CYBRARY

# Hybrid Skills in Cybersecurity

## Educating the Workforce to Advance the Evolution of Future Roles

**AUTHORS:**

Philip H. Kulp | Nikki E. Robinson | Travis D. Howard

*Cybrary Fellowship Research, August 2020*

# Hybrid Skills in Cybersecurity

A Survey of Continuous Learning by Cybersecurity Professionals

## Executive Summary

Cybersecurity roles are transitioning to hybrid jobs composed of technical and soft skills that require practitioners to integrate varying competencies. Practitioners must understand that learning is a journey and not a goal because technology changes so rapidly that new skills must be continuously acquired. The purpose of this study was to survey Cybersecurity and Non-cyber IT professionals to identify the awareness and practice of Hybrid Skills. The analysis of the data focused on understanding if Cybersecurity professionals are currently practicing Hybrid Skills and identify the source of learning. 85% of the participants responded that they relied on self-study to learn new skills, while only 30% of the participants identified a university as the source of continuing knowledge.

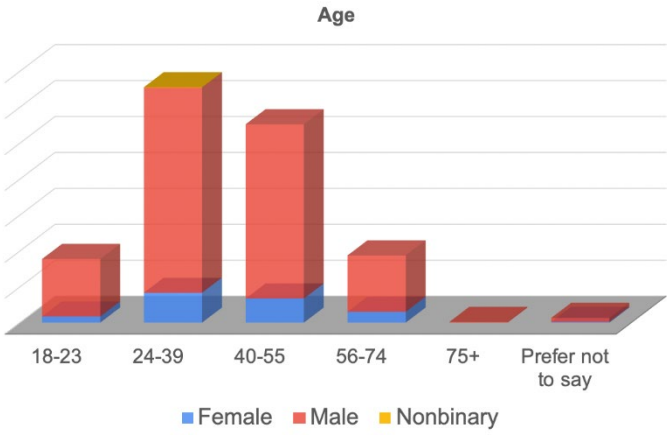
The survey collected data from Cybersecurity and Non-cyber IT professionals to compare responses and identify differences across the industries. The survey responses for respondents' understanding of Hybrid Skills needed for their jobs suggest that Cybersecurity respondents outperform the Non-cyber IT respondents. The respondents were then asked if they review job postings to identify trends in their roles. The results again favored the Cybersecurity respondents. Finally, the responses from Cyber and Non-cyber IT professionals were compared to examine the active implementation of Hybrid Skills in their current roles.

High-level observations from the survey:

- Cyber pros outperformed the expected rate for Hybrid Skills compared to Non-cyber IT roles
- The perception of Hybrid Skills was different than the real-world implementation of the skills
- 85% responded that they rely on self-study which points to a vast market of users hungry for knowledge
- 89% of Cyber pros selected self-study and 75% for certifications as a source of learning
- Both Cyber and Non-cyber IT pros understand the need for continuous learning
- Cyber pros scored poorly in responses for the application of AI and ML skills in their current role
- Cyber pros need to learn statistics and other knowledge to gain Big Data skills
- Data Scientists scored the highest in Hybrid Skills

