CYBERSECURITY SKILLS GAP ANALYSIS

National and Advance Michigan Region Data

July 2017

WIN WORKFORCE INTELLIGENCE NETWORK

Report prepared by the Workforce Intelligence Network for Southeast Michigan

This study was prepared under contract with the Macomb/St. Clair Workforce Development Board, Michigan, with financial support from the Office of Economic Adjustment, Department of Defense. The content reflects the views of the Macomb/St. Clair Workforce Development Board and does not necessarily reflect the views of the Office of Economic Adjustment.

EXECUTIVE SUMMARY

To better understand future workforce demands in the cybersecurity space, the Workforce Intelligence Network for Southeast Michigan (WIN) conducted research to analyze job postings for a broad set of occupations associated with aspects of cybersecurity, including the development of software, testing, hardening, connectivity, business related cyber roles, physical security implications, and general cybersecurity knowledge needs.

The analysis identified a total of 348,975 cybersecurity-related job listings nationally from between July 2015 and June 2016. Of the nearly 350,000 postings, California was the state with the highest reported postings with 45,062 online job advertisements. Virginia, Texas and New York showed high employer demand, with over 20,000 postings in each state.

Although there were nearly 350,000 postings, there were 778,402 cybersecurity workers in the workforce in 2016. States that reported high volumes of job postings across all occupations tended to have high volumes of cybersecurity workers.[1]

The cybersecurity workforce is not monolithic. This report identifies four categories of occupations among the cybersecurity workforce, each associated with distinct aspects of cybersecurity. They are:

- Frontline cybersecurity workers
- Cyber-sensitive service workers
- Physical security and access workers
- Indirect cyber-related workers

The top cybersecurity occupations in-demand nationally were cybersecurity analyst/specialists, cybersecurity engineer, auditors, network engineers/ architects, and software developers.

KEY FINDINGS

- The cybersecurity workforce is not clearly defined among traditional occupation codes; rather it is emerging from within more broadly-defined occupations. As a result, most cybersecurity workers work in occupations that include a mix of cybersecurity workers and workers not focused solely on cybersecurity.

- A clear majority of cybersecurity job postings are for occupations in the frontline workers category. This includes over 76 percent of cybersecurity-related postings nationally and 75 percent of cybersecurity-related postings in Michigan.

- Employer demand for cybersecurity workers in frontline cybersecurity occupations increased by 169 percent from 2010 to 2016, despite falling slightly from 2014-2016.

- While demand for frontline workers has plateaued nationally in recent years, demand in the Advance Michigan region (a 13-county region of southeast Michigan) is still growing at a high rate year after year.[2]

- The top-15 employers with the greatest demand for cybersecurity workers include multiple defense, software, and IT consulting firms, but also includes financial, communications, and health insurance firms.

- A majority (89 percent) of cybersecurity job postings require a bachelor's degree or higher. Among postings specifying a field of study, computer science, engineering, management information systems, information technology, and business administration were the most prominent.

- Industry experts are advising government agencies and private businesses to fill the cybersecurity skills gap by employing workers with certifications rather than relying on traditional four-year IT degree qualified workers.

- Among frontline cybersecurity worker job postings, the most common certifications required were Certified Information Systems Security Professional (CISSP), SANS/GIAC certification, and certified systems auditor. Many postings also required security clearance.

- Frontline cybersecurity occupations pay nearly double the national median hourly wage ($40.09 compared to $21.60 nationally). The median hourly wage of individual occupations in this category range from $23.80 for Computer User Support Specialists, to $63.28 for Computer and Information Systems Managers.

- In the Advance Michigan area, WIN was able to identify a total of 39 institutions offering programs, degrees or training related to cybersecurity. In total, students can choose among more than 90 degree programs and 80 certification programs in the southeast Michigan region.[3]

- It is likely that a lack of standards across the cybersecurity industry complicates recruiting activities for talent. SOC codes for cybersecurity-specific jobs have not been issued and, as a result, are often intertwined with IT jobs. Additionally, there is often not a clear translation of job titles and responsibilities within human resource departments, who may be largely responsible for issuing job postings and assisting with the search for talent. Job titles and responsibilities vary across industries and organizations, complicating the search for talent and making it difficult for students to clearly understand their career options in cybersecurity. Finally, potential employees are often overlooked by automated systems because they may not use the correct keywords within their resumes or job applications or they have the cyber skills required but do not possess a four-year degree.

[1] Total postings and employed cybersecurity workforce figures are from Cyberseek. "Cybersecurity Supply / Demand Heat Map," accessed June 2017, http://cyberseek.org/heatmap.html.

[2] The origin and definition of the 13-county Advance Michigan region are addressed in "Cybersecurity Occupation Categories in the Workforce" on page 7.

[3] Program offerings reflect unique degree-institution combinations and certification-institution combinations in the region.

TABLE OF CONTENTS

INTRODUCTION

DEFINITION AND IMPORTANCE OF CYBERSECURITY

To better understand current workforce demands in the cybersecurity space, the Workforce Intelligence Network for Southeast Michigan (WIN) conducted research to analyze job postings for a broad set of occupations involved in all aspects of cybersecurity, including development of software, testing, hardening, connectivity, business related cyber roles, physical security implications, and general cybersecurity knowledge needs.

Among the most striking changes to our economy and daily life in recent decades has been the revolution in data processing, movement, and production by internet-connected computers and other devices. Firms first used this technology for processing and sharing data within their own walls, then provided data-connected services directly to customers, and now sell connected consumer products such as cars, refrigerators, light bulbs, and doorbells, that people interact with through the internet. Cybersecurity is the protection of these systems and the data they contain from damage, unauthorized use, or exploitation.[4]

While cybersecurity has been a consideration since the start of widespread computer use, its importance has grown rapidly. There is now more data of higher importance moving among more people, objects, and firms. The data is more valuable, and is more relied-upon in daily life, making the potential impact of cyberattacks greater and consequences of disruption even more dire. The systems that manage this data have become much more complex as well, with more connected devices and more firms and people relied upon to manage their security. This complexity makes cybersecurity a challenge, with more potential devices to target, and increasingly wide-spread responsibility for preventing trouble.

The increasing importance of cybersecurity is a priority of our national security community as well.

Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace. Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. Cybersecurity involves protecting information and systems from these threats, such as cyber terrorism, cyber warfare, and cyber espionage. In their most disruptive form, cyber threats take aim at secret, political, military, or infrastructural assets of a nation, or its people. Cybersecurity is therefore a critical part of any organizations' security strategy.[5]

-Department of Homeland Security

[4] The NIST defines cybersecurity as: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

Source: adapted from CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, DHS National Preparedness Goal; White House Cyberspace Policy Review, May 2009. From <https://niccs.us-cert.gov/glossary#C>, accessed May 2017.

[5] https://www.dhs.gov/topic/cybersecurity

CYBERSECURITY OCCUPATION CATEGORIES IN THE WORKFORCE

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 reduce vulnerability, to reacting to intrusions and attacks, to using best practices to keep data secure while working in other business functions.

The analysis in this report builds on work by CyberSeek, a partnership among government, non-profit, and commercial groups to analyze the cybersecurity labor market.[6] WIN's work in this report starts with the occupation codes used in cybersecurity-related job postings identified by CyberSeek, and organizes them into categories by how they engage with cybersecurity issues.

Four main categories of workers were identified in this research with distinct roles and responsibilities and cyber-related skill levels. The categories are:

1. Frontline cybersecurity workers: Responsible for the design and direct implementation of a firm's cybersecurity strategy, such as network administrators, software developers, and information security analysts.

2. Cyber-sensitive service workers: Responsible for operating within a firm's cybersecurity strategy while working with sensitive data, such as auditors, managers, and customer service representatives.

3. Physical security and access workers: Responsible for the physical security of data, computers or infrastructure, or who may have physical access to these assets while doing other work. Examples include security guards, maintenance and repair workers, and retail loss prevention specialists. This category also includes workers who might address the aftermath or investigation of a cyber-attack that has a physical effect, including law enforcement.

4. All other indirect cybersecurity workers: Employers are beginning to recognize the value of a workforce with a general knowledge of cybersecurity, even if those workers do not have distinct cybersecurity duties. They may interact with systems or tools that may be targets or may be vulnerable to cyber-attacks. These workers may interact with sensitive or private data or be able to take simple measures to prevent cyber infiltration. This includes every worker who interacts with software or the internet as part of their duties. Notably in this research, occupations include registered nurses, retail sales workers and human resources professionals.

[6] CyberSeek is a data tool that "provides detailed, actionable data about supply and demand in the cybersecurity job market" (<www.cyberseek.org>, accessed April 2017). The project partners include Burning Glass Technologies, a private provider of real-time job market analytics; the Computing Technology Industry Association, a not-for-profit trade association; and the National Initiative for Cybersecurity Education, a partnership between government, educators, and the private sector, led by the National Institute of Standards and Technology.

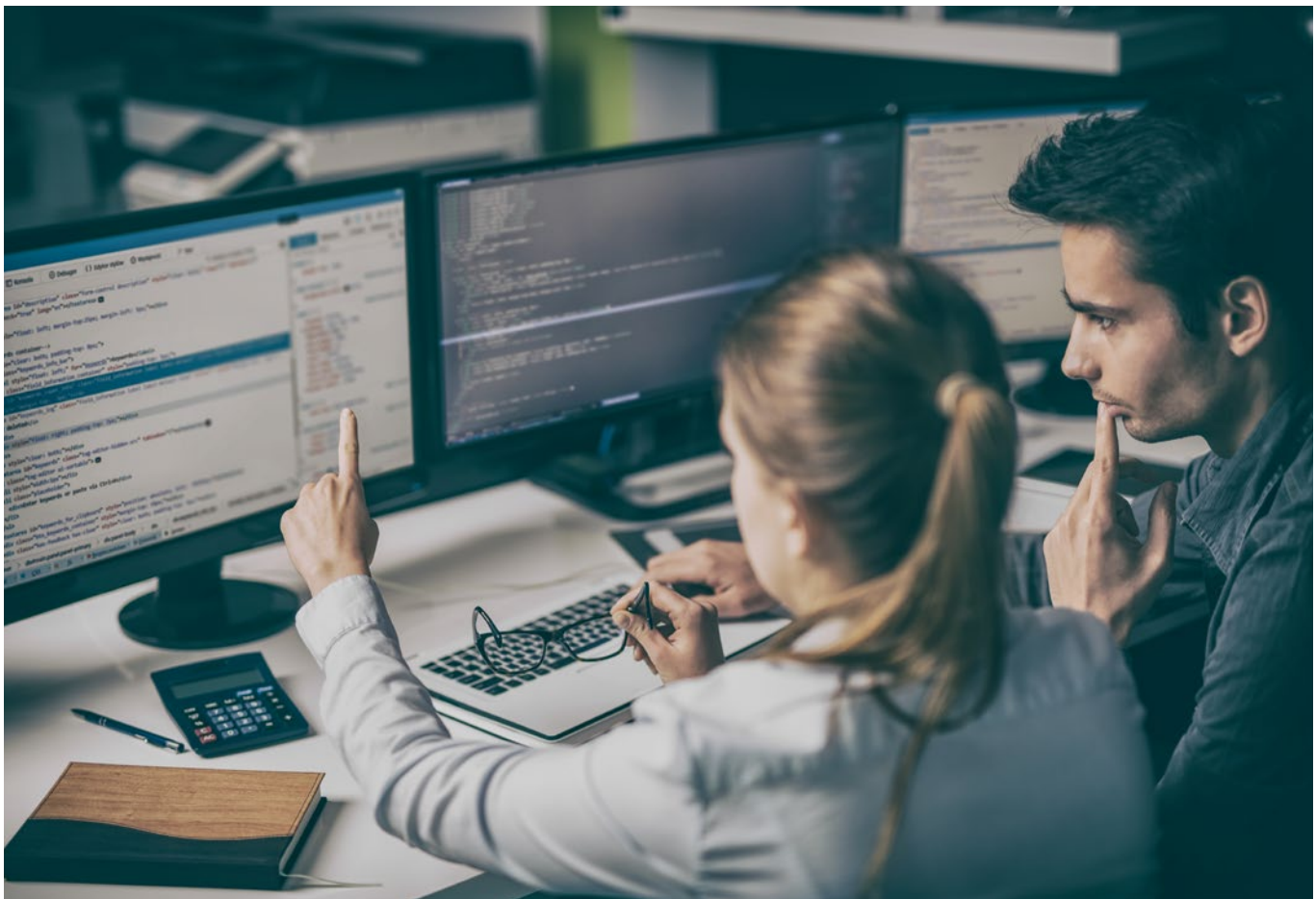
METHODOLOGY

This report focuses on cybersecurity workforce in both the nation as a whole, and in the 13-county Advance Michigan region. The Advance Michigan region was established under the Investing in Manufacturing Partnerships (IMCP), which includes the Advance Michigan Governing Board and the Advance Michigan Defense Collaborative. Under these initiatives, the southeast Michigan (Advance Michigan) region consists of Clinton, Eaton, Genesee, Ingham, Lapeer, Livingston, Macomb, Monroe, Oakland, St. Clair, Shiawassee, Washtenaw, and Wayne. These counties encompass the major cities of Detroit, Pontiac, Lansing, Ann Arbor, and Flint.

OVERALL APPROACH

As noted in the introduction, WIN's analysis builds on the CyberSeek tool created by a group of private, academic, and government partners. The job postings identified in CyberSeek start with a rich database of online job postings maintained by Burning Glass Technologies (one of the CyberSeek partners), and filter them further using a proprietary mix of occupations, skills requirements, and education and certification requirements listed in the job postings. For a deeper analysis of geographies, results can be filtered by state or metro area. Utilizing heat maps and career pathways, this tool shines light on both the supply and demand side of cybersecurity and presents important information for employers and job seekers alike. To access the CyberSeek tool and explore additional cybersecurity workforce data, please visit **www.cyberseek.org**.

While CyberSeek provides baseline data regarding cybersecurity professions, it does not provide several additional data points that employers, workers, and educators may find useful. This report provides figures and analysis to fill this gap, including demand over time, employment levels, top posting employers, education level and experience requirements, in-demand degrees and certifications, and degrees and programs available in southeast Michigan that are helping to reduce these talent gaps. This report aims to provide missing pieces from the cyberseek research and expand upon research of the Southeast Michigan cybersecurity workforce ecosystem using the following approaches listed on the next page:



- WIN's analysis method often includes categorizing occupations relevant to a particular area then analyzing data on that workforce's demographics, employment trends, and demand for workers by local employers. WIN's typical method of research uses government-defined standard occupation codes (SOC), combined with job postings data that includes information about the workers with cybersecurity-related skills that employers need. Due to the newness of cybersecurity, typical occupation codes are not nuanced enough to truly capture cybersecurity workers. WIN has relied on job posting data using a cybersecurity filter developed by Burning Glass, which also feeds CyberSeek, to capture postings data. Using the filter, WIN researchers searched online job postings from Burning Glass to define 200 occupations that have knowledge and skillsets applicable to the growing demand for cybersecurity.

- 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 and may not be captured in industry-focused research.

- This analysis focuses mainly on data collected from job postings. Data pertaining to cybersecurity employment and company-specific workers is difficult to find, as these jobs are held in a wide variety of industries. Job postings allowed WIN researchers to see what companies are looking for and get an idea of what is to come for workers in cybersecurity.

- Employment data from Bureau of Labor Statistics (BLS) and Economic Modeling Specialists International (EMSI) was also used in this report. The data is national unless otherwise noted.

- Data on in-demand degrees, certifications, and skills in cybersecurity is extensive. For the purposes of this report, the data was limited to the top 5 in each category.

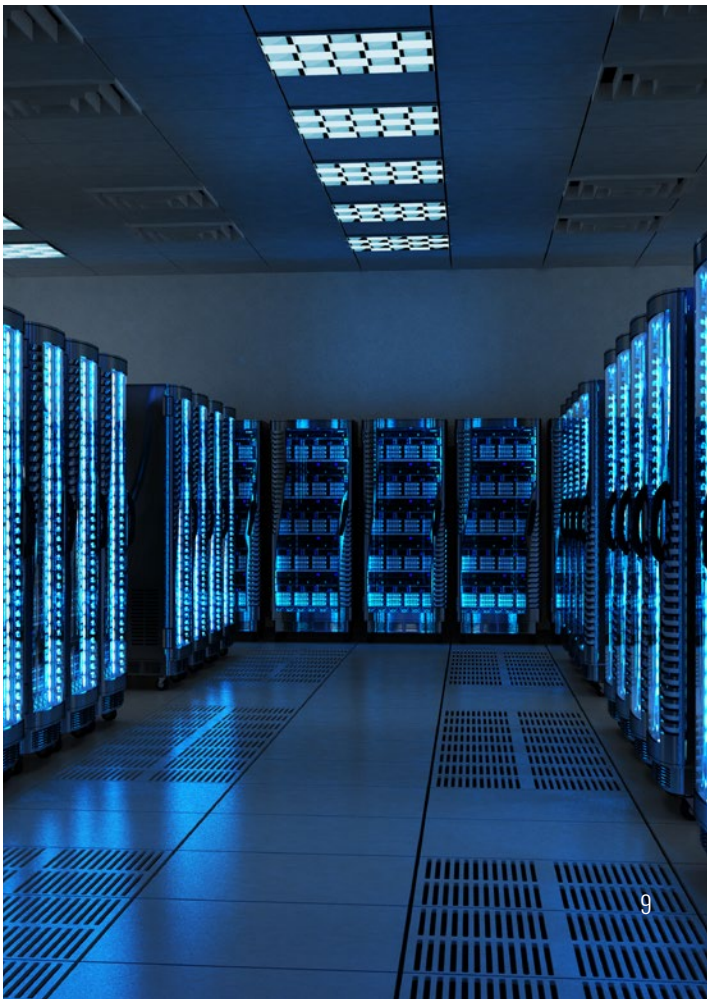
- Top employer data reflects the number of job postings and is arranged in order of the employers posting the most job openings. Top employers were limited to the top 5-15 employers. This data is not inclusive of the number of cybersecurity workers currently employed within organizations.

- This data is not inclusive of the number of cybersecurity workers currently employed within organizations and the possibility exists that other employers may currently employ more cybersecurity workers than those listed but lack current job openings.

- With such a large number of occupations working on a diverse set of problems in the cybersecurity realm, occupational analysis is more easily undertaken and better understood if occupations are grouped into categories, hence the four occupational groups identified in the introduction.

- This data also allows analysis of how common it is for cybersecurity skills to be cited in job postings for any given occupation. For each occupation group, this analysis compares the number of cybersecurity job postings to the total number of job postings (cybersecurity and non-cybersecurity postings) within the same occupation groups. See "Cybersecurity Demand in Context" on page 29.

For a complete list of occupations please see Appendix A. Please see the subsequent section on Occupation Groups to learn more about the categories used in this report.



CYBERSECURITY WORKFORCE OVERVIEW AND DEMAND-CYBERSEEK FINDINGS

CYBERSECURITY WORKFORCE OVERVIEW AND DEMAND-CYBERSEEK FINDINGS

TOTAL CYBERSECURITY OCCUPATIONS OVERVIEW

NATIONAL OVERVIEW

To help close the cybersecurity skills gap, CyberSeek provides detailed, actionable data about supply and demand in the cybersecurity job market.[7] The tool was created through a partnership between Burning Glass Technologies, Computer Technology Industry Association (CompTIA), and the National Initiative for Cybersecurity Education (Nice), to support local employers, educators, guidance and career counselors, students, current workers, policy makers, and other stakeholders as they seek cybersecurity worker information. Utilizing job posting data acquired through Burning Glass Technologies, CyberSeek provides a thorough overview of the cybersecurity landscape throughout the nation. Results can be filtered by state or metro area to conduct a deeper analysis of geographies. Utilizing heat maps and career pathways, this tool shines light on both the supply and demand side of cybersecurity and presents important information for employers and job seekers alike.

