CYBERSECURITY
EMERGING TECHNOLOGY SKILLS GAP ANALYSIS

Compiled by the Workforce Intelligence Network for Southeast Michigan on behalf of the Ralph C. Wilson, Jr. Foundation

SPRING 2020

WIN WORKFORCE INTELLIGENCE NETWORK

RALPH C. WILSON, JR. FOUNDATION

ABOUT THIS REPORT

The **Ralph C. Wilson, Jr. Foundation** is supporting two reports detailing the emerging technologies talent system in southeast Michigan. This report is focused on cybersecurity and will analyze the current and emerging technology workforce in southeast Michigan. Where appropriate, national comparisons are included as well. This report builds upon and updates the original Cybersecurity Skills Gap Analysis published by WIN in 2017 in connection with the Office of Economic Adjustment, Department of Defense[1].

This complementary report seeks to analyze changes in the emerging technologies talent system. Understanding the complexity of the talent supply for cybersecurity and other considerations for upcoming technologies will aid continued economic growth in the region. New occupations will be created to sell, maintain, service and grow these technologies and their integration into teaching and service occupations. Tracking emerging technologies and their impact on the workforce is key to preparing secondary, post-secondary, and other educational markets for changing workforce demands from employers.

As technology continues to become embedded into many facets of life, demand for cybersecurity professionals will continue to grow. Additionally, many other occupations will need additional skills in cybersecurity familiarity and data privacy. Given the high number of training providers in southeast Michigan, the region is poised to make the most of this opportunity. As cybersecurity is important to firms at a regional, national, and global level, this analysis includes data for the entire United States where applicable.

Continued advancements in connected vehicles, the internet of things (IOT), and other, less mature technologies such as artificial intelligence and virtual reality are entwined with many facets of human life, though the impact these technologies have created is yet to be determined and analyzed.

[1] *The original report content reflected the views of the Workforce Intelligence Network and did not necessarily reflect the views of the Office of Economic Adjustment.*

CONTENTS

About WIN 4

Executive Summary 6

Introduction 10

Methodology 16

Cybersecurity Workforce Overview 20

Cybersecurity Workforce Categories 30

Workforce Guidance and Standards 42

Conclusion and Recommendations 44

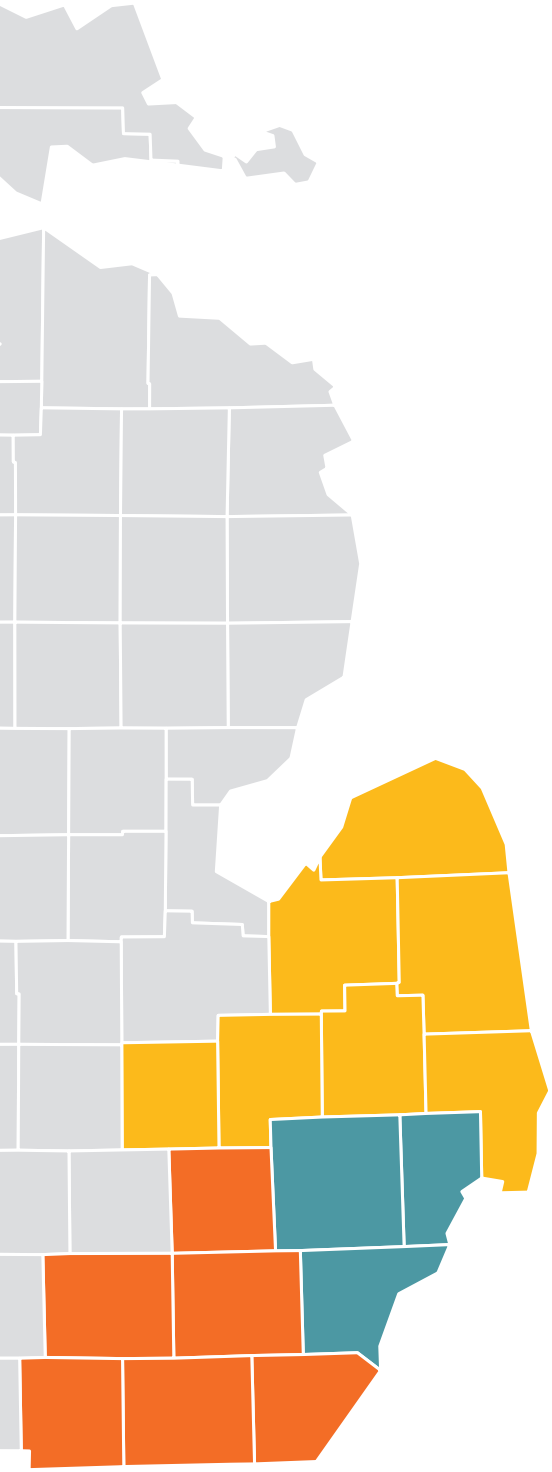
Appendices 48

ABOUT WIN

The Workforce Intelligence Network for Southeast Michigan (WIN) is a partnership of community colleges and workforce development boards, known locally as Michigan Works! Agencies (MWAs), in greater southeast Michigan. The region includes 16 counties, and consortium organizations are depicted in the map. It was established in 2011 to create a comprehensive and cohesive talent development system in the region to ensure workers are prepared for success. Accordingly, WIN serves three primary roles:

1. Gathering, analyzing, and distributing real-time labor supply and demand intelligence on workforce characteristics specific to the southeast Michigan Region;
2. Convening, facilitating, and engaging employers, and serving as the connection point for business, industry and other stakeholders as it relates to workforce development; and
3. Developing strategies and funding proposals for the delivery of regional workforce development programs through its partners.

To learn more about WIN and to explore past reports, visit www.WINintelligence.org.



Acknowledgements

The findings presented in this report were compiled and analyzed by the Workforce Intelligence Network for Southeast Michigan (WIN) in partnership with the Ralph C. Wilson, Jr. Foundation. Many thanks to Jennifer Tisdale of GRIMM and Sarah Tennant of the Michigan Economic Development Corporation (MEDC) for providing their industry expertise.


EXECUTIVE S

SUMMARY

EXECUTIVE SUMMARY

Report Overview 8

Key Findings 9

Recommendations 9

REPORT OVERVIEW

In the time since WIN's Cybersecurity Skills Gap Analysis was published, technology has continued to become integrated into most every workplace and the information workforce has grown substantially. As the technology workforce in Detroit continues to grow, along with increases in the adoption of connected vehicles and other devices, production automation, and a rise in data-sensitive industries such as finance and health care, strategies must be adopted to train cybersecurity workers and ensure all workers are primed to handle data threats. In order to better understand future cybersecurity skills needed to keep the region's workforce safe and expanding, WIN partnered with the **Ralph C. Wilson, Jr. Foundation** to analyze job postings for a broad set of occupations including both direct and indirect cybersecurity workers.

In this report, WIN examines occupations that most heavily rely on cybersecurity skills by analyzing data on the workforce's employment trends, local demand, entry requirements, and regional specialties. A broad range of occupations — including software developers and network architects as well as financiers, engineering managers, and medical data staff — must have cybersecurity skills and familiarity, and the roles of technology workers change rapidly. Therefore, the government's standard occupation codes are not nuanced enough to truly capture cybersecurity workers. The analysis carried out for this report features job posting data from Economic Modeling Systems International (Emsi) for 211 unique occupation codes, including 26 frontline cybersecurity roles as well as critical physical infrastructure designers and those whose jobs require data privacy knowledge. For a closer look, these occupations were linked to cybersecurity-specific duties through the application of keyword and industry filters in data collection. Using data from job postings in the cybersecurity space both nationally and in southeast Michigan from 2016 to 2019, WIN researchers present analysis on the demand for cybersecurity workers.

Key Findings

1. Cybersecurity needs in the workforce are difficult to capture due to lack of nuance regarding emerging and on-the-rise occupations. Additionally, many roles that are focused on technology may require a greater knowledge of cybersecurity threats and best practices than in years past.
2. Increasing adoption of connected devices and data-driven strategy means that top cybersecurity employers reflect the region's overall high-demand sectors. Catering cyber proficiency to industries such as manufacturing or health care, for example, may be necessary. In particular, cybersecurity needs pertaining to connected and automated vehicles are poised to grow in southeast Michigan in coming years.
3. The high number of training providers and high level of industry collaboration in southeast Michigan creates an opportunity to inform and create certification pathways needed for future hiring and occupation development.
4. Some level of cybersecurity familiarity is, increasingly, needed in nearly all occupations and industries. This trend creates a need for a different kind of training that broadly targets workers outside of information technology.

Recommendations

The WIN team also takes this opportunity to look forward. The following recommendations, discussed in detail in the conclusion, suggest considerations and strategies that may both help prepare the direct cybersecurity workforce in the region and provide suggestions that apply to all workers so that the technology and data-driven industries in southeast Michigan continue to expand.

01

1. In order to address the lack of information on both cybersecurity specialist roles and general workforce needs, information must be collected by level of worker to create a "cyber needs" database to target future training and standards.

02

2. Training specific to connected devices and products, including hands-on experience, must be developed and formalized. Curriculum should be oriented toward the vehicles, medical devices, wearable technology, and other industry-specific factors.

03

3. Ongoing learning via certification programs will be increasingly necessary. In combination with a cyber needs database, ongoing certifications should continue to be developed in collaboration between southeast Michigan training providers and employers to ensure new skill needs are consistently met.

04

4. Businesses should take care to continuously communicate their cybersecurity needs to workforce partners, community colleges, and other talent pipeline stakeholders in order to build a workforce with the most up-to-date possible skillset for keeping information safe.

INTRODUCTI

ION

INTRODUCTION

Cybersecurity in Southeast Michigan and the US.....12

Cybersecurity Workforce Category Descriptions.....15

CYBERSECURITY IN SOUTHEAST MICHIGAN AND THE UNITED STATES

In this report, WIN researchers aim to examine the demand metrics covered in the original report and explore major changes since publication. These metrics include the top posting employers, skills, certifications, and degrees for cybersecurity workers, salary distributions, education and experience requirements, and geographic concentration. Industry standards, including training, certifications, and entry-level worker qualifications, will be considered along with their evolution over the past years. Factors such as updated occupation codes, security clearance, and others crucial to the original report will also be touched upon.

Updated findings and recommendations are on page 9 of this report.

