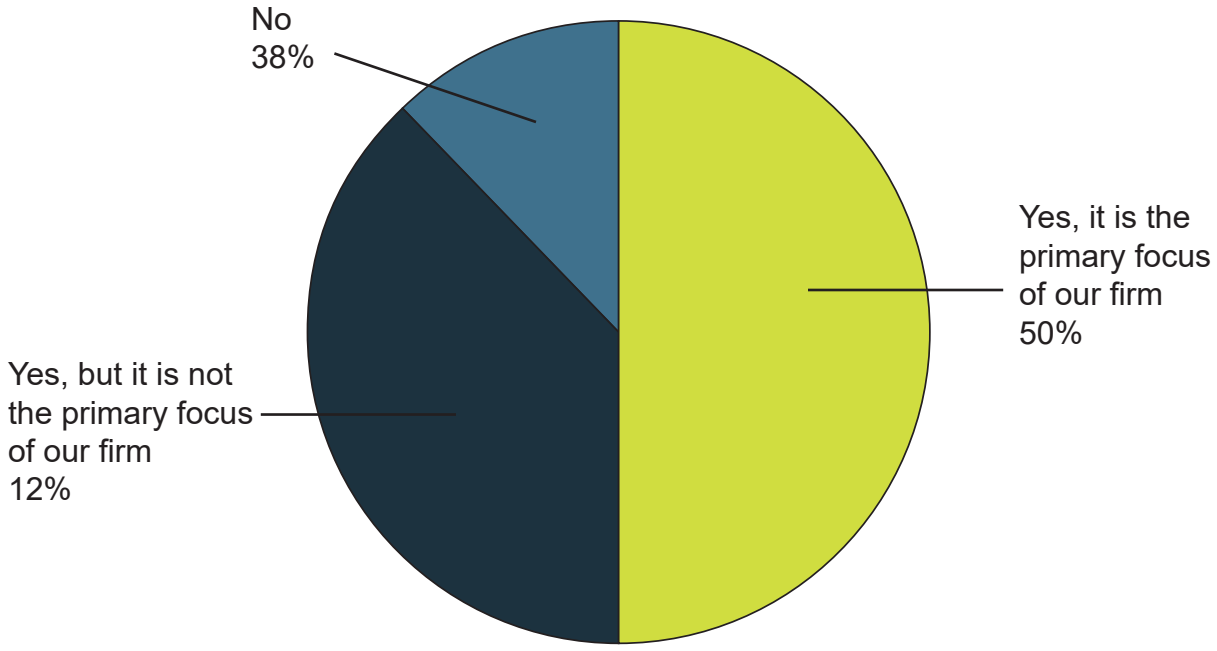
42%
Response Rate

~126
new cybersecurity employees

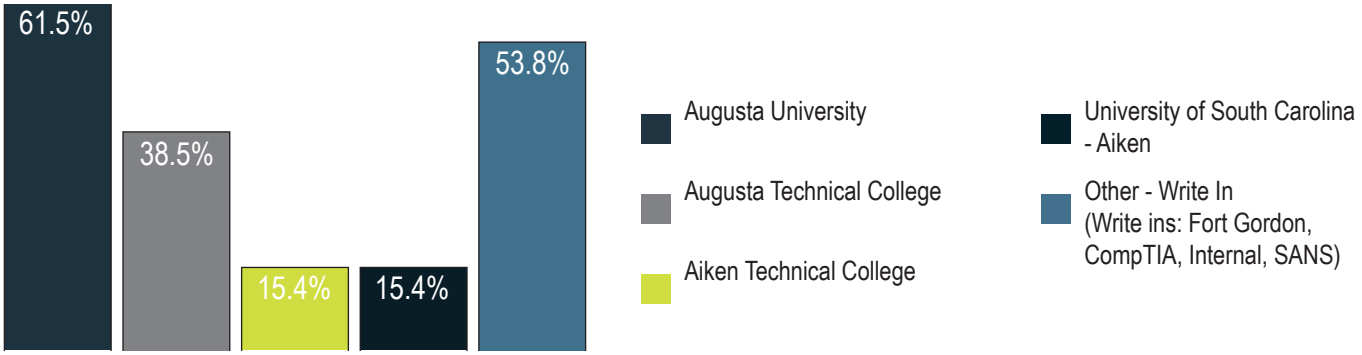
The cybersecurity workforce is expected to grow **33%** within the next year, this is just a small representation of all cyber firms

Appendix B: Summary Highlights of Survey Cont'd

Does your firm directly or indirectly work for the Federal government?



Which training organizations do you work with to train or upskill your workforce?

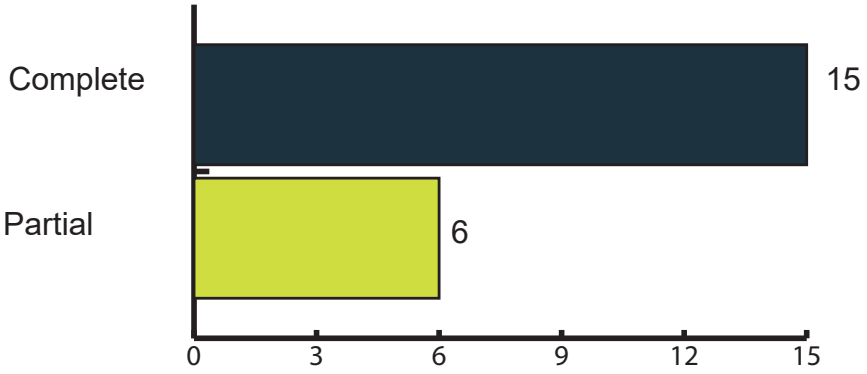


There is a growing market demand in machine learning and Artificial Intelligence. Most firms are advancing in majority of technologies but not much involvement in blockchain technology.

Education and Training were the most important resources needed, followed by regional industry associations for cybersecurity.

Appendix C: Full Survey and Results

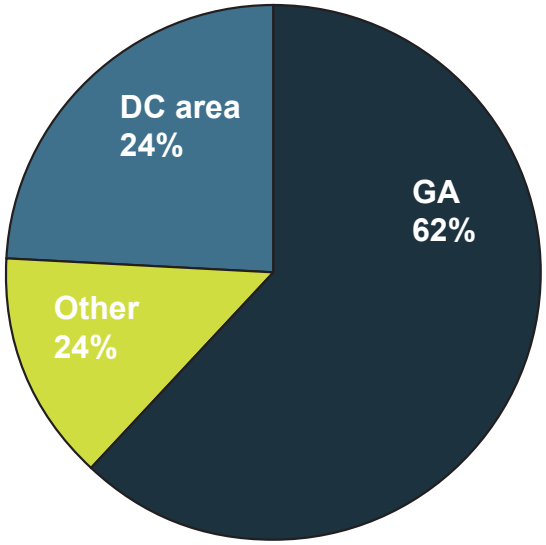
Response Statistics



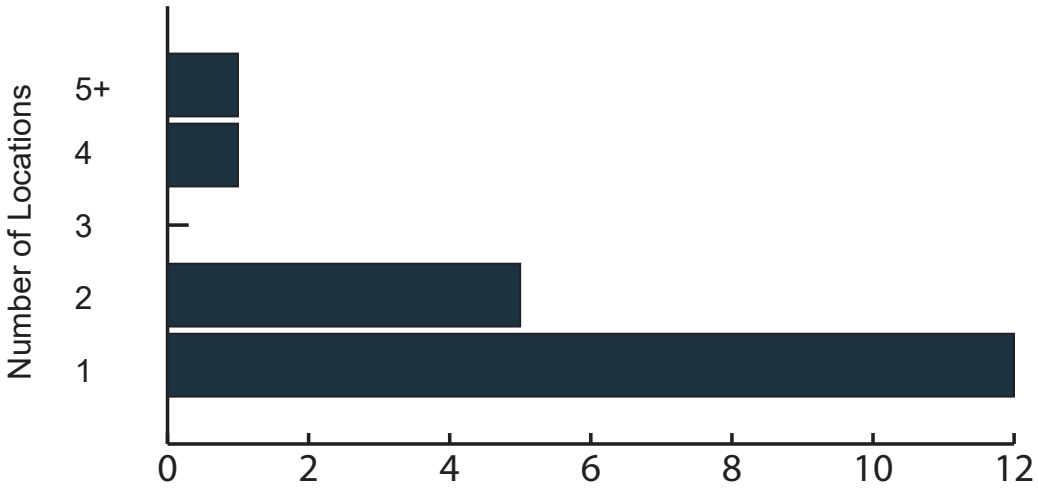
42%
Response Rate

1. What city is the headquarters of your organization?

Augusta, GA	10
Evans, Ga	1
Fairfax, VA	1
Bethesda, MD	1
Washington, GA	1
Atlanta, GA	1
Roseland, NJ	1
Columbia, MD	1
Duluth, MN	1
Little Rock, AR	1
McClean, VA	1
Centerville, VA	1