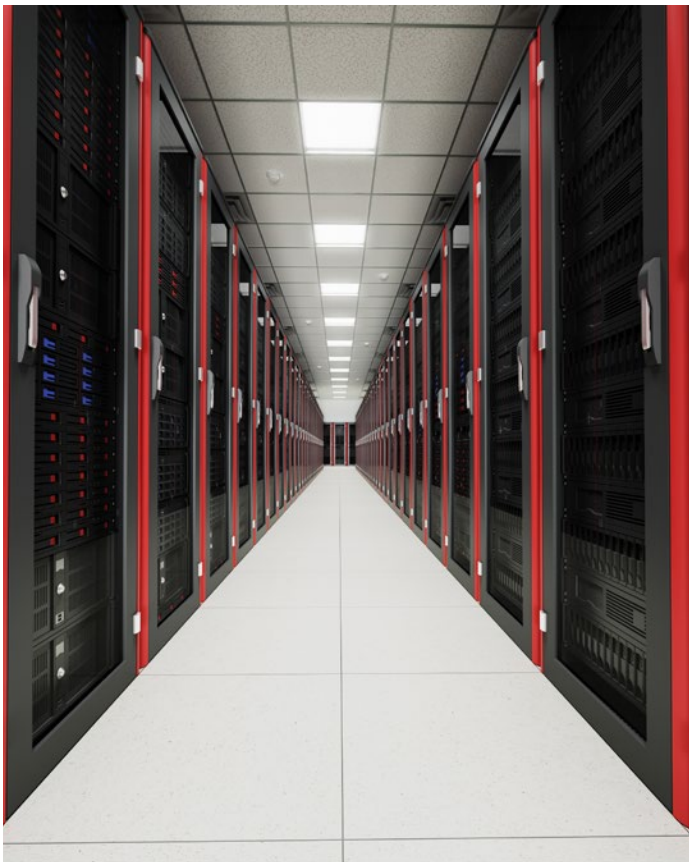
The analysis identified a total of 348,975 cybersecurity-related job listings nationally from between July 2015 and June 2016. Of the nearly 350,000 postings, California was the state with the highest reported postings with 45,062 online job advertisements. Virginia, Texas and New York showed high employer demand, with over 20,000 postings in each state.

Although there were nearly 350,000 total cybersecurity postings, there were 778,402 cybersecurity workers in the workforce during 2016. States that reported high volumes of job postings across all occupations tended to have high volumes of cybersecurity workers. Virginia had the highest number of current cybersecurity workers, with 85,982 workers, while California had a similar supply of workers with 84,415 employed in cybersecurity. Texas, New York, and Florida were other states with a high supply of individuals employed.

When comparing cybersecurity workers to openings, the supply-to-demand ratio was 2.2. The national average supply-to-demand ratio for all jobs is 5.0 showing that the supply for cybersecurity workers is lower than most jobs. States with high volumes of workers or postings showed a very low supply of cybersecurity workers relative to the demand indicating growth opportunities within these states. The only state reporting fewer openings than the current workforce was the state of South Dakota. Virginia, Maryland, and Colorado each has a higher than average concentration of cybersecurity workers. This is measured using location quotients, which compares the concentration of cybersecurity job demand within a geographic area to the national average.

The top cybersecurity occupations in-demand nationally were:

1. Cyber security analyst/specialists: These analysts were the most in-demand occupation in most states as well.
2. Cyber security engineer. This was also the most in-demand occupation in the state of California, a cybersecurity hotspot.
3. Auditors
4. Network engineers/ architects
5. Software developers



An important factor for cybersecurity occupations is having the skills and certifications necessary to enter the cybersecurity field. Security+ was a certification many workers held, but was the third most in-demand certification in online job postings. A total of 92,802 postings expressed interest in applicants with Certified Information Systems Security Professionals (CISSP). A total of 69,549 workers hold these certifications, indicating an opportunity for growth for workers looking to get into the cybersecurity field. Other certifications that were in high demand but a low supply include Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM).

Another metric measured within the CyberSeek mapping platform is the division of postings into Cybersecurity Workforce Framework categories, which identify the type of work new hires may do. The framework used by CyberSeek to categorize workers was established by the National Initiative for Cybersecurity Education (NICE), which itself was created by the National Institute for Standards and Technology. The NICE framework is intended to provide organizations with a common, consistent lexicon that categorizes and describes cybersecurity work.[8] The categories include[9]:

1. Securely Provision: Conceptualizes, designs, and builds secure information technology (IT) systems, with responsibility for aspects of systems and/or networks development

2. Operate and Maintain: Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security

3. Oversee and Govern: Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work

4. Protect and Defend: Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks

5. Analyze: Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence

6. Collect and Operate: Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence

7. Investigate: Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence

The largest number of postings (232,552) were part of the "operate and maintain" category. These workers can expect to provide the support and administration to provide efficient and effective information technology and security. "Securely provision" was another category with high demand, including workers focusing on conceptualizing and designing secure systems while taking part in system development. The third most in-demand category is Analyze, where workers review and evaluate incoming information to determine its usefulness for intelligence.

Cyberseek provides an interactive career pathway tool highlighting different methods of entry within individual cybersecurity occupations. Focusing on entry-level to advanced level occupations, job seekers have access to national data concerning educational requirements, skills, and average advertised wages. This tool shows possible career pathways related to cybersecurity occupations.

---

[7] Cyberseek.org

[8] https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

[9] http://csrc.nist.gov/publications/drafts/800-181/sp800_181_draft.pdf

STATE OF MICHIGAN OVERVIEW

The state of Michigan has a relatively strong presence in cybersecurity. There was a total of 6,789 job postings between July 2015 and June 2016 within the state. The supply within Michigan was also relatively strong with 13,520 current workers. Most of the supply and demand of cybersecurity related jobs comes from the Detroit Metropolitan Statistical Area (MSA), which boasts higher than average metrics compared to other MSAs. Like many states, the ratio of cybersecurity workforce supply was very low compared to demand, with 2 workers employed per posting. This is one fifth smaller than the national average ratio. The location quotient for the state shows that there is a low concentration of cybersecurity demand within the Michigan area compared to the rest of the country.

The top in-demand cybersecurity occupation in the state was cybersecurity analyst/ specialists. Cybersecurity engineers and auditors were also highly sought after, mirroring the national top jobs for cybersecurity. Most job postings fell into the NICE category as "Operate and Maintain" positions. Other NICE categories that saw high demand include "Securely Provision" and "Analyze" related occupations.

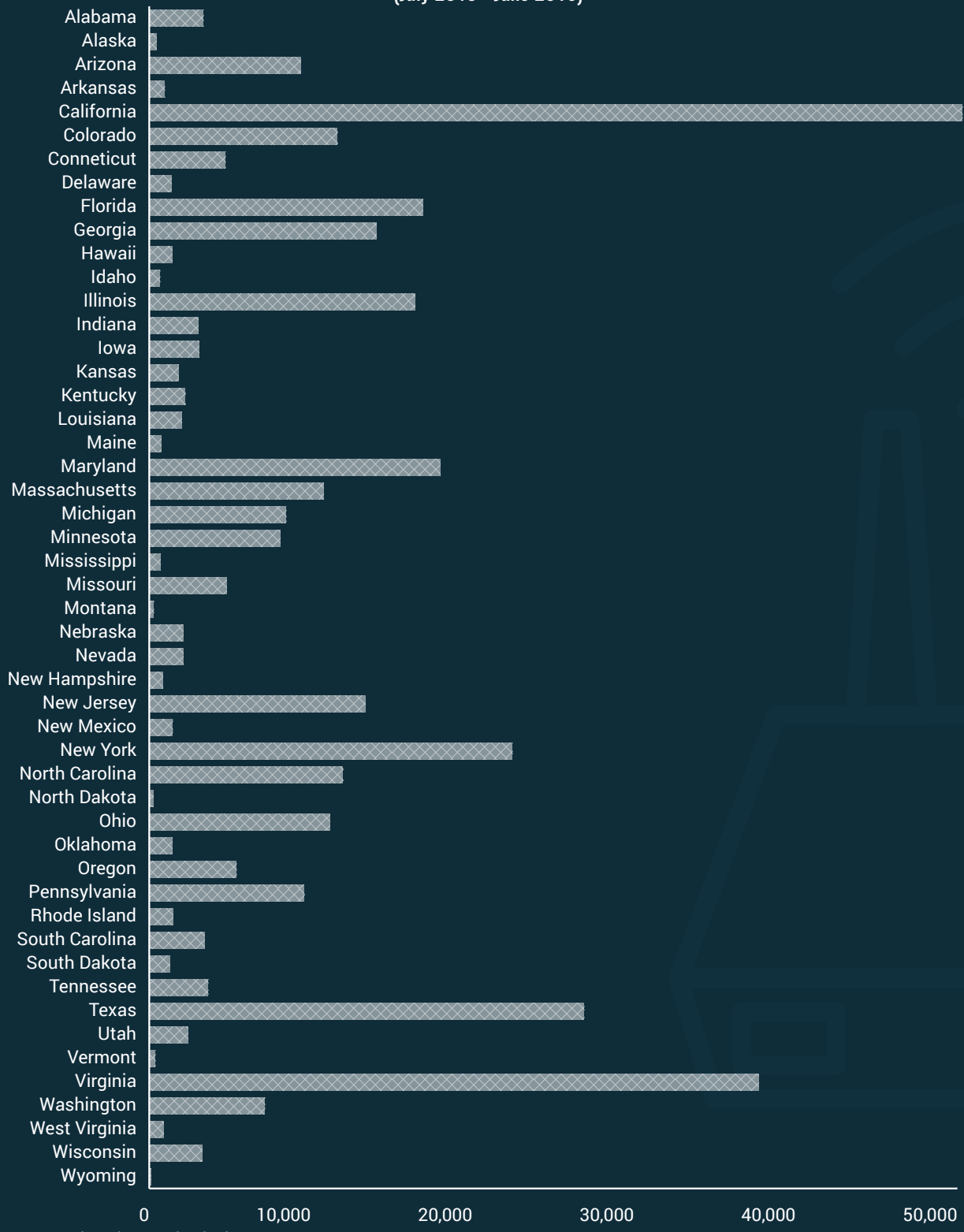
Employers hiring in the cybersecurity field have a high demand for knowledge and skills. Data for Michigan shows that becoming certified in skills and programs is an important way for jobseekers to meet employer demands and serve as a great baseline for measuring applicants' abilities. The most held certification related to cybersecurity was Security+ with over 2,139 Michigan certificate holders. While Security+ serves as a standard for network security and risk management procedure, other certifications were also in high demand. Over 1,800 postings sought Certified Information Systems Security Professional (CISSP), with only 1,121 certificate holders in the market. Certified Information Systems Auditor (CISA) was also in high demand with 1,174 postings searching for applicants with these accolades.

NATIONAL COMPARISON

A national comparison of job postings in cybersecurity across the nation provides a picture of how this sector is developing in each state. Unsurprisingly, the West Coast leads the way with the most postings in March 2017: California nabs the top spot, where the top employer is the California post-secondary education system.

Following closely behind are Virginia and Maryland, whose top employers for these occupations are federal government contractors and consulting firms. Texas also has a large presence in this field, with top employers including commercial real estate managers.

TOTAL POSTINGS BY STATE
(July 2015 - June 2016)



Data: Burning Glass Technologies
Analysis: Workforce Intelligence Network

Note: Data from CyberSeek and the Burning Glass Technologies cybersecurity filter may not match in the number of job postings listed for each state. CyberSeek data is proprietary, therefore methdology from this tool cannot be precisely duplicated. WIN has used the Burning Glass tool to develop a separate but similar methodology to assess demand data using the same resources. Data from cyberseek and this report may not be an exact match.

CYBERSECURITY-RELATED OCCUPATION SUB-GROUPS

OCCUPATION CATEGORY 1

FRONTLINE CYBERSECURITY WORKERS

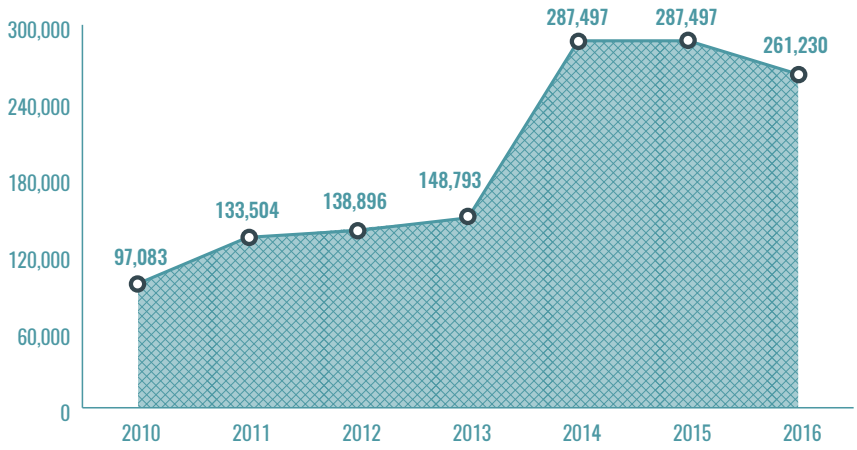
The “Frontline Cybersecurity Workers” category consists of those directly working with the technical design and implementation of cybersecurity strategies. These are the employees who develop the programming related to security, investigate and address virtual threats, and work directly with security platforms. The occupations encompassed in this group include those working directly with security technology such as network administrators, software developers and information security analysts.

Demand Trends

NATIONAL

The “Frontline Cybersecurity Workers” category consists of those directly working with the technical design and implementation of cybersecurity strategies. These are the employees who 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.

NATIONAL FRONTLINE CYBERSECURITY WORKER DEMAND
(2010 - 2016)

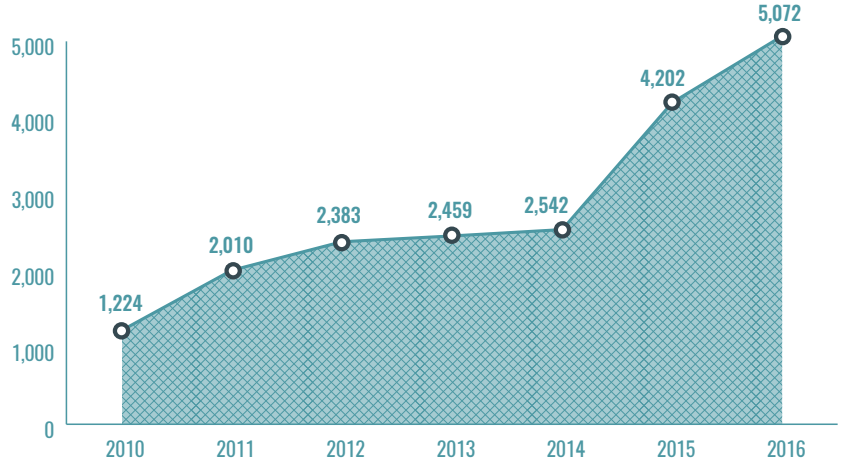


Data: Burning Glass Technologies
Analysis: Workforce Intelligence Network

ADVANCE MICHIGAN REGION

Employer demand for frontline cybersecurity occupations in the Advance Michigan region has continued its steady upward trajectory for the seventh consecutive year. From the 1,224 job postings related to frontline cyber technology in 2010, demand for these workers increased 414 percent to 5,072 postings in 2016. Demand remained steady between 2012 and 2014, hovering around 2,400 postings, but began increasing again in 2015. Currently demand is at an all-time high of 5,072 job postings.

ADVANCE MICHIGAN REGION FRONTLINE CYBER WORKER DEMAND
(2010 - 2016)



Data: Burning Glass Technologies
Analysis: Workforce Intelligence Network

Top Posting Employers

NATIONAL

The top fifteen businesses recruiting for frontline cybersecurity employees were:

- General Dynamics
- Oracle
- Booz Allen Hamilton Inc.
- Deloitte
- Northrop Grumman
- Raytheon
- Mantech International Corp.
- Lockheed Martin Corporation
- CACI
- Verizon Communications Incorporated
- Wells Fargo
- UnitedHealth Group
- Leidos
- Accenture
- BAE Systems

This list includes firms in diverse industries, including defense, software, communications, finance, and health insurance. Most of the top employers for frontline cybersecurity workers are a part of the defense industry, supplying security to government offices and databases. A few employers take part in finance, telecommunications, and healthcare to help protect vital information of consumers. These include securing patient records and financial information we use every day.

ADVANCE MICHIGAN REGION

The top fifteen employers recruiting frontline cybersecurity employees in the Advance Michigan region were:

- General Motors
- Ford Motor Company
- Oracle
- Ciber Incorporated
- Blue Cross Blue Shield of Michigan
- Ascension-Healthcare
- The Detroit News
- Deloitte
- Henry Ford Health System
- Michigan State University
- University of Michigan
- Ally Financial
- Comerica
- DCS Corporation
- Johnson Controls Incorporated

As with the top employers nationally, the Advance Michigan region's top job posting firms include auto, defense, finance, and health. Additionally, media and universities, are represented on this list. General Motors and Ford Motor Company are two of the top employers seeking cyber employees in the Advance Michigan region. These auto manufacturers produce technologically advanced automobiles, so 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.

Advertised Education

NATIONAL

Most employers of frontline cybersecurity positions require that candidates have a bachelor's degree or higher. Of the 181,306, national job posting that specified a desired level of education attainment; 148,200 (82 percent) specified a Bachelor's degree. Only 16 percent of the national job postings are open to workers with a high school diploma and some vocational training (29,356 job postings). In a number of cases, two year degrees can be transferred to four year institutions for bachelor's degree completion. Refer to Appendix B for educational offerings in the region.