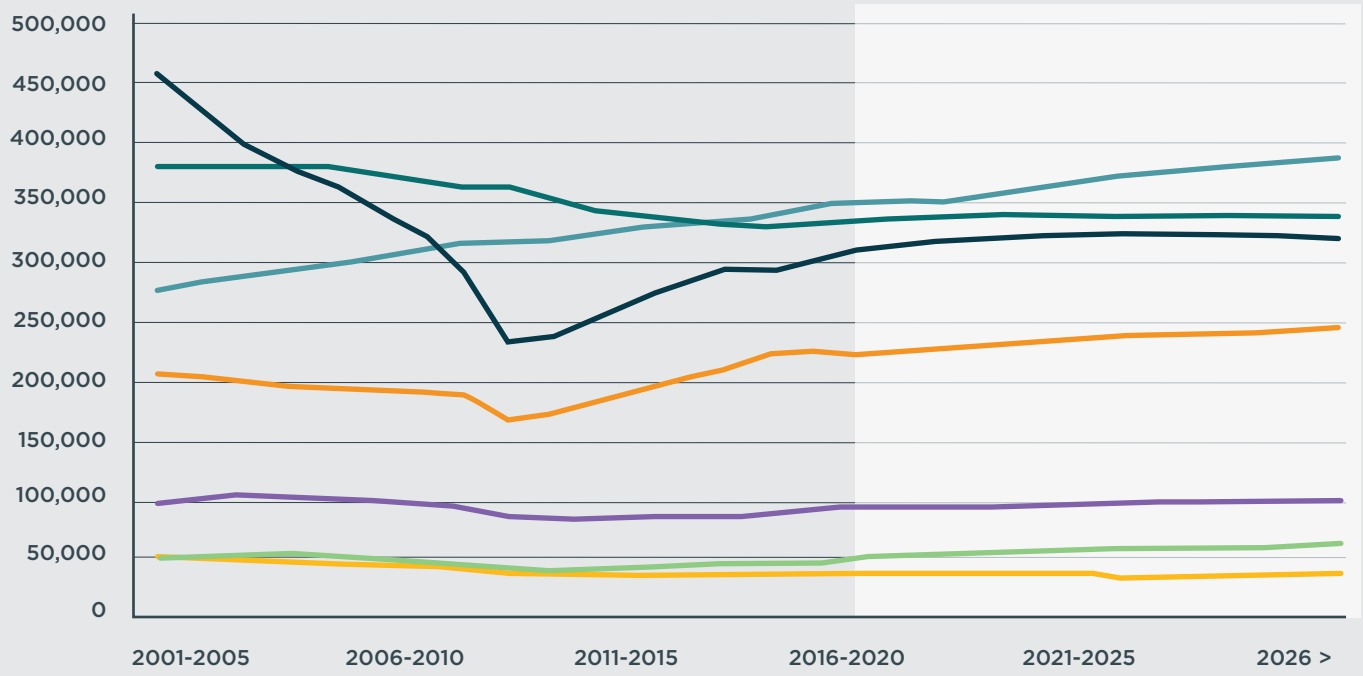
Cybersecurity and the Workforce

Both in southeast Michigan and nationwide, cybersecurity skills are increasingly important for a wide range of firms and occupations. This is especially critical in the region's manufacturing environment, as data security ensures the safety of production automation and connected vehicles and devices. Across all industries, the growing technology concentration in metro Detroit creates a need for a greater volume of workers with tech and privacy skills.

Against this backdrop, the growing need for skilled workers in cybersecurity occupations becomes clear. Cybersecurity workers use techniques and technologies to keep networks and data secure in the face of cyber-attacks. The cybersecurity workforce engages with these issues at all levels, from designing systems, to reducing vulnerability, to reacting to intrusions and attacks, to using best practices to keep data secure while working in other business functions. To the right is a chart depicting employment over time in the top industries employing cybersecurity workers. All of these information-heavy industries are projected to either grow or remain stable over the next ten years, while expansion is particularly rapid for Health Care and Social Assistance and Professional, Technical, and Scientific Services.

In order to keep these major industries strong and encourage further expansion of the tech industry, the workforce must be well-poised to handle cybersecurity threats. As cyber threats continue to evolve, this will require intentional collaboration between educational providers, employers, and the public sector to determine and teach the necessary skills. In addition to demand for talent with four-year degrees, middle skill, middle wage (MSMW) occupations provide pathways to good-paying

Employment by 2 Digit NAICS for Top Cybersecurity Industries



employment for those with short term training. Opportunities in this group are growing across cybersecurity and general information occupations, including computer support and some software development positions as well as many jobs that need data privacy understanding. This designation is described in detail within the Methodology section beginning on page 16. Each category section highlights the importance of middle-skill career opportunities and provides an overview of training and curriculum needs.

Four main categories of workers were identified during the initial research, each with distinct roles and responsibilities and cyber-related skill levels. There are many similarities between indirect cybersecurity and cybersensitive occupations, so the need for security knowledge for non-direct technology workers is discussed in a single section. The next section will provide an overview of these categories, and detailed workforce information about them begins on page 30.

Industry Color Key

- Health Care and Social Assistance
- Finance and Insurance
- Government
- Management Companies and Enterprises
- Manufacturing
- Information
- Professional, Scientific and Technical Services

Data: Emsi | Analysis: Workforce Intelligence Network

Data Security and Health Care

The need for a robust, connected health care system is growing in Michigan and across the nation as the population grows and ages. In 2016, Health Care and Social Assistance (NAICS sector 62) made up 13.5 percent of total employment in the state of Michigan. The state projects that by 2026, this figure will be up to 14.9 percent. Health care employment is projected to grow by 18.2 percent over this ten-year timeframe, more than double the statewide total of 7.0 percent employment growth.

The need to protect sensitive health data is expanding in tandem with demand. The Health Insurance Portability and Accountability Act of 1996[2] (HIPAA) was passed as the health care industry began to move away from paper processes and rely more heavily on the use of electronic information systems for clinical and administrative functions. The act includes the HIPAA Privacy Rule and the HIPAA Security Rule. The Privacy Rule establishes national standards for the protection of certain health information, while the Security Rule provides standards for the electronic transfer of that information. Today, providers are using clinical applications such as computerized physician order entry systems, electronic health records, and radiology, pharmacy, and laboratory systems. Online portals for insurance and clinics provide access to claims, care management, and self-service applications. With ongoing advancements in embedded technology, medical data accessibility and communication will only expand. While this means that the medical workforce can be more mobile and efficient, the rise in the adoption rate of these technologies increases the potential security risks.

Employer demand for healthcare workers with strong cybersecurity skills can be estimated by comparing job posting levels to employment. For example, only 1.3 percent of total workers in the Health Care and Social Assistance industry in southeast Michigan are classified as frontline cybersecurity occupations. Double that amount, 2.6 percent, of online health care industry job postings seek highly cybersensitive occupations and specifically require cybersecurity qualifications. Health care providers are cognizant of the importance of an informed workforce to keep data safe at all levels, however: 13.6 percent of all health care industry postings across all occupations call for cybersecurity skills.

---

[2] *United States Department of Health and Human Services. (2013).*

CYBERSECURITY WORKFORCE CATEGORY DESCRIPTIONS

Cybersecurity occupations employ techniques and technologies to keep networks and data secure. The cybersecurity workforce manages issues at all levels, including designing systems to reduce vulnerability, reacting to intrusions and cyber-attacks, and using best practices to keep data secure working in other business functions. Four main categories of workers were identified in this research with distinct roles and responsibilities and cyber-related skill levels. The categories are:

Frontline Cybersecurity

Frontline cybersecurity occupations are responsible for the design and direct implementation of a firm's cybersecurity strategy, such as network administrators, software developers, and information security analysts. This category includes Cyber-Physical Systems (CPS) security workers, who are central to the securing of data, PII, or other data elements which may be at risk through digital, WiFi, and Bluetooth connected devices.

Physical Security

Physical security occupations are defined in this report as those responsible for the physical security of data, computers or infrastructure, or who may have physical access to these assets while doing other work. Workers who might address the aftermath or investigation of a cyber-attack that has a physical effect, including law enforcement, are also included in this group. Other physical security occupations include security guards, maintenance and repair workers, and retail loss prevention specialists.

Cybersensitive Occupations and Indirect Cybersecurity

Indirect cybersecurity occupations have a general knowledge of cybersecurity, and although workers do not have distinct cybersecurity duties, they still may handle sensitive data. Occupations such as accountants, managers, or customer service workers may interact with systems or tools that may be vulnerable to cyber-attacks. There are gradients of need for cyber skills, so this category is further divided into two sub-categories. Indirect workers may occasionally interact with sensitive or private data or be able to take simple measures to prevent cyber infiltration. This includes workers who interact with software or the internet as part of their duties.


METHODOLO

OGY

METHODOLOGY

Purpose, Timeframe, and Geography 18

PURPOSE, TIMEFRAME, AND GEOGRAPHY

This update to the Cybersecurity Skills Gap Analysis report released by WIN in 2017 was compiled using data on employer demand, gleaned from online job advertisements, from Economic Modeling Specialists International (Emsi). It also includes employment and wage data from the Bureau of Labor Statistics (BLS). The data contained in this report is primarily for the 16 southeast Michigan counties covered by WIN unless otherwise noted. Employment is measured for 2001 to 2018 and projected out to 2028, while online posting data reflects October 2018 to September 2019. All data is focused on occupations categorized by the WIN research team. For a complete list of occupations please see Appendix A.

Occupation Selection

Cybersecurity occupations are emerging and on-the-rise, so typical occupation codes are not nuanced enough to truly capture all workers that need cybersecurity skills. Additionally, many roles that are focused on technology, security, or data privacy may require a greater knowledge of cybersecurity threats and best practices than in years past. WIN's method begins with Standard Occupation Classification (SOC) codes, which are government-defined occupation codes, refined through industries and keywords to better catalog job postings that may be for cybersecurity-focused workers. Combining the list of keywords and occupations that likely align with cybersecurity allows WIN to analyze the data about different areas of these workers in depth.

The first step in the research process was to review the original cybersecurity occupation list to update based on the scope of this report. Using cybersecurity-focused keywords and industry staffing pattern data, WIN researchers defined occupations with applicable knowledge and skillsets necessary to meet the growing demand for cybersecurity skillsets both in and out of programming positions. See the Category Descriptions beginning on page 32 to learn more about the categories used in this report. See Appendix C for a list of all documents used for the literature review, and Appendix B for a list of the keywords and industry filters used.

WIN research typically uses occupations, as opposed to industries, to narrow labor market analysis to the level of the worker. Individuals working in specific occupations can be employed across multiple industries. As cybersecurity workers are employed across many industries, other methods of refining demand information are needed as well. Data pertaining to standards for required training and proficiency in cybersecurity are scarce. Job postings provide insight on what skills companies desire and get a sense of upcoming trends. Keywords for common skills and certifications needed for cybersecurity-focused workers were determined and used to filter job postings. This data may not provide a comprehensive total of cybersecurity workers employed within organizations. Moreover, though familiarity with information security may be an expectation for many positions, it may not be mentioned in all job postings.

Other Occupation Designations

CyberSeek

CyberSeek is a resource supported by Burning Glass Technologies, The Computing Technology Industry Association (CompTIA), and The National Initiative for Cybersecurity Education (NICE). It is designed to provide a data tool serving employers, educators, guidance and career counselors, students, current workers, policymakers, and other stakeholders. The interactive tool includes a supply and demand heat map and a career pathway guide that shows key roles, common transition opportunities, and detailed occupation information. The tool is focused on career pathways for frontline cybersecurity workers; this report is complementary with respect to its broad examination of cybersecurity needs in the workforce, demand trend consideration, and detailed regional data.

Middle Skill Middle Wage Jobs

Middle skill middle wage (MSMW) occupations are important to this industry because they offer pathways for skilled workers without a four-year degree and provide the skills necessary for advancement in these occupations. Middle skill occupations are those that require some education and training beyond high school, but do not require a bachelor's degree. Typically, a wage component is also included when denoting middle skill jobs, i.e., these occupations must earn more than the national, state or local median wage. The importance of middle skill jobs to the United States (and regional economies) cannot be understated — while in the coming years there will be negative job growth for those occupations requiring only a high school diploma or less, middle skill jobs in all occupation groups and industries are expected to grow by eight percent by 2028 in the U.S.