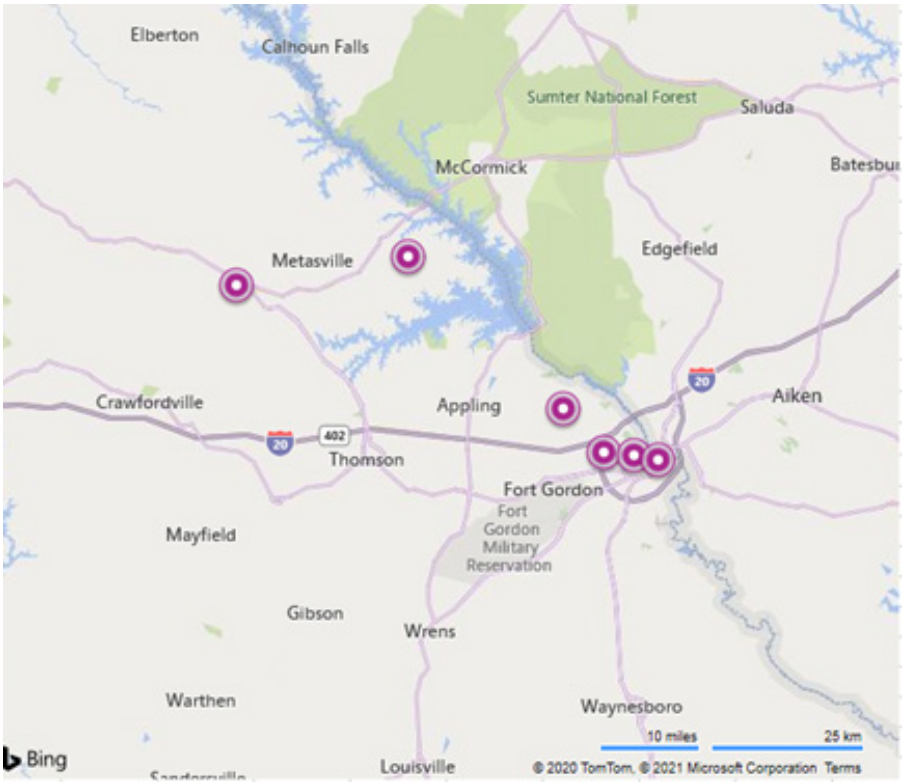


2. How many business locations does your company/organization have in the Augusta MSA?

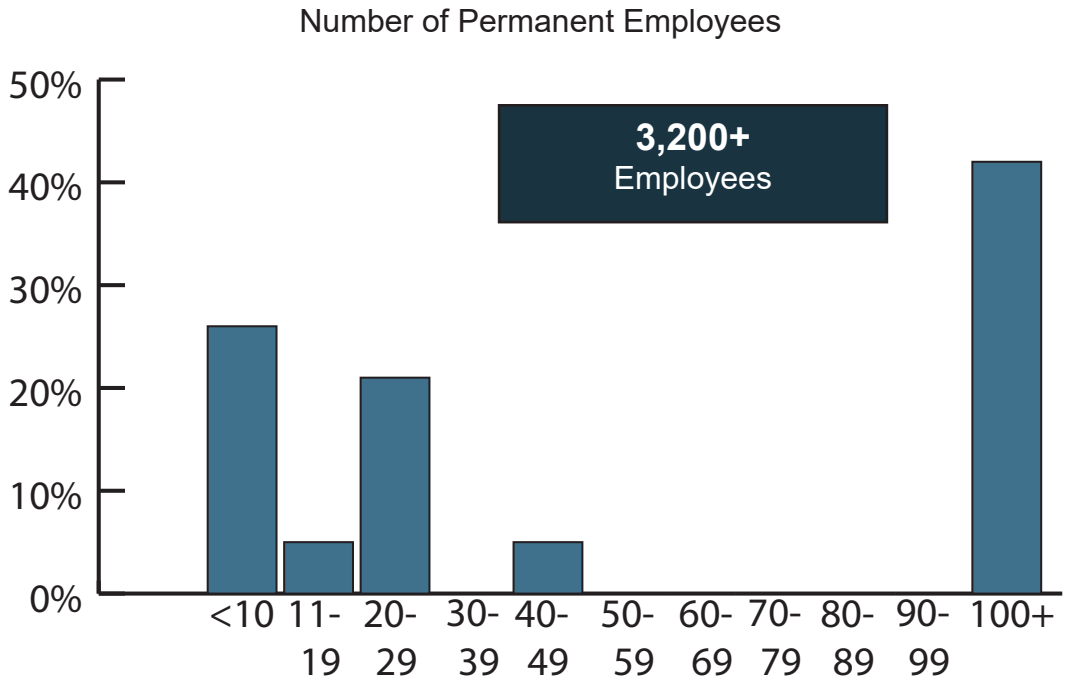


Appendix C: Full Survey and Results Cont'd

3. What is the zip code of your current location? (Please provide response for your current Augusta MSA business location only.)

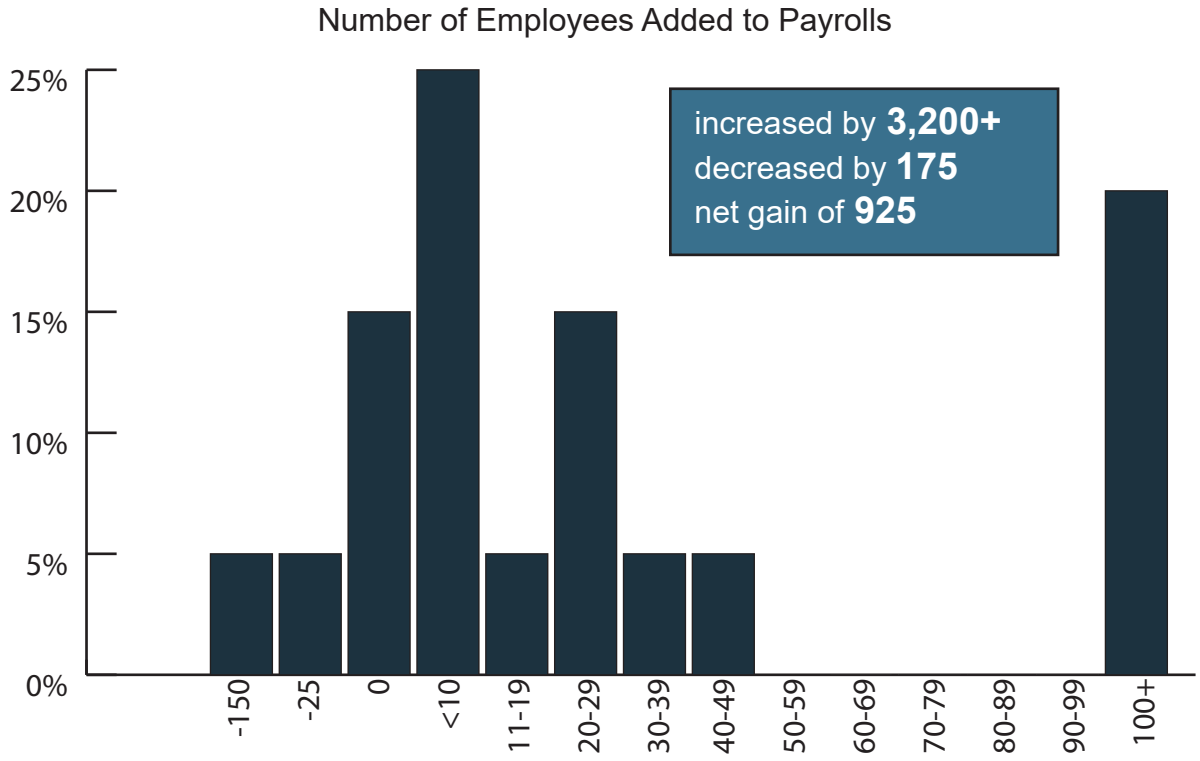


4. How many permanent employees (both part-time and full-time) work at or from your location?



Appendix C: Full Survey and Results Cont'd

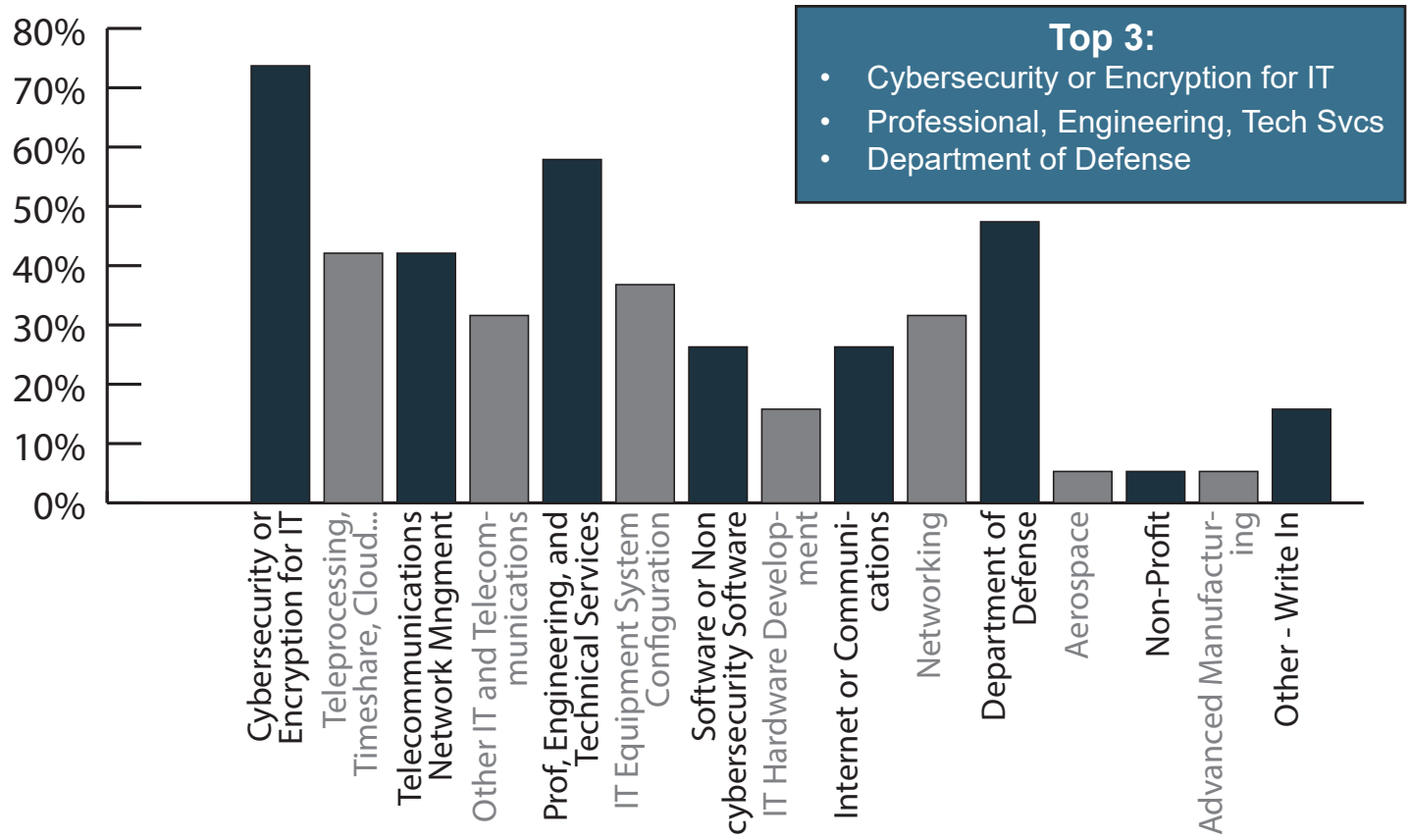
5. Over the last three years, your company has grown or decreased by_____ employees?