While there appears to be a high demand for four-year degrees, cybersecurity experts and the US government are advising that many of the positions posted can be filled with workers who have attained the appropriate certificate or two-year degree. Security businesses tend to look for people with traditional technology credentials instead of recognizing the specialized cyber skills needed. Per an article from the Harvard Business Review, IBM is now addressing talent shortages in cybersecurity by creating "new collar" jobs that prioritize skills, knowledge, and willingness to learn over degrees. As a result, 20 percent of IBM's US hiring in cyber since 2015 has consisted of these new-collar professionals.[10]

Leaders within the US government appear to be pressing federal agencies to use qualified professionals without four-year degrees as well. In a May 4, 2017 letter from a New Democrat Coalition task force to the Office of Personnel Management (OPM), the task force stated, "Offering industry-recognized certification testing would be a valuable tool for agencies to recruit and retain highly-qualified cyber professionals." The letter further questions "we would like to learn more about the OPM degree requirement for cybersecurity-related jobs. It appears that OPM does not mandate cyber professionals have a four-year degree, but we have been informed that the vast majority of job postings ask for one. Given the increasing need for cybersecurity personnel, OPM should be more flexible with job requirements."[11]

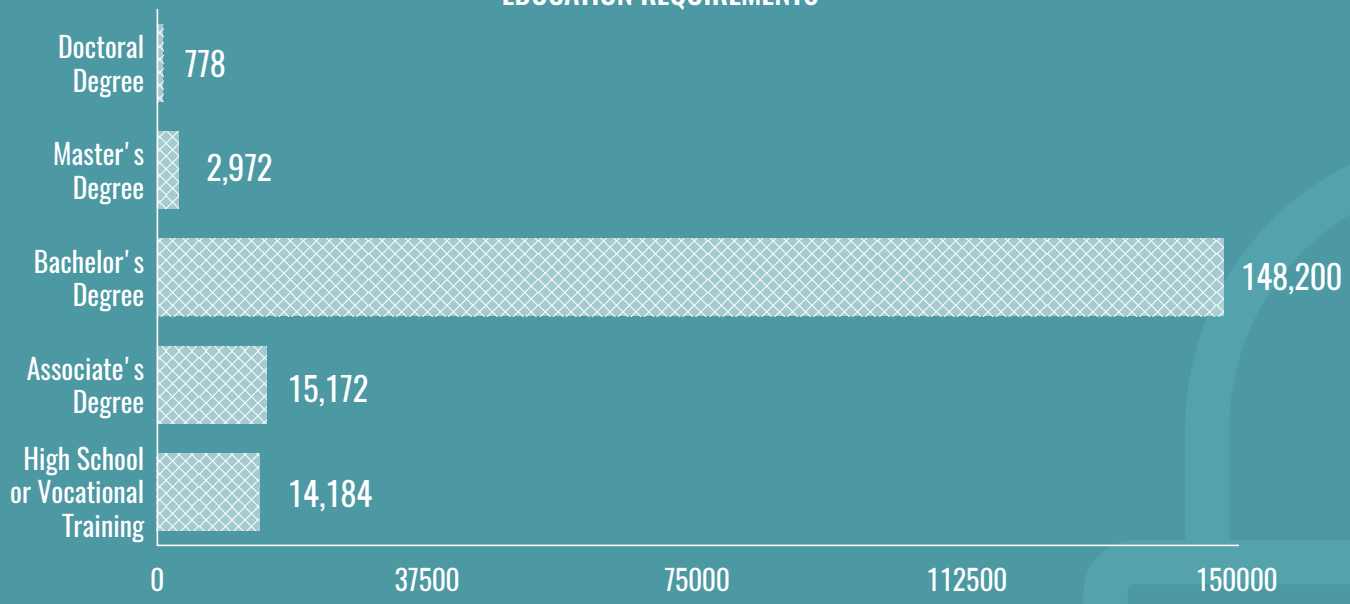
ADVANCE MICHIGAN REGION

Of the 3,653 Advance Michigan job postings that specified a desired level of education attainment; 3,136 (86 percent) specified a Bachelor's degree. Only 11 percent of the national job postings are open to workers with a high school diploma and some vocational training (420 job postings).

[10] Harvard Business Review: https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it

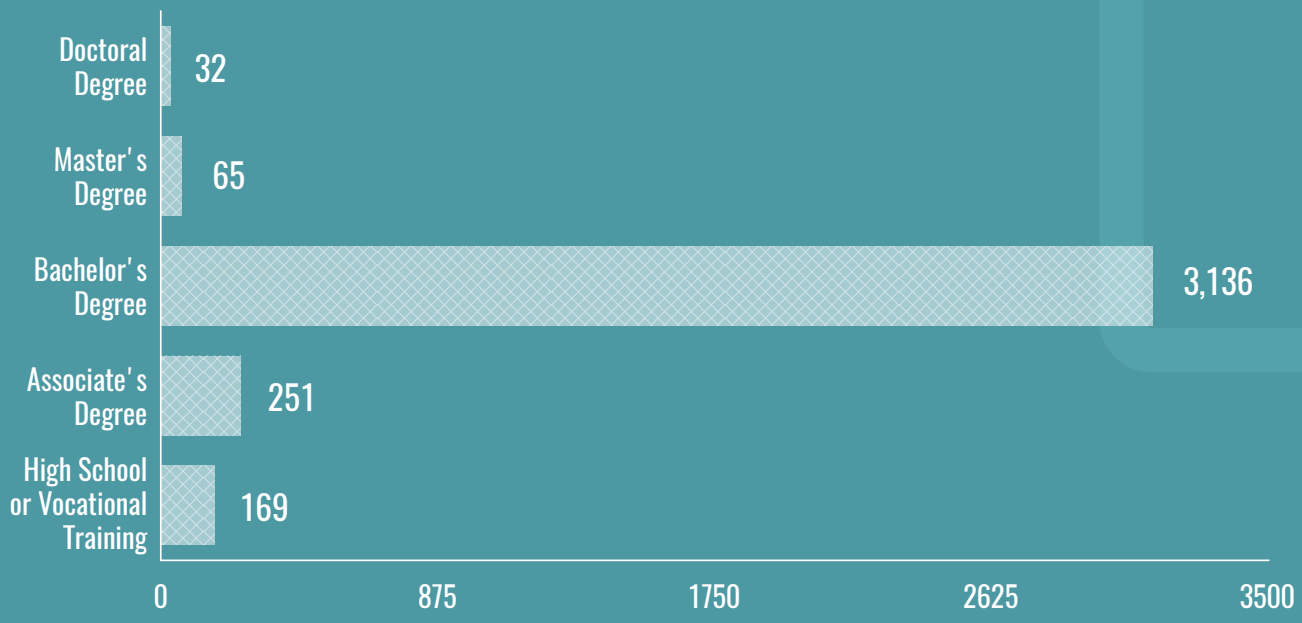
[11] https://newdemocratcoalition-himes.house.gov/sites/newdemocratcoalition.house.gov/files/documents/New%20Dem%20OPM%20Cyber%20Letter%20-%20color.pdf

NATIONAL FRONTLINE CYBERSECURITY EDUCATION REQUIREMENTS



Data: Burning Glass Technologies
Analysis: Workforce Intelligence Network

ADVANCE MICHIGAN FRONTLINE CYBERSECURITY EDUCATION REQUIREMENTS



Data: Burning Glass Technologies
Analysis: Workforce Intelligence Network

In-Demand Degrees

The most sought after degrees by both national and Advance Michigan region employers were:

- Computer science
- Engineering
- Management information systems
- Information technology
- Business administration and management

In-Demand Certifications

NATIONAL

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

- Certified information systems security professional (CISSP)
- Security clearance
- SANS/GIAC certification
- Certified information systems auditor (CISA)
- Cisco certified network associate

ADVANCE MICHIGAN REGION

The top five frontline cybersecurity occupations in demand in the Advance Michigan region include:

- Certified information systems security professional (CISSP)
- Certified information systems auditor (CISA)
- SANS/GIAC certification
- Certified information systems manager (CISM)
- Security clearance

A note on security clearances:

Many of the positions available in cybersecurity require a security clearance. This is not a certificate that may be taught nor learned. Instead, a security clearance is a process of investigation and adjudication. This can only be obtained by United States Government sponsorship and cannot be acquired outside of this scope. Presidential Executive Order 13526 addresses Classified National Security Information[12] and Standard Form 312-Classified Information Nondisclosure Agreement Briefing Booklet provides information regarding responsibilities of individuals receiving access to classified documents. A security clearance is a determination by the United States Government that a person or company is eligible for access to classified information. The term "eligibility for access" is synonymous with the term security clearance. A change under the Obama administration streamlined all processes for eligibility for access and all investigations are now conducted through the Office of Personnel Management (OPM), Federal Investigative Services.[13]

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 to make themselves more attractive to potential employers.

[12] *https://www.archives.gov/isoo/policy-documents/cnsi-eo.html*
[13] *https://www.opm.gov/investigations/background-investigations/*

Completions

NATIONAL

Throughout the nation, a total of 250,648 cybersecurity-related degrees or certificates were completed during 2015, the most recent data available. The most common degrees earned were general computer and information science degrees with nearly 33,000 completions. In 2011, 197,248 students completed educational programs related to cybersecurity. By 2015, that number had increased by 27 percent to 250,648 completions. Thus, the supply of workers with cybersecurity education has increased too.

ADVANCE MICHIGAN REGION

During 2015, a total of 4,527 degree and certificates were awarded within the Advance Michigan region. Most of these completions came from Computer related studies, with 813 completions in general computer and information science degrees alone. From 2011, frontline cybersecurity related degrees have been increasing over time, with the number of completions in 2015 breaking the previous high of 4,481 completions in 2012.

Southeast Michigan Institutions Awarding Degrees and Certificates

Cybersecurity workers can acquire the skills needed through a mix of higher education, formal training, and on-the-job experience. There is scant data on much of the employer-provided and non-degree training on cybersecurity topics. Nevertheless, a look at the output of IT-related higher education programs can give one measure of how many new workers are being "produced" with the broad tools to work on many frontline cybersecurity tasks.[14]

The top Southeast Michigan degree/certification awarding institution in 2015 was the University of Michigan. The computer and information science program awarded 344 Bachelor's degrees, while the University awarded 492 IT-related degrees overall during 2015. Other awarding institutions include Michigan State University, with 135 completions during 2015, and Wayne State University, with 132 completions during the same timeframe. For information about cyber degrees offered at these institutions, refer to Appendix B. Please also refer to the section "Closing the Gap." on page 34.

Worker Experience

Overall, national frontline cybersecurity job postings requested a wide variety of experience levels. The most common level required by job postings, with 46 percent of postings, was for three to five years of experience. The least requested experience level, with just 15 percent, was two years or fewer.

Similar to nationwide postings, job ads in the Advance Michigan region preferred workers with three to five years of experience. This level of experience was requested by 49 percent of postings.

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, the median national hourly pay is $40.11 per hour. At the 25th percentile, workers earn $30.63 per hour, and workers at the 75th percentile earn $51.43 per hour.

In the Advance Michigan region, earnings for current cybersecurity workers were slightly lower than at the national level; $36.67 per hour is the median hourly rate. The earnings at the 25th percentile are $28.09 per hour, while those in the 75th percentile earn $46.40 per hour. A comparison of cost of living may account for the difference in these wages, but has not been performed as part of this study.

[14] Completion totals based on a list of IT-related degree programs compiled by EMSI, Inc. It includes Computer and Information Sciences, Computer Programming, Informatics, Artificial Intelligence, and other Information Technology degrees.

National Median Wages

OCCUPATION	PCT. 10 HOURLY EARNINGS	PCT. 25 HOURLY EARNINGS	MEDIAN HOURLY EARNINGS	PCT. 75 HOURLY EARNINGS	PCT. 90 HOURLY EARNINGS
Computer and Information Systems Managers	$40.86	$50.78	$63.28	$79.48	$122.20
Business Operations Specialists, All Other	$19.17	$25.07	$33.17	$43.27	$54.80
Computer and Information Research Scientists	$34.12	$42.50	$53.09	$65.07	$77.86
Computer Systems Analysts	$25.72	$32.47	$41.41	$51.72	$63.24
Information Security Analysts	$26.26	$33.92	$43.77	$55.01	$65.92
Computer Programmers	$22.97	$29.82	$38.41	$48.70	$59.55
Software Developers, Applications	$29.61	$37.60	$47.68	$58.97	$71.50
Software Developers, Systems Software	$32.53	$40.66	$51.08	$62.66	$74.75
Web Developers	$17.80	$22.53	$29.68	$38.71	$47.83
Database Administrators	$23.02	$29.96	$39.87	$50.38	$59.98
Network and Computer Systems Administrators	$24.05	$30.07	$38.05	$47.58	$57.79
Computer Network Architects	$30.09	$37.97	$48.37	$59.72	$71.65
Computer User Support Specialists	$14.76	$18.60	$23.80	$30.50	$38.46
Computer Network Support Specialists	$18.94	$23.70	$30.56	$39.47	$48.98
Computer Occupations, All Other	$24.11	$31.77	$40.86	$50.18	$59.32
Operations Research Analysts	$23.04	$29.06	$38.47	$49.80	$61.71
Statisticians	$24.83	$31.13	$38.99	$48.82	$59.10
Computer Hardware Engineers	$34.17	$43.09	$54.43	$66.06	$78.81
Frontline Cybersecurity Workers (average)	$24.66	$31.33	$40.09	$50.44	$63.30
Computer and Information Systems Managers	$37.11	$43.83	$53.56	$65.82	$79.31
Business Operations Specialists, All Other	$17.39	$22.42	$31.12	$41.72	$51.93
Computer and Information Research Scientists	$32.73	$39.91	$47.12	$58.82	$70.53
Computer Systems Analysts	$24.69	$32.06	$41.70	$51.52	$60.34
Information Security Analysts	$25.03	$29.73	$41.08	$50.05	$58.93
Computer Programmers	$21.89	$26.68	$33.82	$42.47	$49.61

OCCUPATION	PCT. 10 HOURLY EARNINGS	PCT. 25 HOURLY EARNINGS	MEDIAN HOURLY EARNINGS	PCT. 75 HOURLY EARNINGS	PCT. 90 HOURLY EARNINGS
Software Developers, Applications	$24.67	$31.49	$40.80	$51.49	$60.64
Software Developers, Systems Software	$27.50	$34.16	$43.06	$51.82	$60.48
Web Developers	$17.97	$21.35	$26.77	$33.28	$39.45
Database Administrators	$25.05	$32.44	$43.03	$52.12	$60.24
Network and Computer Systems Administrators	$22.43	$28.22	$36.77	$44.67	$52.72
Computer Network Architects	$35.70	$42.31	$50.89	$59.42	$70.58
Computer User Support Specialists	$13.29	$16.58	$22.11	$29.52	$37.58
Computer Network Support Specialists	$15.55	$20.35	$27.96	$39.00	$49.44
Computer Occupations, All Other	$19.46	$25.98	$34.16	$42.47	$52.17
Operations Research Analysts	$26.50	$32.24	$40.92	$49.20	$58.71
Statisticians	$24.26	$29.61	$36.86	$46.89	$55.61
Computer Hardware Engineers	$18.17	$28.43	$39.92	$53.27	$65.76
Frontline Cybersecurity Workers (total)	$22.00	$27.72	$36.09	$45.59	$54.89

Worker Skills

TECHNICAL

To perform well in a cybersecurity occupation, workers need to have advanced software, information security and technical support skills. Employers seek workers with prowess in many aspects of network administration, including various programs and operating systems. Candidates with the ability to communicate with customers and provide clear technical support are also valued.

Top technical skills in demand:

- Information Security
- Network Security
- LINUX
- Information Systems
- Cryptography
- Cisco
- Technical support/customer service

EMPLOYABILITY

In addition to the advanced software skills necessary in cybersecurity positions, employers want to know that candidates can work effectively as part of a team, as well as troubleshoot any problems that may arise.

Top employability skills in demand:

- Communication Skills
- Writing
- Troubleshooting
- Planning
- Problem Solving
- Research
- Team Work/ Collaboration

OCCUPATION CATEGORY 2

CYBER-SENSITIVE SERVICE WORKERS

Cyber-sensitive occupations are occupations that do not directly generate any technological advancements in cybersecurity, but they are responsible for operating within a firm's cybersecurity strategy while working with sensitive data. These occupations include auditors, managers, and customer service representatives. These occupations are outside the technology field but must use proper cybersecurity practices and depend on the services that cybersecurity provides to safeguard their information. These workers might also help to identify which data, processes, or infrastructure are important to protect.

Top Posting Employers

NATIONAL

The top five firms recruiting for cyber-sensitive occupation employees were:

- Oracle
- Macy's
- Lowe's Companies Inc.
- Sears
- Wells Fargo

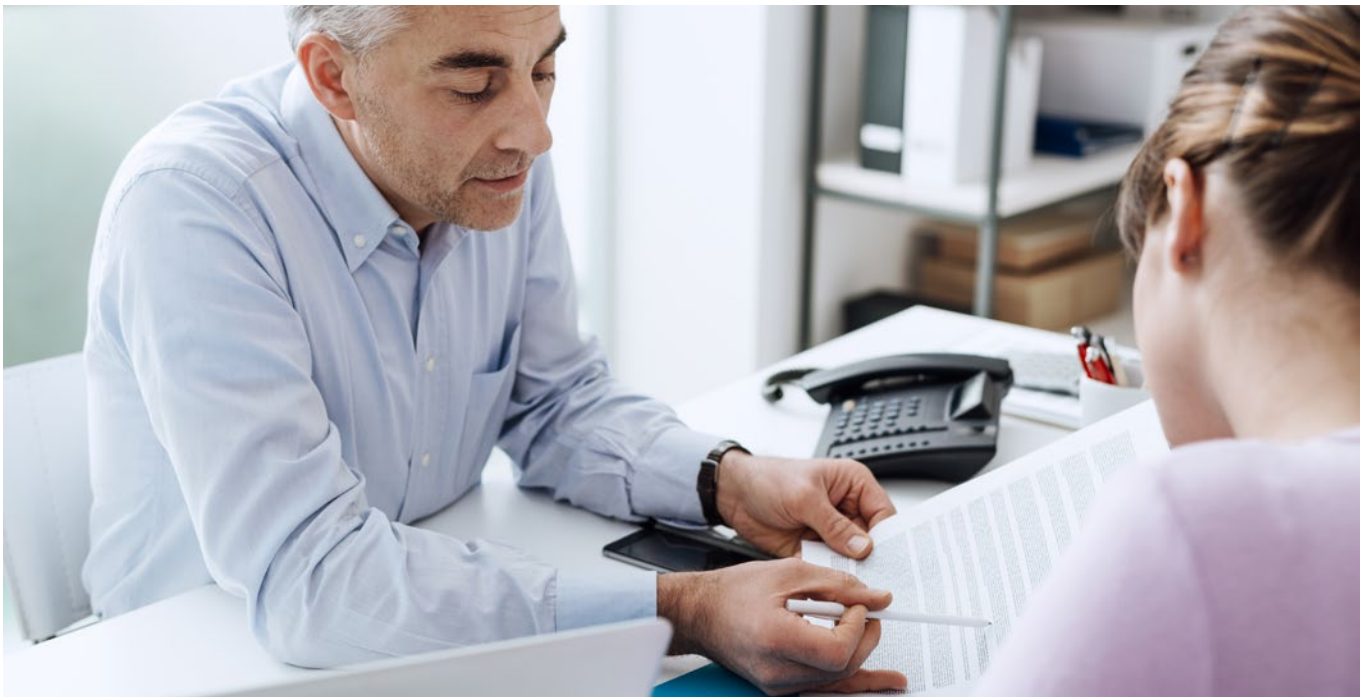
These firms include some industries found in the "frontline cybersecurity workers" analysis above, such as software and finance. However, three are in an industry not strongly tied to demand for frontline workers: retail services.

ADVANCE MICHIGAN REGION

The top five employers recruiting cyber-sensitive employees in the Advance Michigan region were:

- General Motors
- University of Michigan
- Chrysler
- The Detroit News
- Ford Motor Company

This list has little overlap with the national list of top job posting firms in terms of which industries are represented. Notably, this list includes firms in auto manufacturing, media, and higher education.