The occupation categories used by CyberSeek to categorize workers were established by the National Initiative for Cybersecurity Education (NICE), which itself was created by the National Institute for Standards and Technology (NIST). The categories, which may be used to further break out the frontline category within this report, include:

- **Securely Provision:** Conceptualizes, designs, and builds secure IT systems
- **Operate and Maintain:** Provides the administration and maintenance necessary for effective performance and security
- **Oversee and Govern:** Provides leadership, management, direction, or development and advocacy for cybersecurity work
- **Protect and Defend:** Identifies, analyzes, and mitigates threats to internal IT systems and/or networks
- **Analyze:** Performs highly specialized review and evaluation of incoming cybersecurity information
- **Collect and Operate:** Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence
- **Investigate:** Investigates cybersecurity events or crimes related to IT systems, networks, and digital evidence


CYBERSECU
FORCE OVER

RITY WORK-
RVIEW

CYBERSECURITY WORKFORCE OVERVIEW

The Importance of a Cyber-Aware Workforce.....22

Worker Demand Trends 23

Cybersecurity and National Security 28

THE IMPORTANCE OF A CYBER-AWARE WORKFORCE

Tech worker or not, cybercrime has the ability to impact individuals and companies of all kinds. Taking steps to raise familiarity with security practices can help mitigate the impacts. According to a global survey conducted by Norton LifeLock[3] in 2018, 800 million adults in 16 countries had been the victims of cybercrime in the last year, and 117 million individuals were impacted by identity theft. About 38 percent of those experiencing cybercrime had a financial loss, and on average the issues took six hours to resolve. In many cases, simple measures such as not sharing passwords, not opening suspicious files or links, and limiting information shared on social media can make the biggest difference. But in order to encourage these measures, workers must understand their importance. Also as reported by Norton, 40 percent of individuals were using paid antivirus software, and 36 percent utilized an identity theft protection service. Cybercrime can impact organizations as well as individuals; when the data breach includes not only employees, but also clients and partner companies, these attacks can be extremely costly. Below, the number of breaches across the United States, broken down by industry, can be seen.

From the Identity Theft Resource Center End-of-Year Data Breach Report[4]

ITRC Comparison of Breaches in 2017 and 2018				
Industry	2018		2017	
	Number of Breaches	Number of Records Exposed	Number of Breaches	Number of Records Exposed
Banking/Credit/Financial	135	1,709,013	134	3,230,308
Business	571	415,233,143	907	181,630,520
Education	76	1,408,670	128	1,418,455
Government/Military	363	18,236,710	79	6,030,619
Medical/Healthcare	363	9,927,798	384	5,302,845
Annual Totals	**1,244**	**446,515,334**	**1,632**	**197,612,748**

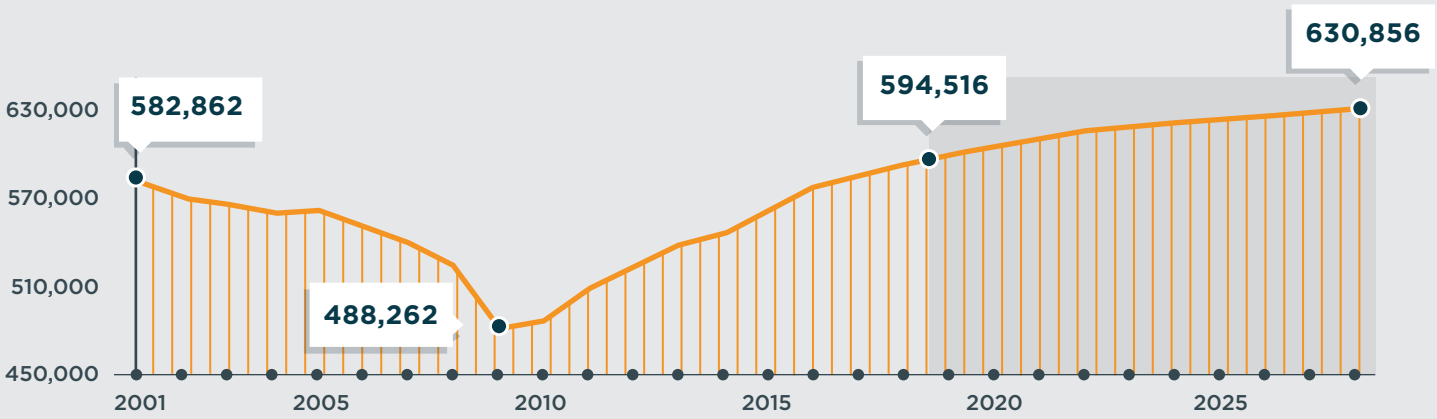
In order to prevent and lessen the cost of identity theft and cybercrime, it is important to understand which workers work most closely with sensitive information or developing cybersecurity defense systems. In addition, employment and demand information may address preventative measures that can be taken at all levels, as well as helpful skills and training opportunities.

[3] *NortonLifeLock. (2019).* [4] *Pescatore. (2019).*

Worker Demand Trends

Each occupation category includes detailed information on employment trends and top occupations; to provide a snapshot of the overall landscape of cybersecurity needs, an aggregation of frontline cyber workers, physical security workers, and the most cybersensitive information workers is presented here. The occupations are detailed in Appendix A. Employment for these exceptionally cyber-intensive workers has increased by 21.8 percent, or over 100,000 workers, since 2010. Growth is projected to continue through 2028 by an additional 6.1 percent, adding 36,000 individuals to the workforce. The fastest-growing occupations are shown in the table below.

Cybersecurity Employment in Southeast Michigan, 2001-2028



Past and Projected Growth for Information Workers, 2010-2028

SOC	Description	2018 Jobs	2010-2018 % Change	2018-2028 % Change
13-2061	Financial Examiners	433	148.8%	17.0%
15-1199	Computer Occupations, All Other	7,522	138.0%	6.3%
13-1161	Market Research Analysts and Marketing Specialists	11,931	119.4%	20.4%
13-1081	Logisticians	5,473	94.9%	5.2%
15-1122	Information Security Analysts	1,124	92.0%	29.1%
11-3121	Human Resources Managers	2,316	89.0%	8.8%
15-1132	Software Developers, Applications	22,116	87.3%	14.6%
41-3031	Securities, Commodities, and Financial Services Sales Agents	6,017	83.0%	7.4%
15-2031	Operations Research Analysts	1,340	77.6%	29.5%
17-2112	Industrial Engineers	23,041	74.7%	11.0%
11-3051	Industrial Production Managers	7,501	71.9%	3.0%
17-2141	Mechanical Engineers	33,655	65.5%	6.1%
17-2071	Electrical Engineers	6,590	61.5%	11.6%
15-1134	Web Developers	1,669	59.7%	13.1%
13-1041	Compliance Officers	3,624	59.3%	10.2%
11-3071	Transportation, Storage, and Distribution Managers	1,650	49.8%	14.1%
13-2051	Financial Analysts	4,268	48.9%	10.3%
11-9021	Construction Managers	2,349	48.4%	20.5%
11-2021	Marketing Managers	2,828	48.3%	14.5%
11-9041	Architectural and Engineering Managers	7,618	47.6%	8.3%

Data: Emsi | Analysis: Workforce Intelligence Network

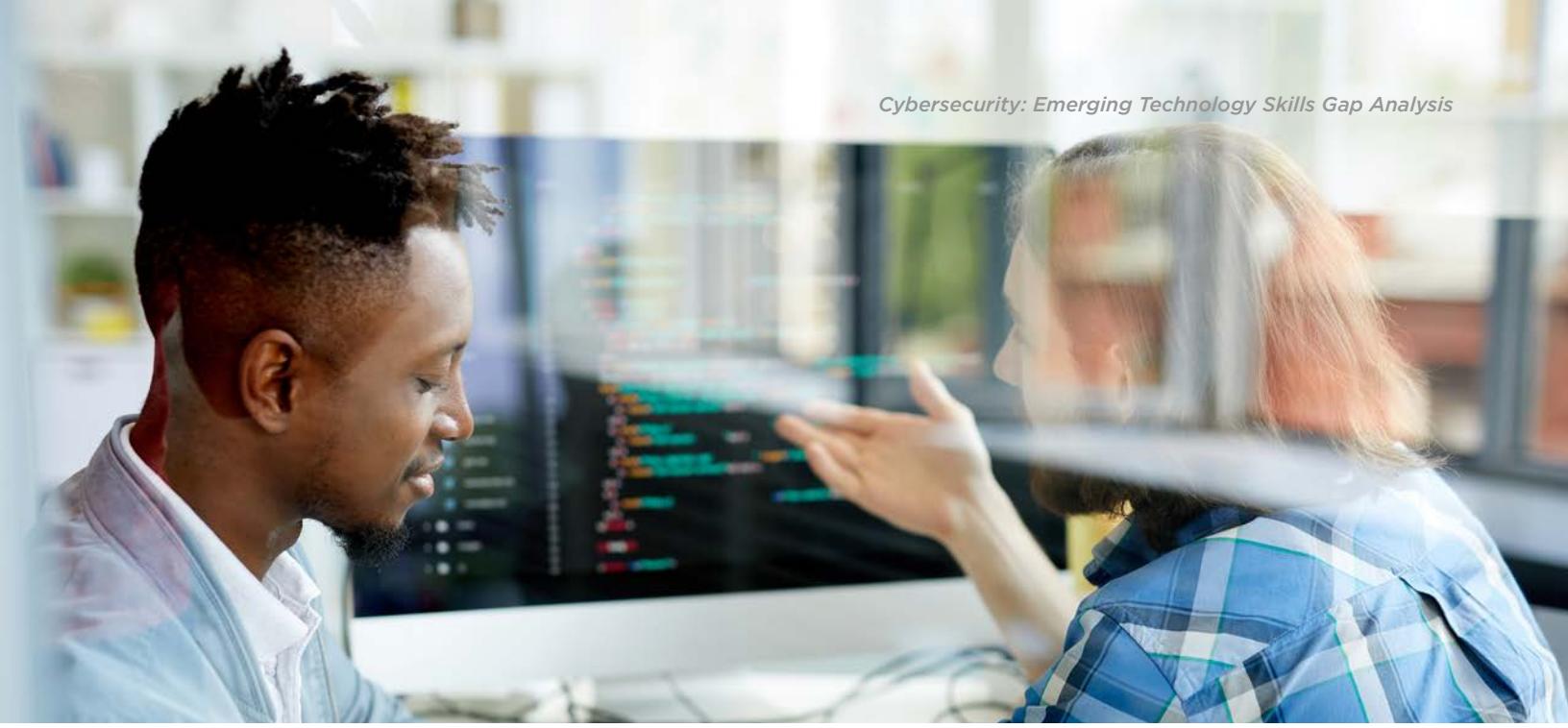
What does “Computer Occupations, All Other” encompass?

The second-fastest growing and third most posted occupation may seem a little general. This occupation is a category including small, detailed occupations, presented in the table below, as well as any other technology worker who does not fit a pre-existing category. Observing trends in this occupation, such as job titles, skills, and certifications, can help us observe emerging roles in cybersecurity, automation, and more, and potentially become the basis for major occupation designations in the future.

Postings by Detailed Occupation Under "Computer Occupations, All Other"

Occupation (O*NET)	Unique Postings (Oct 2018 - Sep 2019)
Software Quality Assurance Engineers and Testers	865
Computer Systems Engineers/Architects	820
Information Technology Project Managers	714
Business Intelligence Analysts	27
Geographic Information Systems Technicians	5
Document Management Specialists	5
Search Marketing Strategists	4
Web Administrators	2
Geospatial Information Scientists and Technologists	1
Database Architects	1

Data: Emsi | Analysis: Workforce Intelligence Network



From October 2018 through September 2019, there were 331,600 job postings for cybersecurity-related workers in the region. The top posted occupations are shown below.