6. How many employees do you expect to have 12 months from now?

Appendix C: Full Survey and Results Cont'd

7. What industry or industries best describes the work that your firm is involved in (check all that apply)?

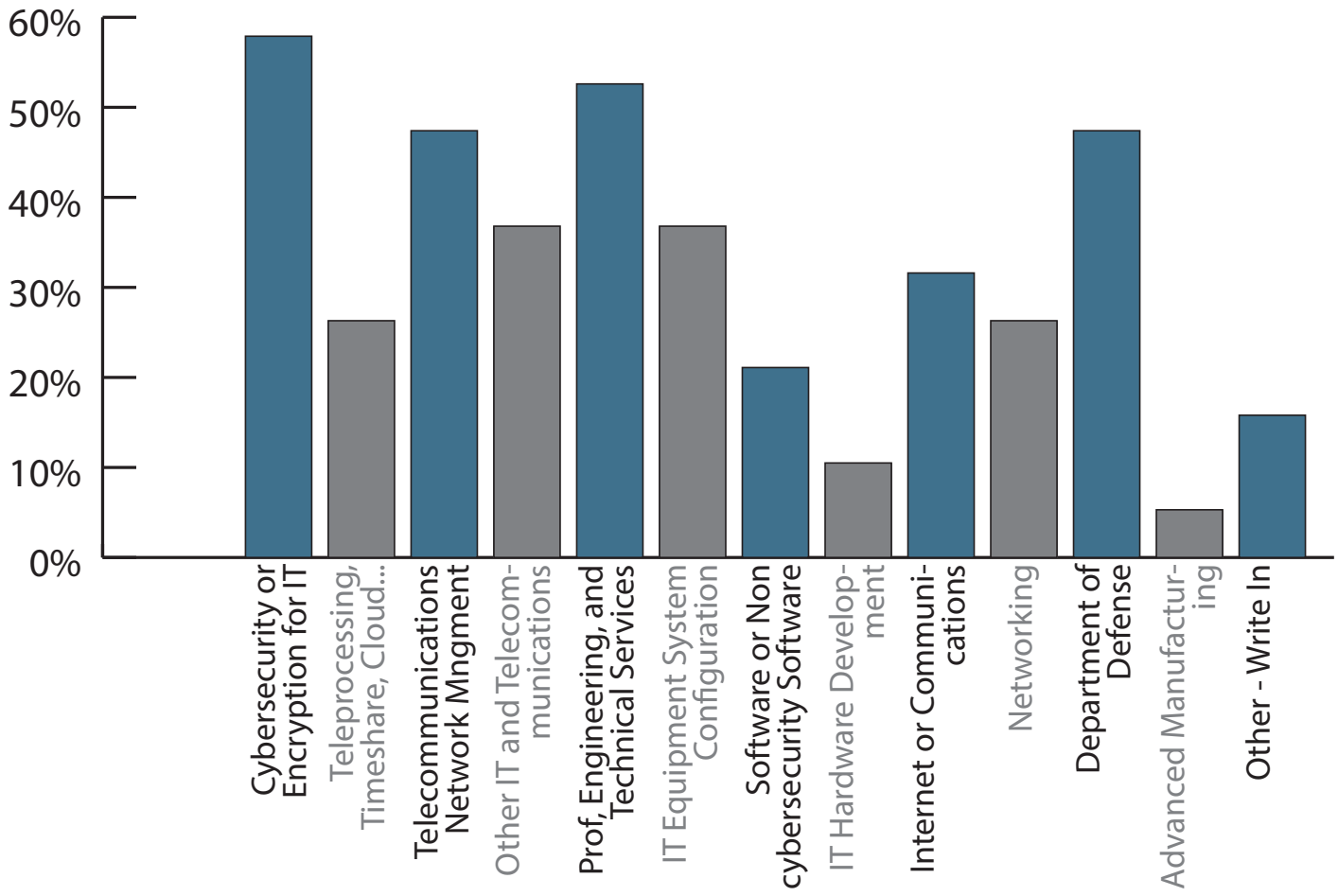


Write Ins:

Computer Science, Information Technology, Cybersecurity Higher Education (1)
Human Capital Management application support (1)
Training (1)

Appendix C: Full Survey and Results Cont'd

8. What industry or industries best describes the work that your firm is involved in your Augusta location (check all that apply)?



Top 4:

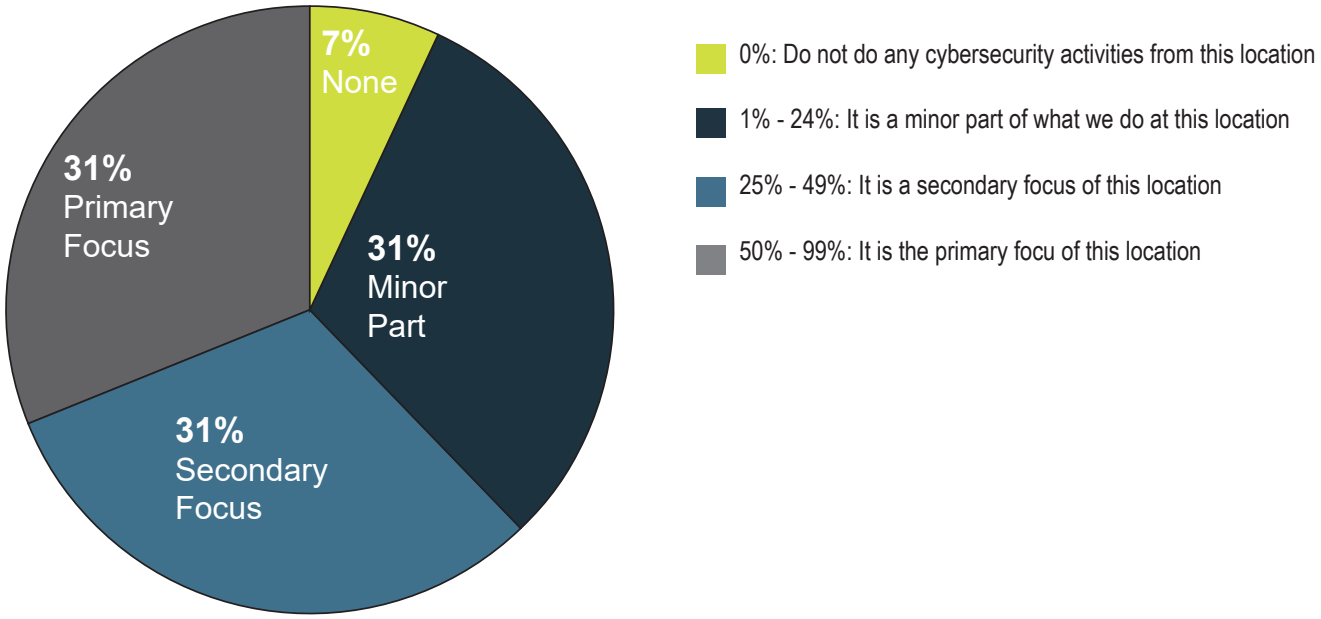
- Cybersecurity or Encryption for IT
- Professional, Engineering, Tech Svcs
- Department of Defense
- Telecomm Network Mngment

Write Ins:

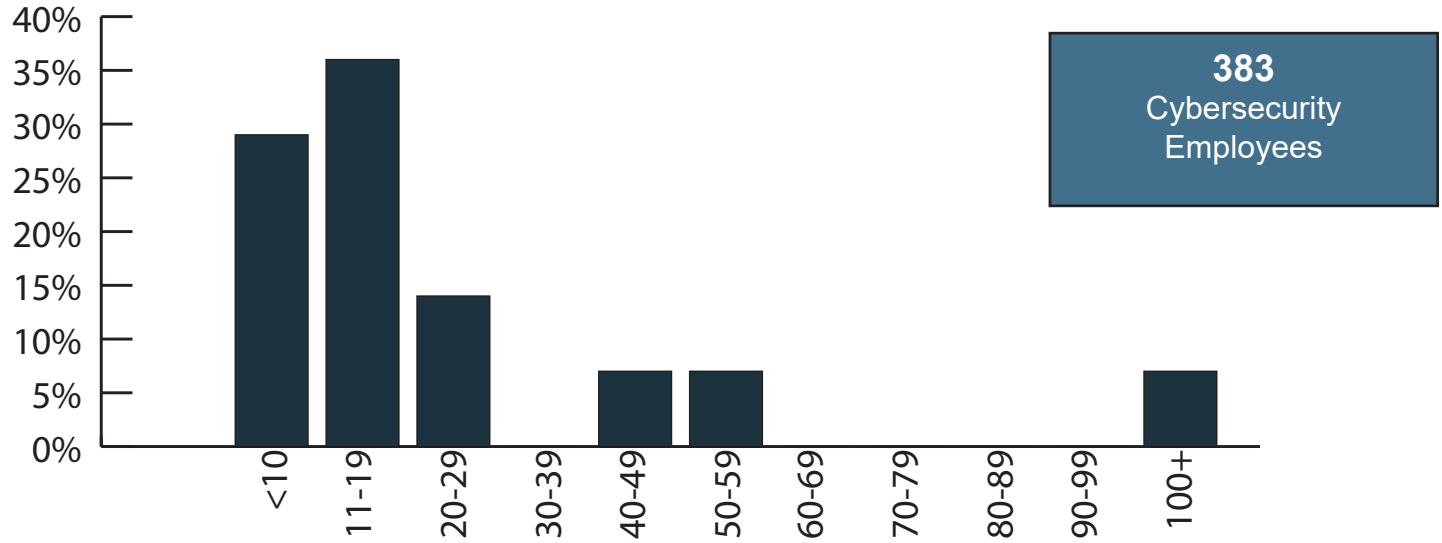
Computer Science, Information Technology, Cybersecurity Higher Education (1)
Human Capital Management application support (1)
Training (1)

Appendix C: Full Survey and Results Cont'd

9. What portion of the work done from this location is focused on cybersecurity?



10. Of the total permanent employees (both part-time and full-time) at your Augusta location(s), how many of these employees are focused on work related to cybersecurity (provide number).