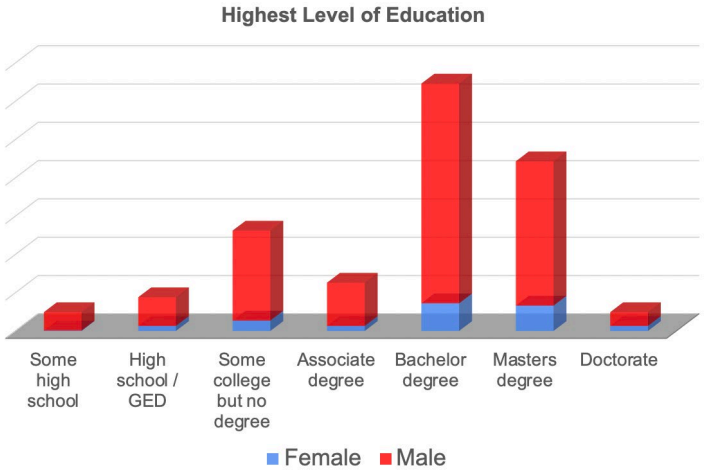
# Demographics

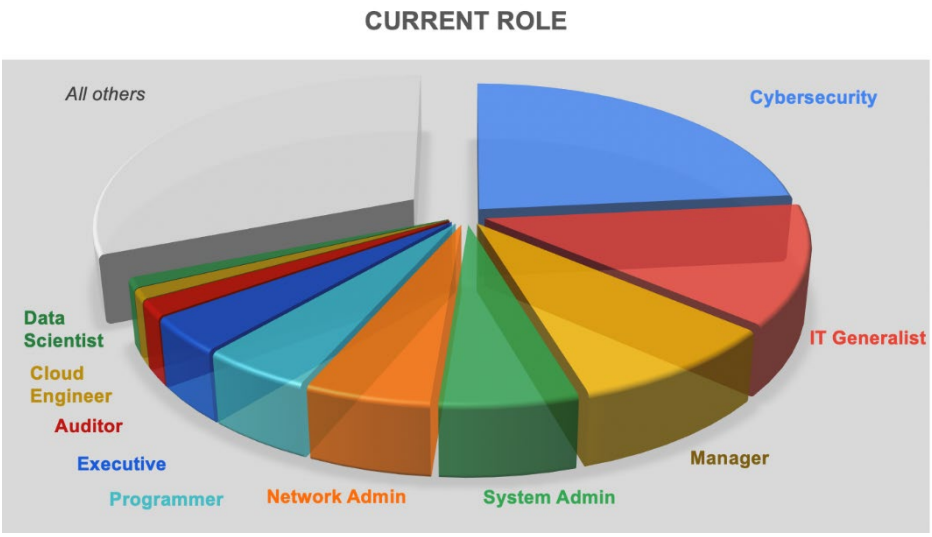
The survey proved to be an overwhelming success with over 1800 people responding from the Cybersecurity and Non-cyber IT roles. Participants reported their age, gender, and the highest level of education achieved. Respondents to the survey also self-reported the title of their current position.




*The largest percentage of the respondents were in the 24-39 age group. A distribution across age and gender groups provided an adequate representation of the Cybersecurity and Non-cyber IT professions. The age group reporting was divided by generations with acceptable representation from the edge cases of Baby Boomers and Generation Z.*

*The most significant portion of the participants had attained a bachelor's degree. 76% of the respondents had achieved at least an associate or higher degree. 39% of the respondents had completed a bachelor's degree, and 27% had a master's degree. These rates are higher than the Census Education Attainment 2019 report percentages of 21% and 9%, respectively. While the average percentage of people in the United States with a doctorate is less than 2%, the respondents in the current survey reported a rate of 3%.*




*Top 10 Reported Roles*

- *25% Cybersecurity*
- *15% IT Generalist*
- *10% Manager*
- *6% System Admin*
- *5% Network Admin*
- *5% Programmer*
- *4% Executive*
- *2% Auditor*
- *1% Cloud Engineer*
- *1% Data Scientist*

# Background

Practitioners must understand that learning is a journey and not a goal because technology changes so rapidly that new skills must be continuously acquired. Automation has been predicted to replace jobs for many years; instead, robots replace tasks and not whole jobs [5]. Workers must contend with multiple factors over a career which could detract from their marketability. Employers must understand those job seekers may also desire careers that are not only challenging but also fulfilling. New professionals entering the workforce are not always looking for the highest paying job; a meaningful job is still attractive. Taking into account the broad aspects of a lifetime of learning, Cybersecurity professionals must create a plan to stay relevant in the job market by monitoring trends and adapting to changes while following a meaningful career path.

## Self-Styled Learning

A combined MITx and Harvardx report on edX identified 66% of registrants as having at least a bachelor's degree [7]. The demographic information portends workers' understanding of the need for further training in specific topics after graduating from a traditional institution. Coding bootcamps and other modular learning opportunities can be leveraged to gain particular skills needed to enhance a career or maintain an existing role. Other forms of modular learning are accessible through Massive Open Online Courses (MOOC) and online learning platforms such as Cybrary. Self-styled learning requires organizational skills and learning from mostly asynchronous material, which may not suit every student. Students must also discover the best methods they need for learning. Students must select the training which will provide a benefit to their current role or position them to meet the requirements of a future job.