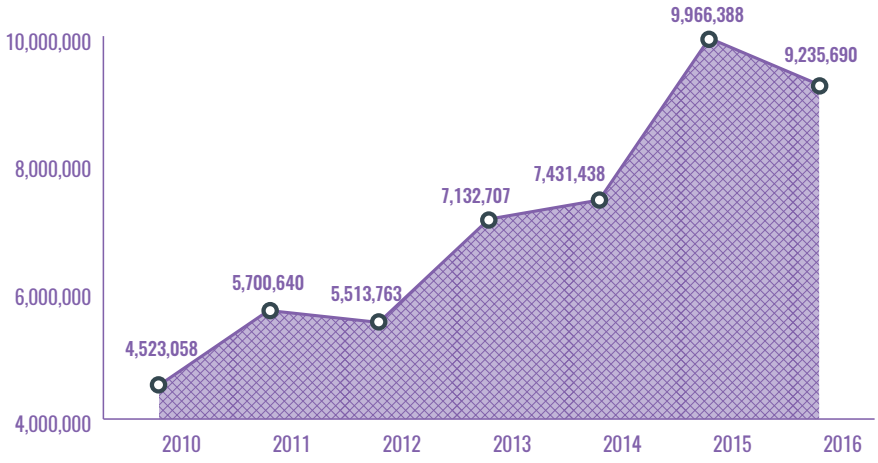


Demand Trends

NATIONAL

National demand for cyber-sensitive occupations generally increased between 2010 and 2016. Demand for these workers increased 204 percent from 4,523,058 in 2015 to 9,235,690 postings in 2016. Demand for these jobs exhibited a large increase of 26 percent to 5,700,640 postings in 2011.Unfortunately, these job postings experienced a four percent decrease in demand in 2012. From 2013 to 2015, job postings increased 39 percent, reaching a high of 9,966,388 postings in 2015, though they fell eight percent moving into 2016. Year-to-year changes in cybersecurity postings could be explained by a combination of factors, including changes in underlying demand for the skills, changes in how job postings are written, and other unknown factors.

NATIONAL CYBER-SENSITIVE OCCUPATION EMPLOYER DEMAND
(2010 - 2016)

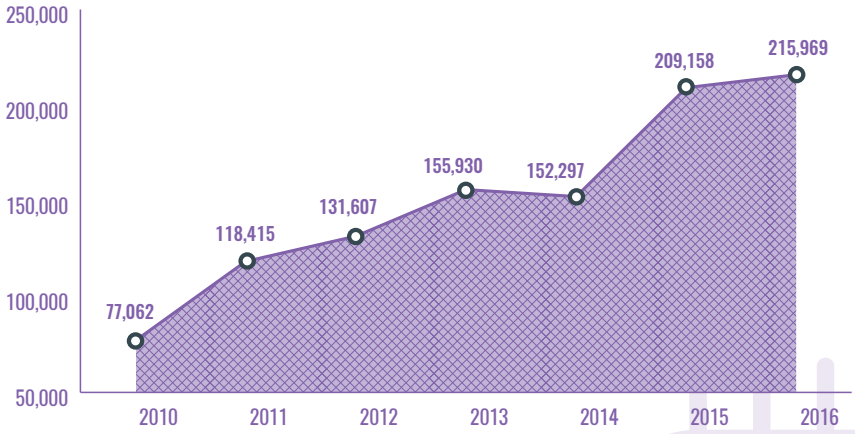


Data: Burning Glass Technologies
Analysis: Workforce Intelligence Network

ADVANCE MICHIGAN REGION

Employer demand for cyber-sensitive occupations in the Advance Michigan region continues a steady upward trajectory for the seventh consecutive year. From the 77,062 job postings related to cyber-sensitive occupations in 2010, demand for these workers increased 280 percent to 215,969 postings in 2016. Demand increased steadily at 14 percent each year between 2011 and 2013, reaching a new high of 155,930 postings in 2013. Demand decreased three percent in 2014 to 152,297 postings. Worker demand increased by 37 percent in 2015, and by a modest four percent in 2016 to 215,969 postings.

ADVANCE MICHIGAN CYBER-SENSITIVE OCCUPATION EMPLOYER DEMAND
(2010 - 2016)



Data: Burning Glass Technologies
Analysis: Workforce Intelligence Network

OCCUPATION CATEGORY 3

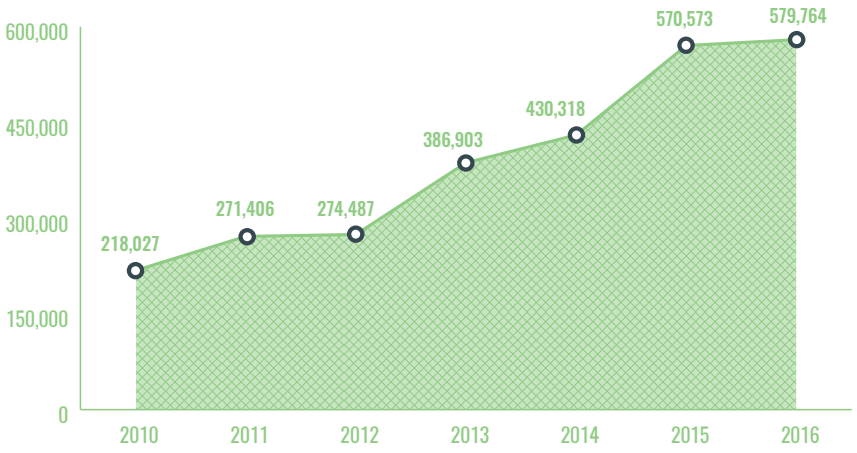
PHYSICAL SECURITY OCCUPATIONS

Physical security and access workers are those workers who are responsible for the physical security of data 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, retail loss prevention specialists, and private detectives.

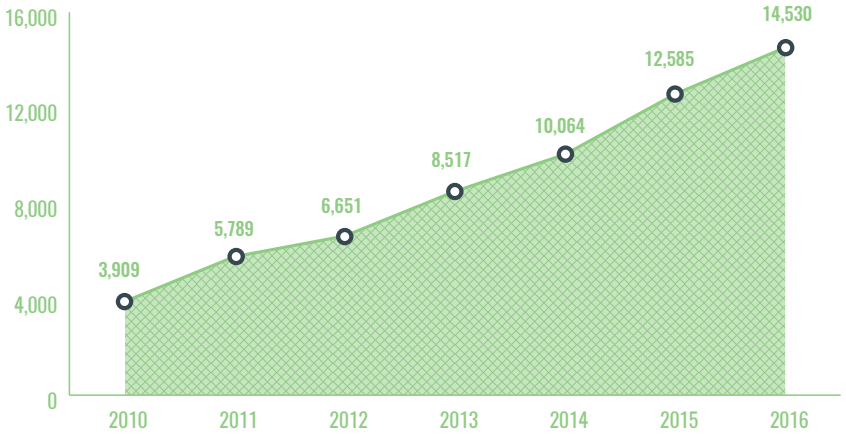
Demand Trends

On both a national level and in the Advance Michigan region, demand for physical security occupations has been experiencing steady growth since 2010. On the national scale, these jobs have nearly tripled in demand. In the Advance Michigan counties, this group had almost four times as many postings in 2016 as 2010. It is unknown whether the level of demand in this occupational category changed, or if employers fluctuated in their desire or practice of requiring some aspect of cybersecurity be included in these postings.

NATIONAL PHYSICAL SECURITY JOB POSTINGS OVER TIME
(2010 - 2016)



ADVANCE MICHIGAN REGION PHYSICAL SECURITY JOB POSTINGS OVER TIME
(2010 - 2016)



Top Posting Employers

NATIONAL

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

- Securitas Security Services USA Incorporated
- G4S
- AlliedBarton Security Services
- G4S Secure Solutions, Inc
- Universal Protection Corporation
- The Home Depot Incorporated
- Macy's
- Kronos Incorporated
- McDonald's
- Sears
- United States Security Associates
- The Detroit News
- Toys"R"Us, Inc
- Allied Universal Corporation
- Chrysler

Physical security occupations account for only 3.5 percent of all cybersecurity employment, both in the Advance Michigan region and nationwide. Due to the relatively small need for physical rather than virtual protection in cybersecurity, this is unsurprising. Cybersecurity focused jobs in physical security comprised about 1.6 percent of total employment for those occupations in Michigan, and 1.4 percent nationwide.

OCCUPATION CATEGORY 4

INDIRECT CYBER-RELATED OCCUPATIONS

These workers may work with sensitive information regularly or work with technology that could utilize cybersecurity. Although these occupations do not work directly within the cybersecurity field, they show the importance of cybersecurity across all jobs and firms. The indirect cyber-related occupations do not work directly with cybersecurity or those deeply involved in the field but do have some related skills and follow some cybersecurity best practices. These workers may work with sensitive information regularly or work with technology that could utilize cybersecurity. Registered nurses may work with patient information and follow secure procedures to ensure client information remains confidential. Graphic designers developing websites may utilize some cybersecurity software or techniques when publishing their content on the web to decrease vulnerabilities. Although these occupations do not work directly within the cybersecurity field, they show the importance of cybersecurity across all jobs and firms.

From our bank accounts, to our Facebook pages, to nuclear power plant control rooms or government offices, we all interact with cybersecurity daily. Although many people cannot claim to know all the mechanics and programming behind the privacy filters of their social media platforms, simply interacting with it is controlling the flow of information and securing what people can see. Logging in to online banking and filling in passwords, verifying identity, and other procedures is working through your banks security to make sure no one else can obtain your financial information. Safeguards are put in place on our country's infrastructure so that we can safely and reliably receive clean water, drive, and power our homes without the fear of hackers bringing down the structures and facilities that let us partake in our daily activities. Even occupations that don't design and manage cybersecurity need to understand the importance of protecting and securing information.

Cybersecurity is present in everyday working environments and used by all kinds of workers. Cybersecurity procedures most workers use in their jobs include identifying and avoiding phishing emails, safely storing information in specific drives, and working with antivirus software. Whether working with worker's social security numbers for fiscal or human resources purposes or providing secure servers to workers in an office, it's important for business to have effective cybersecurity strategies in place and to keep their employees informed. These factors and the involvement of cybersecurity in many daily activities promote the need and importance of general cybersecurity knowledge by countless occupations.

CYBERSECURITY DEMAND IN CONTEXT

Though this report has documented demand for thousands of cybersecurity workers both nationwide and in Michigan, the postings identified as cyber-related through NICE are not typical. For each occupation group, comparing the number of postings requiring cybersecurity skills to all postings for that occupation (both those requiring cybersecurity skills and not) provides an indication of how common it is for job seekers to see these skills asked for in a posting. For workers in the Physical Security and Access, Cyber-sensitive Service, and Indirect occupation groups, cybersecurity postings make up less than 1.7 percent of total job postings with the same occupations. This highlights the challenge that many firms seeking workers with cybersecurity skills and training may be facing: cybersecurity skills are not commonly sought, and thus may not be a typical part of worker training.

Even for occupations included in the category most directly related to the industry (frontline cybersecurity workers) around 90 percent of job postings do not specifically require any specialized training or experience in cybersecurity. This implies that cybersecurity work involves significant specialization within broader occupations, highlighting the emerging nature of cybersecurity work.

	MICHIGAN			NATIONAL		
CATEGORY	CYBERSECURITY POSTINGS	TOTAL POSTINGS IN SAME OCCUPATION CATEGORY	PROPORTION	CYBERSECURITY POSTINGS	TOTAL POSTINGS IN SAME OCCUPATION CATEGORY	PROPORTION
Frontline Cybersecurity Workers	5,072	67,322	7.5%	261,230	2,422,997	10.8%
Cyber-Sensitive Service Workers	1,269	215,969	0.6%	61,057	9,235,689	0.7%
Physical Security and Access Workers	234	14,530	1.6%	8,079	579,764	1.4%
Indirect Cyber-Related Workers	166	96,534	0.2%	10,036	4,282,495	0.2%
Total Cybersecurity Workers	6,741	394,355	1.7%	340,402	16,520,945	2.1%

REGULATIONS AND CYBERSECURITY

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. Workforce guidance is also under development. These regulations and guidance have a major effect on the way companies do business and hire cybersecurity talent.

DATA PRIVACY AND SECURITY REGULATIONS

Within the last decade, several regulations have been created to protect the privacy of personal and business data. The Health Insurance Portability and Accountability Act (HIPAA) and Family Educational Rights and Privacy Act (FERPA) are two such regulations that have far-reaching effects and heavy consequences. The need for compliance because of these regulations is expected to 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.

DOD 8075.1 CYBERSPACE WORKFORCE MANAGEMENT

Cybersecurity guidelines required by the Department of Defense (DoD) are likely to have an enormous impact on the 800 Michigan manufacturers that received a DoD contract in 2016. By December 31, 2017, all DoD contractors (including small businesses) must meet minimum cybersecurity requirements or risk losing DoD business. The standards are outlined in a publication from the National Institute of Standards and Technology (NIST), titled "NIST Special Publication 800-171,"and fall into 14 areas with specific security requirements that must be implemented.

https://www.the-center.org/Events/EXPLORE-Cybersecurity-Compliance

NIST CYBERSECURITY FRAMEWORK

The 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.[15]

DRAFT NICE CYBERSECURITY WORKFORCE FRAMEWORK (NCWF): NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NIST released the draft NICE Cybersecurity Workforce Framework (NCWF) - a reference resource 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.

The NCWF can be viewed as a cybersecurity workforce dictionary that will allow employers, educators, trainers, and those in the workforce to use consistent terms to describe cybersecurity work. It can serve as a reference resource to help organizations define and share information about the cybersecurity workforce in a detailed, consistent, and descriptive way. NCWF was developed by the NIST-led National Initiative for Cybersecurity Education (NICE) with leadership from the U.S. Departments of Defense and Homeland Security with collaboration between industry, government, and academia.

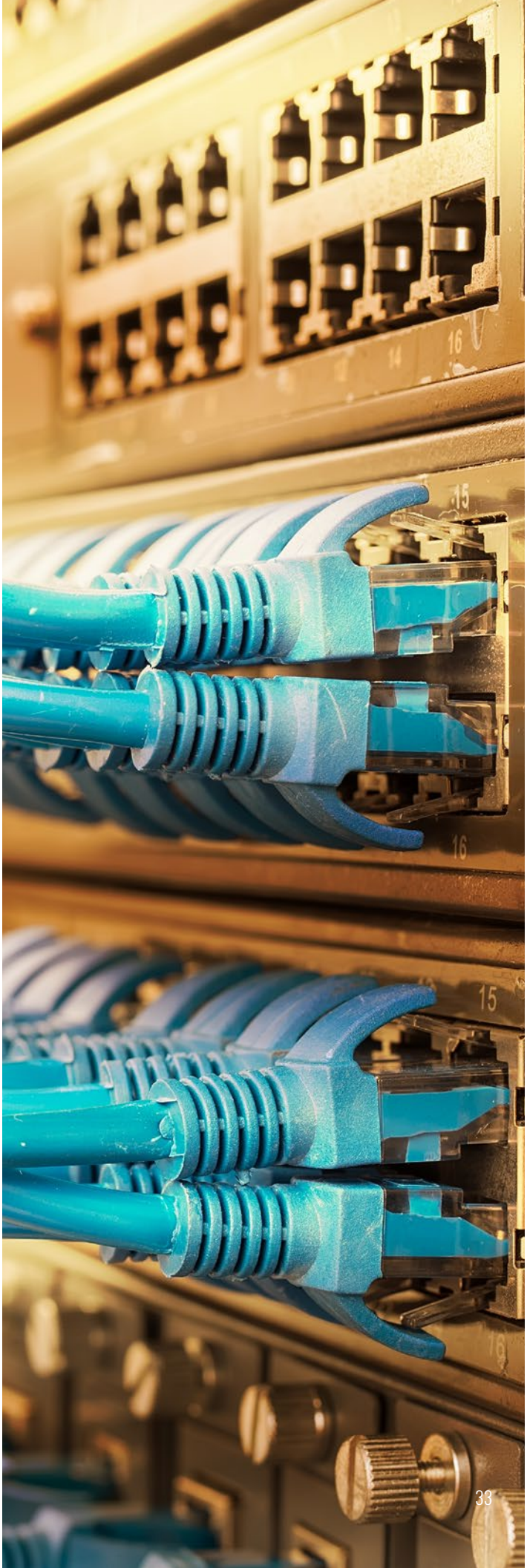
The NCWF will serve as a building block for the development of training standards, as well as for individual career planning. Federal agencies will soon be using the NCWF to identify their cybersecurity workforce as called for by the Federal Cybersecurity Workforce Assessment in the Cybersecurity Act of 2015.[16]

PRESIDENTIAL EXECUTIVE ORDER 13800 ON STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE (MAY 11, 2017)

This executive order includes policies to secure the IT and data of the executive branch, making heads of executive departments and agencies accountable for managing cybersecurity risk to their enterprises. This order also tries to support cybersecurity risk management and transparency efforts of the owners and operators of the nation's critical infrastructure, including Department of Defense warfighting capabilities and industrial base. The order ensures that the internet remains open, interoperable, reliable, and secure. The order includes a statement that "the United States seeks to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving our objectives in cyberspace." An assessment and recommendations regarding how to support the cybersecurity workforce is currently in progress.[17]

PROPOSED RULEMAKING ON ENHANCED CYBER RISK MANAGEMENT STANDARDS

In October 2016, the Board of Governors of the Federal Reserve System (Federal Reserve), the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC), collectively issued an advance notice of proposed rules regarding cybersecurity of the U.S. financial system. The notice proposes 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.



[15] https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-basics

[16] http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-181

[17] https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

CYBERSECURITY FRAMEWORK MANUFACTURING PROFILE

A draft manufacturing implementation of the Cybersecurity Framework, or Profile, has been developed for reducing cybersecurity risk for manufacturers that is aligned with manufacturing sector goals and industry best practices. It focuses on desired cybersecurity outcomes and can be used to identify opportunities for improving the current cybersecurity posture of a manufacturing system. This Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity activities and reducing cyber risk to manufacturing systems. The Manufacturing Profile is meant to enhance, but not to replace, current cybersecurity standards and industry guidelines that the manufacturer is embracing[18].

CYBERSECURITY ACT OF 2015

The Cybersecurity Act of 2015 created a voluntary cybersecurity information sharing process and modified federal network information security procedures.[19] It provides methods for the sharing of information on cybersecurity threats and defensive measures among[20] private sector entities and between private sector and the government.

