Cybersecurity

at Columbus State

# *Columbus State Community College*
# *Evaluator Report*
# *Fall 2018*

*Prepared by:*

University of Wisconsin-Stout
APPLIED
RESEARCH
CENTER
Wisconsin's Polytechnic University

When you partner with the ARC for your applied research needs, you can expect the following from us:

### Experience & Education

The ARC staff has over 50 years of combined experience in conducting institutional research and over 20 years working with quality improvement initiatives. The ARC staff has Masters' and Doctoral degrees in evaluation studies, applied psychology, research design, and qualitative/quantitative analysis.

### Expertise

The ARC staff has active working relationships with UW-Stout faculty, staff and students in survey development, survey administration, statistical analysis, qualitative analysis, and other aspects of research design. The ARC staff also draws on the expertise of over 250 faculty members with content knowledge in a wide array of fields.

### Evidence

The work done by the ARC staff has been recognized not only by our clients, but by the Malcolm Baldrige Quality Program and the Academic Quality Improvement Program.

### Expectations

You can depend on the ARC to provide you with a robust and rigorous approach to your research project. We want your institution to be able to take our research and apply it to your institutional community in the most effective way possible to create meaningful change. You can expect us to provide you with clear, concise reports that are easy to read and interpret.

We will be with you each step of the way to enable you to achieve your goals.

---

## Mission

The office of Planning, Assessment, Research and Quality is responsible for strategic planning and accountability, institutional research and assessment, the Applied Research Center, quality initiatives and university policies. We employ a participatory, collaborative planning process and rigorous approach to research and assessment. Decisions are informed by data and reflect the needs of UW-Stout and our external clients. Our dedication to continuous quality improvement promotes intelligent risk taking and innovative thinking university-wide. Our transparent approach to sharing data and information demonstrates accountability to the university and the public.

## Vision

Living our values to grow the capacity of our campus and external clients to use information for decision-making and meaningful change.

## Values

- We are knowledgeable and professional, with the expertise to provide quality service
- We provide information and resources for decision-making
- We approach our work with honesty and integrity, and infuse ethics throughout all we do
- We value accuracy, efficiency, reliability, and timeliness while upholding the highest standards
- We are flexible, resourceful, and innovative and value continuous quality improvement
- We use participatory and collaborative approaches to planning, decision-making, and research

## Table of Contents

## Index of Figures

*Columbus State Community College Cybersecurity Program*

## *Evaluation Report*

### Overview

Columbus State, in collaboration with Franklin University, NSF ATE National CyberWatch Center (Prince George's Community College), Columbus Downtown High School, Reynoldsburg City Schools, and key industry partners (E&Y, Abercrombie & Fitch, Alliance Data, Ohio Health, Nationwide, The Columbus Collaboratory, and TechColumbus – now Rev1Ventures) are researching and developing an academic and career pathway in Cybersecurity education. Instructional and student support systems are being developed to help establish the optimal environment for student success. The overall project goal is to create a career pathway for cybersecurity professionals with subject matter knowledge to support the increasingly complex technology needs within security while providing program graduates opportunities in a variety of industry and government entities.

### Industry Engagement Survey

A survey was designed to capture the preferences and concerns among potential employers of graduates of the Cybersecurity program was administered by the Applied Research Center. The results are summarized below. Appendix A contains a copy of the survey.

Industry Engagement Executive Summary

1. **Expertise of Entry Level Cyber Security Professionals**
   Areas rated for level of expertise:
   a. Secure Provision: Respondents indicated Proficient or Master levels 75% (N=3) were needed for Systems Security Architecture. Respondents indicated Component or Proficient levels 100% (N=4) were needed for Software Assurance and Security Engineering.
   b. Analyzation: Respondents indicated Competent or Proficient levels 75% (N=3) were needed for Cyber Threat Analysis and Exploitation Analysis. Respondents indicated Novice and Competent levels 75% (N=3) were necessary for All Source Intelligence Target.
   c. Collect and Operate: Respondents indicated Competent or Proficient levels 75% (N=3) were needed for Cyber Operations and Novice or Competent levels 100% (N=4) were needed for Operations Planning and Collection Operations.
   d. Protection and Defense: Majority of respondents 75% (N=3) indicated Proficient levels were needed for Computer Network Defense (CND) Analysis and Computer Network Defense (CND) Infrastructure Support. Respondents indicated Competent or Proficient levels 100% (N=4) were needed for Incident Response and Vulnerability Assessment and Management.
   e. Investigation: Respondents indicated Competent or Proficient levels 100% (N=4) were needed for Investigation. Whereas, 75% (N=3) of respondents indicated only Competent levels were needed for Digital Forensics.
   f. Oversight and Development: Respondents indicated Novice levels 50% (N=2) were needed for; Strategic Planning and Policy development, Security Program Management (CISCO), Information Systems Security Operations (ISSO), and Education and Training. Majority of respondents 75% (N=3) indicated Novice levels were needed for Legal Advice and Advocacy.
   g. Operation and Maintenance: Respondents indicated Proficient or Master levels 100% (N=4) were need for System Administration.  Majority of respondents, 75% (N=3) indicated Proficient

or Master levels were needed for Network Services. In addition, 75% (N=3) indicated Proficient levels were needed for Systems Security Analysis and Customer Service and Technical Support.

Areas of expertise ranked in the cyber security industry:

a. Half of the respondents 50% (N=2) ranked Certifications as the most important area of expertise. Half of the respondents 50% (N=2) ranked the least important areas as Networking.

2. **Interest with Other Cyber Security Organizations**

a. Collaborating on projects and partnerships

- All the respondents 100% (N=4) indicated they are interested in collaborating on projects with other cyber security organizations. All the respondents 100% (N=4) indicated they are interested in partnerships with other cyber security organizations.

3. **Hiring of Computer Science Graduates**

Frequency of hiring cyber security professionals:

a. When participants were asked, "How frequently does your organization hire any type of cyber security professional?" Half of the respondents 50% (N=2) indicated Infrequently and 50% (N=2) indicated Frequently.

Appendix B contains a full report summarizing results for each question.

### Student Data

Success of institutions of higher education is measured across many variables. The standardized method in which data are collected makes it possible to compare benchmarks among institutions at the Federal level. The National Center for Education Statistics uses the following major data points for comparison: enrollment, applicant data, transfer in and out rates, grade point average (GPA), and graduation rates. As a benchmark of success these data were collected from Columbus State Community College at the college level, the computer science (subject) level, and at the program level (Cybersecurity) level. The results are presented below.

The data below reflects student enrollment for the 2016-2017 and the 2017-2018 academic school years as measured in the fall semester. Enrollment data typically follows a fall to fall comparison. Data is not yet available for the 2018-2019 academic school year.

*Enrollment Data*

Table 1 displays application data for Columbus State Community College at the college, subject and program level for Cybersecurity.

Table 1. Application Data

| | FA16 | FA17 | FA18 |
|---|---|---|---|
| Overall CSCC | 18,643 | 20,815 | * |
| CSCC Computer Science | 550 | 646 | * |
| Cybersecurity | * | 174 | * |

Table 2 displays enrollment data for the Cybersecurity program. Enrollment is defined in terms of the show rate which is the number of students who have applied and been accepted to a program.

Enrollment increased from 97 in the fall or 2017 to 152 om the fall of 2018 for a 56% increase in enrollment. Additionally, there was an increase in the number students who receive Federal funding for education in the form of a Pell Grant.

Table 2. Cybersecurity Program Enrollment Data

| | Students | Average GPA | % on Pell Grant |
|---|---|---|---|
| Fall 2017 | 97 | 2.72 | 20% |
| Fall 2018 | 152 | 2.94 | 60% |

Table 3 displays transfer-in data at the college, program, and subject level. The transfer in rate is defined as students entering a program by transferring in. Rates at the college and program level have remained consistent.

Table 3. Transfer In Rate

| | FA16 | FA17 | FA18 |
|---|---|---|---|
| Overall CSCC | 18.6% | 19.2% | * |
| CSCC Computer Science | 27.9% | 27.1 | * |
| Cybersecurity | * | 27.9 | * |

Table 4 displays transfer out data at the college, subject and program level. Rates at the college and program level have remained consistent. The transfer out rate is defined as students exiting a program by transferring out. Overall, transfer out rates have slightly increased over time while the Cybersecurity program has lowest transfer rates. This, however, is likely due the fact that this is a new program.

Table 4. Transfer Out Rate

| | FA16 | FA17 | FA18 |
|---|---|---|---|
| Overall CSCC | 26.2% | 28.7% | * |
| CSCC Computer Science | 9.8% | 12.0% | * |
| Cybersecurity | * | 10.3% | * |

Table 5 displays GPA data at the college, subject and program level. GPA has remained mostly consistent over time but have steadily increased. Cybersecurity students had a higher average GPA as compared to all of CSCC and Computer Science students only.

Table 5: GPA

| | FA16 | FA17 | FA18 |
|---|---|---|---|
| Overall CSCC | 2.72 | 2.75 | * |
| CSCC Computer Science | 2.66 | 2.72 | * |
| Cybersecurity | * | 2.97 | * |

Table 6 displays graduation rates at the college, subject, and program level. Because the Cybersecurity program has a program cycle of two years, three-year graduation rates are displayed. This is in alignment with the way graduation rates are calculated among two-year institutions according to the

National Center for Education Statistics. While Computer Science majors had similar graduation rates to that of all of CSCC, rates are not yet available for the Cybersecurity program.