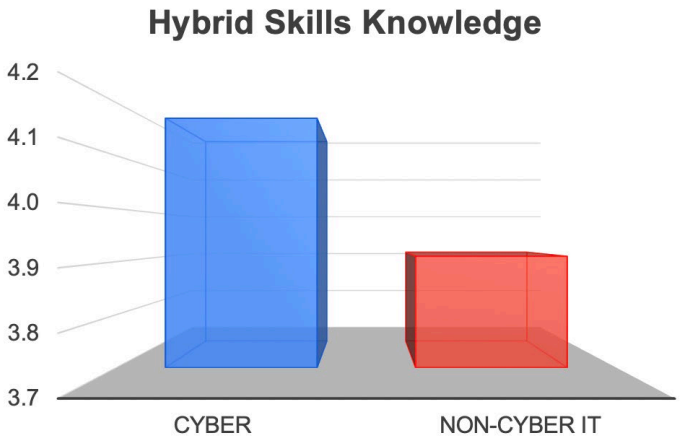
## Hybrid Skills

UC Berkley described data science as the "biggest minor" in the near future, which will prepare students for performing work in other areas of their careers [2]. IT and Cybersecurity roles will require the ability to make sense of data for the business. These jobs will also require the ability to communicate with managers, team members, and engineers on other teams [1]. The jobs of the future will require Hybrid Skills composed of not only hard skills such as data science and statistics, but soft skills such as relationship building, collaboration, and emotional intelligence. The soft and hard skills used in the survey questions were based in part on top competencies Google looks for in candidates [6]. While some jobs may benefit from Hybrid Skills, others may cross functional boundaries and be compromised of skills from diverse fields.

The National Initiative on Cybersecurity Education (NICE) framework created a taxonomy of the terms related to the cybersecurity workforce [4]. While NICE attempted to create a clear distinction among cybersecurity fields, some hybrid jobs already exist, with combined Cybersecurity and Non-cyber IT roles. For example, a cybersecurity legal counsel, privacy compliance officer, or cyber threat intelligence linguist bridge the divide between the law and cybersecurity [3]. As the company's intellectual property and business function become tied to data, cybersecurity awareness will permeate into every role in the organization; cybersecurity hybrid jobs may become the norm.

# Hybrid Skills Analysis

Survey respondents answered questions on a scale from 1 to 5. An answer of 1 represented ***Strongly Disagree,*** and a 5 ***Strongly Agree***. An answer of 3 was a neutral response. The answers were grouped by the respondent's current role for comparison. Questions asked if respondents understood Hybrid Skills and then proceeded with specific examples.




"I understand the hybrid skills needed to maintain my marketability (skills which are not core to my job)."

***The first question was general to see how respondents self-reported. The responses were compared to actual Hybrid Skills to identify the difference between perception and reality.***

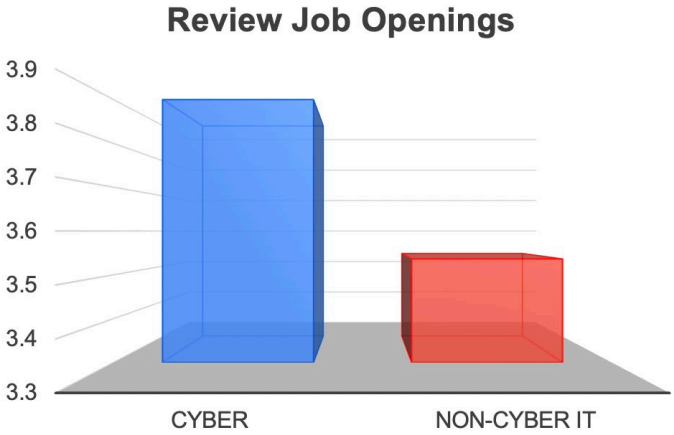
***Cybersecurity respondents reported an average response of 4.2. Non-cyber IT respondents reported an average of 3.9.***

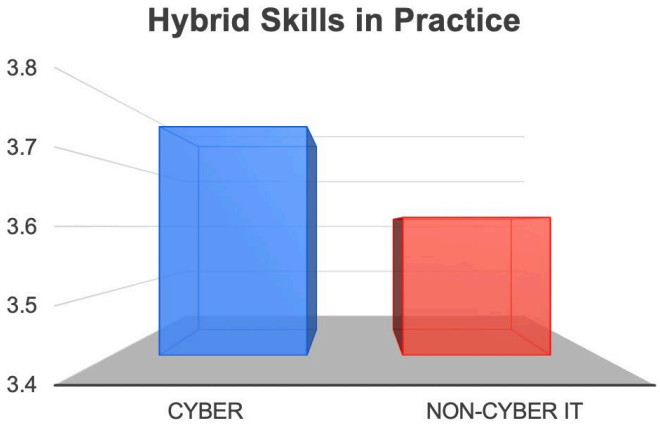
"I review job openings to look for trends in the market."