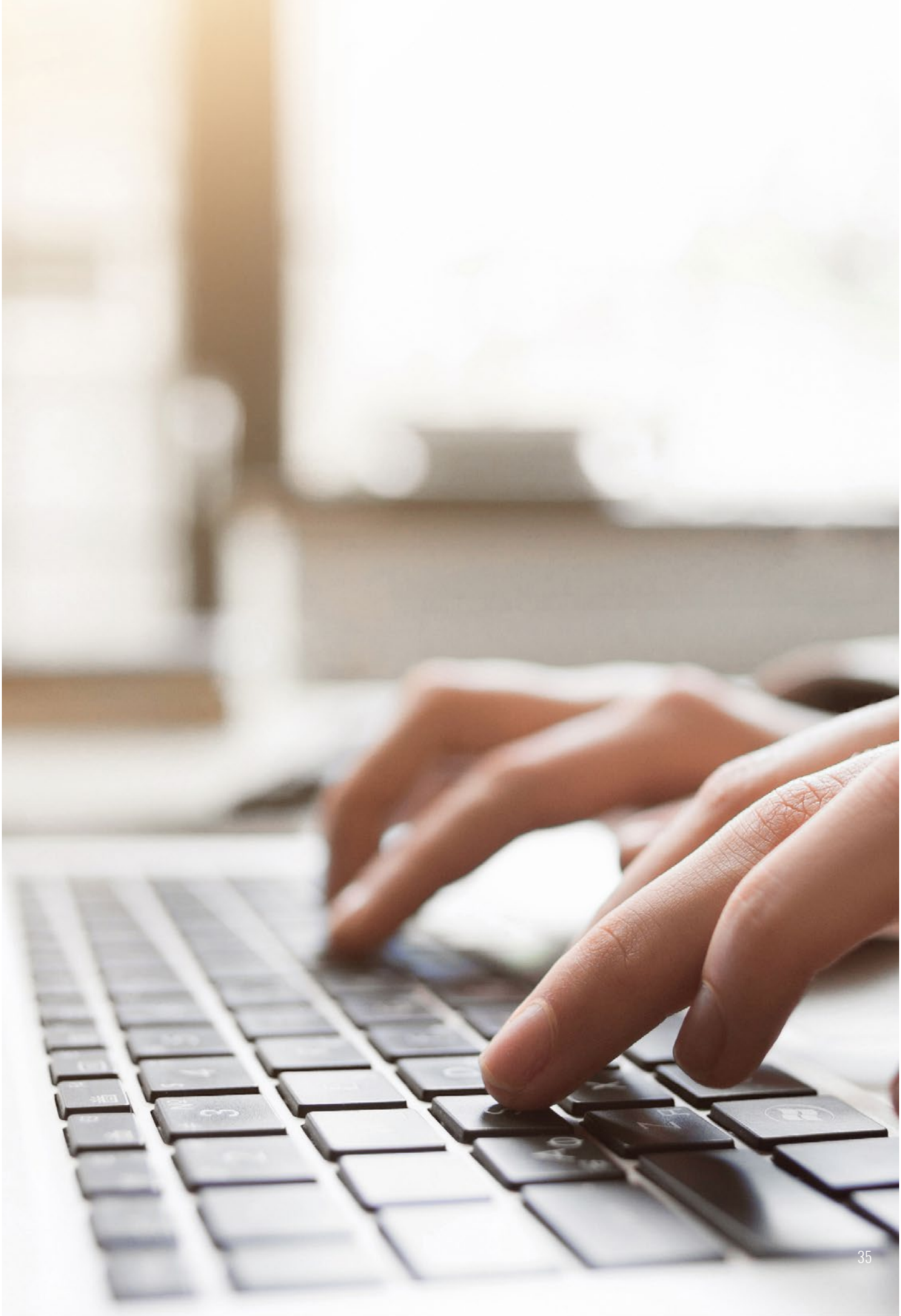
ADDITIONAL FACTORS:

1. Ultimately, cybersecurity occupational demand is likely to ebb and flow in a similar nature to other emergency or danger related professions. When activities occur either within a business or within the public eye that could have been prevented or responded to more effectively by implementing cybersecurity efforts, dollars may be allocated to these occupations quickly, resulting in a higher demand for individuals within these professions. The importance of cybersecurity will become more commonplace, as our world becomes more connected to the devices we use on a regular basis, from automobiles and appliances to computers and telephones, and the need for protecting these connections will increase.
2. In conversations held throughout this research, cybersecurity professionals suggested that a strength of the Southeast Michigan region is development of embedded systems technology, but not necessarily a location to develop software. This may also affect the role of cybersecurity professionals in the Advance Michigan region, with many of them focusing on how to prevent and protect technologies that are being incorporated into other technologies such as connected and automated vehicles and defense technologies, rather than working on cybersecurity when an app or software product is in initial development.
3. Recent education and training initiatives could change the opportunities of cyber-focused students and allow for the growth of cyber professionals within the region. Under the Southeast Michigan region Department of Defense Office of Economic Adjustment Defense Industry Adjustment grant, Merit Network has collaborated with the Advance Michigan Defense Collaborative and the Michigan Economic Defense Corporation to place two new cyber range hubs in the southeast Michigan Region. The Pinckney Community Schools Cyber Training Institute and Sentinel Center and the Wayne State University Advanced Technical Education Center are currently open and providing cybersecurity related education and training opportunities while also providing a place for businesses to test and harden their software. This is in addition to the currently existing Velocity Cyber Range Hub in Sterling Heights.
4. The recruiting of cybersecurity talent is complicated by the lack of standards across the industry. SOC codes for cybersecurity-specific jobs have not been issued and, thus, are often intertwined with IT jobs. Additionally, there is often not a clear translation of job titles and responsibilities within human resource departments, who may be largely responsible for issuing job postings and assisting with the search for talent. Job titles and responsibilities vary across industries and organizations, complicating the search for talent and making it difficult for students to clearly understand their career options in cybersecurity. Finally, potential employees are often overlooked by automated systems because they may not use the correct keywords within their resumes or job applications or they have the cyber skills required but do not possess a four-year degree.

[18] http://csrc.nist.gov/cyberframework/documents/csf-manufacturing-profile-draft2.pdf

[19] https://www.congress.gov/bill/114th-congress/house-bill/2029

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



CLOSING THE GAP

Southeast Michigan Education Cybersecurity Programs

Cybersecurity is an emerging field with a high demand for workers. To fill this demand; southeast Michigan educational institutions are now delivering programs and curriculum specifically designed to train an individual to fill these positions. A total of 39 institutions or organizations provide some form of cybersecurity training, degree, or certificate, with 90 degree programs and 80 certificate programs available in the Southeast Michigan region. The table below identifies both K-12 and post-secondary institutions within the Advance Michigan region that provide either frontline workers cybersecurity programs or have incorporated cybersecurity curriculum into their existing programs. Cyber curriculum is often incorporated into information technology, computer science, and engineering degrees. This data was gathered by visiting institutional websites and/or direct contact with the institution. Because this in an emerging market, there may also be programs under development that are not reflected in this data. Table 1, below, shows the institutions offering degree programs, while Table 2 displays the certificates that are available to fill cybersecurity worker demand. Please also see Appendix B for detailed degree and certificate information by institution.

Education Programs Related to Cybersecurity Frontline Occupations

		COMPUTER SCIENCE	INFORMATION TECHNOLOGY	MANAGEMENT INFORMATION SYSTEMS, GENERAL	ELECTRICAL AND ELECTRONIC ENGINEERING TECHNOLOGIES/ TECHNICIANS, OTHER	SYSTEMS ENGINEERING	COMPUTER AND INFORMATION SYSTEMS SECURITY/ INFORMATION ASSURANCE
TWO YEAR EDUCATION INSTITUTIONS	Henry Ford College				✖		✖
	Jackson Community College						
	Macomb Community College		✖				
	Monroe Community College						✖
	Mott Community College						
	Oakland Community College	✖					✖
	Schoolcraft College						✖
	St. Clair County Community College				✖		✖
	Washtenaw Community College	✖	✖				✖
	Wayne County Community College District		✖				✖

A note on Merit Network:

When looking at the tables below, Merit Network offers many of the certificate programs identified. Merit Network is a non-profit, member-owned organization governed by Michigan's public universities. Founded in 1966, Merit owns and operates America's longest-running regional research and education network.

Merit continues to leverage its experience managing NSFNET, the precursor to the modern Internet, to catapult Michigan into the forefront of networking technologies. Through Merit, organizations have access to network research, state and national collaborative initiatives and international peering. Merit partnerships include K-12, higher education, health care, libraries, government, and non-profits.

Many of the higher education institutions listed within this section are members of Merit and can access Merit's curriculum and programs.

CYBERSECURITY	COMPUTER ENGINEERING	DEGREE NAME
✖		Cybersecurity Certificate
✖		Associate in Applied Science in Cyber Security
		IT-Networking Specialist-Network Security Professional (Cybersecurity) Associate of Applied Science; IT-Networking Specialist-Network Security Professional (Cybersecurity) Certificate
✖		
	✖	Computer Security Certificate
✖		Associate in Applied Science in Cybersecurity; Certificate in Applied Science in Cybersecurity
SOON		Cyber Security/Information Assurance Technology
✖		Foundations of Computer Security Certificate; Principles of Cybersecurity Certificate
✖	✖	Associate in Applied Science in Cybersecurity; Associated in Applied Science in Computer Information Systems; CIS: Cybersecurity Certificate; CIS: Certified Ethical Hacker Certificate; CIS: Network+ certificate; CIS: Security+ Certificate

		COMPUTER SCIENCE	INFORMATION TECHNOLOGY	MANAGEMENT INFORMATION SYSTEMS, GENERAL	ELECTRICAL AND ELECTRONIC ENGINEERING TECHNOLOGIES/ TECHNICIANS, OTHER	SYSTEMS ENGINEERING	COMPUTER AND INFORMATION SYSTEMS SECURITY/ INFORMATION ASSURANCE
4 YEAR INSTITUTIONS	Lansing Community College	✕	✕		✕		
	Walsh College		✕				
	University of Michigan	✕			✕		
	Eastern Michigan University	✕		✕	✕		✕
	Michigan State University	✕	✕		✕		
	Kettering University	✕			✕		
	Wayne State University	✕	✕	✕	✕	✕	
	Concordia University	✕					
	Olivet College	✕					
	UM Flint	✕				✕	✕
	UM Dearborn	✕	✕		✕	✕	✕
	Lawrence Tech	✕	✕		✕		
	Oakland University	✕	✕	✕	✕	✕	
	Davenport University	✕					✕
	Baker College	✕	✕		✕		✕
	University of Detroit Mercy	✕					✕
K-12 INSTITUTIONS	Pinckney High School Cyber Range Hub and Sentinel Center						
	Cybersecurity & Digital Forensics Program at the Capital Area Career Center						
OTHER	Merit Network						
	Velocity Cyber Range Hub						
	Wayne State University ATEC Cyber Range Hub						

CYBERSECURITY	COMPUTER ENGINEERING	DEGREE NAME
	✖	CIT Computer Networking and Cybersecurity program
✖		Cybersecurity Certificate; Master of Science in Information Technology- Cybersecurity Concentration
	✖	
✖	✖	Bachelor of Science in Information Assurance and Cyber Defense
	✖	
✖	✖	Cybersecurity Minor
	✖	
✖	✖	Bachelor of Science in Cybersecurity and Information Assurance
	✖	
✖	✖	Master of Science in Cyber Security
✖		Cyber Defense Bachelor of Science
✖		Cyber Defense Bachelor Degree Program; Information Technology: Cyber Security
✖		Cybersecurity
✖		
✖		
✖		
✖		
✖		

Certifications Related to Cybersecurity

Two Year Education Institutions

	CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP)	SECURITY+	CISCO CERTIFIED NETWORK ASSOCIATE	CISCO CERTIFIED NETWORK PROFESSIONAL (CCNP)	PROJECT MANAGEMENT CERTIFICATION (E.G. PMP)	CERTIFIED ETHICAL HACKER	NETWORK+	CYBERSECURITY	COMPTIA A+	COMPUTER HACKING FORENSIC INVESTIGATOR (CHFI)	CERTIFIED AUTHORIZATION PROFESSIONAL (CAP)	CERTIFIED CLOUD SECURITY PROFESSIONAL (CCSP)
Henry Ford College			✖	✖				✖				✖
Jackson Community College								✖				
Lansing Community College			✖									
Macomb Community College												
Monroe Community College												
Mott Community College												
Oakland Community College		✖	✖		✖			✖				
Schoolcraft College			✖			✖	✖	✖				
St. Clair County Community College												
Washtenaw Community College	✖	✖				✖	✖		✖	✖		
Wayne County Community College District		✖	✖			✖	✖	✖			✖	

Certifications Related to Cybersecurity

Four Year Education Institutions

	CERTIFIED ETHICAL HACKER	NETWORK+	CERTIFIED INFORMATION SYSTEMS SECURITY OFFICER (CISSO)	COMPUTER HACKING FORENSIC INVESTIGATOR (CHFI)	EC-COUNCIL CERTIFIED SECURITY ANALYST (ECSA)	CERTIFIED DIGITAL FORENSICS EXAMINER (CDFE)
Baker College		✖				
Concordia University						
Davenport University						
Eastern Michigan University						
Kettering University						
Lawrence Tech						
Michigan State University						
Oakland University						
Olivet College						
UM Dearborn						
UM Flint						
University of Detroit Mercy	✖			✖	✖	
University of Michigan						
Walsh College						
Wayne State University	✖		✖			✖

Certifications Related to Cybersecurity

	CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP)	CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA)	SECURITY+	CERTIFIED INFORMATION SECURITY MANAGER (CISM)	CERTIFIED ETHICAL HACKER	NETWORK+	COMPTIA A+	CCNAx	CERTIFIED NETWORK FORENSICS EXAMINER (CNFE)	CERTIFIED SECURE WEB APP ENGINEER (CSWAE)	CERTIFIED INFORMATION SYSTEMS SECURITY OFFICER (CISSO)	COMPUTER HACKING FORENSIC INVESTIGATOR (CHFI)	EC-COUNCIL CERTIFIED SECURITY ANALYST (ECSA)	EC-COUNCIL CERTIFIED INCIDENT HANDLER (ECIH)	EC-COUNCIL NETWORK SECURITY ADMINISTRATOR (ENSA)	CERTIFIED AUTHORIZATION PROFESSIONAL (CAP)
K-12 Institutions																
Pinckney High School Cyber Range Hub and Sentinel Center	X				X	X	X	X	X	X	X					
Cybersecurity & Digital Forensics Program at the Capital Area Career Center																
Other																
Merit Network			X		X	X	X				X	X	X	X	X	X
Velocity Cyber Range Hub		X		X	X				X		X			X		
Wayne State University ATEC Cyber Range Hub					X						X					

		✖					CERTIFIED AUTHORIZATION FORENSICS PROFESSIONAL (CCFP)
		✖					CERTIFIED CLOUD SECURITY PROFESSIONAL (CCSP)
		✖					CERTIFIED SECURTY SOFTWARE LIFECYCLE PROFESSIONAL (CSSLP)
	✖	✖					HEALTHCARE INFORMATION SECURITY AND PRIVACY PRACTITIONER (HCISPP)
	✖			✖			CERTIFIED SECURITY SENTINEL (CSS)
	✖						CERTIFIED VULNERABILITY ASSESSOR (CVA)
	✖						CERTIFIED INFORMATION SYSTEMS RISK MANAGER (CISRM)
	✖						CERTIFIED PENETRATION TESTING ENGINEER (CPTE)
	✖						CERTIFIED DIGITAL FORENSICS EXAMINER (CDFE)
	✖						CERTIFIED DISASTER RECOVERY ENGINEER (CDRE)
	✖						CERTIFIED WIRELESS SECURITY ENGINEER (CWSE)
	✖						CERTIFIED INFORMATION SECURITY MANAGEMENT SYSTEMS LEAD AUDITOR (CISMS-LA)
	✖						CERTIFIED INFORMATION SECURITY MANAGEMENT SYSTEMS LEAD IMPLEMENTOR (CISMS-LI)
	✖						CERTIFIED SECURE WEB APPLICATION ENGINEER (CSWAE)
	✖						CERTIFIED VIRTUAL MACHINE ENGINEER (CVME)
	✖						CERTIFIED SECURITY LEADERSHIP OFFICER (CSLO)
	✖						CERTIFIED PENETRATION TESTING CONSULTANT (CPTC)
	✖						INFORMATION SYSTEMS CERTIFICATION AND ACCREDITATION PROFESSIONAL

CONCLUSIONS AND FUTURE DIRECTIONS

1. The cybersecurity workforce is not clearly defined among traditional occupation codes; rather it is emerging from within more broadly-defined occupations. As a result, most cybersecurity workers work in occupations that include a mix of cybersecurity workers and workers not focused solely on cybersecurity.

2. The cybersecurity workforce is not monolithic. This report identifies four categories of occupations among the cybersecurity workforce, each associated with distinct aspects of cybersecurity. They are:

    - Front-line cybersecurity workers,
    - Cyber-sensitive service workers,
    - Physical security and access workers
    - Indirect cyber-related workers.

3. A clear majority of cybersecurity job postings are for occupations in the frontline workers category. This includes over 76 percent of cybersecurity-related postings nationally, and 75 percent for the Advance Michigan region. Cyber-sensitive service workers are the next most prominent (17.9 percent of cybersecurity postings nationally, 18.8 percent in the Advance Michigan region).

4. Most cybersecurity job postings are only a small subset of the broader set of postings for the same occupations. Nationally, only 10.8 percent of postings for occupations included in the frontline cybersecurity workers category were flagged as cybersecurity postings by CyberSeek due to cybersecurity skill and/or education requirements. For occupations in other categories of cybersecurity workers, fewer than 2 percent of postings require cybersecurity skills or education. The industry should monitor whether employers are clearly and consistently communicating their need for cybersecurity skills to workers.

5. For cybersecurity workers in frontline cybersecurity occupations, employer demand has increased by 169 percent from 2010 to 2016, despite falling slightly from 2014-2016.

6. While demand for frontline workers has plateaued nationally in recent years, demand in the Advance Michigan region is still growing at a high rate year over year.

7. The top 15 employers with the greatest demand for cybersecurity workers include multiple defense, software, and IT consulting firms, but also includes finance, communications, and health insurance firms. Recruiting employers in southeast Michigan also include automotive, education, and media.

8. A majority (89 percent) of cybersecurity job postings require a bachelor's degree or higher. Among postings specifying a specific field of study, computer science, engineering, management information systems, information technology, and business administration were the most prominent.

9. Industry experts are advising government agencies and private businesses to fill the cybersecurity skills gap by employing workers with certifications rather than relying on traditional four-year IT degree qualified workers.

10. Among frontline cybersecurity worker job postings, the most common certifications required were Certified Information Systems Security Professional (CISSP), SANS/GIAC certification, and certified systems auditor. Many postings also required security clearance.

11. Frontline cybersecurity occupations pay nearly double the national median hourly wage ($40.09 compared to $21.60 nationally). The median hourly wage of individual occupations in this category range from $23.80 for Computer User Support Specialists, to $63.28 for Computer and Information Systems Managers.

12. Thirty-nine institutions within the Advance Michigan region provide 90 degree programs and 80 certificate programs in the high demand education areas identified in this report.