383
Cybersecurity
Employees

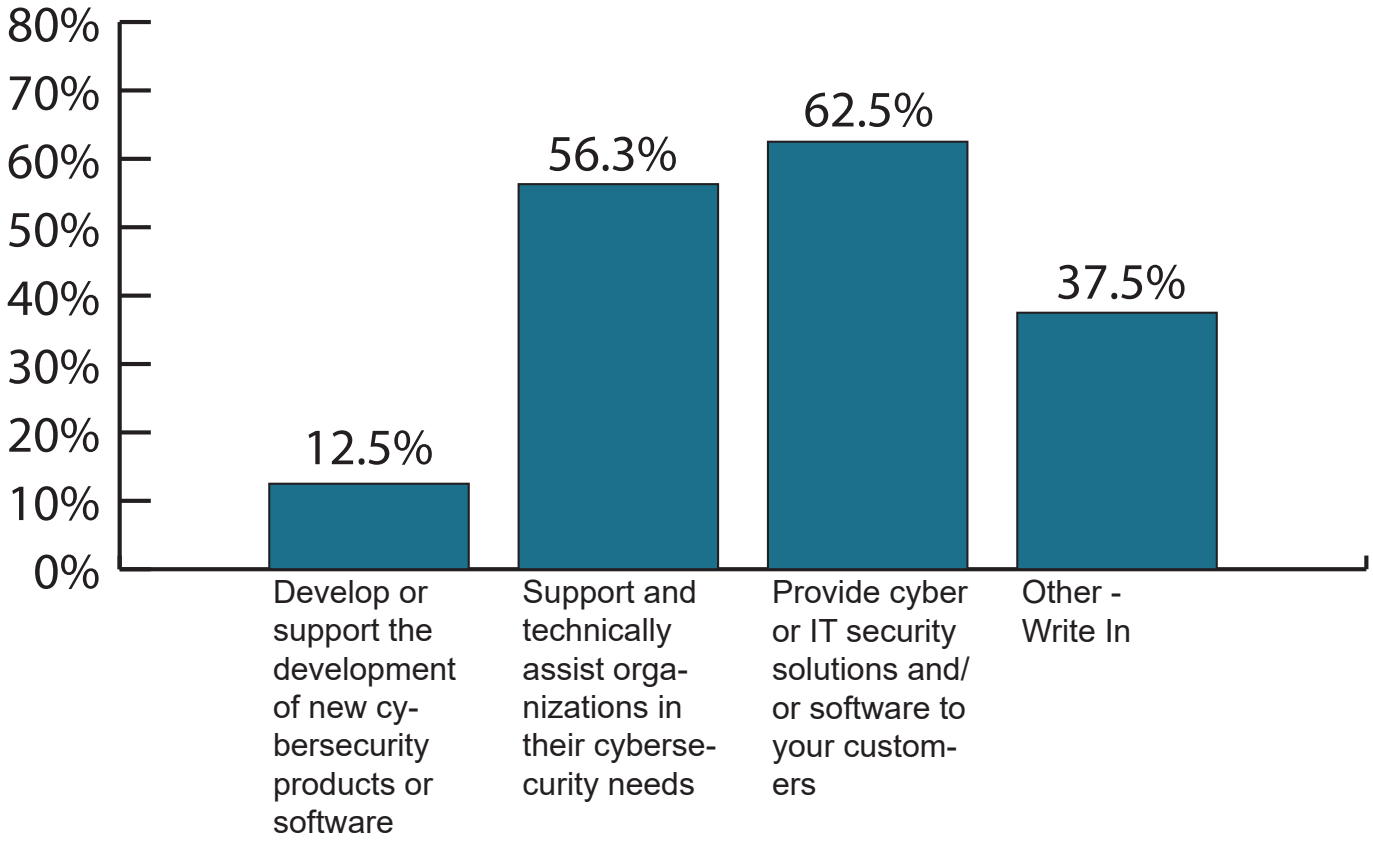
Of the 3,200+ employes, **12%** are focused on work related to cybersecurity

Appendix C: Full Survey and Results Cont'd

11. Of your current cybersecurity workforce in Augusta, how many do you expect to have 12 months from now?

The cybersecurity workforce is expected to grow **33%** (or by ~126) within the next year - this is just a small representation of all cyber firms.

12. Which of the following categories best describes the type of work you do in the cybersecurity realm?



Write Ins: 6

Higher Education in Computer Science, IT and Cybersecurity (1)
Information Assurance and Risk Management Framework (1)
Penetration Testing (1)
Support internal cybersecurity needs (1)
Training, workforce development, and innovation (1)
Support internal operations (1)

Appendix C: Full Survey and Results Cont'd

13. Please list the level of which your firm is involved within the following technologies (check all that apply).

There is a growing market demand in machine learning and AI. Most firms are advancing in the majority of technologies but not much involvement in blockchain technology.

Does not include "Do not know"

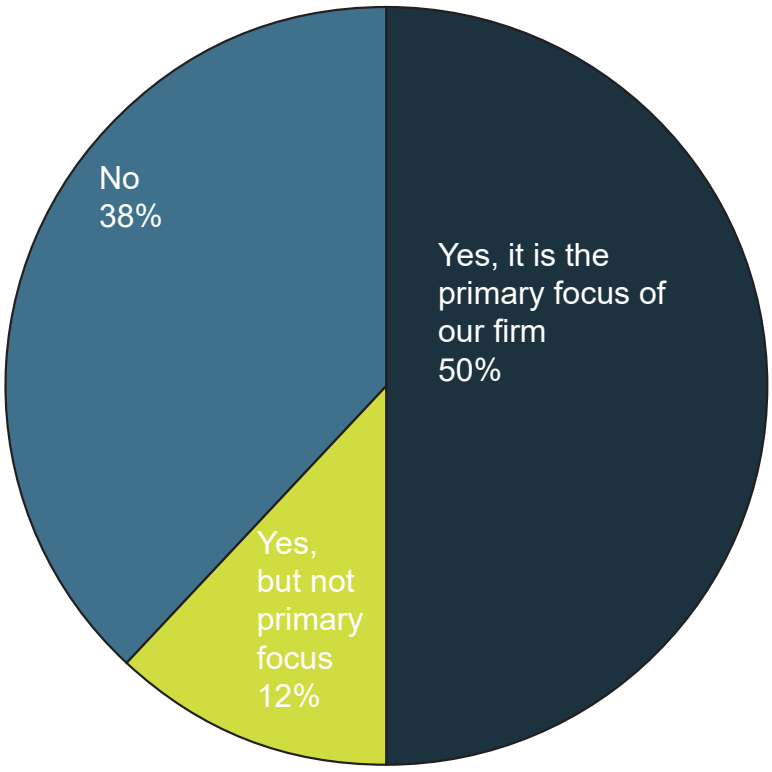
Appendix C: Full Survey and Results Cont'd

13. Please list the level of which your firm is involved within the following technologies (check all that apply). Cont'd

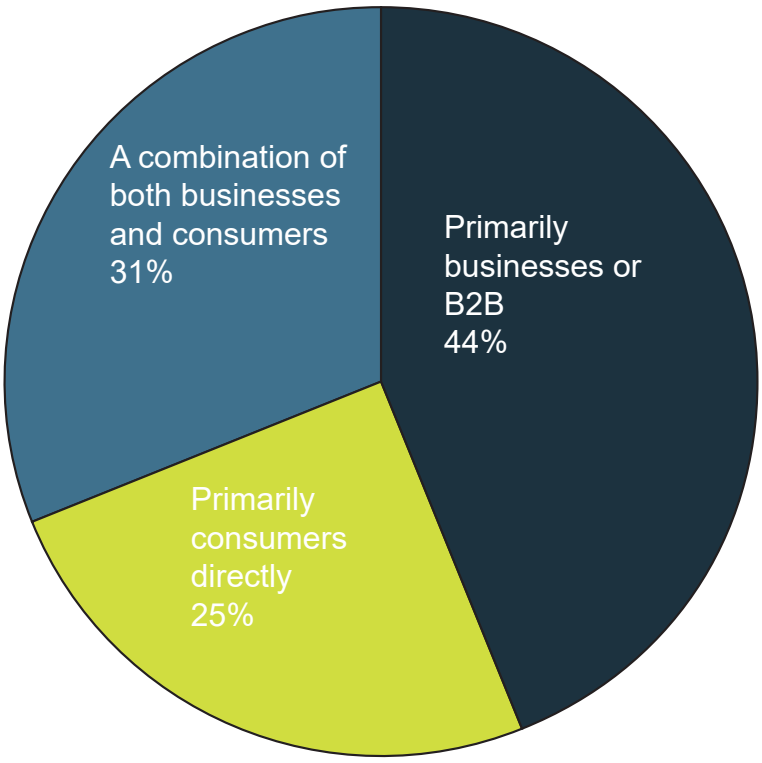
	Growing Market Demand	Advancing	Using but not Developing	Not Involved	Do not know	Total Responses
Blockchain technology	6.7%	13.3%	20%	46.7%	13.3%	15
Machine learning and artificial intelligence	41.2%	23.5%	17.6%	17.6%	0%	17
Risk-based authentication	20%	40%	20%	6.7%	13.3%	15
Data protection and data layer security	31.3%	50%	12.5%	6.3%	0%	16
Resilient and secure computing	25%	50%	18.8%	6.3%	0%	16
Resilient and secure networking	25%	56.3%	56.3%	6.3%	0%	16
Mobile cybersecurity	27.8%	38.9	11.1	22.2%	13.3%	18
Internet of things	21.4%	50%	21.4%	7.1%	0%	14
Distributed computing	0%	100%	0%	0%	0%	1
Penetration testing	0%	100%	0%	0%	0%	1
Security Assessments	50%	50%	0%	0%	0%	2
Total Responses	33%	56.3%	56.3%	6.3%	0%	131
% of Total Responses	25.2%	41.2%	16%	14.5%	3.1%	100%