Table 6: Three-year Graduation Rates

| | FA16 | FA17 | FA18 |
|---|---|---|---|
| Overall CSCC | 6.6% | 6.4% | * |
| CSCC Computer Science | 3.9% | 7.4% | * |
| Cybersecurity | * | * | * |

## Appendix A

*Industry Engagement Survey*

## *Expertise*

*Q1 As an industry partner, we are looking for your feedback regarding cyber security professionals. Your participation in this survey is appreciated and your feedback will help us to better define our program objectives to meet industry needs.*

*Please proceed to complete this survey.*

*Q2 Rate the level of expertise that an entry level cyber security professional should have in each area of Secure Provision.*

| | *Novice* | *Competent* | *Proficient* | *Expert* | *Master* |
|---|---|---|---|---|---|
| *Technology & Research Development* | ❍ | ❍ | ❍ | ❍ | ❍ |
| *System Requirements Planning* | ❍ | ❍ | ❍ | ❍ | ❍ |
| *Systems Security Architecture* | ❍ | ❍ | ❍ | ❍ | ❍ |
| *Software Assurance and Security Engineering* | ❍ | ❍ | ❍ | ❍ | ❍ |
| *Systems Development* | ❍ | ❍ | ❍ | ❍ | ❍ |
| *Test and Evaluation* | ❍ | ❍ | ❍ | ❍ | ❍ |
| *Information Assurance (IA)* | ❍ | ❍ | ❍ | ❍ | ❍ |
| *Compliance* | ❍ | ❍ | ❍ | ❍ | ❍ |

*Q3 What else should a cyber security professional have expertise in regarding this area?*

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________

*Q4 Rate the level of expertise that an entry level cyber security professional should have in each area of Analyzation.*

| | *Novice* | *Competent* | *Proficient* | *Expert* | *Master* |
|---|---|---|---|---|---|
| *Cyber Threat Analysis* | ○ | ○ | ○ | ○ | ○ |
| *All Source Intelligence Targets* | ○ | ○ | ○ | ○ | ○ |
| *Exploitation Analysis* | ○ | ○ | ○ | ○ | ○ |

*Q5 What else should a cyber security professional have expertise in regarding this area?*

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________

*Q6 Rate the level of expertise that an entry level cyber security professional should have in the area of Collect and Operate.*

| | Novice | Competent | Proficient | Expert | Master |
|---|---|---|---|---|---|
| Operations Planning | ○ | ○ | ○ | ○ | ○ |
| Cyber Operations | ○ | ○ | ○ | ○ | ○ |
| Collection Operations | ○ | ○ | ○ | ○ | ○ |

*Q7 What else should a cyber security professional have expertise in regarding this area?*

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________

*Q8 Rate the level of expertise that an entry level cyber security professional should have in each area of Protection and Defense.*

| | Novice | Competent | Proficient | Expert | Master |
|---|---|---|---|---|---|
| Computer Network Defense (CND) Analysis | ○ | ○ | ○ | ○ | ○ |
| Vulnerability Assessment and Management | ○ | ○ | ○ | ○ | ○ |
| Incident Response | ○ | ○ | ○ | ○ | ○ |
| Computer Network Defense (CND) Infrastructure Support | ○ | ○ | ○ | ○ | ○ |

*Q9 What else should a cyber security professional have expertise in regarding this area?*

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________

*Q10 Rate the level of expertise that an entry level cyber security professional should have in each area of Investigation.*

| | *Novice* | *Competent* | *Proficient* | *Expert* | *Master* |
|---|---|---|---|---|---|
| *Investigation* | ○ | ○ | ○ | ○ | ○ |
| *Digital Forensics* | ○ | ○ | ○ | ○ | ○ |

*Q11 What else should a cyber security professional have expertise in regarding this area?*

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________

*Q12 Rate the level of expertise that an entry level cyber security professional should have in each area of Oversight and Development.*

| | *Novice* | *Competent* | *Proficient* | *Expert* | *Master* |
|---|---|---|---|---|---|
| *Strategic Planning and Policy Development* | ❍ | ❍ | ❍ | ❍ | ❍ |
| *Security Program Management (CISCO)* | ❍ | ❍ | ❍ | ❍ | ❍ |
| *Information Systems Security Operations (ISSO)* | ❍ | ❍ | ❍ | ❍ | ❍ |
| *Education and Training* | ❍ | ❍ | ❍ | ❍ | ❍ |
| *Legal Advice and Advocacy* | ❍ | ❍ | ❍ | ❍ | ❍ |

*Q13 What else should a cyber security professional have expertise in regarding this area?*

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________

*Q14 Rate the level of expertise that an entry level cyber security professional should have in each area of Operation and Maintenance.*

| | *Novice* | *Competent* | *Proficient* | *Master* | *Expert* |
|---|---|---|---|---|---|
| *System Administration* | ○ | ○ | ○ | ○ | ○ |
| *Network Services* | ○ | ○ | ○ | ○ | ○ |
| *Customer Service and Technical Support* | ○ | ○ | ○ | ○ | ○ |
| *Systems Security Analysis* | ○ | ○ | ○ | ○ | ○ |
| *Data Administration* | ○ | ○ | ○ | ○ | ○ |
| *Knowledge Management* | ○ | ○ | ○ | ○ | ○ |

*Q15 What else should a cyber security professional have expertise in regarding this area?*

____________________________________________________________________

____________________________________________________________________

____________________________________________________________________

____________________________________________________________________

____________________________________________________________________

*Q16 Rank-order the seven areas of expertise in the cyber security industry in terms of importance for professionals from 1 (least import) to 7 (most important).*

_______ *Certifications*
_______ *Communication*
_______ *Leadership Skill*
_______ *Networking Foundation*
_______ *Degree*
_______ *On-the-Job Training*

*Q17 Why did you choose this order?*

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________

*End of Block: Expertise*

---

*Start of Block: Collaboration & Partnerships*

*Q18 Are you interested in collaborating on projects with other cyber security organizations?*

○ *Yes*

○ *No*

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

*Q19 Are you interested in partnerships with other cyber security organizations?*

○ *Yes*

○ *No*

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

*Page Break*

*End of Block: Collaboration & Partnerships*

---

*Start of Block: Hiring Practices*

*Q20 How frequently does your organization hire any type of cyber security professional?*

- ○ *Never*
- ○ *Infrequently*
- ○ *Sometimes*
- ○ *Frequently*
- ○ *Very Often*

---

*Q21 Do you think this should change? Why or why not?*

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________

---

*Q22 How often does your organization hire an individual with only a 2-year degree in computer science?*

- ○ *Never*
- ○ *Infrequently*
- ○ *Sometimes*
- ○ *Frequently*
- ○ *Very Often*

---

*Q23 Do you think this should change? Why or why not?*

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________

*Q24 How often does your organization hire someone without prior experience in computer science but has obtained relevant education and/or certification?*

- ○ *Never*
- ○ *Infrequently*
- ○ *Sometimes*
- ○ *Frequently*
- ○ *Very Often*

*Q25 Do you think this should change? Why or why not?*

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________

*Q26 Are you interested in providing development opportunities for current or future employees*

- ○ *Not at all interested*
- ○ *Need more information*
- ○ *Somewhat interested*
- ○ *Interested*
- ○ *Very Interested*

***End of Block: Hiring Practices***

***Start of Block: Internships***

*Q27 The last two questions use the following definition:*

***Internship*** *- short-term periods of work experience, typically completed by a student in a semester to gain exposure in their profession.*

*Q28 What level of interest do you have in providing internship opportunities to students?*

○ *Not at all interested*

○ *Need more information*

○ *Somewhat interested*

○ *Interested*

○ *Very interested*

*Q29 Would you be interested in developing a successful intern as a paid employee?*

○ *Not at all interested*

○ *Need more information*

○ *Somewhat interested*

○ *Interested*

○ *Very interested*

***End of Block: Internships***

***Start of Block: Block 5***

*Q38 Please provide your contact information.*

○ *Name* ________________________________________________

○ *Title* ________________________________________________

○ *Organization* ________________________________________________

○ *Phone Number* ________________________________________________

○ *email* ________________________________________________

***End of Block: Block 5***

***Start of Block: Block 4***

*Q30 We thank you for your time spent taking this survey!  Your response has been recorded.*