***The next question was more specific to understand how people discover the Hybrid Job skills they should be learning.***

***Cybersecurity respondents reported an average response of 3.9. Non-cyber IT respondents reported an average of 3.5.***

***A difference between the perceived understanding of Hybrid Skills and the discovery already appeared.***




***Nine questions were asked to understand how practitioners apply Hybrid Skills in their current roles. They were asked about hard skills such as AI, Machine Learning (ML), statistics, and analytic skills. Soft skill questions related to team collaboration, social ability, and emotional intelligence.***

***Cybersecurity respondents reported an average response of 3.8. Non-cyber IT respondents reported an average of 3.6.***

***A further divergence was identified between perceived understanding of hybrid skills and the application of Hybrid Skills in their current role.***

# Conclusions

The responses to the survey were evaluated according to two major themes to determine if a gap exists between the perception that Cybersecurity professionals understand Hybrid Skills and if they are practicing them:

1. Do Cybersecurity professionals understand the Hybrid Skills needed for future jobs?
2. Do Cybersecurity professionals practice Hybrid Skills in their current roles?

The responses were compared between Cybersecurity and Non-cyber IT respondents. The comparison is needed to determine if Cybersecurity professionals are maintaining the skills required to compete in the current and future marketplace. During the compilation of the data, some interesting trends emerged regarding education levels, so further analysis was performed.

### Hybrid Skills Knowledge

Two survey questions were used to measure the understanding of Hybrid Skills. The first question asked respondents, "I understand the hybrid skills needed to maintain my marketability (skills which are not core to my job)." The second was indirect and asked respondents about how they actively tracked job trends with the following questions, "I review job openings to look for trends in the market." The table below includes the average responses to each question and the combined average per reported role.

For both questions, the Chi-square test of homogeneity was used to determine if an equal distribution across the sample could be identified. Cybersecurity professionals exceeded the critical value of both tests, which suggests that the responses comparing Cybersecurity and Non-cyber IT were not evenly distributed. Cybersecurity professionals overperformed the expected rate of self-reported knowledge of the Hybrid Skills needed to maintain marketability by 4.8%. Cybersecurity professionals overperformed the predicted rate by 7.8% when answering the question that they review jobs to understand trends in the market. While the responses to these questions point to encouraging signs for Cybersecurity professionals, the researcher performed additional analysis of the responses.

| Role | Job Openings | Hybrid Skills | Average |
|---|---|---|---|
| Data Scientist | 3.7 | 4.5 | 4.1 |
| Cybersecurity | 3.9 | 4.2 | 4.0 |
| Cloud Engineer | 3.6 | 4.4 | 4.0 |
| System Admin | 3.7 | 4.0 | 3.9 |
| IT Generalist | 3.7 | 3.9 | 3.8 |
| Auditor | 3.5 | 4.0 | 3.7 |
| Network Admin | 3.7 | 3.7 | 3.7 |
| Executive | 3.2 | 4.1 | 3.7 |
| Manager | 3.3 | 3.9 | 3.6 |
| Programmer | 3.2 | 3.9 | 3.6 |

The difference in the responses to the questions presents a possible discrepancy since fewer respondents are reviewing job postings than those which said they understand the skills needed. If respondents are not reviewing the current state of job postings, then how do they know which skills are necessary to maintain marketability? The respondents may have been performing the assessment based on their current role. The overconfidence could also suggest a lack of preparedness for Cybersecurity professionals when they choose which skills to learn.

The responses were separated for each reported role, and the average was calculated. Data Scientists responded with the highest rates, followed by Cybersecurity professionals. An interesting observation was the low ranking for Executives. Upon further review, the data seems to make sense since Executives tend to stay in positions longer than IT professionals, so they would not be searching for job postings. Data Scientists had the highest response values, which is of interest since they also had the highest rate for Hybrid Skills in practice.

## Hybrid Skills in Practice

Nine questions in the survey were used to assess Cybersecurity professionals' practice of Hybrid Skills compared to all other professionals in the IT industry. Some of the questions were related to technical skills such as the use of statistics, Data Science, ML, or AI. Other questions related to soft skills such as team collaboration, artistic, social, and emotional intelligence. The table below includes the averaged responses to each question and the combined average per reported role.