Top Occupations for All Information Workers

Occupation (SOC)	Unique Postings (Oct 2018 - Sep 2019)
Software Developers, Applications	25,777
Mechanical Engineers	15,030
Computer Occupations, All Other	14,923
Industrial Engineers	13,589
Maintenance and Repair Workers, General	12,806
First-Line Supervisors of Office and Administrative Support Workers	12,439
Accountants and Auditors	11,893
Sales Managers	10,112
General and Operations Managers	9,736
Computer User Support Specialists	9,256
Insurance Sales Agents	9,124
Computer Systems Analysts	8,642
Marketing Managers	7,827
Secretaries and Administrative Assistants, Except Legal, Medical, and Executive	7,413
Web Developers	7,410

Data: Emsi | Analysis: Workforce Intelligence Network

When postings are filtered for cybersecurity and data privacy related skills and certifications, there were 138,000 postings in southeast Michigan. Note the changes in top posted jobs. In addition, the advertised salary for cybersecurity-specific postings is about $2,000 higher than for all postings for these occupations. Top posting industries remain consistent between the two, while the list of high-demand skills in the cybersecurity-specific set of advertisements is much more heavily dominated by programming languages. Automation and auditing are major skills needed in all postings for these occupations.

Top Occupations for Information Workers with Cybersecurity Skills

Occupation (SOC)	Unique Postings (Oct 2018 - Sep 2019)
Software Developers, Applications	9,052
Software Developers, Systems Software	3,138
Computer Occupations, All Other	2,464
Insurance Sales Agents	2,368
Information Security Analysts	2,210
Secretaries and Administrative Assistants, Except Legal, Medical, and Executive	1,594
First-Line Supervisors of Office and Administrative Support Workers	1,569
Accountants and Auditors	1,555
Web Developers	1,530
Mechanical Engineers	1,490
Computer Programmers	1,340
Executive Secretaries and Executive Administrative Assistants	1,233
Sales Managers	1,224
Computer Systems Analysts	1,204
Industrial Engineers	1,139
Computer User Support Specialists	1,045
Medical and Health Services Managers	984
Network and Computer Systems Administrators	976
Financial Managers	911
Bookkeeping, Accounting, and Auditing Clerks	811

Data: Emsi | Analysis: Workforce Intelligence Network

To the right are the top posted job titles for these cybersecurity-focused workers. Particularly when considering emerging roles and technology changes, employer-determined job titles may provide additional nuance when compared to traditional occupation codes. Southeast Michigan's strengths in embedded technology and robotics manufacturing may be inferred from this list; Software Engineer positions often combine the roles of Mechanical Engineers and Software Developers, while Test Automation Engineers and Systems Architects play an important role in new infrastructure. For more information on cybersecurity in automated vehicle development, connected devices, and manufacturing processes, see WIN's companion Emerging Technology Skills Gap Analysis for Connected and Automated Vehicles.

Top Posted Job Titles for Information Workers with Cybersecurity Skills

Job Title

Software Engineers

Project Managers

Solutions Architects

Test Automation Engineers

IT Quality Assurance Analysts

Cloud Engineer Architects

Project Managers

Software Team Leads

Technical Architects

Enterprise Architects

Data Architects

Systems Engineers

Systems Architects

Business Analysts

Senior Test Engineers

Scrum Masters

Technical Leads

Performance Engineers

Project Leads

Program Managers
(Computer and Mathematical)

Cybersecurity and National Security: Department of Defense Guidance and Programming

Beyond individual- or business-level threats, cybersecurity breaches pose a threat to national security. The Department of Defense (DoD) continues to emphasize and expand cybersecurity occupations to strengthen and protect our nation's critical cybersecurity infrastructure.

The Department of Defense Directive (DoDD) 8140, a set of critical cybersecurity guidelines produced by the Department of Defense that updates and encompasses DoDD 8570, provides guidance and procedures for workforce management of government employees performing information assurance duties[5]. The standards outline a wide range of baseline certifications critical to information workers in the public sphere. Other agencies have considered this major need as well; the US Department of Homeland Security released a Cybersecurity Workforce Development Toolkit[6] in 2016, with interactive resources hosted online through the National Initiative for Cybersecurity Careers and Studies[7].

The National Defense Industrial Association (NDIA)

The Cybersecurity Division of the NDIA aims to encourage industry, government, and academic involvement in protecting cyber assets and informing policy in the cyber domain. In addition to the national organization, individual states' chapters of the NDIA play an important role in facilitating regional communication.

In addition to workforce certifications and standards, an overall national cybersecurity strategy was released by the DoD in 2018. The following key findings are from the 2018 Cyber Strategy, as published in the NDIA[8] October 2019 "Beyond Obfuscation" report:

1. Ensuring the Joint Force can achieve its missions in a contested cyberspace environment;
2. Strengthening the Joint Force by conducting cyberspace operations that enhance U.S. military advantages;
3. Defending U.S. critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident;
4. Securing DoD information and systems against malicious cyber activity, including DoD information on non-DoD-owned networks; and
5. Expanding DoD cyber cooperation with interagency, industry, and international partners.

Security Clearance

Many of the positions available in cybersecurity require a security clearance[9]. This is not a certificate that can be earned or a teachable skill but a process of investigation and adjudication. This can only be obtained by United States Government sponsorship and cannot be acquired outside of this scope. All investigations are now conducted through the Office of Personnel Management (OPM), Federal Investigative Services. Security clearances are typically awarded as part of a hiring process. This process is not typically conducted outside of hiring and so it is not possible for a recent graduate to seek a security clearance solely for job search purposes.

[5] *https://public.cyber.mil/cw/cwmp/summary/*
[6] *U.S. Department of Homeland Security. (2016).*
[7] *https://niccs.us-cert.gov/*
[8] *NDIA Policy Department. (2019).*
[9] *Workforce Intelligence Network. (2017).*

OTHER DEMAND CONSIDERATIONS

Why consider regional demand?

Gaining national perspective is important to get an accurate picture of an increasingly mobile, connected workforce. Advantages like low cost of living and concentration in specialized industries such as manufacturing and embedded technologies as well as large financial and health care sectors are a boon to talent attraction efforts. Many major cybersecurity organizations have a national focus, and threats are often global. Further, strategies working well for advancing cybersecurity training in one city are likely to provide insight to another.

Location Quotient

Location quotient is a way of quantifying how concentrated an industry or occupation is in a region compared, in this case, to the nation. It is calculated by comparing the industry or occupation's share of the region's employment to its share of employment nationwide. Location quotient is helpful in determining dominant and emerging industries and their impact on the economy at large. It can also indicate a relatively large talent pool even in areas with smaller numbers of workers overall. In this report, location quotient will be used to highlight occupations of particular interest, or of particularly high skill gap, in southeast Michigan.

Automation Index

The automation index is a metric of automation risk for any given occupation based on individual job tasks. It can provide additional insight to the employment growth trends, wage adjustments, and changes in job description. Especially in manufacturing and technology positions, workers with a high level of potentially automated tasks may keep an eye on rapidly changing occupation needs. The metric, calculated by Emsi, analyzes the potential automation risk of occupations based on job task content derived from O*NET work activities. That data is combined with Frey and Osborne's 2013[10] automation risk findings at the occupation level to identify which job tasks are "at risk" and which are resilient. The calculation and sources for the automation index are discussed at greater length in the glossary, Appendix D.

[10] *Frey & Osborne (2013)*


CYBERSECU
FORCE CATE

RITY WORK-GORIES

CYBERSECURITY WORKFORCE CATEGORIES

Indirect and Cybersensitive Cybersecurity Occupations.....32

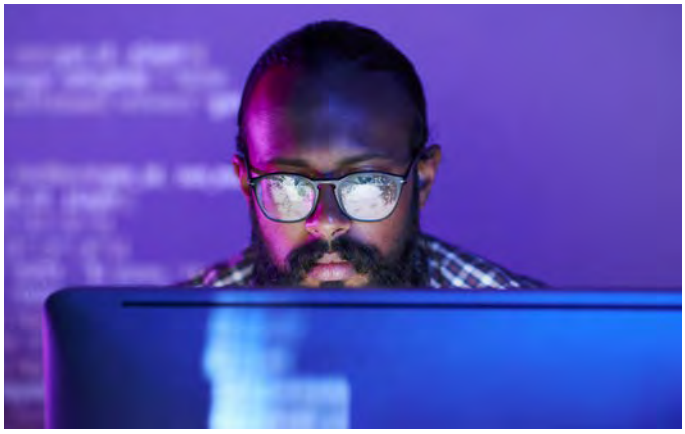
Physical Security.....35

Frontline Cybersecurity.....37

INDIRECT AND CYBERSENSITIVE CYBERSECURITY OCCUPATIONS

Growing Demand for Widespread Cybersecurity Knowledge

Cybersecurity is present in everyday working environments and used by workers in many fields across southeast Michigan. Common procedures most workers use in their jobs include identifying and avoiding phishing emails, safely storing information in specific drives and passwords, and working with antivirus software. Indirect cybersecurity workers may work with sensitive information regularly or work with technology that could benefit from cybersecurity knowledge. Whether working with social security numbers, fiscal or personnel information, or providing secure servers to workers in an office, it's important for businesses to have effective cybersecurity strategies in place and to keep their employees informed. These factors and the handling of cybersensitive information in many daily activities promote the need and importance of general cybersecurity knowledge by a multitude of occupations.



Graphic designers developing websites may utilize some cybersecurity software or techniques when publishing content to decrease vulnerabilities. Other particularly sensitive occupations include Bookkeeping, Accounting, and Auditing Clerks, Education Administrators, and Lawyers. Although these occupations do not work directly within the cybersecurity field, they show the importance of cybersecurity across all jobs and firms.

Highly Cybersensitive Occupations

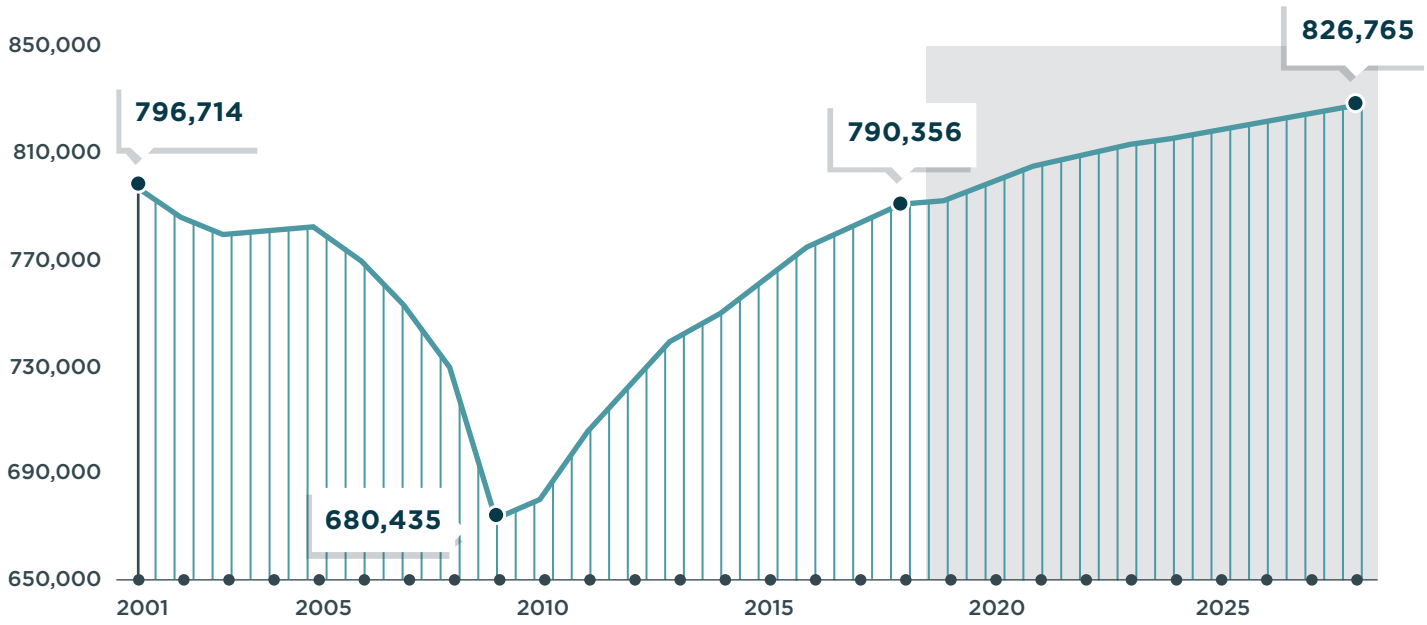
Many occupations outside of direct cybersecurity infrastructure require a general knowledge of data security practices. Workers who interact with computer systems and sensitive information can be found in many industries as the technology becomes more integrated within general business practices. Indirect occupations have cyber-related skills and must follow cybersecurity best practices. For example, registered nurses work with confidential patient information and follow secure procedures to ensure the safety of this information.