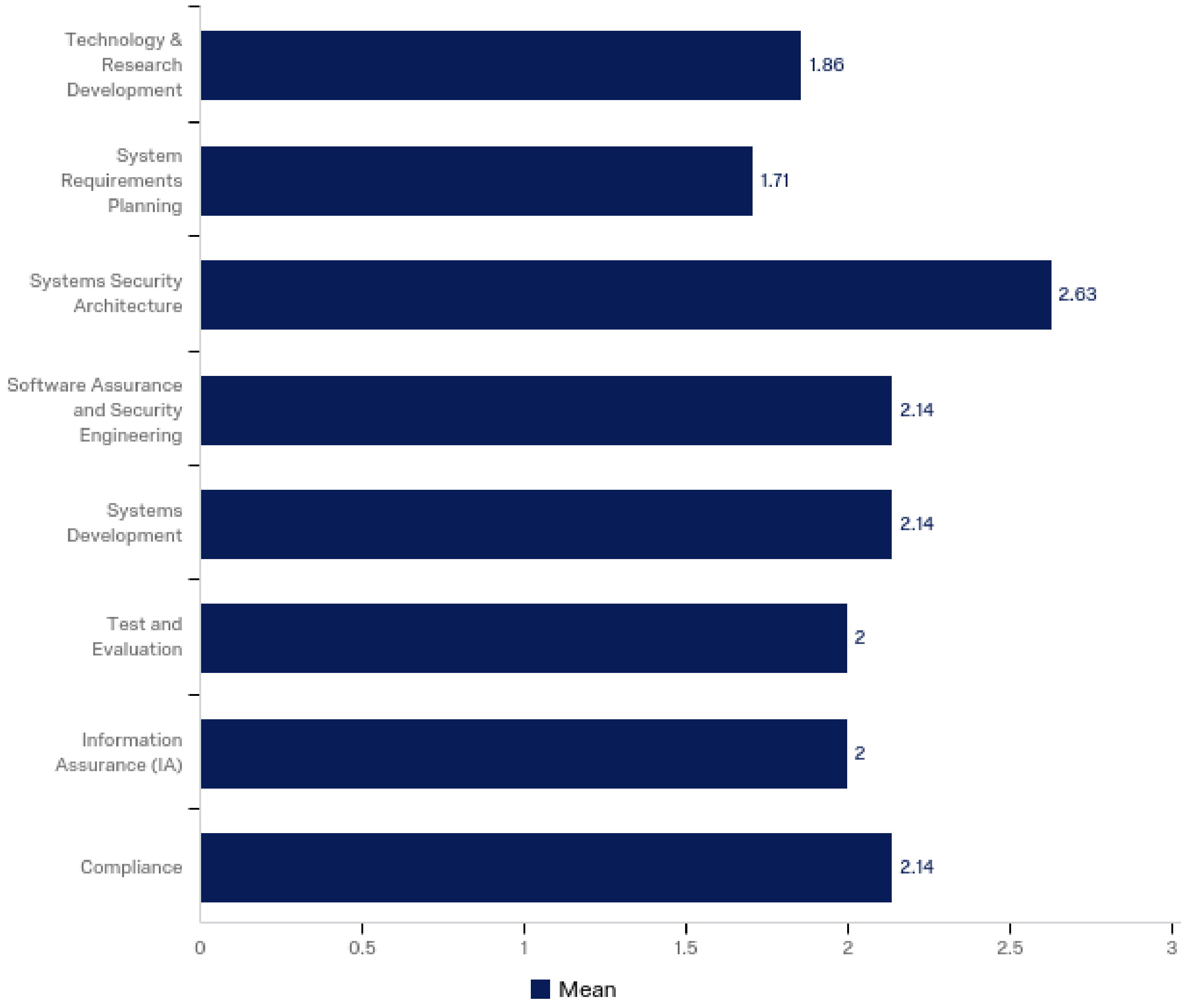
***End of Block: Block 4***

**Appendix B**

*Industry Engagement Survey Results*

## *Cyber Security Industry Engagement & Feedback*

### *Q2 - Rate the level of expertise that an entry level cyber security professional should have in each area of Secure Provision.*



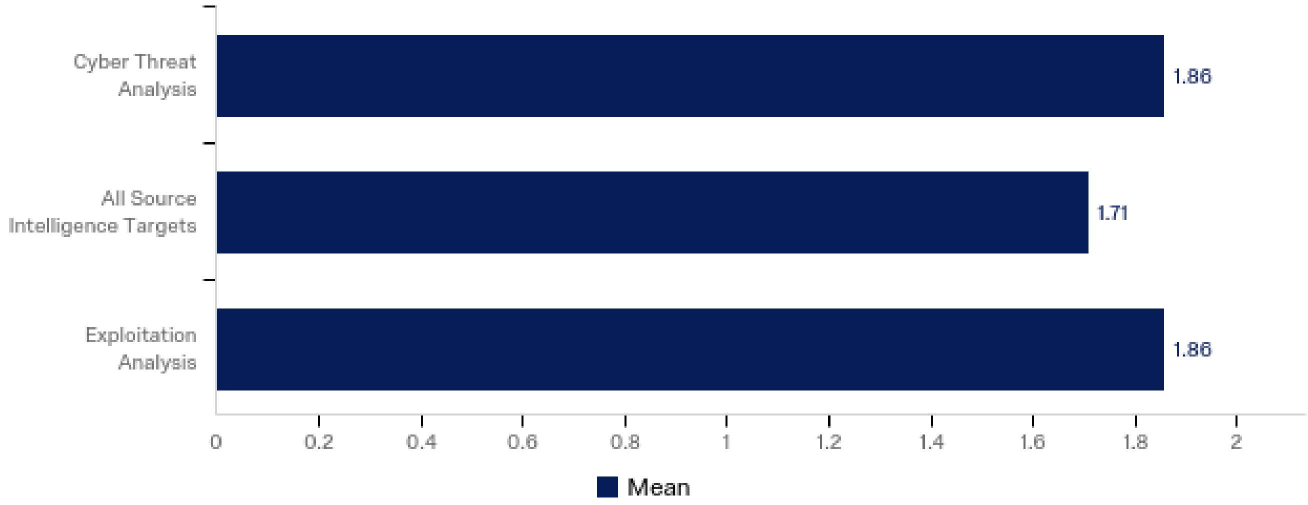
| # | Question | Novice | | Competent | | Proficient | | Expert | | Master | | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Technology & Research Development | 42.86% | 3 | 28.57% | 2 | 28.57% | 2 | 0.00% | 0 | 0.00% | 0 | 7 |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *9* | *System Requirements Planning* | *28.57%* | *2* | *71.43%* | *5* | *0.00%* | *0* | *0.00%* | *0* | *0.00%* | *0* | *7* |
| *10* | *Systems Security Architecture* | *12.50%* | *1* | *37.50%* | *3* | *37.50%* | *3* | *0.00%* | *0* | *12.50%* | *1* | *8* |
| *11* | *Software Assurance and Security Engineering* | *14.29%* | *1* | *57.14%* | *4* | *28.57%* | *2* | *0.00%* | *0* | *0.00%* | *0* | *7* |
| *12* | *Systems Development* | *14.29%* | *1* | *57.14%* | *4* | *28.57%* | *2* | *0.00%* | *0* | *0.00%* | *0* | *7* |
| *13* | *Test and Evaluation* | *14.29%* | *1* | *71.43%* | *5* | *14.29%* | *1* | *0.00%* | *0* | *0.00%* | *0* | *7* |
| *14* | *Information Assurance (IA)* | *28.57%* | *2* | *42.86%* | *3* | *28.57%* | *2* | *0.00%* | *0* | *0.00%* | *0* | *7* |
| *15* | *Compliance* | *28.57%* | *2* | *28.57%* | *2* | *42.86%* | *3* | *0.00%* | *0* | *0.00%* | *0* | *7* |

## *Q3 - What else should a cyber security professional have expertise in regarding this area?*

| *What else should a cyber security professional have expertise in regarding this area?* |
|---|
| *Risk Management* |
| *Depending on the definitions of the above, and any additional items, the level of expertise noted would change.  I would consider a 'competent' or 'proficient' individual in one light as compared to other recent graduates; but in a wholly different light as compared to seasoned professionals.  When compared to the latter, I've not encountered any new graduates who would rate much above 'novice' simply due to the lack of real-world experience.* |
| *Technical writing, Cloud based technology* |

### *Q4 - Rate the level of expertise that an entry level cyber security professional should have in each area of Analyzation.*

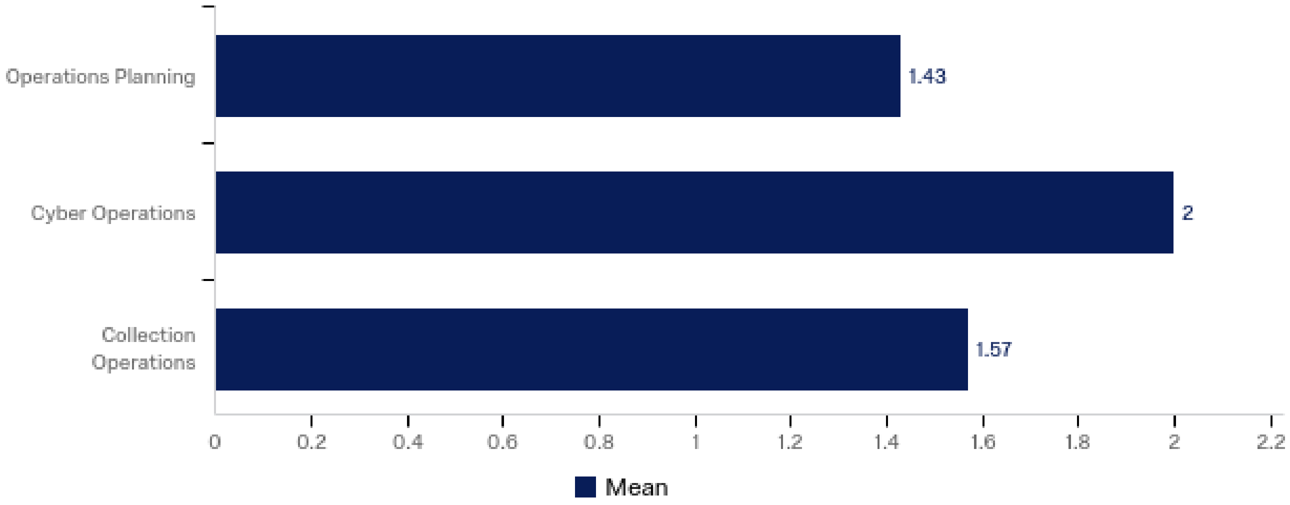


| # | Question | Novice | | Competent | | Proficient | | Expert | | Master | | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Cyber Threat Analysis | 42.86% | 3 | 28.57% | 2 | 28.57% | 2 | 0.00% | 0 | 0.00% | 0 | 7 |
| 5 | All Source Intelligence Targets | 42.86% | 3 | 42.86% | 3 | 14.29% | 1 | 0.00% | 0 | 0.00% | 0 | 7 |
| 6 | Exploitation Analysis | 28.57% | 2 | 57.14% | 4 | 14.29% | 1 | 0.00% | 0 | 0.00% | 0 | 7 |