APPENDIX A: OCCUPATION CODES AND CATEGORIES

Occupation (O*NET Code)

Category 1: Frontline Cybersecurity Workers

Computer and Information Systems Managers (11-3021.00)

Security Management Specialists (13-1199.02)

Computer and Information Research Scientists (15-1111.00)

Computer Systems Analysts (15-1121.00)

Information Security Analysts (15-1122.00)

Computer Programmers (15-1131.00)

Software Developers, Applications (15-1132.00)

Software Developers, Systems Software (15-1133.00)

Web Developers (15-1134.00)

Database Administrators (15-1141.00)

Network and Computer Systems Administrators (15-1142.00)

Computer Network Architects (15-1143.00)

Telecommunications Engineering Specialists (15-1143.01)

Computer User Support Specialists (15-1151.00)

Computer Network Support Specialists (15-1152.00)

Computer Occupations, All Other (15-1199.00)

Software Quality Assurance Engineers and Testers (15-1199.01)

Computer Systems Engineers/Architects (15-1199.02)

Web Administrators (15-1199.03)

Database Architects (15-1199.06)

Data Warehousing Specialists (15-1199.07)

Information Technology Project Managers (15-1199.09)

Operations Research Analysts (15-2031.00)

Clinical Data Managers (15-2041.02)

Computer Hardware Engineers (17-2061.00)

Category 2: Cyber Sensitive Service Workers

Chief Executives (11-1011.00)

General and Operations Managers (11-1021.00)

Marketing Managers (11-2021.00)

Sales Managers (11-2022.00)

Public Relations and Fundraising Managers (11-2031.00)

Administrative Services Managers (11-3011.00)

Treasurers and Controllers (11-3031.01)

Financial Managers, Branch or Department (11-3031.02)

Industrial Production Managers (11-3051.00)

Quality Control Systems Managers (11-3051.01)

Purchasing Managers (11-3061.00)

Storage and Distribution Managers (11-3071.02)

Human Resources Managers (11-3121.00)

Training and Development Managers (11-3131.00)

Construction Managers (11-9021.00)

Education Administrators, Elementary and Secondary School (11-9032.00)

Education Administrators, Postsecondary (11-9033.00)

Architectural and Engineering Managers (11-9041.00)

Lodging Managers (11-9081.00)

Medical and Health Services Managers (11-9111.00)

Property, Real Estate, and Community Association Managers (11-9141.00)

Social and Community Service Managers (11-9151.00)

Emergency Management Directors (11-9161.00)

Managers, All Other (11-9199.00)

Compliance Managers (11-9199.02)

Supply Chain Managers (11-9199.04)

Loss Prevention Managers (11-9199.08)

Purchasing Agents, Except Wholesale, Retail, and Farm Products (13-1023.00)

Claims Examiners, Property and Casualty Insurance (13-1031.01)

Regulatory Affairs Specialists (13-1041.07)

Cost Estimators (13-1051.00)

Human Resources Specialists (13-1071.00)

Logisticians (13-1081.00)

Logistics Analysts (13-1081.02)

Management Analysts (13-1111.00)

Meeting, Convention, and Event Planners (13-1121.00)

Compensation, Benefits, and Job Analysis Specialists (13-1141.00)

Training and Development Specialists (13-1151.00)

Market Research Analysts and Marketing Specialists (13-1161.00)

Business Continuity Planners (13-1199.04)

Online Merchants (13-1199.06)

Accountants (13-2011.01)

Auditors (13-2011.02)

Assessors (13-2021.01)

Credit Analysts (13-2041.00)

Financial Analysts (13-2051.00)

Personal Financial Advisors (13-2052.00)

Insurance Underwriters (13-2053.00)

Financial Examiners (13-2061.00)

Credit Counselors (13-2071.00)

Loan Officers (13-2072.00)

Risk Management Specialists (13-2099.02)

Fraud Examiners, Investigators and Analysts (13-2099.04)

Geospatial Information Scientists and Technologists (15-1199.04)

Search Marketing Strategists (15-1199.10)

Video Game Designers (15-1199.11)

Document Management Specialists (15-1199.12)

Statisticians (15-2041.00)

Mathematical Science Occupations, All Other (15-2099.00)

Chemical Engineers (17-2041.00)

Civil Engineers (17-2051.00)

Electrical Engineers (17-2071.00)

Electronics Engineers, Except Computer (17-2072.00)

Radio Frequency Identification Device Specialists (17-2072.01)

Environmental Engineers (17-2081.00)

Industrial Engineers (17-2112.00)

Mechanical Engineers (17-2141.00)

Engineers, All Other (17-2199.00)

Validation Engineers (17-2199.02)

Civil Engineering Technicians (17-3022.00)

Electronics Engineering Technicians (17-3023.01)

Mechanical Engineering Technologists (17-3029.07)

Manufacturing Production Technicians (17-3029.09)

Quality Control Analysts (19-4099.01)

Lawyers (23-1011.00)

Medical Records and Health Information Technicians (29-2071.00)

First-Line Supervisors of Retail Sales Workers (41-1011.00)

First-Line Supervisors of Non-Retail Sales Workers (41-1012.00)

Retail Salespersons (41-2031.00)

Insurance Sales Agents (41-3021.00)

Sales Agents, Financial Services (41-3031.02)

Sales Representatives, Services, All Other (41-3099.00)

Sales Representatives, Wholesale and Manufacturing, Technical and Scientific Products (41-4011.00)

Sales Representatives, Wholesale and Manufacturing, Except Technical and Scientific Products (41-4012.00)

Real Estate Sales Agents (41-9022.00)

Sales Engineers (41-9031.00)

First-Line Supervisors of Office and Administrative Support Workers (43-1011.00)

Bill and Account Collectors (43-3011.00)

Bookkeeping, Accounting, and Auditing Clerks (43-3031.00)

Tellers (43-3071.00)

Brokerage Clerks (43-4011.00)

Customer Service Representatives (43-4051.00)

Loan Interviewers and Clerks (43-4131.00)

Human Resources Assistants, Except Payroll and Timekeeping (43-4161.00)

Category 2: Cyber Sensitive Service Workers (continued)

Receptionists and Information Clerks (43-4171.00)

Production, Planning, and Expediting Clerks (43-5061.00)

Executive Secretaries and Executive Administrative Assistants (43-6011.00)

Secretaries and Administrative Assistants, Except Legal, Medical, and Executive (43-6014.00)

Computer Operators (43-9011.00)

Data Entry Keyers (43-9021.00)

Office Clerks, General (43-9061.00)

Office and Administrative Support Workers, All Other (43-9199.00)

Category 3: Physical Security and Access Workers

Security Managers (11-9199.07)

Architects, Except Landscape and Naval (17-1011.00)

First-Line Supervisors of Protective Service Workers, All Other (33-1099.00)

Criminal Investigators and Special Agents (33-3021.03)

Private Detectives and Investigators (33-9021.00)

Security Guards (33-9032.00)

Retail Loss Prevention Specialists (33-9099.02)

Telecommunications Equipment Installers and Repairers, Except Line Installers (49-2022.00)

Security and Fire Alarm Systems Installers (49-2098.00)

Telecommunications Line Installers and Repairers (49-9052.00)

Maintenance and Repair Workers, General (49-9071.00)

Category 4: Indirect Workers

Business Intelligence Analysts (15-1199.08)

Biologists (19-1020.01)

Foresters (19-1032.00)

Medical Scientists, Except Epidemiologists (19-1042.00)

Climate Change Analysts (19-2041.01)

Remote Sensing Scientists and Technologists (19-2099.01)

Archeologists (19-3091.02)

Political Scientists (19-3094.00)

Social Scientists and Related Workers, All Other (19-3099.00)

Biological Technicians (19-4021.00)

Environmental Science and Protection Technicians, Including Health (19-4091.00)

Forensic Science Technicians (19-4092.00)

Forest and Conservation Technicians (19-4093.00)

Educational, Guidance, School, and Vocational Counselors (21-1012.00)

Social Workers, All Other (21-1029.00)

Social and Human Service Assistants (21-1093.00)

Paralegals and Legal Assistants (23-2011.00)

Legal Support Workers, All Other (23-2099.00)

Computer Science Teachers, Postsecondary (25-1021.00)

Vocational Education Teachers, Postsecondary (25-1194.00)

Postsecondary Teachers, All Other (25-1199.00)

Career/Technical Education Teachers, Middle School (25-2023.00)

Teachers and Instructors, All Other (25-3099.00)

Library Technicians (25-4031.00)

Instructional Designers and Technologists (25-9031.01)

Commercial and Industrial Designers (27-1021.00)

Graphic Designers (27-1024.00)

Designers, All Other (27-1029.00)

Public Relations Specialists (27-3031.00)

Editors (27-3041.00)

Technical Writers (27-3042.00)

Copy Writers (27-3043.04)

Interpreters and Translators (27-3091.00)

Audio and Video Equipment Technicians (27-4011.00)

Registered Nurses (29-1141.00)

Medical and Clinical Laboratory Technicians (29-2012.00)

Radiologic Technologists (29-2034.00)

Licensed Practical and Licensed Vocational Nurses (29-2061.00)

Health Technologists and Technicians, All Other (29-2099.00)

Occupational Health and Safety Specialists (29-9011.00)

Medical Assistants (31-9092.00)

Intelligence Analysts (33-3021.06)

Animal Control Workers (33-9011.00)

First-Line Supervisors of Food Preparation and Serving Workers (35-1012.00)

Combined Food Preparation and Serving Workers, Including Fast Food (35-3021.00)

Waiters and Waitresses (35-3031.00)

Janitors and Cleaners, Except Maids and Housekeeping Cleaners (37-2011.00)

Fitness Trainers and Aerobics Instructors (39-9031.00)

Graders and Sorters, Agricultural Products (45-2041.00)

Operating Engineers and Other Construction Equipment Operators (47-2073.00)

First-Line Supervisors of Mechanics, Installers, and Repairers (49-1011.00)

Avionics Technicians (49-2091.00)

Automotive Specialty Technicians (49-3023.02)

Control and Valve Installers and Repairers, Except Mechanical Door (49-9012.00)

Heating and Air Conditioning Mechanics and Installers (49-9021.01)

Installation, Maintenance, and Repair Workers, All Other (49-9099.00)

First-Line Supervisors of Production and Operating Workers (51-1011.00)

Inspectors, Testers, Sorters, Samplers, and Weighers (51-9061.00)

Production Workers, All Other (51-9199.00)

Driver/Sales Workers (53-3031.00)

Laborers and Freight, Stock, and Material Movers, Hand (53-7062.00)

Military Officer Special and Tactical Operations Leaders, All Other (55-1019.00)

APPENDIX B: SOUTHEAST MICHIGAN CYBERSECURITY EDUCATION RESOURCES

A total of 39 institutions are offering programs, degrees or training related to cybersecurity. These institutions offer more than 90 degrees and 80 certifications in the southeast Michigan region.

This information was gathered either directly from the institutions listed or from the websites of each respective institution. Any errors or omissions are unintentional.

Community Colleges

HENRY FORD COLLEGE

Computer Networking Academy: Provides students with the skills for designing, building, and maintaining computer networks. The College offers a preparation program for CCNA (Cisco Certified Network Associate) and CCNP (Cisco Certified Network Professional) industry certifications. The CCNA certificate program consists of four courses and is designed to be completed within one year. Students learn how to install and configure Cisco routers and switches in multi-protocol local and wide area networks, perform basic troubleshooting and improve network performance and security. The CCNA courses are also part of the required core courses for the Associate of Applied Science in Computer Information Systems - Network Administration and are electives for the Associate of Applied Science in Computer Information Systems - Information Assurance.

For more information, visit: **https://www.hfcc.edu/academics/programs/computer-networking-academy**

Cybersecurity Certificate: Provides a mid-level understanding of the technological needs, threats, and vulnerabilities of hardware, software, operating systems, networks, and the Internet. Students will examine operating systems, networks, tools and protocols needed to navigate, use, and manage security technologies as well as gain insight into the legal, social, and political dynamics of the cyber universe. Designed for students interested in cyber defense or IT professionals seeking a fundamental understanding of cybersecurity.

For more information, visit: **https://www.hfcc.edu/academics/programs/cis-information-assurance-cybersecurity**

JACKSON COLLEGE

Cybersecurity-Associate in Applied Science: This program provides the foundations of cybersecurity, an emphasis on the methods attackers use to infiltrate computer systems, and the means to mitigate or defeat these attacks. The courses in this program help prepare the student for a variety of industry and vendor certifications.

For more information, visit: **https://www.jccmi.edu/program/cyber-security/**

LANSING COMMUNITY COLLEGE

Computer Networking and Cybersecurity, Associate in Business Degree: Students learn to design, create, and administer efficient information technology networks of data, voice, image, and video communications. Students learn to provide the technical management and support to keep systems running 24/7, and to safeguard the data they control. This degree focuses on technical competencies as well as communication with users, management, and project planning skills. Students will be prepared to earn several industry respected certifications. Students completing this curriculum may also be eligible to apply for certificates of completion in Cisco Certified Network Associate Certification Preparation (CCNA) (1469) and in Information Technology Foundations (0766).

For more information, visit: **http://www.lcc.edu/catalog/degree_certificateprograms/current/applied/1453.pdf**

MACOMB COMMUNITY COLLEGE

Cybersecurity related programs include:

Information Technology-Networking Specialist-Network Security Professional (Cybersecurity), AAS

Information Technology-Networking Specialist-Network Security Professional (Cybersecurity), Certificate

Information Technology-Networking Specialist-Information Assurance (Cybersecurity), Skill Specific Certificate

For more information, visit: **http://www.macomb.edu/future-students/choose-program/information-technology-networking-specialist-network-security-professional/index.html**

MONROE COUNTY COMMUNITY COLLEGE

Cybersecurity and Information Assurance: The Associate of Applied Science degree in computer Information systems with a program designation of cybersecurity and information assurance is designed to provide an opportunity for students to acquire the foundational skills needed for an entry-level position supporting corporate security operations. The term "information assurance" encompasses the scientific, technical and management disciplines required to ensure computer and network security. For more information, visit: **http://www.monroeccc.edu/business/busdiv.htm**

MOTT COMMUNITY COLLEGE

Cybersecurity related programs include:

- Certificate Programs
  - Computer Repair Technology
  - Computer Networking Technology
  - Computer Security Certificate
  - Computer Support Services & Help Desk Certificate
- Associate Degree Programs
  - Computer Network Engineering
  - Computer Occupations Technology - umbrella degree
- Specialization areas in:
  - Computer Security
  - Applications Developer
  - Applications Specialist
  - Network Technician
  - Web Developer

For more information, visit: **http://www.mcc.edu/technology/index.shtml**

OAKLAND COMMUNITY COLLEGE

Associate in Applied Science in Cybersecurity: The requirements for the Cybersecurity program are based upon guidelines set forth in the National Security Agency and the Department of Homeland Security National Centers of Academic Excellence in Information Assurance and Cyber Defense programs.

Certificate in Applied Science in Cybersecurity: Provides skills in information system security, using the current technologies and tools available in the industry. The certificate also gives students a solid foundation in computer-based systems concepts.

For more information, visit: **https://www.oaklandcc.edu/programs/cis/cybersec.aspx**

SCHOOLCRAFT COLLEGE

Schoolcraft College offers three associate of applied science degrees and six certificates. The educational options include:

- *Introductory Certificate:* This certificate program introduces students to the operating system, concepts of programming logic, programming language and software applications. During or after the first year of this certificate program, students may choose to earn one of the computer information system associate degrees, provided all degree requirements are fulfilled.

- *Cisco Networking Academy Skills Certificate:* This certificate program is designed to provide students with an understanding of network fundamentals, proficiency working with network equipment such as routers and switches, and the latest LAN and WAN technologies in preparation to achieve the Cisco Certified Network Associate (CCNA) certification.

- *Networking Technology Integration Certificate:* The certificate curriculum provides students with an in-depth understanding of the theory, hardware and software of computer networking and is applicable for both those who are new to the field or have networking experience.

- *Computer Support Technician Associate of Applied Science Degree:* This degree program prepares students for entry-level positions supporting users of microcomputer components of the operating system. Technicians assist users by recommending hardware and software, interpreting manuals, organizing storage, networking workstations and creating systems solutions using the microcomputer.

- *Programming Skills Certificate:* This certificate program is designed to introduce students to the top computer programming languages used in software development and web applications. Students will also learn how to use the Microsoft.NET framework, which is the common environment for building, deploying and running web services and applications in Windows. In addition, the new Visual Studio.NET will be used, a common development environment for the new .NET framework.

- *Programming Associate of Applied Science Degree:* This degree offers students a schedule of core computer courses and electives to prepare them for a position as an entry- level programmer. Students will learn how a computer programmer analyzes problems and writes step-by-step instructions to enable a computer system to process data efficiently.

- *Web Specialist Certificate:* This certificate program provides an overview of technical programming and graphic design for web page development. Areas of study include programming logic, design concepts and technology and web design and development. Students will also learn about the latest in web technology and design programs, such as Adobe Flash, Illustrator and Photoshop and JavaScript.

- *Web Specialist AAS Degree:* This degree program prepares students to be able to design web pages and program for the web. It provides working knowledge in various programming languages, multimedia technologies, graphic development, and web design tools.

- *Post-Associate Certificate:* For working professionals who have earned an associate degree in applied science and have experience and/ or training in the computer field, it provides insight into computer technology and will enhance their ability to meet the needs of the computer information systems environment.

For more information, visit:
http://www.schoolcraft.edu/academics

ST. CLAIR COUNTY COMMUNITY COLLEGE

Computer Information Systems-Network Associate in Applied Arts and Science Degree: Courses in this program cover topics such as cabling, network device configuration, network operating systems, local and wide area networks, analysis and troubleshooting tools, security, and network design. Students who complete this program will have the necessary training to sit for applicable industry certification exams, including CompTIA's Network+, Security+, Linux+ and Project+, as well as Cisco's CCENT and CCNA certification exams.

For more information, visit: **http://www.sc4.edu/cis-programming/**

Computer Information Systems Industry Certification Equivalency List: College credit may be given for earned industry certifications (see list below). Student must provide proof of completion to receive credit. Testing and/or a personal meeting may be required. For questions, call the Business and Information Technologies division at (810) 989-5628. If other certifications have been earned, contact the Business and Information Technology division for articulation review.

WASHTENAW COMMUNITY COLLEGE

Cybersecurity related programs include:

- **Information Technology**
  - Certificates:
    - Applied Data Science
    - C# Programming for Modern Computing Environments
    - Computer Systems Technology
    - Foundations of Computer Security
    - Foundations of Information Systems
    - Linux/Unix systems
    - Principles of Cybersecurity
  - Advanced Certificate
    - C++ Programming
    - Computer Networking Academy I
    - Computer Networking Operating Systems I
    - Mobile Device Programming
    - Network Security
    - Program in Java

    - Web Database Programming
    - Web Database Programming Professional
  - Associate in Science
    - Computer Science: Programming in Java
    - Information Systems: Programming in C++
  - Associate in Applied Science
    - Computer Systems and Networking
- **Workforce Development Non-Credit Training**
  - Big Data and Business Analytics:
    - VMware® vSphere: Install, Configure, Manage v5.5
    - VMware® vSphere: Install, Configure, Manage v6.0
- **Information Protection and Cybersecurity:**
  - Certified Ethical Hacker Certification
  - Certified Information Systems Security Professional
  - Cloud Computing Security Knowledge Certification
  - CompTIA Security+ Certification
  - Computer Hacking Forensic Investigator Certification
- **Platform Management Certifications**
  - CompTIA Cloud Essentials Certification
  - CompTIA Mobility+ Certification
- **Project Management / Process Improvement**
  - Lean Six Sigma Green Belt Boot Camp
  - Lean Six Sigma Black Belt Boot Camp
  - PMI Agile Certified Professional (PMI-ACP)® Exam Preparation
- **Software Programming and Networking:**
  - 20486 Developing ASP.NET MVC 4 Web Applications
  - Advanced Python 3
  - Cisco® Interconnecting Cisco® Networking Devices Accelerated v3.0 (CCNAX)
  - CompTIA A+ Certification
  - CompTIA Network+ Certification
  - Introduction to Python 3
  - Microsoft 20480 Programming in HTML5 with JavaScript and CSS3

Washtenaw Community College also recently announced a partnership with Eastern Michigan University. EMU entered a new articulation agreement with Washtenaw Community College (WCC) that will allow students participating in WCC's new cyber security program to transfer seamlessly to Eastern after two years to receive a bachelor's degree in the field.

For more information, visit:
http://www.wccnet.edu/academics/programs/

WAYNE COUNTY COMMUNITY COLLEGE DISTRICT

Computer Information Systems-Cybersecurity: The Cybersecurity program offers a 2-year Associates in Applied Science Degree, a 1-year Certificate as well as Short-Term certificates. This program is based on the National Initiative for Cybersecurity Education (NICE) framework and provides students with a solid foundation in the fundamentals of secure information technology system design, construction, and maintenance of Cyber infrastructure and systems defense. Students will utilize virtual environments, including Cybersecurity video games/simulations to demonstrate mastery of competencies, knowledge, and skills, while preparing for industry recognized Cybersecurity certifications. For more information, call 313-496-2600 or visit **www.wcccd.edu**

- Information Technology Certificates:
  - Business Analytics Certification
  - Application Developer Certification
  - Computer Support Specialist Certification
  - Database Administrator Certification
  - Network Administrator Certification
  - Office Specialist Certification
  - Video Game Design and Animation Certification
  - Website Developer Certification
- Cybersecurity Certificates:
  - CompTIA Network+ Certification
  - CompTIA Security+ Certification
  - Certified Ethical Hacker Certification
  - Cisco Certified Network Associate
  - Certified Authorization Professional

Four-Year Universities

EASTERN MICHIGAN UNIVERSITY

Information Assurance Program: The Eastern Michigan University Information Assurance Program is a Center of Academic Excellence in Information Assurance, sponsored by the National Security Agency. Their course work is mapped at Committee on National Security Systems at the 4011 and 4012 Standards. The program is a partner in the National Initiative for Cybersecurity Education (NICE) focused on cybersecurity awareness, education, training, and professional development. The EMU IA Program is committed to awareness and competence across the nation to develop an agile, highly skilled workforce capable of responding to a dynamic and rapidly developing array of cyber threats. Our course work at the bachelors and graduate levels meets the NICE Cybersecurity Workforce Framework and puts forth a working taxonomy and common lexicon that can be overlaid onto any organization's existing occupational structure. Our course framework addresses emerging work requirements to help meet and exceed the national need for cybersecurity professionals. Students have four study areas to choose from, all leading to career opportunities with the federal government or private industry. Each concentration has a shared foundation area of study.