Training for Cybersensitive Workers

Considering the growing number of workers interacting with a high volume of sensitive data each day, and therefore the potential for data breaches and the potential enormous costs associated, cyber awareness training is becoming an increasingly high priority. Many companies are adopting organization-wide security best practice training at all levels, and the Society of Human Resource Managers (SHRM) offers a wide variety of cybersecurity training resources[11]. Ongoing learning for all workers is key. Traditional college curricula cannot keep up with the technological pace of change, and cybersecurity training cannot be limited to IT professionals. We will now examine the wide range of workers who need these skills.

[11] *https://www.shrm.org/resourcesandtools/pages/cybersecurity.aspx*

Cybersensitive Workers Employment in Southeast Michigan
2001-2028



Data: Emsi | Analysis: Workforce Intelligence Network

Demand Trends

In southeast Michigan, demand for cybersensitive occupations has been experiencing steady growth since 2010, with an 8.5 percent growth, and is projected to continue to grow by an additional 4.6 percent through 2028. Occupations showing the strongest growth in the region include Customer Service Representatives, Mechanical Engineers, General and Operations Managers, Sales Representatives, Wholesale and Manufacturing, Except Technical and Scientific Products, and Industrial Engineers. Between October 2018 and September 2019, there were 350,472 online job postings for cybersensitive occupations, with 134,131 postings, or 38.3 percent, requiring a bachelor's degree. Comparatively, employers are interested in workers with zero to two years of experience, accounting for 27.3 percent across all indirect cybersecurity occupations.

Top Posting Employers

The major employers* recruiting indirect cybersecurity occupations in the southeast Michigan are listed below:

- **Dollar General Corporation**
- **Robert Half International Inc.**
- **H&R Block, Inc.**
- **Oracle Corporation**
- **University of Michigan**
- **Assurance**
- **Anthem, Inc.**
- **Kelly Services, Inc.**
- **FCA US LLC**
- **Ford Motor Company**
- **CVS Health Corporation**
- **The Home Depot Inc**
- **Deloitte LLP**
- **General Motors Company**
- **Shipt LLC**

** Employer names are listed as they appear in online job postings*

Data: Emsi | Analysis: Workforce Intelligence Network

Employment Regional Specialization

Southeast Michigan has high concentrations of cybersensitive occupations, with Mechanical Engineers (6.59), Mechanical Engineering Technicians (5.04), and Industrial Engineers (4.95) all having location quotients well above the national average. The cities heavily demanding cybersensitive workers in the region include Detroit (62,792 postings), Troy (25,652 postings), Ann Arbor (21,759 postings), Auburn Hills (15,172 postings), and Southfield (14,837 postings).

Top Posting Industries

The top industries demanding workers who may work with sensitive data in southeast Michigan are listed below:

- **Retail Trade**
- **Administrative and Support and Waste Management and Remediation Services**
- **Professional, Scientific, and Technical Services**
- **Manufacturing**
- **Finance and Insurance**
- **Health Care and Social Assistance**
- **Information**
- **Accommodation and Food Services**
- **Wholesale Trade**
- **Real Estate and Rental and Leasing**

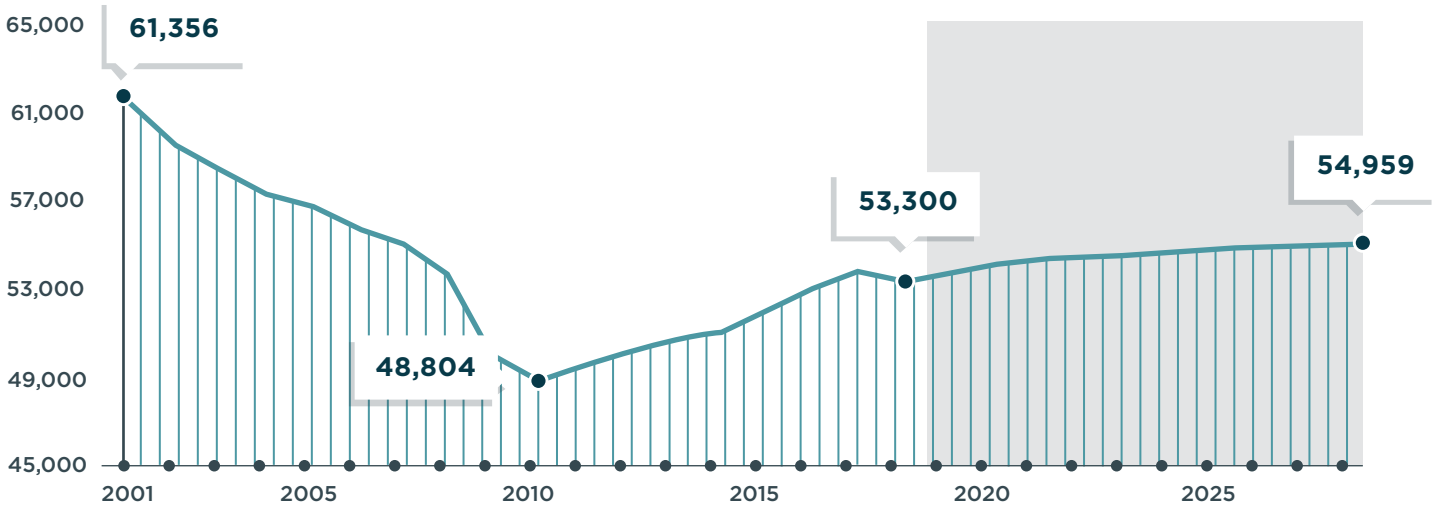
PHYSICAL SECURITY

Physical security and access workers are defined here as those workers who are responsible for the physical security of servers, data storage, and computers, or those who may have access to these assets during other work. Although they are more indirectly related to software protection, these workers are key in protecting data from physical break-ins and hardware issues. They also provide important system maintenance. Examples of occupations in this subgroup include security guards, maintenance and repair workers, security and fire alarm systems installers, and private detectives.

Demand Trends

In southeast Michigan, demand for physical security occupations has been experiencing steady growth since 2010 and is projected to continue to grow through 2028. On the national scale, employment in these jobs has seen an 11.1 percent increase and is projected to increase by another 7.4 percent over the next ten years. Southeast Michigan counties have mirrored this trend, with an 8.4 percent increase in employment since 2010 and an additional 3.0 percent growth projected through 2028. Between October 2018 and September 2019, there were 22,392 online job postings for physical security occupations, with 10,692 postings (47.8 percent) requiring a high school diploma. Employers are interested in workers with zero to two years of experience, accounting for 24.0 percent of postings across all physical security occupations.

Physical Security Employment in Southeast Michigan
2001-2028



Data: Emsi | Analysis: Workforce Intelligence Network

Top Posting Employers

The major employers recruiting physical cybersecurity occupations in the southeast Michigan are listed below:

- **CRST International, Inc.**
- **HealthCare Employment Network**
- **Uber Technologies, Inc.**
- **Oracle Corporation**
- **Teach for America, Inc.**
- **Anthem, Inc.**
- **Robert Half International Inc.**
- **C.R. England, Inc.**
- **Dollar General Corporation**
- **HomeAdvisor, Inc.**
- **J.B. Hunt Transport Services, Inc.**
- **U.S. Xpress, Inc.**
- **Care.com, Inc.**
- **McDonald's Corporation**
- **Soliant Health, Inc.**

Physical security occupations account for only 4.5 percent of all cybersecurity employment in southeast Michigan. Due to the relatively small need for physical rather than virtual protection in cybersecurity, this is unsurprising. Cybersecurity-focused job postings for physical security occupations comprised about 1.2 percent of total employment for those occupations in Michigan, and 0.03 percent nationwide.

Data: Emsi | Analysis: Workforce Intelligence Network

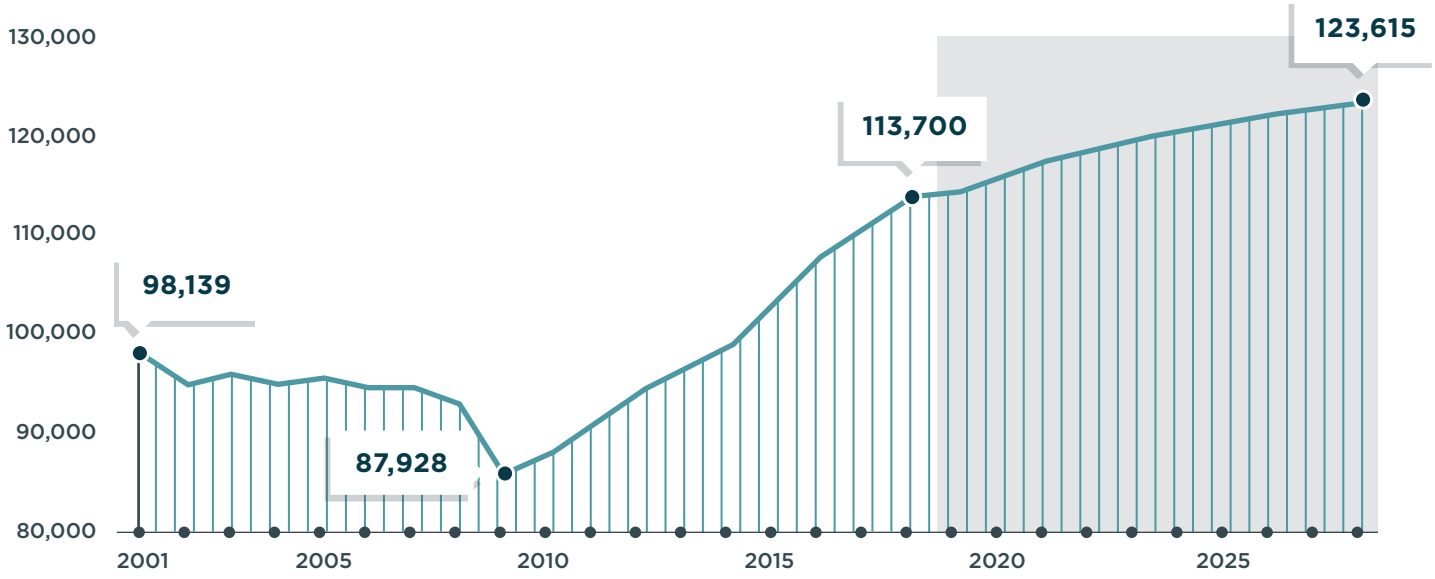
FRONTLINE CYBERSECURITY

The Frontline Cybersecurity Workers category consists of those directly working with the technical design and implementation of cybersecurity strategies. These employees develop the programming related to security, investigate and address virtual threats, and work directly with security platforms. The occupations encompassed in this group include those working directly with security technology such as network administrators, software developers and information security analysts. Analysis in this section will primarily focus on southeast Michigan, but will also include a comparison of this unique, manufacturing-dominant ecosystem to the United States as a whole.