## *Q5 - What else should a cyber security professional have expertise in regarding this area?*

| *What else should a cyber security professional have expertise in regarding this area?* |
|---|
| *Again, the level to be compared to would provide much more value.  These three areas are ones where many work and attempt to research, but the full understanding and capability within the space is extremely challenging without some sort of real-world experience.* |
| *Understand motivation of threats, capabilities they have and prevention, detection and response controls that exist* |

## *Q6 - Rate the level of expertise that an entry level cyber security professional should have in the area of Collect and Operate.*

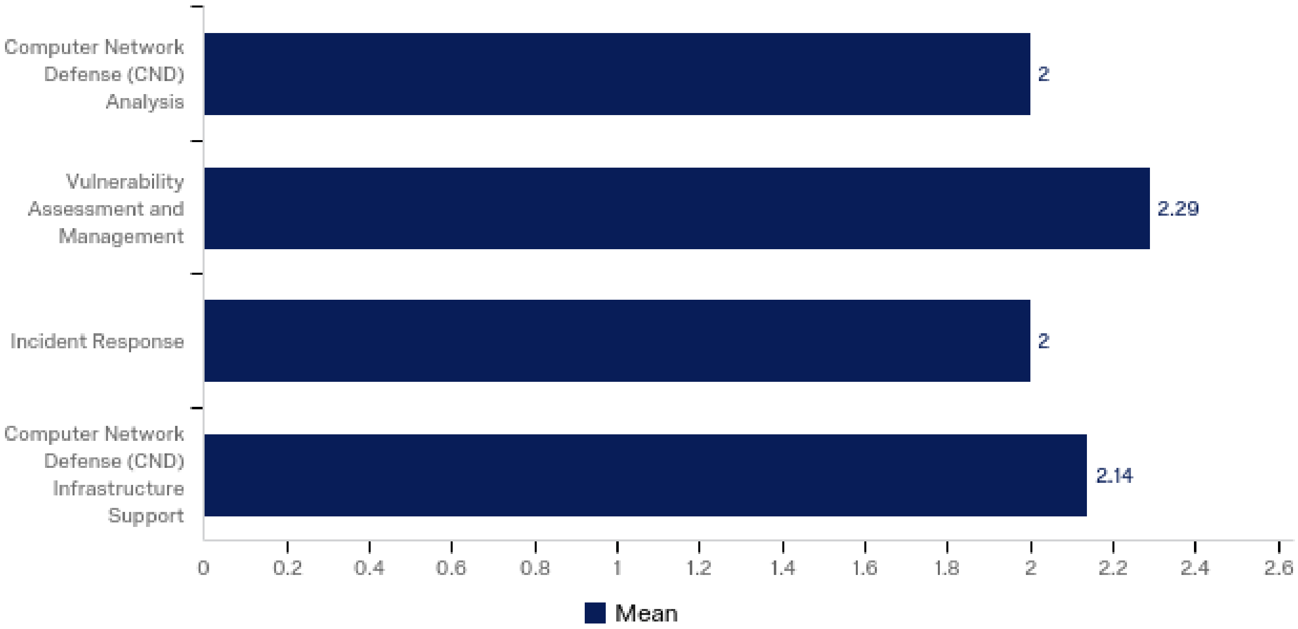


| # | Question | Novice | | Competent | | Proficient | | Expert | | Master | | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *1* | *Operations Planning* | *57.14%* | *4* | *42.86%* | *3* | *0.00%* | *0* | *0.00%* | *0* | *0.00%* | *0* | *7* |
| *11* | *Cyber Operations* | *14.29%* | *1* | *71.43%* | *5* | *14.29%* | *1* | *0.00%* | *0* | *0.00%* | *0* | *7* |
| *12* | *Collection Operations* | *42.86%* | *3* | *57.14%* | *4* | *0.00%* | *0* | *0.00%* | *0* | *0.00%* | *0* | *7* |

***Q7 - What else should a cyber security professional have expertise in regarding this area?***

*What else should a cyber security professional have expertise in regarding this area?*

### *Q8 - Rate the level of expertise that an entry level cyber security professional should have in each area of Protection and Defense.*



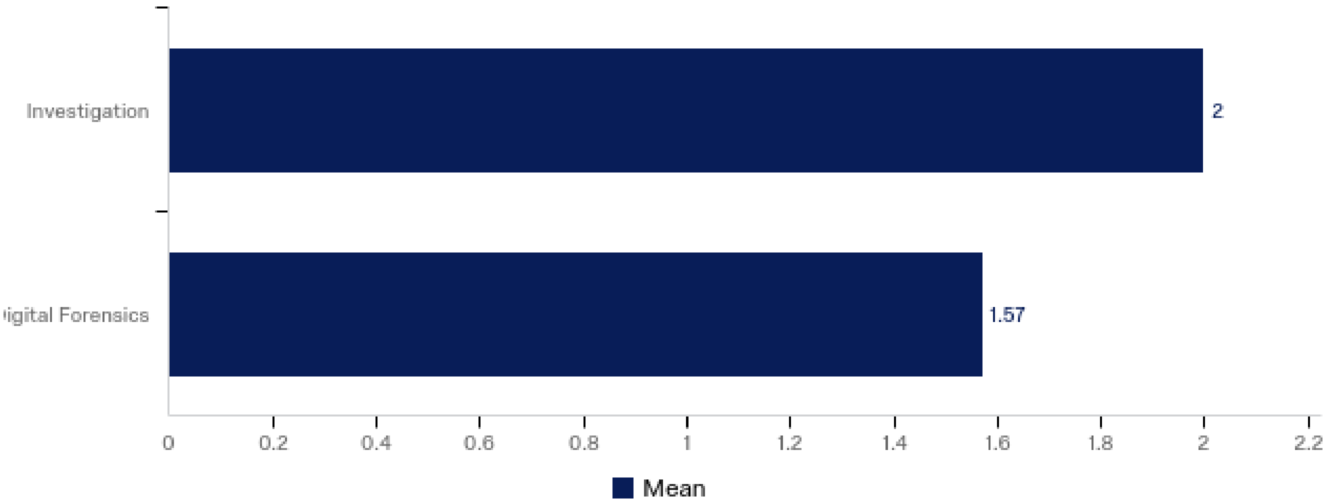
| # | Question | Novice | | Competent | | Proficient | | Expert | | Master | | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *1* | *Computer Network Defense (CND) Analysis* | *42.86%* | *3* | *14.29%* | *1* | *42.86%* | *3* | *0.00%* | *0* | *0.00%* | *0* | *7* |
| *6* | *Vulnerability Assessment and Management* | *14.29%* | *1* | *42.86%* | *3* | *42.86%* | *3* | *0.00%* | *0* | *0.00%* | *0* | *7* |
| *7* | *Incident Response* | *28.57%* | *2* | *42.86%* | *3* | *28.57%* | *2* | *0.00%* | *0* | *0.00%* | *0* | *7* |
| *8* | *Computer Network Defense (CND) Infrastructure Support* | *42.86%* | *3* | *0.00%* | *0* | *57.14%* | *4* | *0.00%* | *0* | *0.00%* | *0* | *7* |

## *Q9 - What else should a cyber security professional have expertise in regarding this area?*

| *What else should a cyber security professional have expertise in regarding this area?* |
|---|
| *dfd md f* |
| *Secure coding* |

### *Q10 - Rate the level of expertise that an entry level cyber security professional should have in each area of Investigation.*