For the nine questions regarding the practice of Hybrid Skills, the same Chi-square test was used to determine if an equal distribution across the sample could be identified. Cybersecurity professionals exceeded the critical value of the test, which suggests that the responses comparing Cybersecurity and Non-cyber IT were not evenly distributed. The Cybersecurity professionals exceeded the expected value of the responses as compared to Non-cyber IT professionals.

| Role | Statistics | Data Science | AI/ML | Collaborate | Business | Creative | Social | Analytic | Emotional | Avg. |
|---|---|---|---|---|---|---|---|---|---|---|
| Data Scientist | 4.5 | 4.7 | 3.6 | 3.9 | 4.1 | 4.4 | 3.9 | 4.9 | 3.5 | 4.2 |
| Executive | 3.6 | 3.1 | 2.8 | 4.4 | 4.4 | 3.8 | 4.6 | 4.6 | 4.2 | 3.9 |
| Cybersecurity | 3.4 | 3.1 | 2.6 | 4.4 | 4.0 | 3.5 | 4.4 | 4.5 | 3.9 | 3.8 |
| Manager | 3.6 | 3.1 | 2.1 | 4.3 | 4.0 | 3.6 | 4.5 | 4.5 | 4.2 | 3.7 |
| Auditor | 3.3 | 3.0 | 2.0 | 4.2 | 4.3 | 3.4 | 4.5 | 4.5 | 4.1 | 3.7 |
| Cloud Eng. | 3.4 | 2.6 | 2.9 | 4.4 | 3.9 | 3.7 | 4.3 | 4.5 | 4.0 | 3.7 |
| IT Generalist | 3.1 | 2.8 | 2.4 | 4.0 | 3.7 | 3.5 | 4.2 | 4.3 | 3.9 | 3.6 |
| SysAdmin | 3.2 | 2.9 | 2.3 | 4.0 | 3.7 | 3.4 | 4.2 | 4.5 | 3.6 | 3.5 |
| Network Admin | 3.2 | 2.7 | 2.3 | 3.7 | 3.5 | 3.3 | 4.1 | 4.2 | 3.7 | 3.4 |
| Programmer | 2.8 | 2.7 | 2.5 | 4.0 | 3.5 | 3.7 | 4.0 | 4.3 | 3.6 | 3.4 |

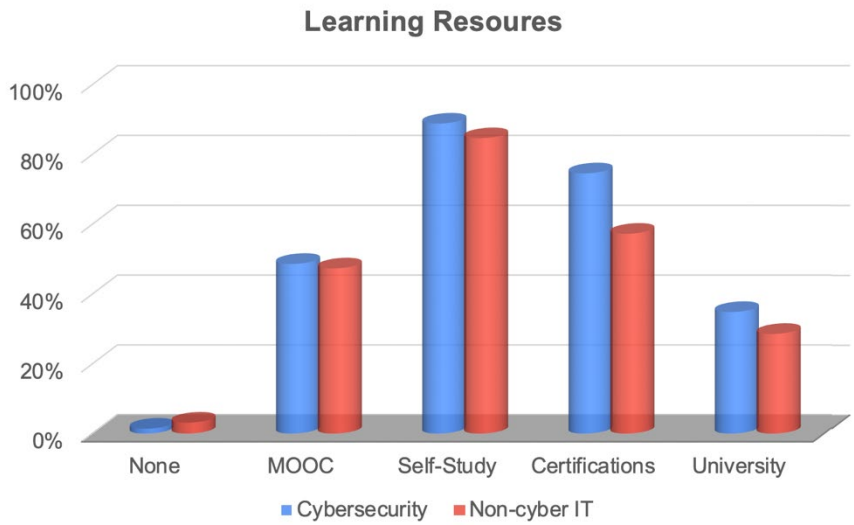
Cybersecurity professionals exceeded the median response in all survey questions except Creative skills and Emotional intelligence. The cumulative Cybersecurity responses ranked above the median for all IT roles reported by the respondents, but the group responses were negative for critical technical Hybrid Skills of Data Science, AI, and ML. These skills are essential for future jobs that require the knowledge to handle Big Data. Cybersecurity professionals need to allocate additional resources to statistics and other mathematical skills required to gain Big Data skills.

## Learning Resources

*"What resources do you use to acquire new skills?"*

Across all industries, 85% selected self-study, 48% selected MOOC, and 62% selected certifications. Only 30% selected universities. These results do not discount the value of higher education since universities build the foundation and structure for a lifetime of learning. The respondents high rate of self-study suggests they understand traditional education is not the end of the experience, and continuous knowledge is a requirement.