Demand Trends

Employer demand for frontline cybersecurity occupations in the 16 county WIN region continues its steady upward trajectory. From the 88,000 frontline cyber workers employed in 2010, demand for these workers steadily and rapidly grew by 29.3 percent to 113,700 workers in 2018. The growth in employment is projected to continue, increasing 8.7 percent to 123,600 jobs in 2028. There were 97,844 online job postings between October 2018 and September 2019, of which 25,027 mentioned cybersecurity-specific topics and credentials. Software Developers, Applications are both the highest employed and top-posted occupation, encompassing over 22,000 workers in southeast Michigan and garnering nearly 9,000 cybersecurity-focused postings. Software Developers, Systems Software, Information Security Analysts, and Computer Occupations, All Other were also major posted cyber-concerned occupations. The "All Other" category encompasses smaller specific occupations such as Software Quality Assurance Engineers and Testers, Computer Systems Engineers, and IT Project Managers. About 9,600 annual openings are expected each year. Information Security Analysts anticipate a 23.5 percent growth by 2028, adding about 250 jobs, while middle skill Web Developers anticipate a 15.0 percent growth.

Frontline Cybersecurity Employment in Southeast Michigan
2001-2028



Data: Emsi | Analysis: Workforce Intelligence Network

There are auto manufacturing, finance, health care, and defense firms represented alongside tech companies as southeast Michigan's top job posting firms. Cybersecurity needs are widespread with increasing adoption of connected devices and focus on data-driven strategy, so top cybersecurity employers reflect the region's overall high-demand sectors. Ford Motor Company, General Motors, Fiat Chrysler, and several major suppliers are among top employers seeking cyber employees in the area. Especially with the advances in standard vehicle technology and expanding development of connected vehicles, cybersecurity is essential to ensure that when consumers execute any technology in their vehicles, they have the functionality and capability to execute those programs safely and without interference. In addition, cybersecurity best practices are needed by many manufacturing firms at the production level due to automated practices used during assembly.

Top Posting Employers

Southeast Michigan

- **Ford Motor Company**
- **Oracle Corporation**
- **Deloitte LLP**
- **Renature, Inc.**
- **Teksystems, Inc.**
- **Anthem, Inc.**
- **University of Michigan**
- **General Motors Company**
- **V2soft Inc.**
- **Fast Switch, Ltd.**
- **Cybercoders, Inc.**
- **ALTAIR ENGINEERING, INC.**
- **Quicken Loans Inc.**
- **Kelly Services, Inc.**
- **Kforce Inc.**
- **Virtual Vocations**
- **Robert Bosch LLC**
- **Msx International, Inc.**
- **FCA US LLC**
- **Computer Task Group, Incorporated**

National Comparison

The top fifteen businesses recruiting for frontline cybersecurity employees were:

- **Oracle Corporation**
- **Revature**
- **Anthem, Inc.**
- **Deloitte LLP**
- **Cybercoders, Inc.**
- **International Business Machines Corporation**
- **Amazon.com, Inc.**
- **Robert Half International Inc.**
- **Booz Allen Hamilton Holding Corporation**
- **Leidos Holdings, Inc.**
- **General Dynamics Corporation**
- **Kforce Inc.**
- **U.S. Bancorp**
- **Wells Fargo & Company**
- **Raytheon Company**

Data: Emsi | Analysis: Workforce Intelligence Network

Education and Experience

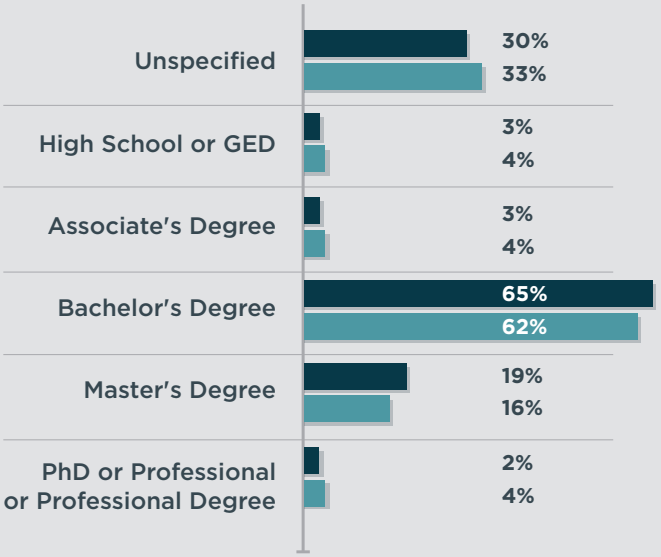
Posting Requirements

Most employers of frontline cybersecurity positions require that candidates have a bachelor's degree or higher. Of the 1,605,075 national job postings that specified a desired level of education attainment 1,100,846 (68.6 percent) specified a bachelor's degree and another 359,808 (22.4 percent) specified an advanced degree. Just over 70,000 national postings each were open to individuals with a high school diploma or an associate degree. By comparison, in southeast Michigan, 70 percent of frontline cybersecurity postings require a college degree and 23.5 percent prefer an advanced degree. In a number of cases, however, two-year degrees can be transferred to four-year institutions for bachelor's degree completion and coursework at this level can be used as part of an apprenticeship completion. The occupation most open to individuals with less than a college degree is Computer User Support Specialists. High-demand Software Developers, Applications and Business Operations Specialists, All Other are also represented in postings for less than a college degree; since they typically require a bachelor's for entry, this may indicate a change in employer requirements for these hard-to-fill occupations. At the national level, Information Security Analysts with the right skills and certifications also have flexible degree requirements. Below, observe the difference between the education and experience requirements posted at the regional and national levels.

About 70 percent (1,240,418 ads) of national job postings specified a minimum experience requirement for candidates. Experience requirements are more variable than education requirements, with about 21 percent of job postings open to entry-level workers. About two-thirds of postings sought moderately experienced workers with two to six years of experience. In southeast Michigan, though the educational requirements trend slightly higher than the national figures, there are a greater number of openings for entry-level workers. One quarter of job postings were open to candidates with less than a year of experience, and another 39 percent seeking two or three years.

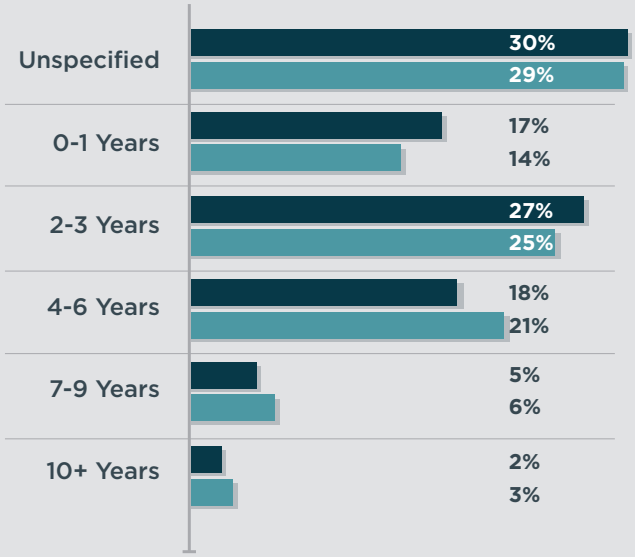
Comparative Education Requirements in Posted Jobs

Southeast Michigan and US



Comparative Experience Requirements in Posted Jobs

Southeast Michigan and US



SE Michigan US

Data: Emsi | Analysis: Workforce Intelligence Network

Worker Salary

While the wages of workers employed directly in cybersecurity positions are not available, examining the wages of workers in the broader occupation groups can provide insight into the labor market conditions in which workers and employers are operating. For those currently employed in frontline cybersecurity occupations, median hourly earnings are near or above $30 per hour for all occupations, growing to over $60 per hour for experienced workers. These high wages can go even further in southeast Michigan. The low cost of living in Michigan compared to coastal tech hubs is an oft-cited benefit to locating near Detroit or Ann Arbor.

SOC Code	Description	10th Percentile Wages	25th Percentile Wages	Median Wages	75th Percentile Wages	90th Percentile Wages
11-3021	Computer and Information Systems Managers	$38.87	$49.25	$62.24	$77.06	$96.94
13-1199	Business Operations Specialists, All Other	$17.95	$23.95	$32.68	$45.41	$58.11
13-2099	Financial Specialists, All Other	$18.24	$22.63	$30.38	$46.97	$65.60
15-1111	Computer and Information Research Scientists	$29.94	$39.67	$49.80	$58.58	$66.36
15-1121	Computer Systems Analysts	$25.29	$31.63	$39.47	$49.20	$60.10
15-1122	Information Security Analysts	$28.94	$34.30	$44.02	$56.47	$65.60
15-1131	Computer Programmers	$20.09	$27.82	$36.45	$44.97	$52.70
15-1132	Software Developers, Applications	$28.00	$34.46	$43.62	$54.50	$63.21
15-1133	Software Developers, Systems Software	$23.34	$33.54	$43.22	$52.88	$62.83
15-1134	Web Developers	$10.32	$18.63	$29.16	$40.22	$49.31
15-1141	Database Administrators	$24.46	$31.45	$42.55	$53.41	$61.17
15-1142	Network and Computer Systems Administrators	$24.74	$30.52	$37.83	$47.43	$57.23
15-1143	Computer Network Architects	$29.81	$40.00	$53.18	$64.33	$75.48
15-1151	Computer User Support Specialists	$13.13	$16.74	$22.62	$29.50	$37.58
15-1152	Computer Network Support Specialists	$17.82	$22.04	$28.95	$37.08	$46.23
15-1199	Computer Occupations, All Other	$19.52	$26.06	$36.56	$48.44	$60.01
15-2031	Operations Research Analysts	$25.02	$33.31	$42.89	$52.68	$61.79
15-2041	Statisticians	$25.86	$31.19	$39.39	$49.18	$57.34
17-2061	Computer Hardware Engineers	$20.12	$28.63	$43.61	$56.24	$65.12
33-3021	Detectives and Criminal Investigators	$27.41	$32.64	$41.78	$55.94	$68.80

Data: Emsi | Analysis: Workforce Intelligence Network

Middle Skill, Middle Wage Occupations

By both employer demand metrics and BLS data, most frontline cybersecurity occupations require a bachelor's degree, and all pay high wages. The landscape is shifting, however, as the demand for cybersecurity workers continue to grow; certifications, on-the-job training, and apprenticeships are increasingly viewed as good alternatives, and the interpersonal and problem-solving skills from outside the technology industry are often appreciated as well. Currently, Web Developers, Computer User Support Specialists, Computer Network Support Specialists, and Detectives and Criminal Investigators are all open career tracks for individuals with more than a high school diploma but less than a college degree, and this list is likely to expand in the future.