Appendix C: Full Survey and Results Cont'd

15. Does your firm directly or indirectly work for the Federal Government?

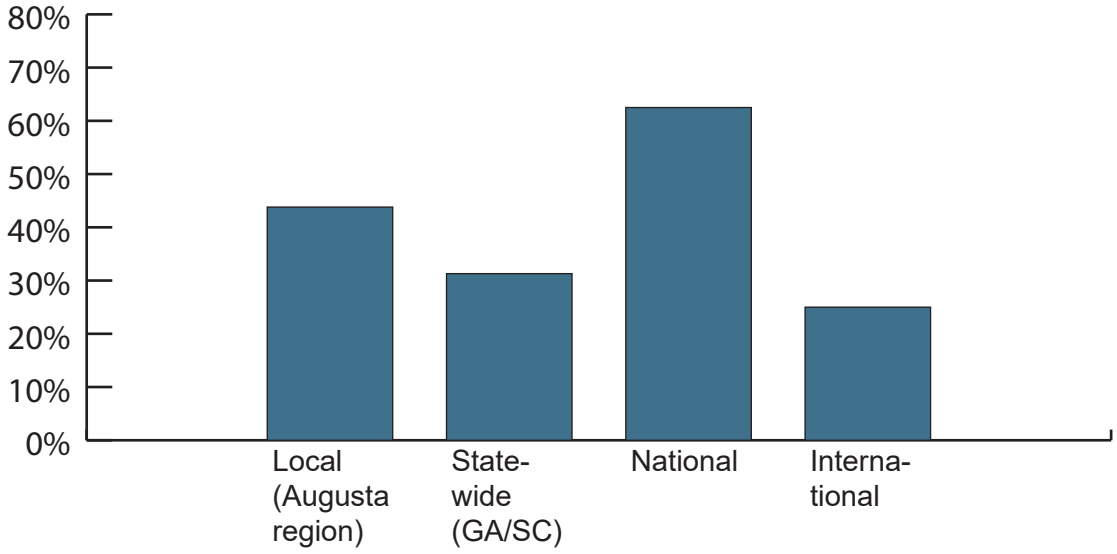


16. Pertaining to your firm's cybersecurity activities, what is the primary market focus?



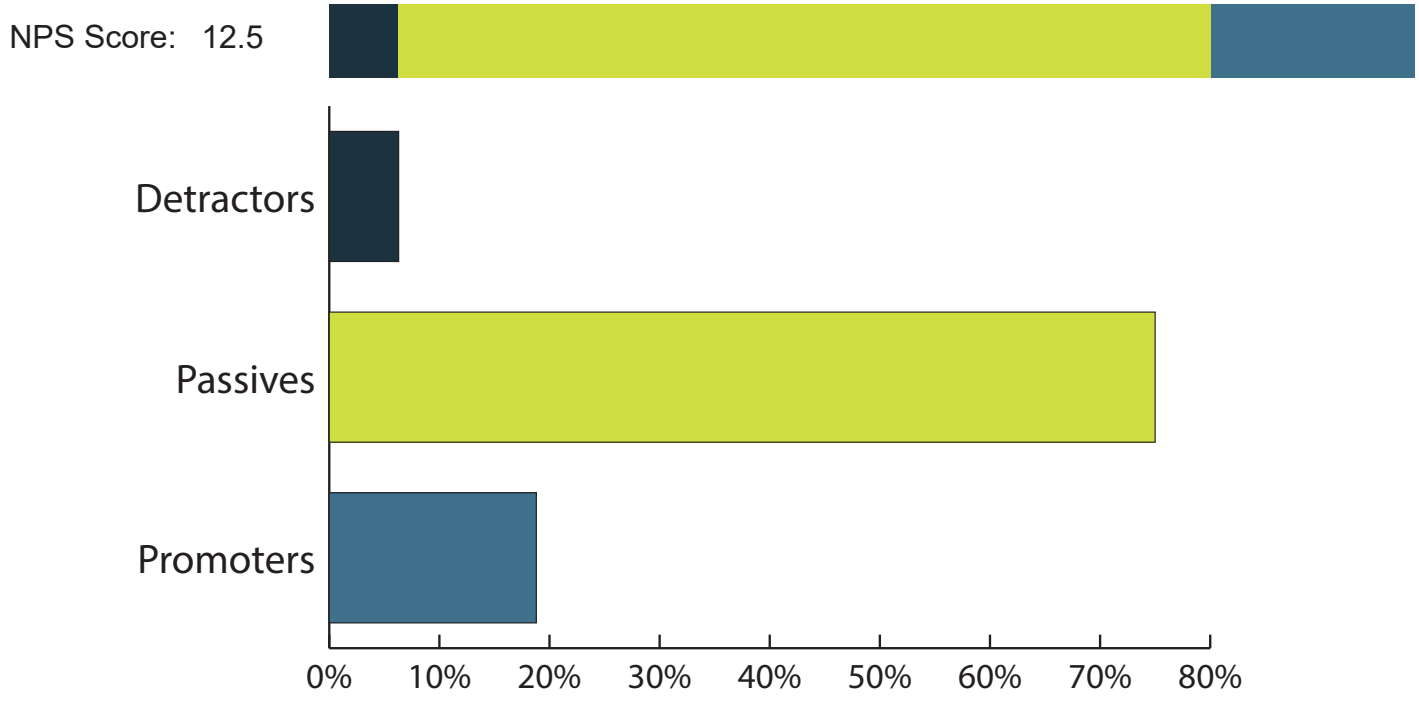
Appendix C: Full Survey and Results Cont'd

17. Where is your customer base located from your Augusta location (check all that apply)?



18. How would you rate Augusta as a place for cybersecurity firms to do business?

The Net Promoter Score is an index ranging from -100 to 100 that measures the willingness of business to recommend a region to others. it is used as a proxy for gauging the businesses overall satisfaction with a region and the businesses loyalty to the region.



Appendix C: Full Survey and Results Cont'd

19. How would you rate the following resources, in the Augusta MSA, compared to other areas your business could be located? (one star = lowest and five stars = highest)

	Accessibility
Access to capital, banking and funding	★★★☆☆ Count: 6 Not Applicable: 10
Access to clients and customers	★★★★☆ Count: 15 Not Applicable: 1
Access to vendors and suppliers	★★★½☆ Count: 14 Not Applicable: 2
Access to talent and skilled workforce	★★★½☆ Count: 16 Not Applicable: 0
Access to firms and organizations that are doing cyber-related research and development	★★★☆☆ Count: 13 Not Applicable: 3

Strength - 4 Stars

- Access to clients and customers

Weakness - 3 Stars

- Access to cyber-related R&D
- Access to capital, banking, and
- funding

Opportunity - 3.5 Stars

- Access to talent and skilled work-force
- Access to vendors and suppliers

Threat - 3 Stars

- Access to cyber-related R&D
- Access to capital, banking, and
- funding

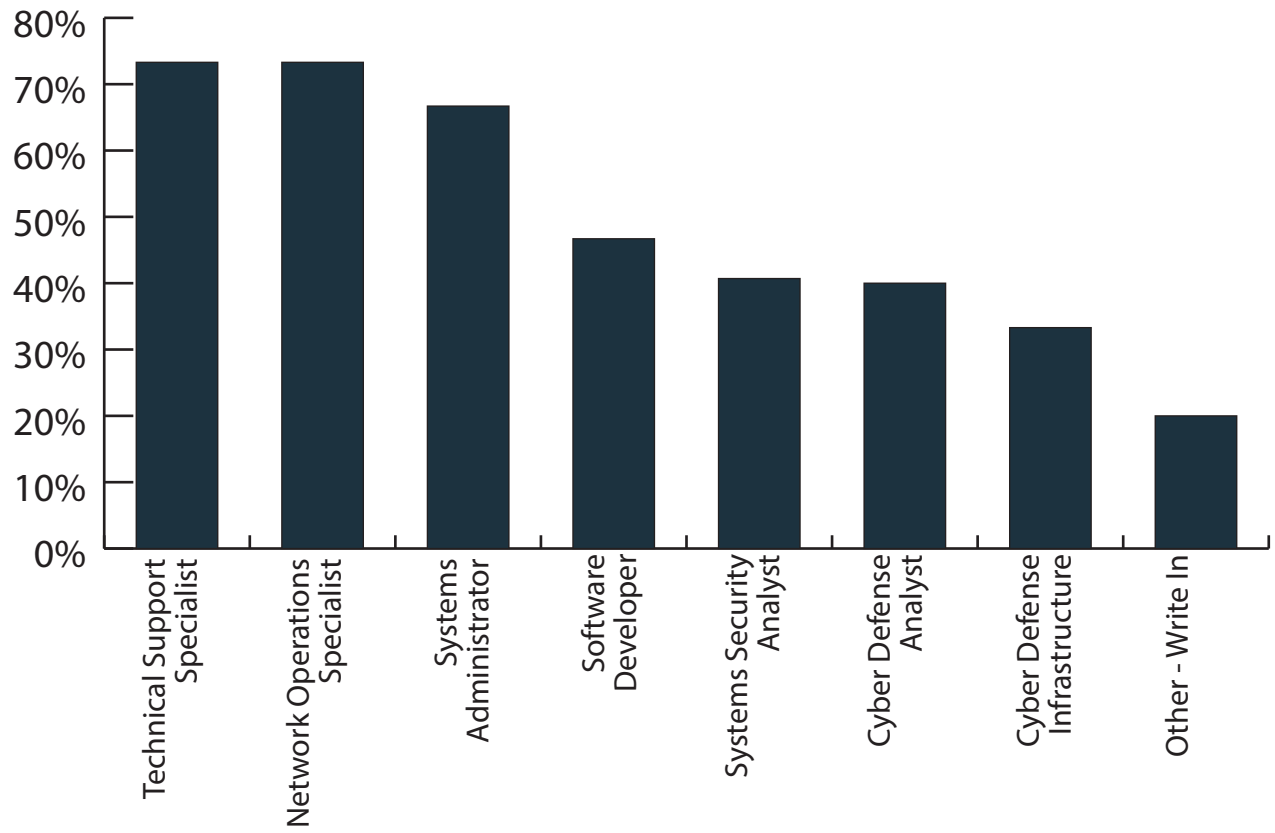
Appendix C: Full Survey and Results Cont'd

20. How important are the following resources and organizations to your firm and its work related to cyber and information security?

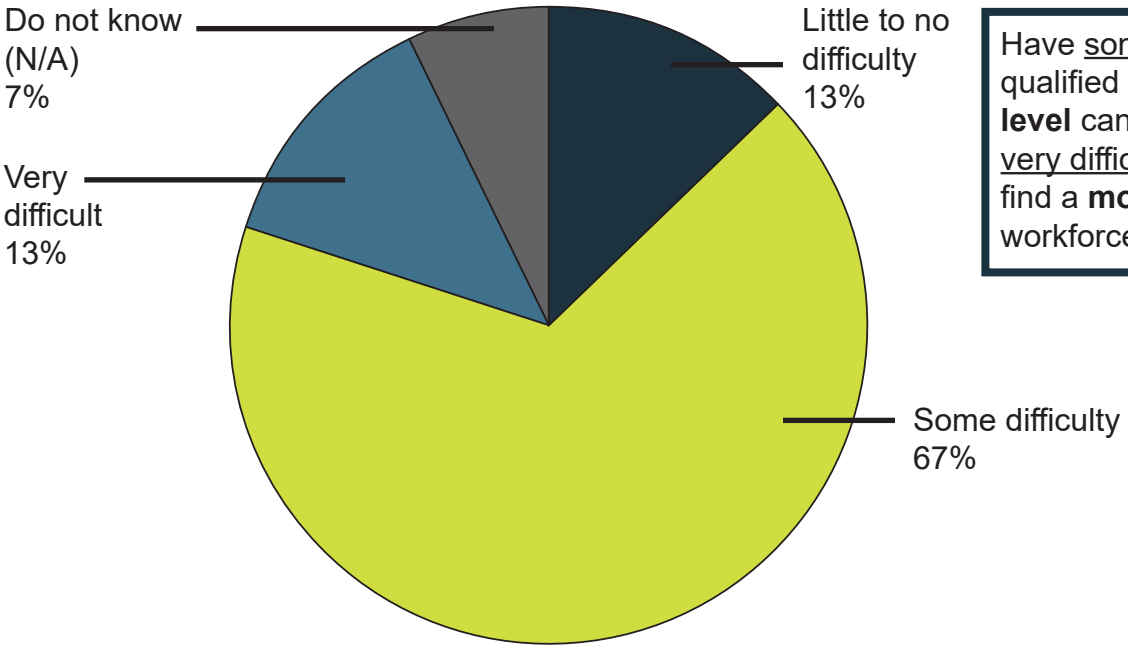
	Do not know	It depends	Not at all important	Somewhat Important	Extremely important	Responses
Universities doing cyber work	0 0%	2 12.5%	0 0%	9 56.3%	5 31.3%	16
Education and training institutions offering cyber-related content	0 0%	2 12.5%	0 0%	4 25%	10 62.5%	16
Technology transfers and institutions looking to assist in commercializing	1 6.3%	4 25%	5 31.3%	3 18.8%	3 18.8%	16
Regional industry associations for cybersecurity	0 0%	2 12.5%	1 6.3%	11 68.8%	2 12.5%	16
Access to new commercial technologies in cyberspace	0 0%	3 18.8%	2 12.5%	7 43.8%	4 25%	16
Number of Responses % Share	1 1%	13 16%	8 10%	34 43%	24 30%	80 100%