Information Assurance Management Bachelor's Degree: Information assurance management will enable the student to focus on management of information systems. The practice of vulnerability, risk, countermeasures, and ethics enable the IA manager to meet cybersecurity in the 21st century. This concentration of study will enable that management oriented student to apply secure computing concepts in the protection of cyberspace.

Applied Information Assurance Bachelor's Degree: Applied information assurance management prepares the student with hands-on applications for analysis, prevention, deterrence and countermeasures of information security and integrity in the global arena. Students who select this concentration of study will find that hands-on application will enable them to embrace the concepts studied in lecture format and apply those concepts in a laboratory setting.

Information Assurance Encryption Bachelor's Degree: Information assurance encryption will prepare the students for master's or doctoral work. The sustained and rapid advance of information technology in the 21st century dictates the adoption of a flexible and adaptable cryptographic strategy for protecting national security information. This strategy complements the existing policy for the use of the advanced encryption standard (AES) to protect national security systems and information as specified in The National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information (CNSSP-15)

Network Security/Administration Bachelor's Degree: The Network Security and Administration concentration prepares the student with hands-on applications for administration, design, and implementation of secure computer networks. Students will learn to administer network environments to be scalable, secure, and available. Student work will center on best practice administration across Microsoft, Open Source and CISCO products. Students will implement these products and build countermeasures for defending services that underpin the product solution. Students who select this concentration of study will find that hands-on application of classes will enable them to embrace the concepts studied in lecture format and apply those concepts in a laboratory setting.

Masters of Arts in Technology Studies provides for a concentration in three areas related to Information Assurance:

- Information Assurance Management
- Network Security
- Digital Investigations

Eastern Michigan University is a member of the International Cybersecurity Education Coalition (IC-SEC) www.ICSEC.org. The purpose of the International Cybersecurity Education Coalition is to provide unified leadership for information assurance education and research initiatives in both the public and private sector. It will conduct research, provide scholarships for education and training programs, and provide services to promote excellence in Information Assurance (Security) education. Member community colleges form the basis for our vertical articulation for students to follow from high school through the community college system to terminal degree at EMU. Current articulation agreements are presented:

- Henry Ford Community College
- Oakland Community College
- Washtenaw Community College
- Lansing Community College
- Owens Community College (Pending)
- Bay Community College (Pending)
- Sinclair Community College (Pending)
- Delta Community College
- Macomb Community College
- Monroe Community College

For more information, visit: **https://www.emich.edu/cot/isac/programs/ia/**

MICHIGAN STATE UNIVERSITY

Michigan State University Cybersecurity Lab: The mission of the Cybersecurity Lab at Michigan State University is to design cryptographic algorithms and network security protocols for the next generation internet, ad-hoc and sensor networks where power efficiency and security are of major concerns. The Cybersecurity Lab also works on secure digital copyright protection and management.

For more information, visit: **http://www.egr.msu.edu/cybersec/**

Cybersecurity related programs include:

- *Computer Science Doctoral Program*
- *Undergraduate Computer Science*
- *Undergraduate Computer Engineering*
- *Minor in Computer Science*
- *Graduate Programs in Computer Science and Engineering*

For more information, visit: **http://www.cse.msu.edu/**

MSU Annual Interdisciplinary Conference on Cybercrime: This event brings researchers from the social and technical disciplines together along with practitioners from across the globe to discuss how to improve knowledge and policy responses to cybercrime.

For more information, visit: **http://cj.msu.edu/programs/interdisciplinary-conference-cybercrime/**

OAKLAND UNIVERSITY

Master of Science Cybersecurity: The Master of Science in Cybersecurity (MSC) degree program is designed to provide a strong foundation and detailed technical knowledge in information security, computer security, network security, and software security, as well as an appreciation of the social, policy, ethical, and legal aspects of security and privacy. The MSC program offers two tracks: a research track and a professional track. The program is run in collaboration with Oakland's School of Business Administration.

For more information, visit: **https://oakland.edu/secs/masters-of-science-programs/cyber-security/**

Bachelor of Science-Computer Science: The program in Computer Science (CS) prepares students for professional practice in systems programming, software design and computer applications, or for graduate study in computer science. The program provides a solid foundation based on the organization, processing and display of information. The major in Computer Science is accredited by the ABET Computing Accreditation Commission (CAC). The BSE in Computer Science program is accredited by the Computing Accreditation Commission of ABET.

For more information, visit: **https://oakland.edu/secs/undergraduate-programs/computer-sciences/**

Computer Science Advanced Summer Camp: This camp is for middle and high school students who have already attended a computer science camp, or are themselves advanced computer programmers. Topics will be more challenging and continue into deeper programming concepts. Higher-level programming languages will be covered and there will be programming challenges throughout the camp. IT security and hacking will be covered in this camp as well.

For more information, visit: **https://oakland.edu/secs/outreach-programs/**

UNIVERSITY OF MICHIGAN-DEARBORN

Cybersecurity Center for Education, Research, and Outreach: The Cybersecurity Center for Education, Research, and Outreach (CCERO) was established to integrate university-wide existing activities and initiatives in cybersecurity research, education, and outreach. It is dedicated to facilitating collaboration in research among faculty members, providing degree and certificate programs, advising student groups, and organizing events in cybersecurity and information assurance. CCERO is helping to address the national concern for producing more cybersecurity professionals and advancing the knowledge and practice of cybersecurity. The Cybersecurity Center works closely with the college's Extended Learning and Outreach department to develop programs that prepare K-12 students for a career in cybersecurity or other STEM fields. The Center also provides a variety of training programs and services that bridge the talent gap for corporate customers to meet the rising demand for cybersecurity professionals.

https://umdearborn.edu/cecs/research/centers/cybersecurity-center-education-research-and-outreach

Undergraduate Certificate in Practical Aspects of Computer Security (PACS): The PACS undergraduate certificate will provide students with computer science concepts, basic security principles, and the tools and experience necessary for an entry-level position in IT-Security. This certificate provides a foundational knowledge in computer security principles, firewalls, malware, intrusion detection, physical security, wireless network security, mobile device security, social network security, and web application security.

MS in Computer and Information Science: The Computer and Information Science master's degree program, in conjunction with the Rackham School of Graduate Studies, is designed to prepare students for professional practice, as well as further studies and research in the computing field. The program offers a 30-credit hour curriculum consisting of required core courses and technical electives. The department will schedule all CIS courses during late afternoons or evenings to enable students to earn their master's degree through part-time study. The program may be completed entirely on campus, entirely online, or through a combination of on-campus and online courses.

Ph.D. in Computer and Information Science: The CIS Ph.D. program is a research-oriented degree designed to address the growing needs of industries and organizations for engineering professionals with advanced knowledge, technical skills, and the ability to conduct high quality applied research in computer and information science. The program offers concentrations

in data management, data science, systems and security, and software engineering. All students admitted for full-time study will receive a competitive financial aid package in the form of an appointment as a graduate student instructor (GSI) or research assistant (GSRA).

Beginning Fall 2017, the Computer and Information Science Department at U of M Dearborn will offer a BS in Cybersecurity and Information Assurance with two concentrations: (1) Cybersecurity and Privacy or (2) Digital Forensics.

For more information, visit: **https://umdearborn.edu/cecs/departments/computer-and-information-science/undergraduate-programs/bs-cybersecurity-and-information-assurance**

UNIVERSITY OF MICHIGAN-FLINT

Computer Science and Information Systems Master's Degree: The MS in Computer Science and Information Systems program offers concentrations in Computer Science or Information Systems, as well as a preparatory Fast Track for those without a computer science background.

https://www.umflint.edu/graduateprograms/computer-science-information-systems-ms

UNIVERSITY OF MICHIGAN

Center for Computer Security and Society: The Center for Computer Security and Society (C2S2) is an interdisciplinary center based at the University of Michigan. The center is dedicated to the investigation of emerging threats to critical embedded systems and networks, and on the impact of cybersecurity attacks on critical infrastructure, governments, and sensitive data.

For more information, visit: **http://security.engin.umich.edu/**

Cyber-related degree programs include:

- *Computer Science and Engineering Graduate Program*
- *Electrical and Computer Engineering Graduate Program*
- *Computer Engineering Undergraduate program*
- *Computer Science Undergraduate Program-College of Engineering or LSA*
- *Data Science Undergraduate Program*
- *Electrical Engineering Undergraduate Program*

For more information, visit: **https://www.cse.umich.edu/**

Security and Privacy Research group:

The Security and Privacy Research Group at the University of Michigan consists of over a dozen energetic people working broadly on research problems pertaining to trustworthy computing. They explore the research frontiers of computer science, electrical and computer engineering, and healthcare. Their latest project examines the susceptibility of analog sensors to electromagnetic interference signal injection attacks.

Group Related initiatives include:

- Center for Future Architectures Research (C-FAR)
- RFID Consortium for Security and Privacy (RFID-CUSP)
- Medical Device Security Center
- Strategic Healthcare IT Advanced Research Projects on Security (SHARPS)

For more information, visit: **https://spqr.eecs.umich.edu/**

RobustNet Research Group:

The RobustNet research group at University of Michigan is actively involved in various hot topics in networking research area. Their recent emphases are mainly related to internet routing, measurement and security, wide-area and enterprise network management, malware behavior analysis and host-based security in general.

http://vhosts.eecs.umich.edu/robustnet//

UMTRI-Transportation Research Institute:

UMTRI is heavily working in cybersecurity and privacy with a focus on commercially feasible cybersecurity. The UMTRI cybersecurity team is interested in all areas around cybersecurity and privacy and has worked in the following areas:

- Risk assessment
- In-vehicle platform security design
- Security strategies
- Transportation cybersecurity test lab
- Connected vehicle / V2X cybersecurity and privacy
- Intrusion detection and prevention systems (IPS)
- Secure controller area network (CAN)
- Protection of component integrity
- Transportation privacy

WAYNE STATE UNIVERSITY

WSU Advanced Technology Education Center (ATEC) Cyber Range Hub: Cybersecurity courses in the Department of Computer Science are offered in full semester and accelerated formats. Classes are held on the main campus in Detroit and in the Cyber Range Hub at ATEC Warren. Courses for academic credit apply to a bachelor's in computer science and include industry certifications. Courses offered through Executive and Professional Development rotate throughout the year and can be delivered in custom formats based on the needs of an organization. Clients can test applications and systems in a totally secure environment called a "secure sandbox," which simulates a networked environment. Classes are offered at the Cyber Range Hub or at client locations/offices. Industry certifications are available through EPD.

For more information, visit: **https://wayne.edu/educationaloutreach/cyber-range/**

Cyber-related programs also include:

- *Computer Science Bachelor of Science*
- *Computer Science Bachelor of Arts*
- *Bachelor of Arts in Information Systems Technology*
- *Minor in Computer Science*

Private Institutions

BAKER COLLEGE

Computer and Cybersecurity Program: Baker's Information Technology program with the Cybersecurity major prepares students for a career in designing, managing, and securing private networks using firewall technologies with practical job skills in information security and security management. Through a combination of classroom study, labs, and an internship experience, students receive hands-on training in the technical components of security—including hardware and software firewalls, virtual private networks, and security testing tools. As a program graduate, students will be ready to sit for the Comp TIA Network+ and Core Security's Core Impact Certified Professional certification exams.

For more information, visit: **https://www.baker.edu/programs-degrees/computer-technologies/information-technology-cyber-security/**

Cyber Defense Bachelor of Science: The Cyber Defense Bachelor Degree program at Baker develops knowledge and skills in information technology and security. The program includes a concentration in cyber defense. The curriculum is designed to develop a foundation in platform hardware, software, networking, and operating systems. Students gain skills in analyzing and responding to computer infrastructure problems, and learn how to identify and defend against internal and external threats.

For more information, visit: **https://www.baker.edu/programs-degrees/computer-technologies/cyber-defense/**

Information Technology and Security Bachelor of Science: In Baker's Information Technology and Security program, students develop the broad base of skills and knowledge needed to manage information technology teams and handle the technical aspects of the network infrastructure and security.

For more information, visit: **https://www.baker.edu/programs-degrees/computer-technologies/information-technology-and-security/**

Baker College has also indicated that an online Cybersecurity Master's Degree will be available soon. For more information, visit: **http://www.mlive.com/news/muskegon/index.ssf/2017/05/cybersecurity_masters_degree_p.html**

CONCORDIA UNIVERSITY

Computer Science Program: CUAA's Computer Science program is designed for students who want to create software and design computer systems. This degree provides a foundation in computer science and prepares students to pursue computer game design, "big data" analysis, and information assurance.

For more information, visit: **https://www.cuaa.edu/programs/computerscience/index.html**

Master of Science in Computer Science: The MS in computer science will prepare the student to be a software developer, a manager of information technology (IT) systems, a leader of a technical team, or a student in a Ph.D. program in computer science or in a related field. Building on the student's undergraduate background in the field (including relevant coursework in mathematics and the equivalent of at least a minor in computer science), the program is designed to deepen the student's skills and knowledge in the principal areas of computer science. Problem solving, collaboration, creative design processes, close contact with professional literature, writing, presentation, and ethical practices grounded in Christian teaching are all incorporated throughout the program.

For more information, visit: **https://www.cuaa.edu/programs/mscs/index.html**

DAVENPORT UNIVERSITY

Cyber Defense, Bachelor of Science: In this program the hands-on tools and techniques, supported by the trends and case studies, will cover topics to present what cybersecurity is and how to best protect an organization's information assets. Students will learn the performance-based skills and develop the knowledge set to ensure appropriate treatment of risk, compliance, and assurance from internal and external perspectives. The Bachelor of Science in Cyber Defense can be completed in-seat or online. Davenport University is a DHS/NSA nationally recognized Center of Academic Excellence in Information Assurance Education. Specialty areas include: Health Care Information and Assurance, Information Assurance, and Mathematical modeling.

For more information, visit: **https://www.davenport.edu/programs/technology/bachelors-degree/cyber-defense-bs**

Other Cybersecurity-related Bachelor's Degrees offered by Davenport include:

- *Computer Science*
- *Computer Information Systems*
- *Digital Forensics*
- *Technology Project Management*
- *Network Management and Security*
- *Database Systems and Programming*

KETTERING UNIVERSITY

Cybersecurity Minor:

For more information, visit: **http://catalog.kettering.edu/undergrad/academic-programs/minors/system-data-security/**

LAWRENCE TECHNOLOGICAL UNIVERSITY

Cybersecurity related programs include:

Bachelor of Science in Computer Science or minor: The program offers the flexibility to accommodate students from a variety of backgrounds – recent high school graduates can gain the specialized knowledge necessary to work in such areas as software engineering, scientific computing, business applications and cloud computing, and game development by working with leading internationally recognized professors.

For more information, visit: **https://www.ltu.edu/arts_sciences/mathematics_computer_science/bachelor-of-computer-science.asp**

Bachelor of Science in Information Technology:

For more information, visit: **https://www.ltu.edu/management/bachelor-of-information-technology.asp**

OLIVET COLLEGE

Olivet College offers a *Computer Science bachelor's degree or minor*.

For more information, visit: **https://www.olivetcollege.edu/undergraduate/academics/list-of-majors/mathematics-computer-science/computer-science-major/**

UNIVERSITY OF DETROIT MERCY

Center for Cybersecurity & Intelligence Studies: The Center for Cybersecurity & Intelligence Studies (Center) provides the education, experience, and resources to cultivate leaders in today's digitally dependent world. University of Detroit Mercy has been a National Security Agency/U.S. Department of Homeland Security National Center of Academic Excellence for the past decade. The Center combines University of Detroit Mercy's software management, criminal justice, and computer expertise with its liberal arts foundations.

For more information, visit: **https://liberalarts.udmercy.edu/academics/cis/center-for-cyber-intel-studies.php**

University of Detroit Mercy offers the following cybersecurity-related degree programs:

- Undergraduate Degrees
  - Bachelor of Science in Computer and Information Systems with a major in Cybersecurity
  - Bachelor of Science with a major in Criminal Justice
- Graduate Degrees
  - Master of Science in Computer & Information Systems with a major in software management
  - Master of Science in Information Assurance with a major in Cybersecurity
  - Master of Arts with a major in Criminal Justice
  - Master of Science in Intelligence Analysis
  - Master of Science with a major in Security Administration
- 5-year Accelerated Degrees (Bachelor's to Master's)
  - Bachelor of Science in Computer & Information Systems (cybersecurity major); Master of Science in Information Assurance (cybersecurity major)
  - Bachelor of Science in Computer & Information Systems (cybersecurity major); Master of Science in Intelligence Analysis
  - Bachelor of Science (criminal justice major); Master of Science in Intelligence Analysis

For more information, visit: **http://liberalarts.udmercy.edu/academics/cis/**

Cybersecurity Lab: The Center's lab equipment includes digital forensics workstations, portable data acquisition devices, threat analysis software, wireless antennae, advanced encryption software, and malware debugging software. Students engage in hands-on activities using specialized tools and technology, including exposure to simulated environments using virtual machine technologies.

WALSH COLLEGE

Master of Science in Information Technology-Cybersecurity Concentration: The Walsh College Master of Science in Information Technology (MSIT-CS) with a concentration in Cybersecurity degree is focused on preparing IT professionals to optimize information technology management to support of business strategies and goals.

http://www.walshcollege.edu/masters-ms-degree-information-technology-cybersecurity

Cyber Spring Program Series:

Walsh College offers a series of information technology- and cybersecurity-focused seminars, webinars, courses, and events at its Troy campus, at area venues, and online. "Cyber Spring" has been designed in response to the immediate and growing industry need for advanced and continuing education for students and industry practitioners in these key fields. Walsh College is designated as a Center of Academic Excellence in Cyber Defense (CAE/CD) through 2020. In addition to ensuring that its programs meet the CAE requirements, Walsh programs align with two other external standards: Department of Defense 8570 (a directive that military personnel need to follow to obtain Cybersecurity access to various military systems) and the Department of Homeland Security NICE Framework.

For more information, visit:
http://www.walshcollege.edu/cyberspring

Additional cybersecurity related programs include:

- *Cybersecurity Certificate*
- *Bachelor of Science in Information Technology*

K-12

INGHAM COUNTY INTERMEDIATE SCHOOL DISTRICT CAPITAL AREA CAREER CENTER

Cybersecurity and Digital Forensics: Areas of study for this program will include; basic computer security, social engineering, essential security awareness, implementing countermeasures, and methods of deception.

For more information, visit: **http://www.inghamisd.org/cacc/futurestudents/programsbypathways/businessmanagementmarketingandtechnology/cybersecurity-and-digital-forensics/**

MCISSE CYBERPATRIOT PROGRAM

CyberPatriot is the premier national youth cyber education program created to inspire high school and middle school students toward careers in cybersecurity or other science, technology, engineering, and mathematics (STEM) disciplines critical to our nation's future. The program was created by the Air Force Association. The Northrop Grumman Foundation is the presenting sponsor.