In-Demand Degrees

Though universities are increasingly developing cybersecurity-specific curricula, most current frontline cybersecurity professionals have earned more general computer science degrees, or come from more varied backgrounds, and developed specific cybersecurity skills through work experience and additional coursework. The degrees with the highest number of completions in southeast Michigan are:

- **Computer and Information Sciences, General**
- **Finance, General**
- **Mathematics, General**
- **Computer Programming/Programmer, General**
- **Criminal Justice/Police Science**
- **Computer Engineering, General**
- **Information Science/Studies**
- **Management Information Systems, General**
- **Computer and Information Systems Security/ Information Assurance**
- **Information Technology**

In-Demand Certifications

Frontline cybersecurity occupations require extremely specialized training and certifications. Cyber certifications include:

- **Certified Information Systems Security Professional (CISSP)**
- **Project Management Professional (PMP) Certification**
- **Cisco Certified Network Associate**
- **Microsoft Certified Professional**
- **Certified Information System Auditor (CISA)**
- **ITIL Certifications**
- **Microsoft Certified Systems Engineer**
- **GIAC Certifications**
- **Certified Information Security Manager**
- **Cisco Certified Network Professional**

Data: Emsi | Analysis: Workforce Intelligence Network

GUIDANCE STANDARDS

WORKFORCE GUIDANCE AND STANDARDS

Since cybersecurity is an emerging industry, regulations are being developed to keep up with the fast movement of cybersecurity activities. Many policies and regulations have been developed and guidance produced to address cybersecurity in many areas, including defense and homeland security, finance, and manufacturing. These regulations and guidance have a major effect on the way companies do business and hire cybersecurity talent. HIPAA and the Family Educational Rights and Privacy Act (FERPA), for example, drive the need for training in the applications and monitoring of the types of data that these acts protect. This may also drive the need for workers with credentials needed for auditing, including CISA, CISM, and/or CISSP. In addition to those outlined below, Department of Defense-specific standards are discussed within the Workforce Overview.

NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework is a voluntary guidance program for organizations to better manage and reduce their risks. The framework is based on existing standards, guidelines, and practices[12]. Specific frameworks for manufacturing cybersecurity and internet of things adaptations have been released as well.

2017 NICE Cybersecurity Workforce Framework (NCWF)

The NIST-led National Initiative for Cybersecurity Education (NICE) finalized their Cybersecurity Workforce Framework (NCWF) in 2017. This provides a reference that will allow the nation to more effectively identify, recruit, develop and maintain its cybersecurity talent. The framework provides a common language to categorize and describe cybersecurity work that will help organizations build a strong labor staff to protect systems and data.

FDIC, OCC, and Federal Reserve Joint Statements on Cyber Risk Management Standards

In October 2016, the Board of Governors of the Federal Reserve System , the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC), collectively issued an advance notice of proposed minimum standards for financial institutions in five categories: cyber risk governance, cyber risk management, internal dependency management, external dependency management, and incident response, cyber resilience, and situational awareness. This built off the Interagency Guidelines Establishing Information Security Standards previously developed by the Federal Reserve, and has since been expanded to include statements on heightened cybersecurity risks and other topics.

Cybersecurity Act of 2015

The Cybersecurity Act of 2015 created a voluntary cybersecurity information sharing process and modified federal network information security procedures[13]. It provides methods for the sharing of information on cybersecurity threats and defensive measures among[14] private sector entities and between private sector and the government.

---

[12] *www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-basics*

[13] *www.congress.gov/bill/114th-congress/house-bill/2029*

[14] *www.dlapiper.com/en/us/insights/publications/2016/02/cybersecurity-2015s-top-legal-developments*


CONCLUSIO
RECOMMEN

N AND
DATIONS

CONCLUSION AND RECOMMENDATIONS

2020 Emerging Technology
Workforce Recommendations.....47

Cybersecurity knowledge is critical due to the overall shift in technology adoption throughout everyday life, such as connected devices, machine learning, and an increased need for data privacy as social media and other online services facilitate data collection. In southeast Michigan, this is especially key for the auto manufacturers, transportation planners, and policymakers working to expand the frontier of connected vehicles and smart infrastructure, the health care systems keeping the population healthy, and the growing technology sector in greater Detroit.

To enable smooth growth in new technology and increased mobility, workers at every level of technology usage need to know how cybersecurity best practices impact them.

In keeping with this updated cybersecurity workforce report's focus on talent pipelines in southeast Michigan, WIN provides the following recommendations for continuing cultivation of a robust, innovative skill pool in the region:

2020 Emerging Technology Workforce Recommendations:

01

1 In order to address the lack of information on both cybersecurity specialist roles and general workforce needs, information must be collected by level of worker to create a "cyber needs" database with which to target future training and standards.

02

2 Training specific to connected devices and products, including hands-on experience, must be developed and formalized. Curriculum should be oriented toward the vehicles, medical devices, wearable technology, and other industry-specific factors.

03

3 Ongoing learning via certification programs will be increasingly necessary. In combination with a cyber needs database, ongoing certifications should continue to be developed in collaboration between southeast Michigan training providers and employers to ensure new skill needs are consistently met.

04

4 Businesses should take care to continuously communicate their cybersecurity needs to workforce partners, community colleges, and other talent pipeline stakeholders in order to build a workforce with the most up-to-date possible skillset for keeping information safe.

APPENDICES

Appendix A: Occupation Codes by Category 49

Appendix B: Cybersecurity Keyword and Certification Data Collection Filters..... 34

Appendix C: Works Cited 34

Appendix D: Glossary 35

Appendix A: Occupation Codes by Category

Occupations in **bold** font are included in the Workforce Overview aggregate data.

Frontline Cybersecurity Workers

SOC	OCCUPATION
11-3021	Computer and Information Systems Managers
13-1199	Security Management Specialists
13-2099	Risk Management Specialists
15-1111	Computer and Information Research Scientists
15-1121	Computer Systems Analysts
15-1122	Information Security Analysts
15-1131	Computer Programmers
15-1132	Software Developers, Applications
15-1133	Software Developers, Systems Software
15-1134	Web Developers
15-1141	Database Administrators
15-1142	Network and Computer Systems Administrators
15-1143	Computer Network Architects
15-1143	Telecommunications Engineering Specialists
15-1151	Computer User Support Specialists
15-1152	Computer Network Support Specialists
15-1199	Computer Occupations, All Other
15-1199	Software Quality Assurance Engineers and Testers
15-1199	Computer Systems Engineers/Architects
15-1199	Web Administrators
15-1199	Database Architects
15-1199	Data Warehousing Specialists
15-1199	Information Technology Project Managers
15-2031	Operations Research Analysts
15-2041	Clinical Data Managers
17-2061	Computer Hardware Engineers
33-302 1	Intelligence Analysts

Cybersensitive Occupations

11-9199	Security Managers
11-9199	Loss Prevention Managers
11-1011	Chief Executives
11-1021	General and Operations Managers
11-2021	Marketing Managers
11-2022	Sales Managers
11-2031	Public Relations and Fundraising Managers
11-3011	Administrative Services Managers
11-3031	Financial Managers
11-3031	Treasurers and Controllers
11-3031	Financial Managers, Branch or Department
11-3051	Industrial Production Managers
11-3051	Quality Control Systems Managers
11-3061	Purchasing Managers
11-3071	Storage and Distribution Managers
11-3121	Human Resources Managers
11-3131	Training and Development Managers
11-9021	Construction Managers
11-9041	Architectural and Engineering Managers
11-9111	Medical and Health Services Managers
11-9151	Social and Community Service Managers
11-9161	Emergency Management Directors
11-9199	Managers, All Other
11-9199	Compliance Managers
11-9199	Supply Chain Managers
13-1023	Purchasing Agents, Except Wholesale, Retail, and Farm Products
13-1031	Claims Examiners, Property and Casualty Insurance
13-1041	Compliance Officers
13-1041	Regulatory Affairs Specialists
13-1051	Cost Estimators
13-1071	Human Resources Specialists
13-1081	Logisticians
13-1081	Logistics Analysts
13-1111	Management Analysts
13-1141	Compensation, Benefits, and Job Analysis Specialists
13-1151	Training and Development Specialists
13-1161	Market Research Analysts and Marketing Specialists
13-1199	Business Operations Specialists, All Other
13-1199	Business Continuity Planners
13-1199	Online Merchants
13-2011	Accountants and Auditors
13-2011	Accountants
13-2011	Auditors
13-2021	Assessors
13-2041	Credit Analysts

Appendix A: Occupation Codes by Category

Occupations in **bold** font are included in the Workforce Overview aggregate data.

SOC	OCCUPATION
13-2051	**Financial Analysts**
13-2052	**Personal Financial Advisors**
13-2053	**Insurance Underwriters**
13-2061	**Financial Examiners**
13-2071	**Credit Counselors**
13-2072	**Loan Officers**
13-2099	**Financial Specialists, All Other**
13-2099	**Fraud Examiners, Investigators and Analysts**
15-1199	**Geospatial Information Scientists and Technologists**
15-1199	**Business Intelligence Analysts**
15-1199	**Search Marketing Strategists**
15-1199	**Document Management Specialists**
17-2011	**Aerospace Engineers**
17-2041	**Chemical Engineers**
17-2051	**Civil Engineers**
17-2071	**Electrical Engineers**
17-2072	**Electronics Engineers, Except Computer**
17-2072	**Radio Frequency Identification Device Specialists**
17-2081	**Environmental Engineers**
17-2112	**Industrial Engineers**
17-2141	**Mechanical Engineers**
17-2199	**Engineers, All Other**
17-2199	**Validation Engineers**
19-4099	**Quality Control Analysts**
23-1011	**Lawyers**
29-2071	**Medical Records and Health Information Technicians**
41-3021	**Insurance Sales Agents**
41-3031	**Sales Agents, Financial Services**
41-9031	**Sales Engineers**
43-1011	**First-Line Supervisors of Office and Administrative Support Workers**
43-3011	**Bill and Account Collectors**
43-3031	**Bookkeeping, Accounting, and Auditing Clerks**
43-4011	**Brokerage Clerks**
43-4131	**Loan Interviewers and Clerks**
43-4161	**Human Resources Assistants, Except Payroll and Timekeeping**
11-9032	Education Administrators, Elementary and Secondary School
11-9033	Education Administrators, Postsecondary
11-9081	Lodging Managers
11-9131	Postsecondary Teachers
11-9141	Property, Real Estate, and Community Association Managers
13-1121	Meeting, Convention, and Event Planners
15-1199	Video Game Designers
15-2041	Statisticians
15-2099	Mathematical Science Occupations, All Other
17-3012	Electrical and Electronics Engineering Technicians
17-3022	Civil Engineering Technicians
17-3023	Electronics Engineering Technicians
17-3029	Mechanical Engineering Technologists
17-3029	Manufacturing Production Technicians
41-1011	First-Line Supervisors of Retail Sales Workers
41-1012	First-Line Supervisors of Non-Retail Sales Workers
41-2031	Retail Salespersons
41-3099	Sales Representatives, Services, All Other
41-4011	Sales Representatives, Wholesale and Manufacturing, Technical and Scientific Products
41-4012	Sales Representatives, Wholesale and Manufacturing, Except Technical and Scientific Products
41-9022	Real Estate Sales Agents
43-3071	Tellers
43-4051	Customer Service Representatives
43-4171	Receptionists and Information Clerks
43-5061	Production, Planning, and Expediting Clerks
43-6011	Executive Secretaries and Executive Administrative Assistants
43-6014	Secretaries and Administrative Assistants, Except Legal, Medical, and Executive
43-9011	Computer Operators
43-9021	Data Entry Keyers
43-9061	Office Clerks, General
43-9199	Office and Administrative Support Workers, All Other