Appendix C: Full Survey and Results Cont'd

21. Do you have employees at your Augusta location who generally fit the following job roles (check all that apply)?



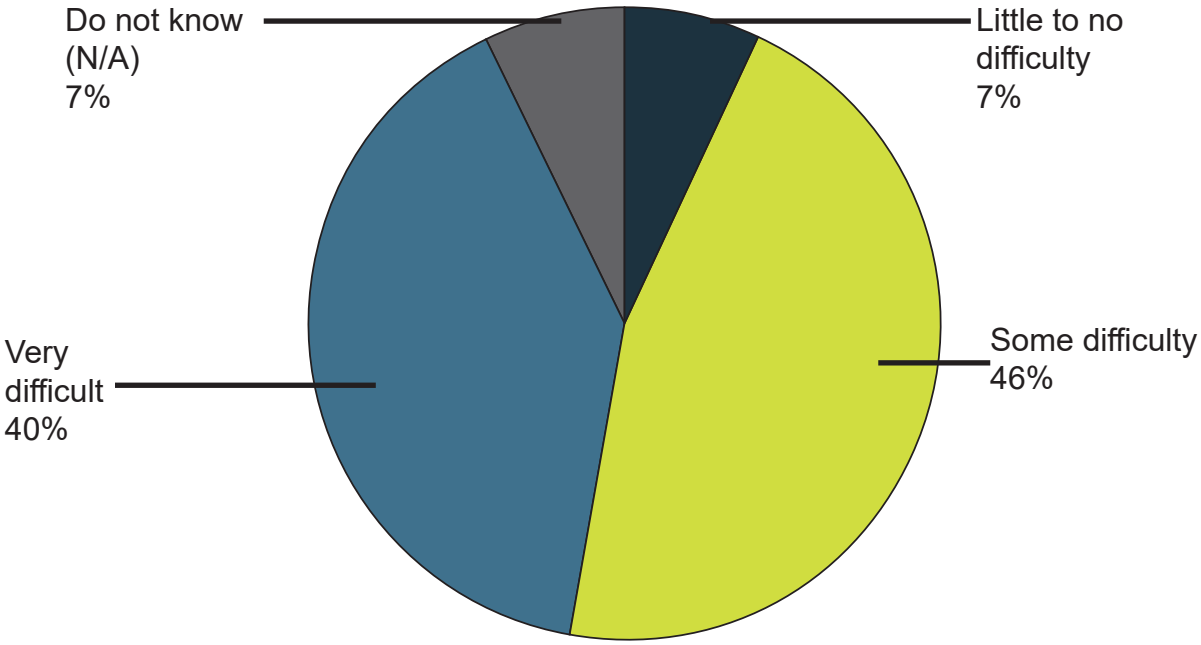
22. How difficult is it to find qualified entry- to mid-level cybersecurity applicants



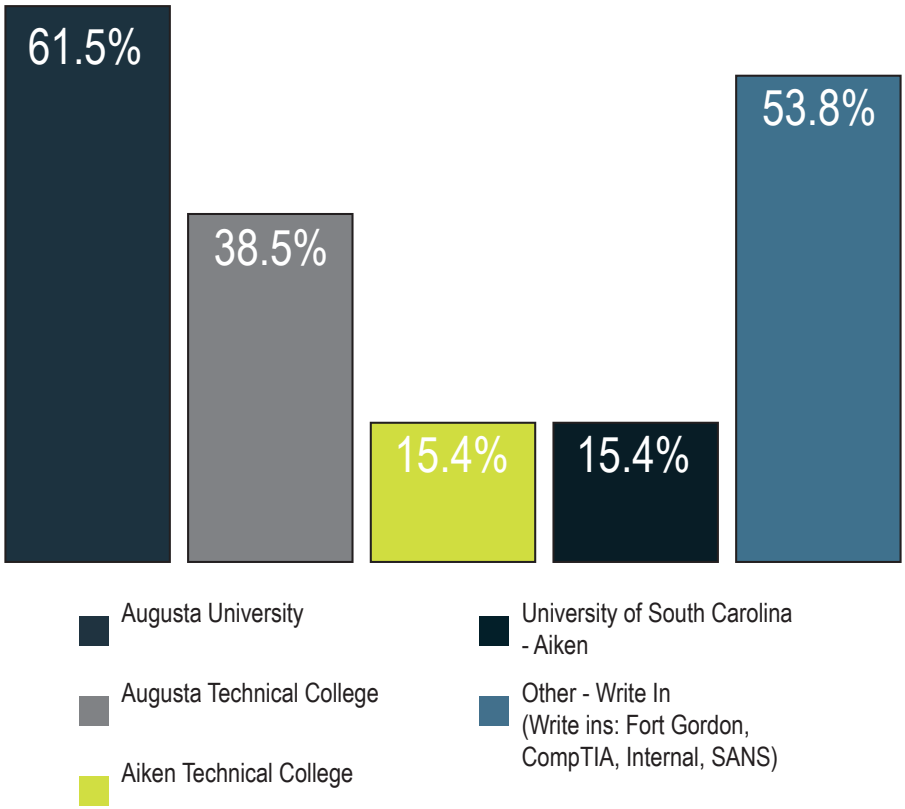
Have <u>some difficulty</u> finding qualified **entry- to mid-level** candidates jumps to <u>very difficult</u> when trying to find a **more experienced** workforce.

Appendix C: Full Survey and Results Cont'd

23. How difficult is it to find qualified experienced cybersecurity professionals at your Augusta location?



24. Which training organizations do you work with to train or upskill your workforce?



Appendix C: Full Survey and Results Cont'd

25. How important are the following items when considering candidates for available cybersecurity positions at your Augusta location?

	Do not know (N/A)	It depends	Not at all important	Some-what important	Very important	Somewhat important + very important
An industry recognized credential or certification	7%	0%	7%	33%	53%	86%
At least one year of industry-related work experience	7%	0%	0%	53%	40%	93%
A four-year college degree or higher	7%	7%	0%	40%	47%	87%
Technical training and expertise specific to the position	7%	7%	0%	47%	40%	87%

Appendix C: Full Survey and Results Cont'd

26. How important are the following certifications when considering candidates for available cyber or information security positions at your Augusta location?

	Do not know (N/A)	It depends	Not at all important	Somewhat important	Very important	Responses
GIAC Security Essentials Certification (GSEC)	18.2%	9.1%	27.3%	45.5%	0%	11
Cisco Certified Network Associate (CCNA)	0%	21.4%	14.3%	35.7%	28.6%	14
CISCO certified Network-ing Professional (CCNP)	0%	21.4%	28.6%	14.3%	35.7%	14
Security+	0%	21.4%	7.1%	28.6%	42.9%	14
Certified Information Systems Security P rofessional (CISSP)	0%	16.7%	0%	50%	33.3%	12
Certified Information Security Manager (CISM)	0%	23.1%	7.7%	46.2%	23.1%	13
Certified Information Systems Auditor (CISA)	7.7%	7.7%	15.4%	61.5%	7.7%	13
Microsoft Certified Professional (MCSA)	0%	30.8%	0%	61.5%	7.7%	13
Microsoft Certified Solu-tions Associate (MCSA)	7.1%	28.6%	0%	57.1%	7.1%	14
Offensive Security Certified Professional(OSCP)	0%	15.4%	30.8%	53.8%	0%	13
Network + Certified	0%	15.4%	23.1%	46.2%	15.4%	13
Security Clearance (Secret)	0%	15.4%	23.1%	15.4%	46.2%	13
Security Clearance (Top Secret)	0%	7.1%	28.6%	21.4%	42.9%	14
SANS/GIAC Certification	0%	33.3%	25%	25%	16.7%	12
Security Clearance (TS w/ Full Scope Poly)	0%	0%	0%	0%	100%	1

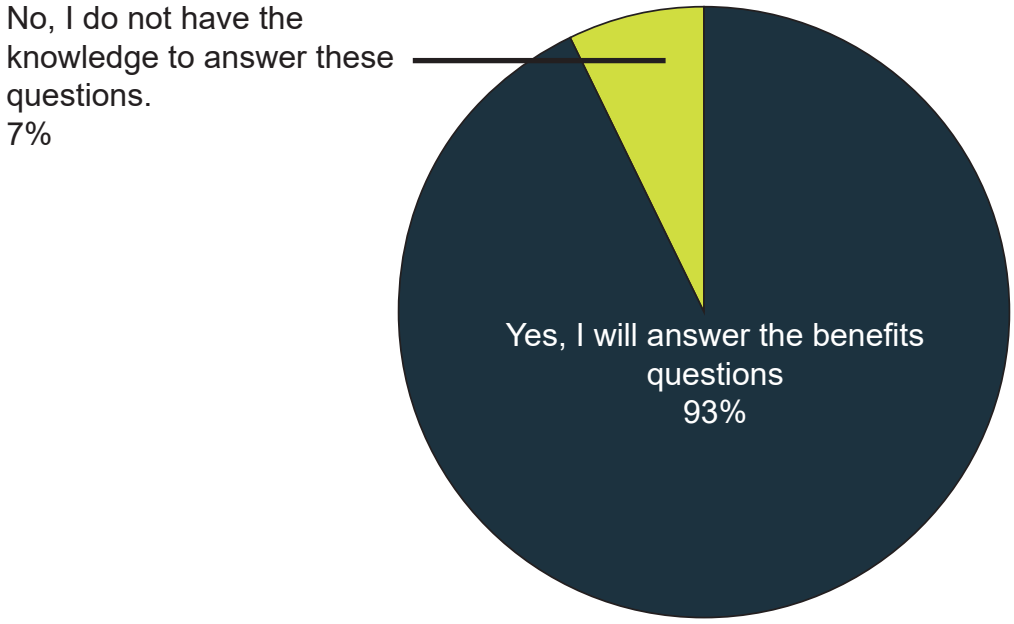
Security Clearance is the most important requirement, followed by the following certifications:

- Certified Information Systems Auditor
- Microsoft Certified Professional
- Microsoft Certified Solution Associate

Appendix C: Full Survey and Results Cont'd

27. The following questions relate to your organization's benefits. If you do not feel confident in providing approximate resonses, you may skip these questions.