For more information, visit: **http://www.mcisse.info/cyberpatriot.html**

MICE INITIATIVE

MICE is a proposed career and technical education cybersecurity program with the main goal of creating a train the trainer professional development workshops, a central repository of cyber education curriculum, and offering learning management system courses at the K-12 career and technical education level.

PINCKNEY HIGH SCHOOL CYBER TRAINING INSTITUTE AND SENTINEL CENTER

The Pinckney Cyber Training Institute offers hands-on cyber courses, cyber exercises and product testing using the Michigan Cyber Range. Many of the training courses, workshops, and exercises available through Merit Network are available through this center.

For more information, visit: **http://pinckneycti.org/**

Additional Resources

CAPITAL AREA IT COUNCIL (CAITC)

The CAITC provides members with access to training programs and emerging talent pools that complement the professional development and work experience employers provide to a new IT professional—at no additional cost. These training programs are specifically developed to meet the demand of local IT employers by using CAITC local educational resources and partners.

For more information, visit: **https://www.capitalareaitcouncil.net/**

DETROIT REGIONAL TECH CONSORTIUM

A Detroit Regional Tech Consortium started in the City of Detroit Mayor's Office of Workforce Development will develop and retain talent, promote Detroit as a tech hub, and create a talent pipeline. These efforts include support of training programs to build capacity for tech employers and regional collaboration with industry trade groups, IT management from diverse companies across the region to define demands and career pathways, and vet the best education and training programs to meet employer demand in the entire region.

MERIT NETWORK

Michigan Cyber Range: The Michigan Cyber Range features a cybersecurity education experience based upon the National Institute of Standards and Technology National Initiative for Cybersecurity Education (NICE). The MCR heavily leverages Merit's network to conduct classes that provide 17 CNSS accredited certificates on various aspects of cybersecurity. In addition to classes, the Range hosts a variety of exercises that train information technology or cybersecurity professionals. Finally, the MCR leases virtual infrastructure to organizations for their own classes, exercises, and testing. Many of these offerings make use of Alphaville, MCR's virtual training environment. Notable Merit cybersecurity training partnerships include, but are not limited to: ISC2, CompTIA, ISACA, EC-Council, Cyber World Institute, and the Cloud Security Alliance. The following classes are available as either a private class or an on-demand class. EC-Council Certification Courses

- EC-Council Certification Courses
  - Certified Chief Information Security Officer - CCISO
  - Certified Ethical Hacker - CEH
  - Computer Hacking Forensic Investigator – CHFI
  - EC-Council Certified Incident Handler - ECIH
  - EC-Council Certified Security Analyst - ECSA
  - EC-Council Network Security Administrator - ENSA
  - Licensed Penetration Tester - LPT
- CompTIA Certification Courses
  - CompTIA A+
  - CompTIA Network+
  - CompTIA Security+

- (ISC)2 Certification Courses
  - Certified Authorization Professional - CAP
  - Certified Computer Forensics Professional - CCFP
  - Certified Cloud Security Professional - CCSP
  - Certified Information Systems Security Professional - CISSP
  - Certified Secure Software Lifecycle Professional - CSSLP
  - HealthCare Information Security and Privacy Practitioner – HCISPP

Merit Cyber Range Hubs offer more than 40 cybersecurity certifications at

- Pinckney High School – Pinckney
- Velocity Hub & Cyber Institute – Sterling Heights
- Wayne State University ATEC – Warren

For more information, visit: **https://www.merit.edu/**

MICHIGAN INFRAGARD

Michigan InfraGard is a public-private partnership with the FBI dedicated to the protection of the United States and the American people and in particular critical infrastructures and key resources. This alliance holds quarterly meetings and an annual conference, which was held in Detroit in May 2017.

For more information, visit: **http://www.michiganinfragard.org/index.html**

MICHIGAN MANUFACTURING TECHNOLOGY CENTER (MMTC)

All Department of Defense (DoD), General Services Administration (GSA) and NASA contractors must meet the Federal Acquisition Regulation (FAR) minimum cybersecurity standards by December 31, 2017—or risk losing federal contracts. The Michigan Manufacturing Technology Center has assembled a team of cybersecurity experts to determine if a business is compliant with the standards described in NIST Special Publication 800-171.

For more information, visit: **https://www.the-center.org/Our-Services/Cybersecurity**

MICHIGAN STATE POLICE

Michigan Cyber Command Center: The MC3 is responsible for the coordination of combined efforts of cyber emergency response during critical cyber incidents in Michigan. Emphasis is placed upon prevention, response, and recovery from cyber incidents.

Computer Crimes Unit: The CCU provides investigative support in the seizure, acquisition, and analysis of digital evidence, including digital device forensic examinations, for the law enforcement community.

Michigan Internet Crimes Against Children Task Force: MSP CCU has oversight over the statewide Michigan Internet Crimes Against Children (ICAC) Task Force. The task force includes over 50 federal, state, and local law enforcement agencies who work together to investigate offenders who use the internet, online communication systems, or computer technology to sexually exploit children.

MICHIGAN WORKS! AGENCIES:

Several programs/initiatives are available through the Michigan Works! agencies that can be utilized for cybersecurity training. These resources may include:

- Workforce Innovation and Opportunity Act Dislocated Worker Program
- Workforce Innovation and Opportunity Act Adult Program
- Workforce Innovation and Opportunity Act Youth Program
- Trade Adjustment Assistance Program
- Reemployment Services and Eligibility Assessment Work-Based Learning Program
- Michigan Skilled Trades Training Fund
- Michigan New Jobs Training Program (through the community colleges)

Please contact your local Michigan Works! Agency for more information. To find a local service center, visit: **http://www.michiganworks.org/about-michigan-works/one-stop-service-centers/**

SANS INSTITUTE

SANS is a virtual training center. SANS provides intensive, immersion training designed to employers and workers master the practical steps necessary for defending systems and networks against the most dangerous threats - the ones being actively exploited. SANS training can be taken in a classroom setting from SANS-certified instructors, self-paced over the Internet, or in mentored settings in cities around the world.

For more information, visit: **https://www.sans.org/**

VELOCITY CENTER CYBER RANGE HUB

The Velocity Cyber Range Hub at the Macomb -OU Incubator in the Velocity Collaboration Center can hold certification courses for more than 20 different cybersecurity disciplines. Each certification, hosted by Mac-OU INC through the Merit Network, can be obtained through a four-to-five day course including an exam. These programs run through Oakland University's Professional & Continuing Education and can earn participants continuing education units.

For more information, visit: **https://www.oakland.edu/macombouinc/cyber-institute/education**

APPENDIX C: CYBERSECURITY COLLABORATION GROUPS

Several groups and organizations are convening stakeholders in cybersecurity or information technology. The list below represents collaboration efforts, cybersecurity initiatives or resources in the southeast Michigan region. This information was gathered either directly from the organizations listed or from the websites of each respective institution. Any errors or omissions are unintentional.

ANN ARBOR SECURITY MEETUP (ARBSEC)

An informal meetup of information security professionals in Ann Arbor.

https://www.arbsec.org/

AUTOMOTIVE INFORMATION SHARING AND ANALYSIS CENTER (AUTO-ISAC)

The auto-ISAC is an industry-operated environment created to enhance cybersecurity awareness and collaboration across the global automotive industry—light- and heavy-duty vehicle OEMs, suppliers, and the commercial vehicle sector.

https://www.automotiveisac.com/

CAPITAL AREA IT COUNCIL

The Capital Area IT Council is a Michigan Regional Skills Alliance that was formed to address the specific workforce development challenges facing the local information technology industry. Employer led and directed, the Capital Area IT Council is a coalition of industry, education, economic development, and government partners committed to identifying, developing, and implementing real solutions for improving the quantity and quality of IT professionals in the region.

https://www.capitalareaitcouncil.net/

DEFENSE AUTOMOTIVE TECHNOLOGIES CONSORTIUM (DATC)

Started by US Army TARDEC and SAE, DATC's objective is to provide members from private industry, not-for-profit and academia opportunities to develop and transition advanced automotive technologies to all branches of military and government agencies. Consortium members receive simplified access, reduced bureaucracy, and enhanced visibility. Focus areas of automotive technology include:

- Automotive Cybersecurity
- Vehicle Safety Technologies
- Vehicle Light Weighting
- Autonomous Vehicles and Intelligent Systems
- Connected Vehicles
- Advanced Energy Storage Technologies
- Propulsion Technologies
- Active Suspension Technologies

http://datc.saeitc.org/

DETROIT AREA IAM USER GROUP

A vendor neutral user group designed to be a forum for discussing the best practices for both technology and business usage of Identity and Access Management frameworks.

MADCAT:

Through a grassroots effort, leaders from the government, education, non-profit and private sectors formed the Michigan Automotive and Defense Cyber Assurance Team (MADCAT) in 2014 to address the growing threat of cybersecurity breaches to Southeast Michigan's primary industries. MADCAT's aim is to establish Macomb County as a cybersecurity center of excellence and attract businesses and institutions that support the development, growth, and retention of the talent pool.

http://madcat.org/

MICHIGAN CYBER CIVILIAN CORPS

The Michigan Cyber Civilian Corps (MiC3) is a group of trained cybersecurity experts who volunteer to provide expert assistance to enhance the State's ability to rapidly resolve cyber incidents when activated under a Governor declared State of Emergency. The group includes volunteers from government, education, and business sectors.

The MISSION of MiC3 is to work with government, education, private sector organizations, and volunteers to create and implement a rapid response team to be activated under a Governor declared cyber State of Emergency and to provide mutual aid to government, education, and business organizations in the State of Michigan.

http://www.michigan.gov/som/0,4669,7-192-78403_78404_78419---,00.html

MICHIGAN STATE POLICE MICHIGAN CYBER COMMAND CENTER (MC3)

The MC3 is responsible for the coordination of combined efforts of cyber emergency response during critical cyber incidents in Michigan. Emphasis is placed upon prevention, response, and recovery from cyber incidents.

http://www.michigan.gov/msp/0,4643,7-123-72297_72370_72379---,00.html

NORTH AMERICAN INTERNATIONAL CYBER SUMMIT

The North American International Cyber Summit is hosted each year by Michigan Governor Rick Snyder in downtown Detroit. The event brings together experts to address a variety of cyber-security issues impacting the world. The Governor's High School Cyber Challenge finals take place at this summit.

https://events.esd.org/cyber-summit/

MICHIGAN STATE POLICE, EMERGENCY MANAGEMENT AND HOMELAND SECURITY DIVISION (MSP/EMHSD)

The purpose of the Michigan State Police is to prevent, mitigate, prepare for, respond to, and recover from emergencies, disasters, and threats to our homeland.

http://www.michigan.gov/msp/0,4643,7-123-72297_60152---,00.html

Michigan cybersecurity resources also include:

- Michigan Information Sharing and Analysis Center (MI-ISAC)
- Michigan Intelligence Operations Center (MIOC)
- Michigan National Guard Cyber Teams (MI-NGCT)
- Multi-State Information Sharing and Analysis Center (MS-ISAC)

#MISEC

#misec is a collective of Michigan based information security professionals (or maybe just people interested in security) looking to share knowledge and make the world a safer place. #misec launched with BSides Detroit 2011. They started with a simple idea: make the BSides experience an ongoing part of life in Southeast Michigan. This expanded into monthly meet-ups, workshops, capture-the-flag teams, and more. They continue to put on the BSides Detroit conference, and to send speakers and volunteers to conferences around the region. Currently #misec has expanded to three locations: Southfield, Jackson, and Lansing. This has allowed them to interact with many professionals throughout the area and continue to grow the number of available.

http://michsec.org/

OPPORTUNITY DETROIT TECH

Opportunity Detroit Tech (ODT) envisions the Greater Detroit Region as a place where an improved information technology ecosystem can be the answer to industry and community economic success. ODT leverages strategic partnerships with workforce development agencies, community colleges, and IT industry leaders to identify and address the needs of the region's information technology ecosystem. Empowered by the use of actionable labor market intelligence, ODT looks to raise awareness of and shape community response to the industry's talent, customer, supply chain, and other growth needs to improve both the industry itself and the region as a whole.

http://www.opportunitydetroittech.com/

US ARMY TARDEC NATIONAL AUTOMOTIVE CENTER

The National Automotive Center (NAC) now included as part of the TARDEC External Business Office is a charted organization continuing its 20 plus year affiliation with the automotive industry, acting as the Army focal point to leverage dual-use automotive technologies and development - for application to military ground vehicles. Dual-use partners include automotive, trucking, and off-road vehicle manufacturers, their supplier base, and associations. The NAC links with these entities to build collaborative relationships based on mutual technical interests and legislative impacts, standards, and research. Current Focus areas include: Vehicle Cybersecurity, Vehicle Autonomy, Hydrogen power vehicles and their infrastructure, vehicle and infrastructure electronics architecture and vehicle energy efficiency.

https://www.army.mil/article/128385/collaborate_with_tardec_through_the_external_business_office

WEST MICHIGAN CYBERSECURITY CONSORTIUM (WMCSC)

The West Michigan Cyber Security Consortium (WMCSC) is a multi-jurisdictional, public/private partnership whose purpose is to enhance the prevention, protection, response and recovery to cyber security threats, disruptions, and degradation to critical information technology functions. Its membership includes individuals from government, health care, law enforcement, and private businesses. The group meets quarterly to share information around cyber security issues. WMCSC hosts the Michigan Cyber Security Conference each year in Grand Rapids, to be held in October 2017.

ADDITIONAL CYBER ASSETS:

Michigan Cyber Range: The Michigan Cyber Range (MCR) provides a secure environment for cybersecurity education, training, and testing. It also performs research as an advanced platform for industrial control systems security.

The MCR is an unclassified private cloud operated by Merit. It delivers cybersecurity classes and exercises and enables product development and testing to clients and Merit Members across the nation and throughout the world.

The Michigan Cyber Range provides a strategic advantage over other states by providing a secure place for businesses to test and harden their products outside of their current operating environment. The Michigan Cyber Range currently has three hubs: Pinckney, Wayne State University ATEC Center, and Velocity.

For more information, visit: **https://www.merit.edu/cyberrange/**

Regional Cybersecurity Education Collaboration (RCEC): The Michigan Cyber Range Regional Cybersecurity Education Collaboration is currently under development. This initiative involves the higher education community and private sector partners to address the gap between the supply of skilled cybersecurity professionals and the demand for these skills. The long-term goal is to provide a robust cybersecurity curriculum to institutions throughout the state via a mix of face-to-face and distance learning courses at 2-year and 4-year colleges.

For more information, visit: **https://www.merit.edu/cybered/**


600GB 10K
600GB 10K
600GB 10K

APPENDIX D: WORKFORCE DATA TERMS GLOSSARY

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.

Burning Glass Technologies: The primary source for job postings data used in this analysis. Burning Glass Technologies collects online job ads from nearly 40,000 sources and de-duplicates same job postings to provide a collection on job demand across the Internet.

Certifications: This research filter in the Burning Glass Technologies tool allows researchers to collect data on professional certifications required or preferred in online job postings.

Completions: Per the Integrated Postsecondary Education Data System (IPEDS) data collection system glossary: This annual component of IPEDS collects number of degrees and other formal awards (certificates) conferred. These data are reported by level (associate's, bachelor's, master's, and doctor's), as well as by length of program for some. Both are reported by race/ethnicity and gender of recipient, and the field of study, using the Classification of Instructional Programs (CIP) code. Institutions report all degrees and other awards conferred during an entire academic year, from July 1 of one calendar year through June 30 of the following year.

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

Educational attainment: This dataset from Burning Glass Technologies overviews the level of educational attainment specified (required or preferred) in online job postings for a particular occupation or job.

Experience: Like 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).

Job demand: Approximated by total number of online job postings for a specific occupation in this analysis using job postings data from Burning Glass Technologies.

Location Quotient: Per the Economic Modeling Specialists, Inc. (EMSI), Location quotient (LQ) is a valuable way of quantifying how concentrated a particular industry, cluster, occupation, or demographic group is in a region as compared to the nation. It can reveal what makes a particular region "unique" in comparison to the national average. In more exact terms, location quotient is a ratio that compares a region to a larger reference region per some characteristic or asset. Suppose X is the amount of some asset in a region (e.g., manufacturing jobs), and Y is the total number of assets of comparable types in the region (e.g., all jobs). X/Y is then the regional "concentration" of that asset in the region. If X' and Y' are similar data points for some larger reference region (like a state or nation), then the LQ or relative concentration of that asset in the region compared to the nation is (X/Y) / (X'/Y').

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 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).

Programs of study: Drawn from online job postings data from Burning Glass Technologies, companies hiring may specify a degree and/or degree program which is required or preferred for the open role.

Salary/wages: Advertised in online job postings collected by Burning Glass Technologies, employers may specify a salary range or hourly wage. The data is represented as annual salary-equivalents.

Skills, employability: Coded from online job postings, Burning Glass Technologies presents these as baseline skills necessary for successful employment in the open position.

Skills, technical: Coded from online job postings, Burning Glass Technologies presents these as the technical skills necessary for successful employment in the open position.

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 Burning Glass Technologies, 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.

ABOUT WIN AND AMDC

WORKFORCE INTELLIGENCE NETWORK FOR SOUTHEAST MICHIGAN:

The Workforce Intelligence Network for Southeast Michigan (WIN) helps to cultivate a comprehensive and cohesive talent system to ensure employers' success. WIN is a partnership of 10 community colleges and 6 Michigan Works! Agencies in southeast Michigan. WIN's mission is to cultivate a comprehensive and cohesive talent system to ensure employers find the workers they need for success. WIN specializes in fostering collaboration among talent partners, including workforce development, community colleges, four-year postsecondary institutions, K-12 schools, economic development organizations, government, community based organizations, employers, and others.

WIN board institutions include:

Colleges

Henry Ford College

Jackson College

Macomb Community College

Monroe County Community College

Mott Community College

Oakland Community College

Schoolcraft College

St. Clair County Community College

Washtenaw Community College

Wayne County Community College District

Michigan Works! Agencies

Detroit Employment Solutions Corporation

Genesee Shiawassee Thumb Michigan Works!

Macomb/St. Clair Workforce Development Board

Oakland County Michigan Works!

Southeast Michigan Community Alliance

Southeast Michigan Consortium

ADVANCE MICHIGAN DEFENSE COLLABORATIVE:

The Advance Michigan Defense Collaborative (AMDC) is a group of organizations that provides immediate and sustained assistance to firms and workers in a 13-county region in Southeast Michigan affected by reduced Department of Defense procurement. The group coordinates assistance to organizations that promote research, industrial development, and talent development relevant to the defense industry. Efforts support resiliency and capacity in autonomous transportation and connected mobility, lightweight materials manufacturing sector, and information technology, with a focus on increasing security of automated transportation systems and products. The core coalition of partners includes the Macomb/St. Clair Workforce Development Board, Workforce Intelligence Network for Southeast Michigan, Michigan Defense Center-an operation of the Michigan Economic Development Corporation, Merit Network, and Macomb County Office of Economic Development and Planning.

Key projects support worker transition from defense to other growing regional industries; planning and partnership development around the identified growth clusters; encourage planning and implementation of urban innovation challenges to support industry diversification and entrepreneurship; and enhance bid-targeting efforts to help defense-industry firms affected by downsizing find new contracting opportunities.


WIN
WORKFORCE
INTELLIGENCE
NETWORK