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

EXECUTIVE SUMMARY

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.

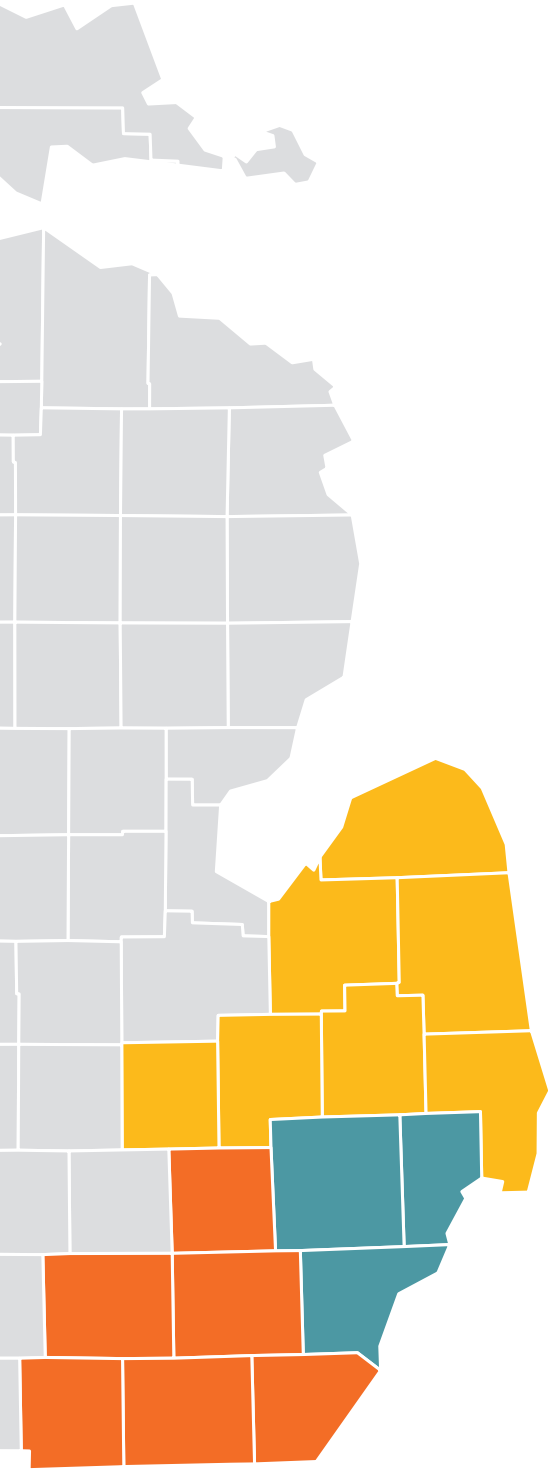
[1] *The original report content reflected the views of the Workforce Intelligence Network and did not necessarily reflect the views of the Office of Economic Adjustment.*

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.



MOTT COMMUNITY COLLEGE

GST MICHIGAN WORKS! — GENESEE SHIAWASSEE THUMB

MICHIGAN WORKS! MACOMB/ST. CLAIR

OAKLAND COMMUNITY COLLEGE

Macomb Community College

Schoolcraft College

HENRY FORD COLLEGE — FUTUREDRIVEN

Wayne County Community College District

SEMCA MICHIGAN WORKS!

Detroit Employment Solutions Corporation

Oakland County MICHIGAN WORKS!

MONROE COUNTY COMMUNITY COLLEGE

Washtenaw Community College

Jackson COLLEGE

MICHIGAN WORKS! SOUTHEAST

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.

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.

To view the full report, visit:
winintelligence.org/report/cybersecurity-report

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 following recommendations, discussed in detail in the conclusion of the full report, 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.

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

To view the full report, visit:
winintelligence.org/report/cybersecurity-report