If you skip, please provide contact information from someone in your office who can provide responses.

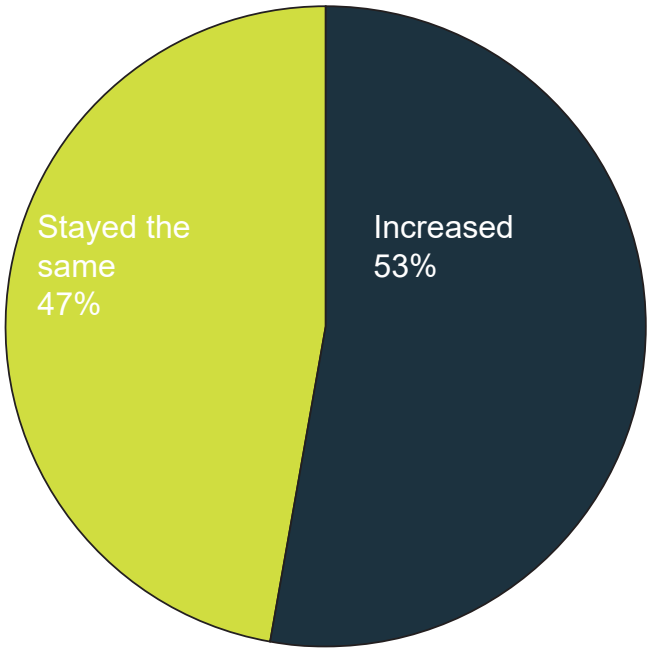


28. Please indicate benefits offered to employees.

	Yes	No
Dental (Family)	100%	0%
Medical (Family)	100%	0%
Dental (Employee)	100%	0%
Vision	100%	0%
Life	100%	0%
Optional Life	100%	0%
Short-term Disability	100%	0%
Long-term Disability	100%	0%
Prescription Drug Plan	93.3%	6.70%
HMO available	84.6%	15.40%
PPO available	85.7%	14.30%

Appendix C: Full Survey and Results Cont'd

29. At the time of your last renewal, your premium cost _____.

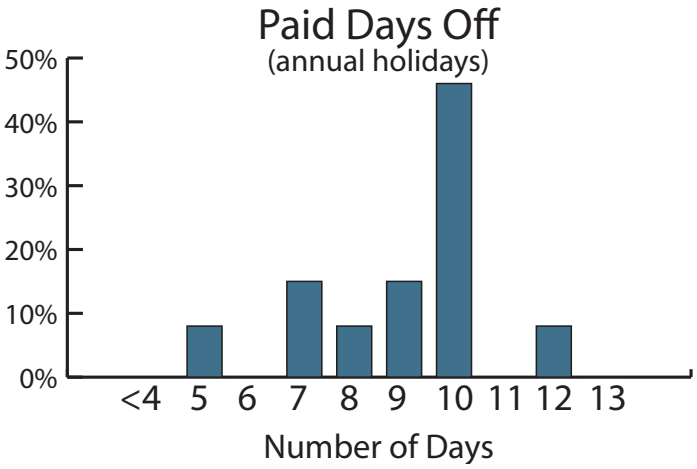


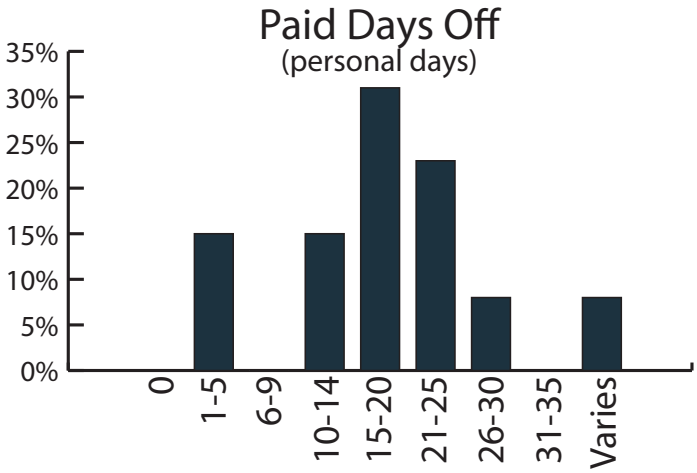
30. Does your organization offer any of the following benefits?

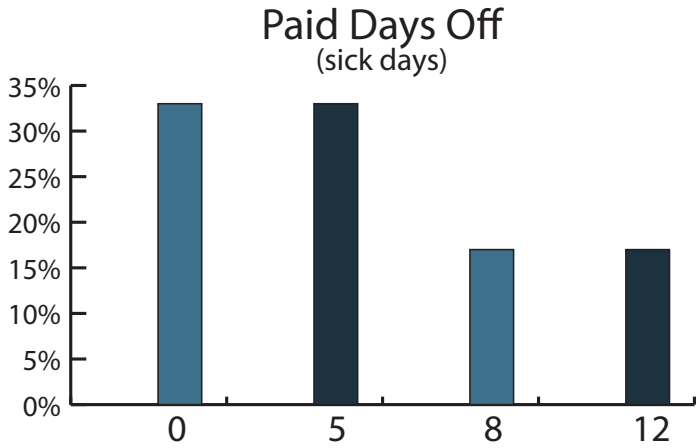
	Yes	No
401(k)	93.3%	6.7%
Stock Purchase	35.7%	64.3%
Company Paid Pension	20.0%	80.0%
Profit/Gain Share	38.5%	61.5%
Education Assistance	100.0%	0%
Bonus and commission plan following?	0%	0%
Certificate reimbursement	100.0%	0%
TRP/ORP	100.0%	0%

Appendix C: Full Survey and Results Cont'd

31. Please indicate the number of days your organization allows for the following paid time off benefits for a person with 5 years qualified experience in the industry.







Responses dropped off: 6 responders

32. After how many years of service do employees receive vacation (check all that apply)?

	After 1 year of employment	2 years	3 years	4 years	5-7 years	8-9 years	10+ years	Total
1 week vacation	100%	0%	0%	0%	0%	0%	0%	5
2 weeks vacation	80%	20%	0%	0%	0%	0%	0%	10
3 weeks vacation	44%	11%	0%	0%	33%	0%	11%	9
4 weeks vacation	33%	0%	11%	0%	11%	0%	44%	9
5+ weeks vacation	33%	0%	0%	17%	33%	0%	17%	6
% of Total Checks	56%	8%	3%	3%	15%	0%	15%	100%

Appendix C: Full Survey and Results Cont'd

33. What do you consider to be the biggest opportunity for Augusta leadership to further development of Cyber in the MSA?

Cyber education and partnering with local industry, academic, and government entities to build a sustainable workforce and sustainable growth.
An aggressive certification program.
Generate more talent.
Publicizing the impact of cyber on the city to attract additional talent and industry.
Visibility of opportunities. Community based initiatives.
The continued development of the Augusta downtown area (new housing, dining, entertainment, etc.) is critical to attract the younger cyber talent needed to meet the demand of cyber jobs (in both the public and private sector) and to make Augusta an internationally recognized cyber hub.
Quality of life improvements to attract cyber/IT talen to relocate to Augusta area.
Collaboration of industry professionals.
Access to qualified software development talent.
A revitalized downtown that attracts young workforce to relocate here. Improved K-12 education to attract families in cybersecurity arena to relocate here
The biggest opportunity is the proximity to Fort Gordon: Army Cyber Command, Army Cyber Center, Cyber School, Cyber Protection Brigade, NSA/CSS Georgia, etc.
Getting the incubator concept moving for the GCC so cyber opportunities are borne, developed, evaluated, and delivered from Augusta.

Appendix D: Members of Technology Association of Georgia located in the Augusta MSA

Company	
A3 Missions	JASINT Consulting and Technologies, LLC
Aecom	LEAD Endeavors LLC
Alanguard	MOSAIC Technologies Group, LLC
Assured Bridge	Network Designs, Inc.
Assured Information Security (AIS)	Northrop Grumman
ATLASTA.NET	OPS Consulting, LLC
BAE Systems	Palmetto Cyber, LLC
Booz Allen Hamiltion	Parsons Corporation
CALIBRE Systems, Inc.	PC Techware, Inc
Carolina Business Equipment	Peraton
CenCore, LLC	Perspecta (Peraton)
Chase Cyber, Inc.	Quantum Dynamics
Chateau-Lav	Raytheon
Community Cyber	Rendition Infosec
Corsica Technologies	RLM Communications, Inc.
Cyber Discovery Group	SAIC
Cyber Fusion Innovation Center (CFIC)	Savannah River National Laboratory
Cyber Security Solutions	Security Management and Integration
Cyber Security Solutions Inc.	Security Onion Solutions, LLC
CyberSafe360, LLC	SOFTACT Solutions, LLC
CYNWAVE Solutions, LLC	Steelgate, LLC
Defense Digital Service	Systematech Co.
H2	The PED Group, LLC
IntelliGenesis LLC	theClubhou.se
IntelliSystems	Two Six Labs
JANUS Research Group	Unisys
	Zapata Technology

Appendix E: Top Cybersecurity Companies in 2021

Source: Cybersecurity Ventures

Company	Year Established	Headquarters	Description
United States			
ThreatConnect	2011	Arlington VA	Threat-Centric Security Operations
Telos	1969	Ashburn VA	Cybersecurity Solutions & Services
OneTrust	2016	Atlanta GA	Privacy, Security & Data Governance
Pindrop Security	2011	Atlanta GA	Cybersecurity for Call Centers
Secureworks	1999	Atlanta GA	Cybersecurity Solutions & Services
Forcepoint	2016	Austin TX	Integrated Cloud Security Platform
SailPoint	2005	Austin TX	Cloud Identity Governance Platform
SparkCognition	2013	Austin TX	AI & ML Powered Cyber Defense
ZeroFOX	2013	Baltimore MD	Digital Risk Protection Platform
RSA	1982	Bedford MA	Digital Risk Management Solutions
Auth0	2013	Bellevue WA	Identity Platform for Developers
BitSight	2011	Boston MA	Security Ratings Platform
Cybereason	2012	Boston MA	Cyber Defense & Response Platform
iboss	2003	Boston MA	Cloud Network Security Platform
Rapid7	2007	Boston MA	Security & Compliance Solutions
Tufin	2005	Boston MA	Network Security Policy Automation
LogRhythm	2003	Boulder CO	Next Generation SIEM Platform
Veracode	2006	Burlington MA	Application Security Platform
Devo	2011	Cambridge MA	Cloud Native Security Analytics
ReversingLabs	2009	Cambridge MA	Advanced Malware Analysis Platform
Darktrace	2013	Cambridge, UK	Cyber AI Technology & Platform
Barracuda	2003	Campbell CA	Email, Network & Cloud Security
Bitglass	2013	Campbell CA	Cloud Data & Threat Protection
Fortalice	2008	Charlotte NC	Customized Cyber Defense Services
Keeper Security	2011	Chicago IL	Enterprise Password Management
KnowBe4	2010	Clearwater FL	Security Awareness Training Platform
Immuta	2014	College Park MD	Data Privacy & Security Platform
Tenable	2002	Columbia MD	Vulnerability Management Platform
Zix	1988	Dallas TX	Email Encryption & Security Solutions
CyberGRX	2015	Denver CO	Cyber Risk Management Platform
Deepwatch	2015	Denver CO	Managed Security Services
Ping Identity	2001	Denver CO	Intelligent Identity Platform

