CYBERSECURITY
EMERGING TECHNOLOGY SKILLS GAP ANALYSIS

SOUTHEAST MICHIGAN

WIN WORKFORCE INTELLIGENCE NETWORK

RALPH C. WILSON, JR. FOUNDATION

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.

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

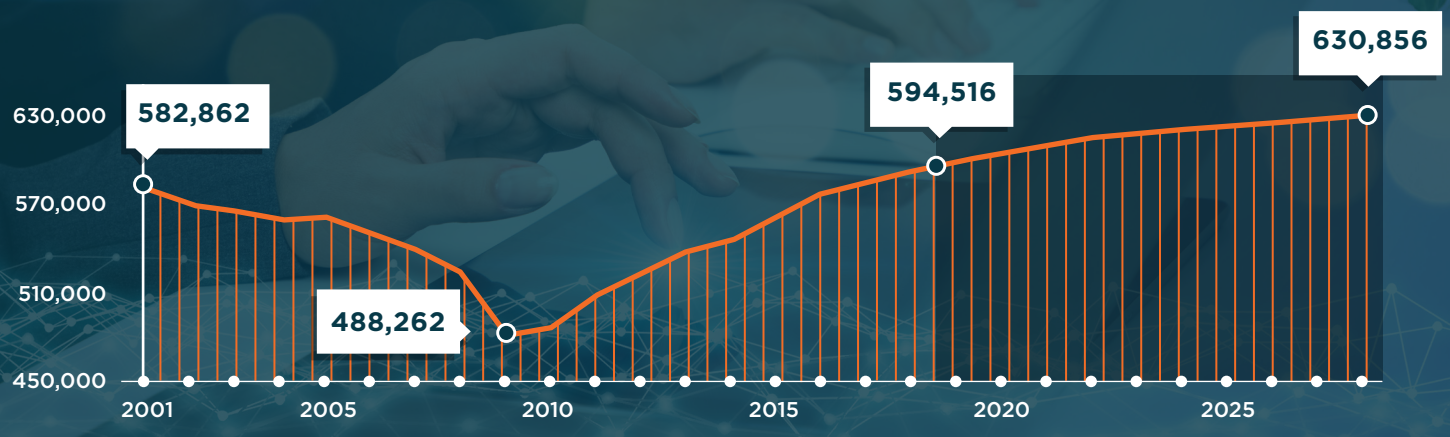
3 Ongoing learning via certification programs will be increasingly necessary. In combination with a cyber needs database, ongoing certifications should continue to be developed in collaboration between southeast Michigan training providers and employers to ensure new skill needs are consistently met.

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.

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

Cybersecurity Employment in Southeast Michigan, 2001-2028



Data: Emsi | Analysis: Workforce Intelligence Network