Physical Security Occupations

17-1011	**Architects, Except Landscape and Naval**
33-1099	**First-Line Supervisors of Protective Service Workers, All Other**
33-3021	**Detectives and Criminal Investigators**
33-3021	**Criminal Investigators and Special Agents**

SOC	OCCUPATION
33-9021	**Private Detectives and Investigators**
33-9032	**Security Guards**
33-9099	**Retail Loss Prevention Specialists**
49-2022	**Telecommunications Equipment Installers and Repairers, Except Line Installers**
49-2098	**Security and Fire Alarm Systems Installers**
49-9052	**Telecommunications Line Installers and Repairers**
49-9071	**Maintenance and Repair Workers, General**

Indirect Cybersecurity Occupations

19-2099	Remote Sensing Scientists and Technologists
19-4092	Forensic Science Technicians
55-1019	Military Officer Special and Tactical Operations Leaders, All Other
19-1020	Biologists
19-1032	Foresters
19-1042	Medical Scientists, Except Epidemiologists
19-2041	Climate Change Analysts
19-3091	Archeologists
19-3094	Political Scientists
19-3099	Social Scientists and Related Workers, All Other
19-4021	Biological Technicians
19-4091	Environmental Science and Protection Technicians, Including Health
19-4093	Forest and Conservation Technicians
21-1012	Educational, Guidance, School, and Vocational Counselors
21-1029	Social Workers, All Other
21-1093	Social and Human Service Assistants
23-2011	Paralegals and Legal Assistants
23-2099	Legal Support Workers, All Other
25-1021	Computer Science Teachers, Postsecondary
25-1194	Vocational Education Teachers, Postsecondary
25-1199	Postsecondary Teachers, All Other
25-2023	Career/Technical Education Teachers, Middle School
25-3099	Teachers and Instructors, All Other
25-4031	Library Technicians
25-9031	Instructional Designers and Technologists
27-1021	Commercial and Industrial Designers
27-1024	Graphic Designers
27-1029	Designers, All Other
27-3031	Public Relations Specialists
27-3041	Editors
27-3042	Technical Writers
27-3043	Copy Writers
27-3091	Interpreters and Translators
27-4011	Audio and Video Equipment Technicians
29-1141	Registered Nurses
29-2012	Medical and Clinical Laboratory Technicians
29-2034	Radiologic Technologists
29-2061	Licensed Practical and Licensed Vocational Nurses
29-2099	Health Technologists and Technicians, All Other
29-9011	Occupational Health and Safety Specialists
31-9092	Medical Assistants
33-9011	Animal Control Workers
35-1012	First-Line Supervisors of Food Preparation and Serving Workers
35-3021	Combined Food Preparation and Serving Workers, Including Fast Food
35-3031	Waiters and Waitresses
37-2011	Janitors and Cleaners, Except Maids and Housekeeping Cleaners
39-9031	Fitness Trainers and Aerobics Instructors
45-2041	Graders and Sorters, Agricultural Products
47-2073	Operating Engineers and Other Construction Equipment Operators
49-1011	First-Line Supervisors of Mechanics, Installers, and Repairers
49-2091	Avionics Technicians
49-3023	Automotive Specialty Technicians
49-9012	Control and Valve Installers and Repairers, Except Mechanical Door
49-9021	Heating and Air Conditioning Mechanics and Installers
49-9099	Installation, Maintenance, and Repair Workers, All Other
51-1011	First-Line Supervisors of Production and Operating Workers
51-3021	Buyers and Purchasing Agents
51-9061	Inspectors, Testers, Sorters, Samplers, and Weighers
51-9199	Production Workers, All Other
53-3031	Driver/Sales Workers
53-7062	Laborers and Freight, Stock, and Material Movers, Hand

Appendix B: Cybersecurity Keyword and Certification Data Collection Filters

- cybersecurity OR
- "information security" OR
- confidentiality OR
- HIPAA OR
- FERPA OR "
- Certified Information Systems Security Professional" OR "
- CISSP" OR "
- CompTIA Advanced Security Practitioner" OR "
- CompTIA Security+" OR "
- Certified Ethical Hacker" OR "
- Certified Information System Auditor" OR "
- CISA" OR "CompTIA Cybersecurity Analyst" OR
- CySA+ OR
- CISM OR "
- Certified Information Security Manager" OR "
- GIAC Security Essentials Certification" OR "
- Cisco Certified Security Professional"

Appendix C: Works Cited

Beyer, R., Brummel, B. (2015). Implementing Effective Cyber Security Training for End Users of Computer Networks.
Retrieved from www.bit.ly/2UUwm36

Frey, C.B., & Osborne, M. A. (2013). The Future of Employment: How Susceptible are Jobs to Computerisation?. University of Oxford, Oxford. - References - Scientific Research Publishing

Internet Society. (2017). Internet Society Global Internet Report. Paths to Our Digital Future.
Retrieved from www.bit.ly/3bWEGEW

NDIA Policy Department. (2019). Beyond Obfuscation: The Defense Industry's Position within Federal Cybersecurity Policy.

NortonLifeLock. (2019). Cyber Safety Insights Report Global Results.
Retrieved from www.bit.ly/2RmU0Tz

Pescatore, J. (2019, April). SANS Top New Attacks and Threat Report.
Retrieved from www.bit.ly/2Ro02Dh

SANS. (2018). Interactive NICE Framework Mapping.
Retrieved from www.sans.org/courses/niceframework

Spitzner, L., deBeaubien, D., Ideboen, A., Xu, Dr. H., Zhang, Dr. N, Andrews, H., & Sonaike, A. (2019). 2019 SANS Security Awareness Report. The Rising Era of Awareness Training.
Retrieved from www.knowbe4.com/hubfs/SANS-Security-Awareness-Report-2019.pdf

United States Department of Health and Human Services. (2013).
Accessed 2019 from www.hhs.gov/hipaa

U.S. Department of Homeland Security. (2016). Cybersecurity Workforce Development Toolkit. How to Build a Strong Cybersecurity Workforce.
Retrieved from www.vbgov.com/residents/public-safety/practice-safe-cyber/Documents

VanDerwerken, J., Ubell, R. (2011, June). Cyber Security Frontlines.
Retrieved from www.bit.ly/3bY8z7K

Verizon. (2019). 2019 Data Breach Investigations Report.
Retrieved from www.enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

Workforce Intelligence Network. (2017). Cybersecurity Skills Gap Analysis.

Data Sources: United States Department of Labor, Bureau of Labor Statistics, Bureau of Economic Analysis, O*NET, and Emsi Knowledge Base.

Appendix D: Glossary

Automation Index
Measure for each occupation provided by Emsi:

> "The automation index captures an occupation's risk of being affected by automation using four measures:
>
> - % of time spent on high-risk work
> - % of time spent on low-risk work
> - Number of high-risk jobs in compatible occupations
> - Overall industry automation risk
>
> This methodology starts with the underlying work on task content. We use estimated task time shares, derived from O*NET work activities, and regress them for each occupation based on Frey and Osborne's published "computerization probabilities" (2013). This helps us identify which tasks are positively and negatively correlated with automation risk. This classification is then linked with the task time shares to identify the share of each occupation's time spent in high- and low-risk work, from an automation perspective. Then we look at the place of an occupation in the broader context of labor market automation risk. Using occupation compatibility scores, we look at all similar roles (defined as having an O*NET compatibility score over 75) and find the percentage of jobs in those similar roles that are at risk of automation. Finally, using staffing pattern data, we multiply the share of an occupation's jobs in 3-digit NAICS industries by that industry's share of at-risk jobs to calculate the overall industry automation risk. We then standardize all these measures and scale the index so that 100 = the "average worker," defined as the average index across all occupations, weighted by job numbers in 2018. The index has a standard deviation of 15. Note that the share of time spent on low-risk work is a negative contributor to an occupation's index score (making the index score lower) while the other three measures are positive contributors (making the index score higher)."

Bureau of Labor Statistics (BLS)
Under the United States Department of Labor, the Bureau of Labor Statistics is the preeminent collector and distributor of labor market and economic data at the federal level.

Certifications
Professional certifications or qualifications required or preferred in online job postings.

Demand Concentration
For the purposes of this analysis, demand concentration refers to the share of CAV-related job postings relative to total job postings at the level of the metropolitan statistical level (MSA).

Education Requirements
This dataset from Emsi overviews the level of educational attainment specified (required or preferred) in online job postings for a particular occupation or job.

Experience
Similar to educational attainment, this information is pulled from job postings to illustrate the level of experience that employers seek from candidates for an open position.

Industry
A category that defines the activities of a business. See also: North American Industry Classification System (NAICS).

Internet of Things
A system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

Location Quotient
An analytical statistic that measures a region's industrial specialization relative to a larger geographic unit (usually the nation). An LQ is computed as an industry's share of a regional total

for some economic statistic (earnings, GDP by metropolitan area, employment, etc.) divided by the industry's share of the national total for the same statistic. For example, an LQ of 1.0 in mining means that the region and the nation are equally specialized in mining; while an LQ of 1.8 means that the region has a higher concentration in mining than the nation.

Job Demand
Approximated by total number of online job postings for a specific occupation in this analysis through the use of job postings data from Emsi.

North American Industry Classification System (NAICS)
Adopted in 1997 by the United States Economic Classification Policy Committee (ECPC) and partner departments in Mexico and Canada, the NAICS is a standard system for defining the activities of businesses.

Occupation
A category that defines the knowledge, skills, and functions of a worker. For the purposes of this analysis, defined by some classification system in order to operationalize worker type. See also: O*NET, Standard Occupational Classification System (SOC).

O*NET: Occupational Information Network, maintained by the United States Department of Labor. O*NET catalogs the essential duties, knowledge, and skills required of a certain job, resulting in a set of 8-digit codes delineating distinct occupations. See also: Standard Occupational Classification System (SOC).

Salary/Wages
Percentile hourly wage data, available at the county level, is provided through the BLS.

Skills, Foundational
Coded from online job postings, Emsi presents these as baseline skills necessary for successful employment in the open position.

Skills, Technical
Coded from online job postings, Emsi present these as the technical skills necessary for successful employment in the open position.

Southeast Michigan
In this report, southeast Michigan refers to the 16 counties comprising the WIN region: Genesee, Hillsdale, Huron, Jackson, Lapeer, Lenawee, Livingston, Macomb, Monroe, Oakland, Sanilac, Shiawassee, St. Clair, Tuscola, Washtenaw, and Wayne counties.

Standard Occupational Classification (SOC)
Used by the federal government to define worker type, this classification system features a set of 6-digit codes (aligned with O*NET codes) to delineate distinct occupations. See also: O*NET.

Top Posting Employers
Based on online job postings data from Emsi, these are the employers that posted the most online job ads for an occupation over the analysis period. Online job postings are often seen as an indicator of a company's willingness to hire.

RALPH C. WILSON, JR.
FOUNDATION

Report compiled by the Workforce Intelligence Network for Southeast Michigan on behalf of the Ralph C. Wilson, Jr. Foundation

WIN WORKFORCE INTELLIGENCE NETWORK

WINintelligence.org