Appendix E: Top Cybersecurity Companies in 2021 Cont'd

Source: Cybersecurity Ventures

Company	Year Established	Headquarters	Description
United States			
Arcserve	1983	Eden Prairie MN	Data & Ransomware Protection
Arctic Wolf	2012	Eden Prairie MN	Cloud Native Security Operations
Agari	2009	Foster City CA	Email & Phishing Threat Protection
Qualys	1999	Foster City CA	Cloud Based Security Platform
Attivo Networks	2011	Fremont CA	Cyber Threat Detection Platform
Enveil	2016	Fulton MD	Data Encryption & Security
Refirm Labs	2017	Fulton MD	Firmware Security Analysis
Sonatype	2008	Fulton MD	Open Source Security Management
Dragos, Inc.	2013	Hanover MD	Industrial Control Systems Security
Expel	2016	Herndon VA	Managed Detection & Response
GuidePoint Security	2011	Herndon VA	Cybersecurity Solutions & Services
BeyondTrust	2006	Johns Creek GA	Privileged Access Management
Tanium	2007	Kirkland WA	Endpoint Management Platform
Imprivata	2001	Lexington MA	Healthcare Digital Identity
Contrast Security	2014	Los Altos CA	Application Security Platform
vArmour	2011	Los Altos CA	Application Security Management
Orca Security	2019	Los Angeles CA	Cloud Security Platform
RangeForce	2014	Manassas VA	Cloud Based Cyber Range Platform
IronNet	2014	McLean VA	Cyber Defense Platform & Services
Cimcor	1997	Merrillville IN	IT Integrity, Security & Compliance
BVSystems	1972	Metuchen NJ	Wireless Threat Detection Tools
FireEye	2004	Milpitas CA	Cybersecurity Solutions & Services
SonicWall	1991	Milpitas CA	Cybersecurity Products & Services
Code42	2001	Minneapolis MN	Insider Risk Detection & Response
Entrust	1994	Minneapolis MN	Digital Security & Issuance
Kaspersky	1997	Moscow Russia	Cybersecurity for Home & Business
Menlo Security	2012	Mountain View CA	Web & Email Security Platform
SentinelOne	2013	Mountain View CA	AI Powered Security Platform
Cloud Range	2018	Nashville TN	Next Generation Cyber Range
Avanan	2014	New York City NY	Cloud Email Security Platform
Axonius	2017	New York City NY	Cybersecurity Asset Management

Appendix E: Top Cybersecurity Companies in 2021 Cont'd

Source: Cybersecurity Ventures

Company	Year Established	Headquarters	Description
United States			
Beyond Identity	2019	New York City NY	Passwordless Identity Management
BigID	2015	New York City NY	Data Privacy & Protection
BlueVoyant	2017	New York City NY	Managed Security Services
Claroty	2014	New York City NY	Operational Technology Security
Deep Instinct	2015	New York City NY	Deep Learning Cybersecurity
HYPR	2014	New York City NY	Secure Authentication Platform
IntSights	2015	New York City NY	Threat Intelligence Platform
Prove	2008	New York City NY	Security Platform for Phone Identity
SCADAfence	2014	New York City NY	OT & IoT Cybersecurity Platform
SecurityScorecard	2013	New York City NY	Security Ratings & Risk Management
Varonis	2005	New York City NY	Enterprise Data Security Platform
INTRUSION	1983	Plano TX	Security-as-a-Service Appliance
Tripwire	1997	Portland OR	Security & Compliance Solutions
Sumo Logic	2010	Redwood City CA	Cloud Security Platform
Synack	2013	Redwood City CA	Crowdsourced Penetration Testing
Venafi	2000	Salt Lake City UT	Machine Identity Protection
Mitek	1986	San Diego CA	Digital Identity Verification
Abnormal Security	2018	San Francisco CA	Cloud Native Email Security
Bugcrowd	2011	San Francisco CA	Crowdsourced Security Platform
Cloudflare	2009	San Francisco CA	Cybersecurity for the Internet
Coalition	2017	San Francisco CA	Cybersecurity & Cyberinsurance
ForgeRock	2010	San Francisco CA	Identity & Access Management
HackerOne	2012	San Francisco CA	Hacker Powered Security Platform
Lookout	2007	San Francisco CA	Mobile Endpoint Security
Okta	2009	San Francisco CA	Identity & Access Management
OneLogin	2009	San Francisco CA	Identity & Access Management
Sysdig	2013	San Francisco CA	Secure DevOps Platform
ValiMail	2015	San Francisco CA	Cloud-Based Email Security
A10 Networks	2004	San Jose CA	Secure Cloud Application Services
Forescout	2000	San Jose CA	Unified Device Visibility for IT & OT
Securiti	2018	San Jose CA	Data Privacy & Security Platform

Appendix E: Top Cybersecurity Companies in 2021 Cont'd

Source: Cybersecurity Ventures

Company	Year Established	Headquarters	Description
United States			
Vectra	2010	San Jose CA	Cyber Threat Detection & Response
Zscaler	2008	San Jose CA	Enterprise Cloud Security Platform
GM Sectec	1970	San Juan, Puerto Rico	Managed Security Services
Imperva	2002	San Mateo CA	Data & Application Security
Centrify	2004	Santa Clara CA	Privileged Identity Management
Kenna Security	2009	Santa Clara CA	Modern Vulnerability Management
McAfee	1987	Santa Clara CA	Cybersecurity for Home & Business
Netskope	2012	Santa Clara CA	Cloud, Network & Data Security
Palo Alto Networks	2005	Santa Clara CA	Cyber Threat Detection & Prevention
Trusona	2015	Scottsdale AZ	Enterprise-wide Passwordless MFA
DomainTools	2002	Seattle WA	Threat Intelligence & Investigation
ExtraHop	2013	Seattle WA	Cloud-Native Detection & Response
F5	1996	Seattle WA	Application & Infrastructure Security
WatchGuard	1996	Seattle WA	Network & Endpoint Security
Recorded Future	2009	Somerville MA	Universal Threat Intelligence Solution
CrowdStrike	2011	Sunnyvale CA	Endpoint Protection Platform
Fortinet	2000	Sunnyvale CA	End-to-End Infrastructure Security
Illumio	2013	Sunnyvale CA	Security Segmentation Platform
Proofpoint	2002	Sunnyvale CA	Enterprise Security & Compliance
ReliaQuest	2007	Tampa FL	SaaS Security Platform
NortonLifeLock	1982	Tempe AZ	Cyber Safety Protection
Digital Guardian	2003	Waltham MA	Enterprise Data Loss Prevention
International			
1Password	2005	Toronto, Canada	Secure Enterprise Password Manager
Absolute	1993	Vancouver, Canada	Endpoint Defense Platform
BlackBerry	1984	Waterloo, Canada	End-to-End IoT Security Solutions
eSentire	2001	Waterloo, Canada	Managed Detection & Response
Sophos	1985	Abingdon, UK	Cybersecurity for Home & Business

Appendix E: Top Cybersecurity Companies in 2021 Cont'd

Source: Cybersecurity Ventures

Company	Year Established	Headquarters	Description
International			
BreachLock	2018	Amsterdam, Netherlands	PenTesting-as-a-Service
ESET	1992	Bratislava, Slovakia	Cybersecurity for Home & Business
Bitdefender	2001	Bucharest, Romania	Cybersecurity for Home & Business
F-Secure	1999	Helsinki, Finland	Cybersecurity for Home & Business
Skybox Security	2002	Herzliya Israel	Security Posture Management
Karamba Security	2015	Hod Hasharon, Israel	Automotive Security & IoT Protection
ThetaRay	2013	Hod Hasharon, Israel	Big Data Security Analytics
Digital Shadows	2011	London, UK	Digital Risk Protection Solutions
Mimecast	2003	London, UK	Email Security & Continuity
Onfido	2012	London, UK	Biometric & Document Verification
Privitar	2014	London, UK	Enterprise Data Privacy
Snyk	2015	London, UK	Cloud Native Application Security
NCC Group	1999	Manchester UK	Cybersecurity & Risk Mitigation
CyberArk	1999	Petach Tikva, Israel	Privileged Access Security
Avast	1988	Prague, Czechia	Antivirus, VPN & Security
Cyberbit	2015	Ra'anana, Israel	Cyber Range Training & Sim
Aqua Security	2015	Ramat Gan, Israel	Cloud Native Application Protection
Checkmarx	2006	Ramat Gan, Israel	Software Security for DevOps
Semperis	2013	Ramat Gan, Israel	Identity Driven Cyber Resilience
Cymulate	2016	Rishon LeZion, Israel	Breach & Attack Simulation Platform
Secure Code Warrior	2015	Sydney, Australia	Developer Secure Code Training
BioCatch	2010	Tel Aviv, Israel	AI-Driven Behavioral Biometrics
Cato Networks	2015	Tel Aviv, Israel	Cloud Network Security Platform
Check Point	1993	Tel Aviv, Israel	Cybersecurity Solutions & Services
Guardicore	2013	Tel Aviv, Israel	Hybrid Cloud Security Platform
Hysolate	2016	Tel Aviv, Israel	Workspace-as-a-Service Platform
IronScales	2013	Tel Aviv, Israel	Self-Learning Email Security
Perimeter 81	2018	Tel Aviv, Israel	Secure Access for Remote Workforce
Trend Micro	1988	Tokyo, Japan	Cloud Security Services Platform

Appendix F: Top Cybersecurity Consulting Firms

Company	Location
Cylance	Irvine, CA
Optiv	Denver, CO
IANS	Boston, MA
Equilibrium IT Solutions	Chicago, IL
Flashpoint	New York, NY
Myriad360	New York, NY
EzeCastle	Boston, MA
Lucideus	Palo Alto, CA
SecureWorks	Atlanta, GA
inCyberSecurity	Chicago, IL
SecurityScorecard	New York, NY
Deloitte	New York, NY
Cisco	San Jose, CA
FireEye	Milpitas, CA
Accenture	Chicago, IL
IBM	Armonk, NY