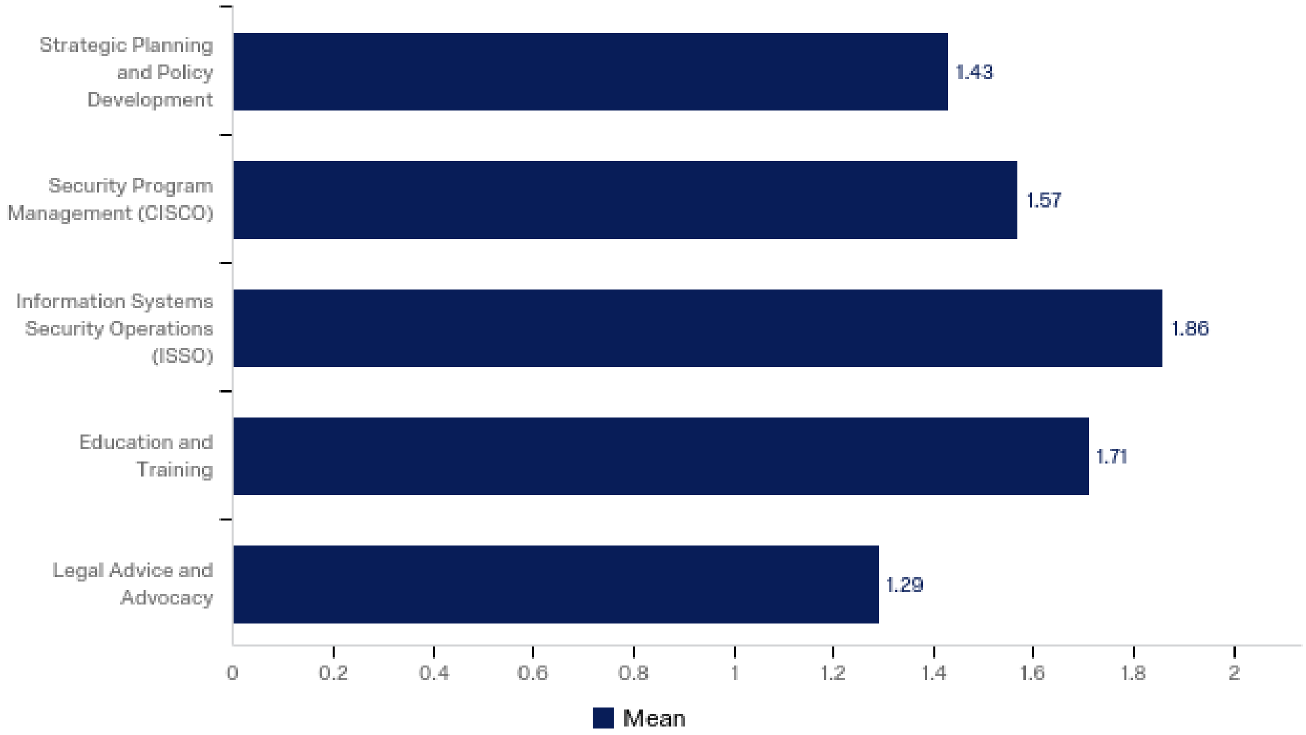
| # | Question | Novice | | Competent | | Proficient | | Expert | | Master | | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *1* | *Investigation* | *28.57%* | *2* | *42.86%* | *3* | *28.57%* | *2* | *0.00%* | *0* | *0.00%* | *0* | *7* |
| *5* | *Digital Forensics* | *42.86%* | *3* | *57.14%* | *4* | *0.00%* | *0* | *0.00%* | *0* | *0.00%* | *0* | *7* |



## *Q11 - What else should a cyber security professional have expertise in regarding this area?*

| *What else should a cyber security professional have expertise in regarding this area?* |
|---|
| *dfd* |

## *Q12 - Rate the level of expertise that an entry level cyber security professional should have in each area of Oversight and Development.*

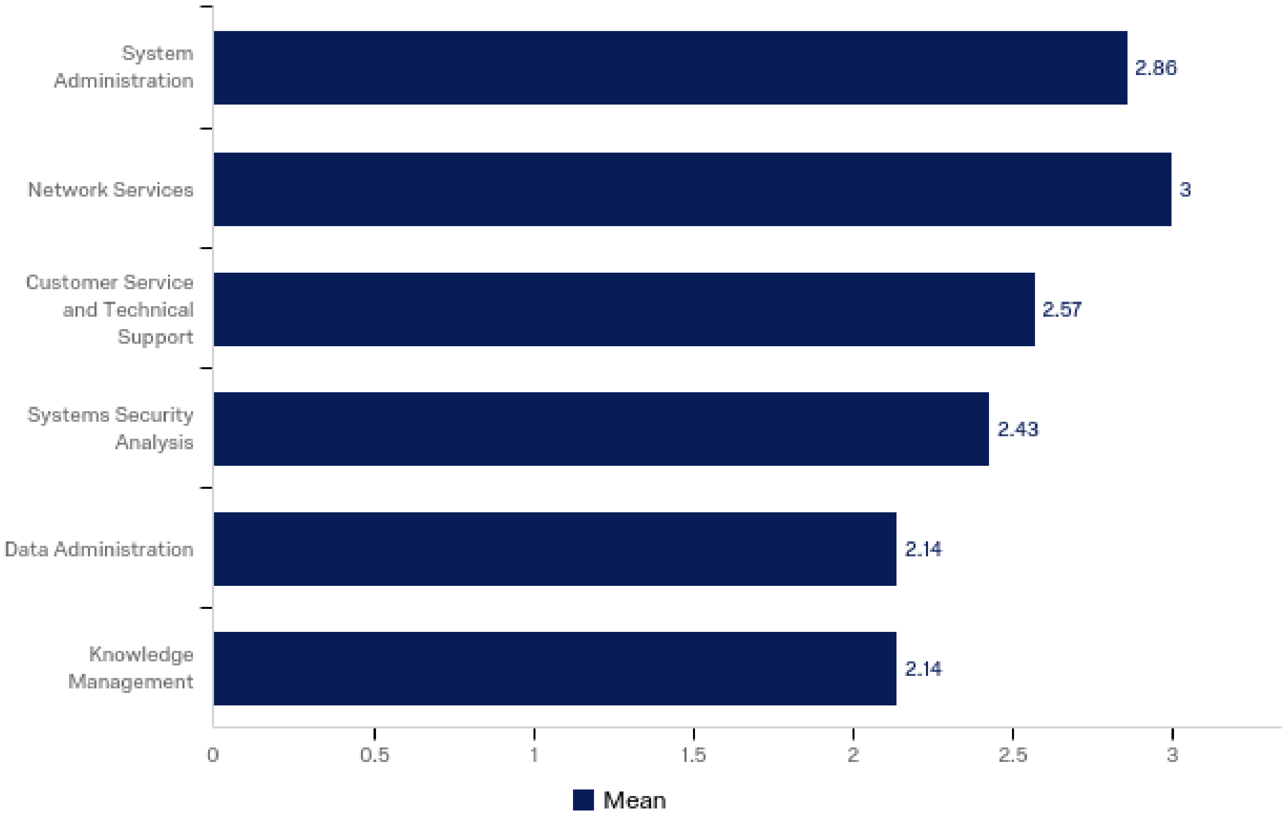


| *#* | *Question* | *Novice* | | *Competent* | | *Proficient* | | *Expert* | | *Master* | | *Total* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *1* | *Strategic Planning and Policy Development* | *71.43%* | *5* | *14.29%* | *1* | *14.29%* | *1* | *0.00%* | *0* | *0.00%* | *0* | *7* |
| *2* | *Security Program Management (CISCO)* | *42.86%* | *3* | *57.14%* | *4* | *0.00%* | *0* | *0.00%* | *0* | *0.00%* | *0* | *7* |
| *3* | *Information Systems Security Operations (ISSO)* | *42.86%* | *3* | *28.57%* | *2* | *28.57%* | *2* | *0.00%* | *0* | *0.00%* | *0* | *7* |
| *4* | *Education and Training* | *42.86%* | *3* | *42.86%* | *3* | *14.29%* | *1* | *0.00%* | *0* | *0.00%* | *0* | *7* |
| *5* | *Legal Advice and Advocacy* | *71.43%* | *5* | *28.57%* | *2* | *0.00%* | *0* | *0.00%* | *0* | *0.00%* | *0* | *7* |

## *Q13 - What else should a cyber security professional have expertise in regarding this area?*

| *What else should a cyber security professional have expertise in regarding this area?* |
|---|
| *Learn how to learn, active list of resources for key domains* |

## *Q14 - Rate the level of expertise that an entry level cyber security professional should have in each area of Operation and Maintenance.*

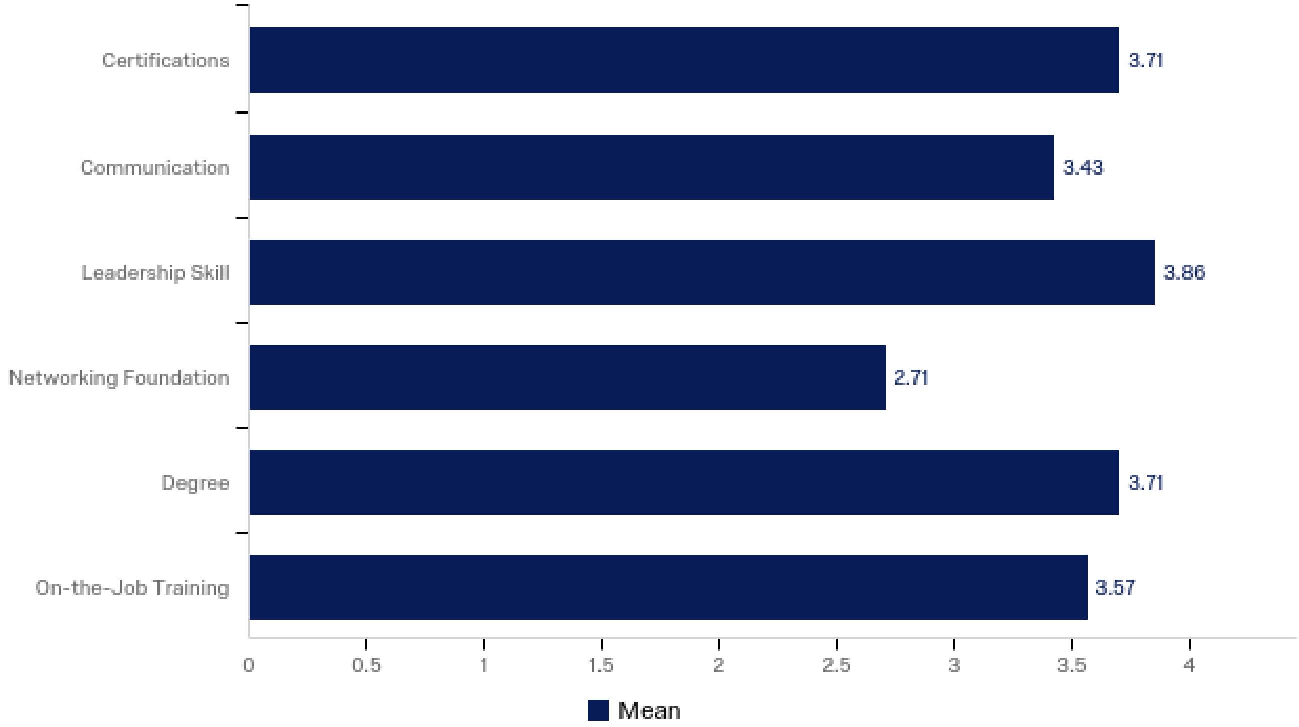


| # | Question | Novice | | Competent | | Proficient | | Master | | Expert | | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | System Administration | 14.29% | 1 | 14.29% | 1 | 57.14% | 4 | 0.00% | 0 | 14.29% | 1 | 7 |
| 2 | Network Services | 0.00% | 0 | 33.33% | 2 | 50.00% | 3 | 0.00% | 0 | 16.67% | 1 | 6 |
| 3 | Customer Service and Technical Support | 0.00% | 0 | 42.86% | 3 | 57.14% | 4 | 0.00% | 0 | 0.00% | 0 | 7 |
| 4 | Systems Security Analysis | 14.29% | 1 | 28.57% | 2 | 57.14% | 4 | 0.00% | 0 | 0.00% | 0 | 7 |
| 5 | Data Administration | 0.00% | 0 | 85.71% | 6 | 14.29% | 1 | 0.00% | 0 | 0.00% | 0 | 7 |
| 6 | Knowledge Management | 0.00% | 0 | 85.71% | 6 | 14.29% | 1 | 0.00% | 0 | 0.00% | 0 | 7 |

## *Q15 - What else should a cyber security professional have expertise in regarding this area?*

| *What else should a cyber security professional have expertise in regarding this area?* |
|---|
| *Cloud & DevOps & DevSecOps Virtualization w/Docker & other containerization tech* |

### *Q16 - Rank-order the seven areas of expertise in the cyber security industry in terms of importance for professionals from 1 (least import) to 7 (most important).*

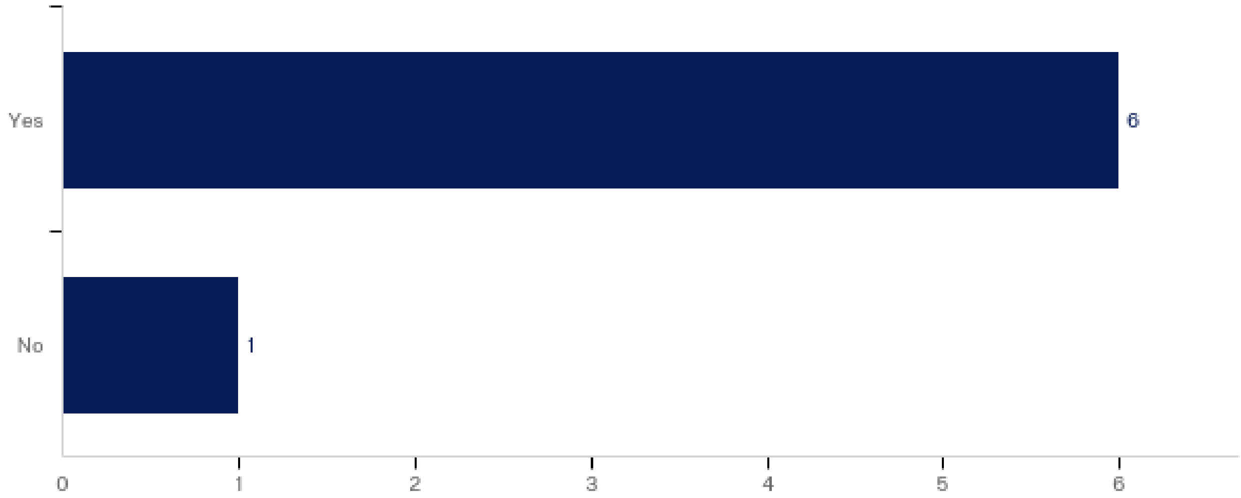


| # | Question | 1 | | 2 | | 3 | | 4 | | 5 | | 6 | | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Certifications | 28.57% | 2 | 0.00% | 0 | 14.29% | 1 | 14.29% | 1 | 14.29% | 1 | 28.57% | 2 | 7 |
| 2 | Communication | 14.29% | 1 | 14.29% | 1 | 28.57% | 2 | 14.29% | 1 | 14.29% | 1 | 14.29% | 1 | 7 |
| 3 | Leadership Skill | 0.00% | 0 | 14.29% | 1 | 0.00% | 0 | 71.43% | 5 | 14.29% | 1 | 0.00% | 0 | 7 |
| 4 | Networking Foundation | 42.86% | 3 | 14.29% | 1 | 14.29% | 1 | 0.00% | 0 | 14.29% | 1 | 14.29% | 1 | 7 |
| 5 | Degree | 0.00% | 0 | 28.57% | 2 | 28.57% | 2 | 0.00% | 0 | 28.57% | 2 | 14.29% | 1 | 7 |
| 6 | On-the-Job Training | 14.29% | 1 | 28.57% | 2 | 14.29% | 1 | 0.00% | 0 | 14.29% | 1 | 28.57% | 2 | 7 |

## *Q17 - Why did you choose this order?*

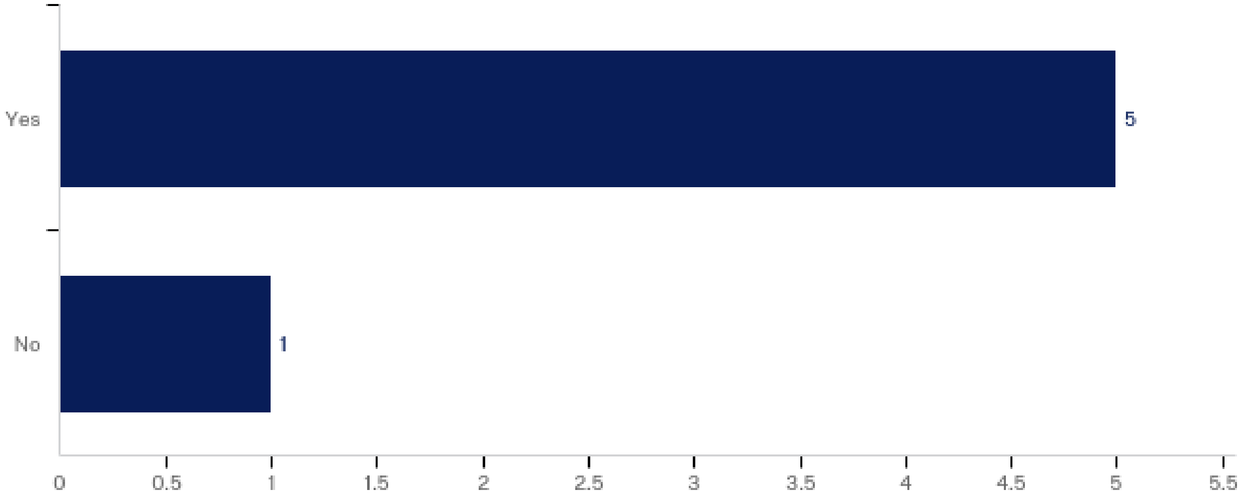
| *Why did you choose this order?* |
|---|
| *Being able to communicate; both delivering the message and understanding the information coming to you.  Entry level cyber security personnel need to understand that ultimately everything they do comes down to a business decision.  understand your organization and the risk tolerance.* |
| *For professionals in cyber security, the skill foundation and on the job training are the keystones to building out the ability to truly interpret the activity being investigated.  I placed certifications and degrees at the bottom not due to their lack of importance, but simply due to the number of 'paper' degree or certification holders I've encountered over the years.  Gaining the knowledge and being able to accurately apply to routine and out of the box scenarios should be the goal rather than the paper showing achievement/completion.* |
| *My experience listening to hiring managers.* |
| *Basic tech skills are key, followed by the ability to communicate, this more than anything will demonstrate their competence* |
| *Fundamental skills don't always come from certs & degrees - they come from real-world experience! If degree is based on real experience that helps* |

## *Q18 - Are you interested in collaborating on projects with other cyber security organizations?*



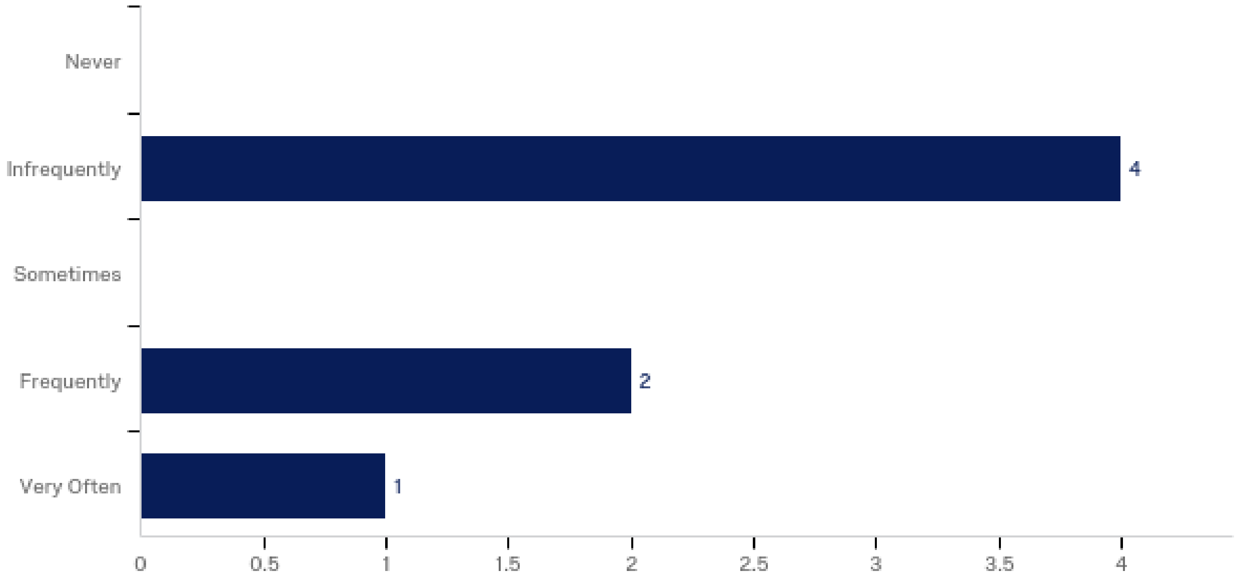
| *#* | *Answer* | *%* | *Count* |
|---|---|---|---|
| *1* | *Yes* | *85.71%* | *6* |
| *2* | *No* | *14.29%* | *1* |
| | *Total* | *100%* | *7* |

## *Q19 - Are you interested in partnerships with other cyber security organizations?*



| *#* | *Answer* | *%* | *Count* |
|---|---:|---:|---:|
| *1* | *Yes* | *83.33%* | *5* |
| *2* | *No* | *16.67%* | *1* |
|  | *Total* | *100%* | *6* |

## Q20 - How frequently does your organization hire any type of cyber security professional?

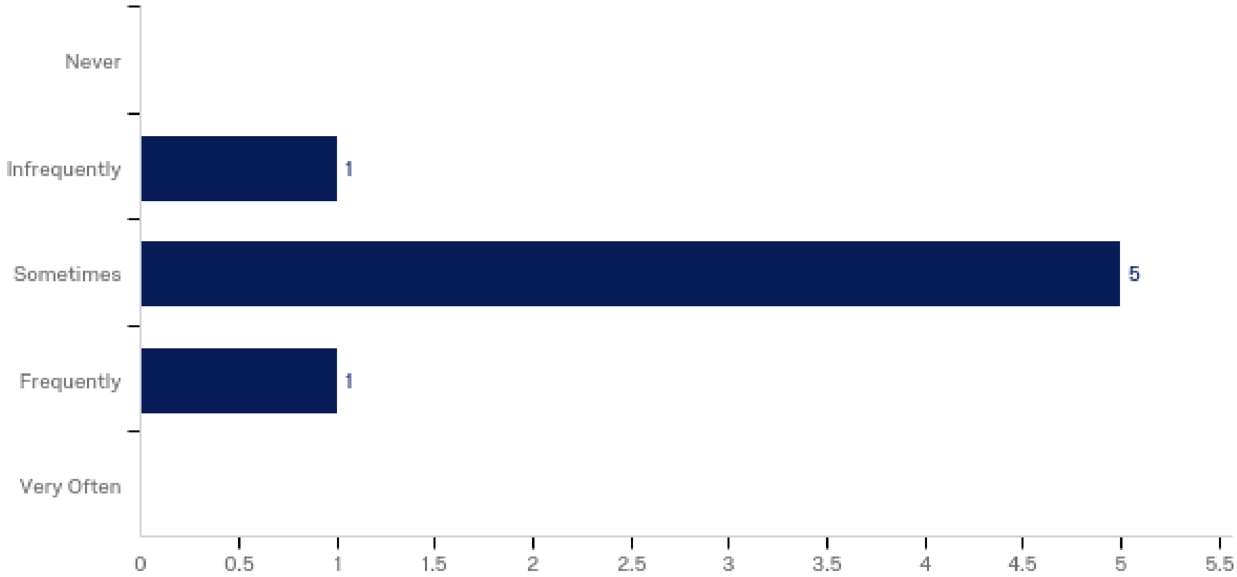


| # | Answer | % | Count |
|---|---|---|---|
| 1 | Never | 0.00% | 0 |
| 2 | Infrequently | 57.14% | 4 |
| 3 | Sometimes | 0.00% | 0 |
| 4 | Frequently | 28.57% | 2 |
| 5 | Very Often | 14.29% | 1 |
|  | Total | 100% | 7 |

## *Q21 - Do you think this should change? Why or why not?*

| *Do you think this should change? Why or why not?* |
|---|
| *We currently have a long tenured team, with a diverse blend of talent and skill.  As the organization continues to grow and evolve, the security team has to keep pace to be successful.  This should not only create opportunities internally but most likely raise the need for additional head count.* |
| *My organization is very small.* |
| *Yes, we need to build the workforce enough to reduce the constant churn* |
| *As we grow we will need dedicated, security employees, but at a small business we hire multi-disciplined i.e. dev w/security, DevOps w/security knowledge* |

### *Q22 - How often does your organization hire an individual with only a 2-year degree in computer science?*

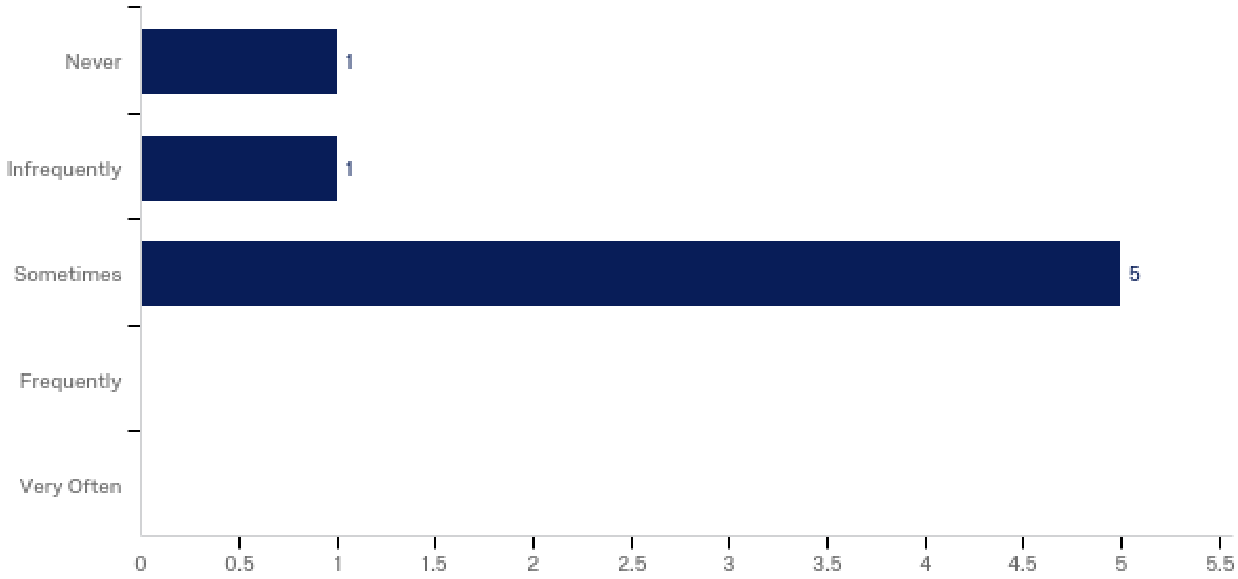


| *#* | *Answer* | *%* | *Count* |
|---|---|---|---|
| *1* | *Never* | *0.00%* | *0* |
| *2* | *Infrequently* | *14.29%* | *1* |
| *3* | *Sometimes* | *71.43%* | *5* |
| *4* | *Frequently* | *14.29%* | *1* |
| *5* | *Very Often* | *0.00%* | *0* |
|  | *Total* | *100%* | *7* |

## *Q23 - Do you think this should change? Why or why not?*

| *Do you think this should change? Why or why not?* |
|---|
| *For me this all comes down to the candidate and the role they are pursuing. If they can demonstrate a high level of proficiency then I have not issue. The challenge for the candidate is getting through a screening process where so many others will have a 4 year degree.* |
| *I think there is a stigma currently attached to those with 2 year degrees of their not having the same ability or drive. I think there should be more inroads into collaboration and getting those with 2 year degrees into cyber security organizations. Perhaps with an understanding to push these folks into a 4 year degree as they are simultaneously gaining work experience.* |
| *fdf* |
| *For recon this would be sufficient.* |
| *No, this is often an appropriate skill level for entry level positions* |
| *We look for capability & experience - not always the degree* |
| *Yes, we need to tear down the misconception that degrees are a pre-req for qualifying talent. They certainly help demonstrate the ability to learn but they're only one piece.* |

## *Q24 - How often does your organization hire someone without prior experience in computer science but has obtained relevant education and/or certification?*

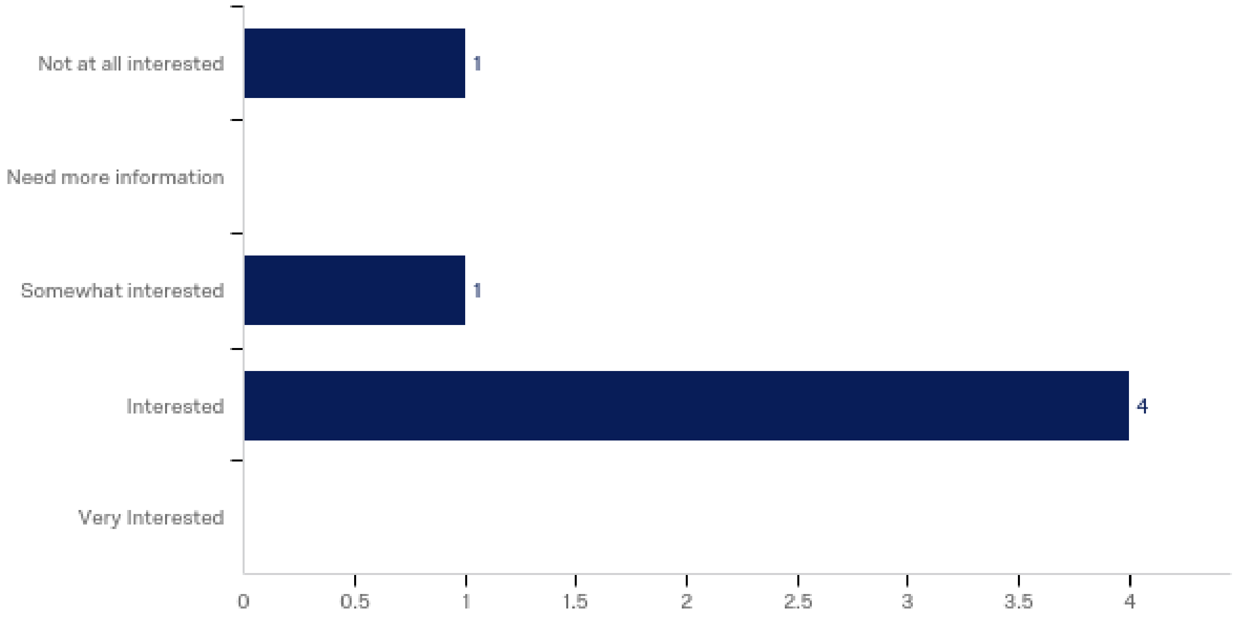


| # | Answer | % | Count |
|---|---|---|---|
| 1 | Never | 14.29% | 1 |
| 2 | Infrequently | 14.29% | 1 |
| 3 | Sometimes | 71.43% | 5 |
| 4 | Frequently | 0.00% | 0 |
| 5 | Very Often | 0.00% | 0 |
|  | Total | 100% | 7 |

## *Q25 - Do you think this should change? Why or why not?*

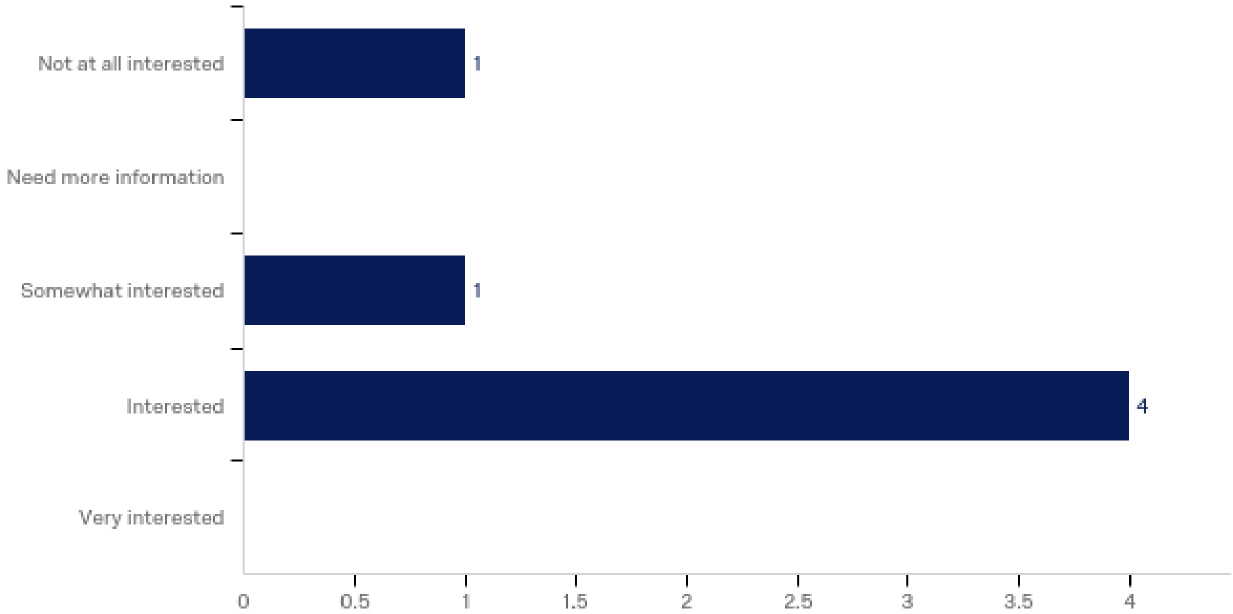
| *Do you think this should change? Why or why not?* |
|---|
| *In today's business climate we need candidates that can make an immediate impact. Some on the job training will always be necessary, but if the perception is that the candidate will require special training, or simply more training, it does not feel like a good investment.* |
| *The majority of new hires within this category are via an intern program where those without prior experience work as interns initially. If their performance is successful, they are often hired.* |
| *Yes, we would prefer to hire fellows with more hands on background to complement their training* |
| *We'd love to hire straight out of college but many lack minimum experience* |
| *Yes, we must think differently.* |

## Q26 - Are you interested in providing development opportunities for current or future employees



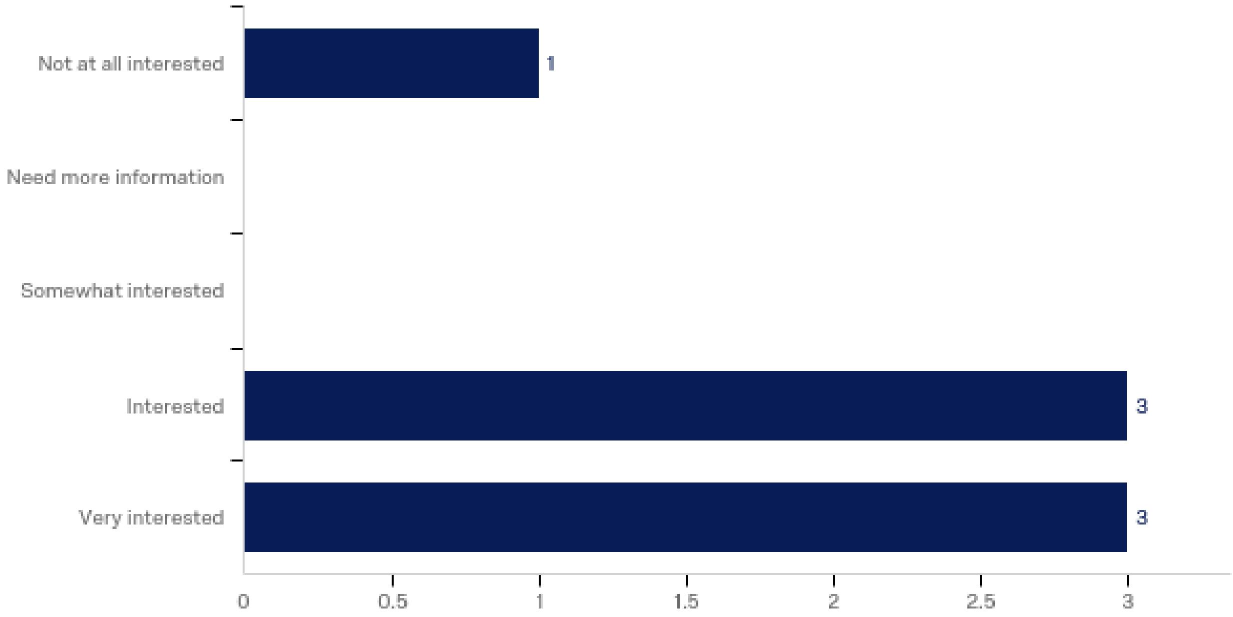
| # | Answer | % | Count |
|---|---|---|---|
| 1 | Not at all interested | 16.67% | 1 |
| 2 | Need more information | 0.00% | 0 |
| 3 | Somewhat interested | 16.67% | 1 |
| 4 | Interested | 66.67% | 4 |
| 5 | Very Interested | 0.00% | 0 |
|  | Total | 100% | 6 |

## *Q28 - What level of interest do you have in providing internship opportunities to students?*



| # | Answer | % | Count |
|---|---|---|---|
| 1 | Not at all interested | 16.67% | 1 |
| 2 | Need more information | 0.00% | 0 |
| 3 | Somewhat interested | 16.67% | 1 |
| 4 | Interested | 66.67% | 4 |
| 5 | Very interested | 0.00% | 0 |
|  | Total | 100% | 6 |

## *Q29 - Would you be interested in developing a successful intern as a paid employee?*



| # | Answer | % | Count |
|---|---|---|---|
| 1 | *Not at all interested* | *14.29%* | *1* |
| 2 | *Need more information* | *0.00%* | *0* |
| 3 | *Somewhat interested* | *0.00%* | *0* |
| 4 | *Interested* | *42.86%* | *3* |
| 5 | *Very interested* | *42.86%* | *3* |
|  | *Total* | *100%* | *7* |

### *Q38 - Please provide your contact information.*

| *Name* | *Title* | *Organization* | *Phone Number* | *email* |
|---|---:|---:|---:|---:|
| *Tony DeAngelo* | *Director, Information Security* | *Motorists Insurance Group* | *614-225-8541* | *tony.deangelo@motoristsgroup.com* |
| *Joe Brown* | *Director, Vulnerability Management* | *Nationwide Insurance SCC* | *614-677-7030* | *brownj5@nationwide.com* |
| *Bill Sempf* | *Application Security Architect* | *POINT* | *614-402-7207* | *bill@pointweb.net* |