A free form field was provided to enter learning resources other than the pre-defined fields. The respondents reported resources such as Cybrary, YouTube, webinars, military, and conferences. Some of the resources such as Cybrary, the military, and conferences are taught by professional educators, but other resources such as YouTube may be taught by practitioners.

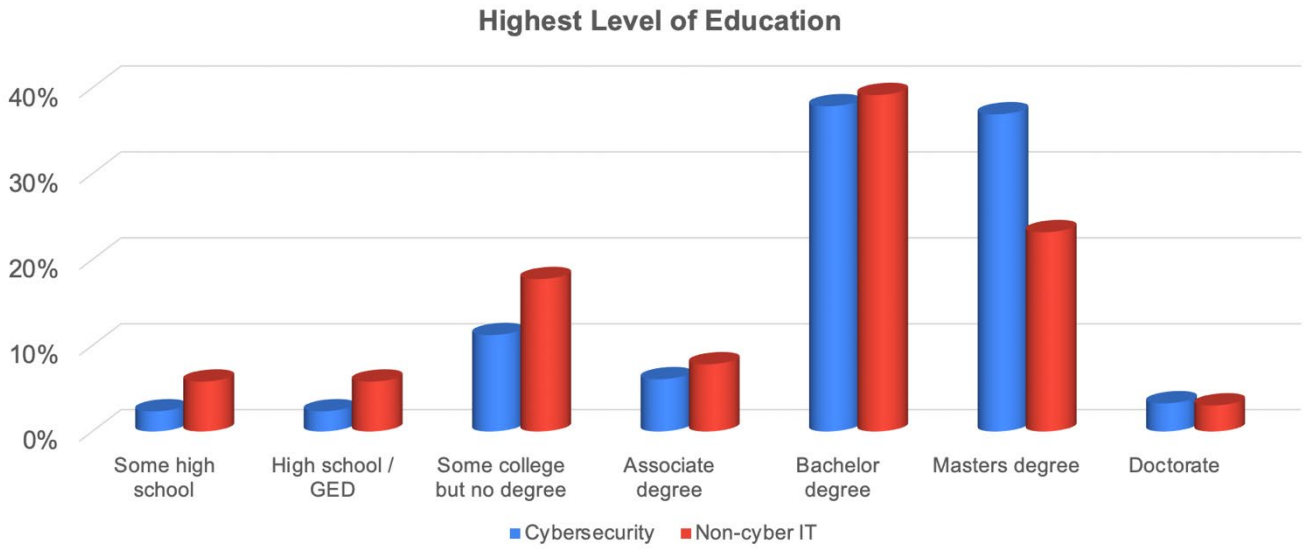



Cybersecurity and Non-cyber IT professional chose 'None' and 'MOOC' at approximately the same rate. 'Self-study' was chosen at similar rates, with Cybersecurity at 89% and Non-cyber IT at 85%. The two groups diverged further when selecting certifications with Cybersecurity responding at 75% and Non-cyber IT at 57%. Some differences were observed with the response for 'University' with Cybersecurity selecting the response 35% and Non-cyber IT at 29%.

The differences between the two groups may be associated with the entrance requirements into the field, either realistic or perceived. The question "How can I break into the cybersecurity field," is encountered continuously by those already in cybersecurity. Cybersecurity professionals do not always point to universities as their source of knowledge for their job, but they responded with higher rates than the Non-cyber IT respondents. With the high response rates of 89% and 75% for self-study and certifications, respectively, cybersecurity professionals appear to understand the need for continuous learning. The need for self-study and attaining certifications may also affect the responses by Cybersecurity professionals to the question regarding how a newcomer can break into the industry.

## Highest Level of Education

After analyzing the results of learning resources, the demographic data for education was re-visited and divided by the job role to review the differences between Cybersecurity and Non-cyber respondents.




Cybersecurity roles reported much lower rates for education below the associate level as compared to Non-cyber IT respondents. These results suggest that Cybersecurity roles require a higher level of education and could support the idea that Cybersecurity roles have a higher threshold for entry into the industry. 6% of Cybersecurity and 8% of Non-cyber IT respondents reported an associate degree as the highest level attained. A bachelor's degree was reported by 38% of Cybersecurity and 39% of Non-cyber IT. The most significant disparity arose at the master's level, with 37% of Cybersecurity and 23% of Non-cyber IT reporting attaining the degree. The two groups then converged at the doctorate level, with 3% of both Cybersecurity and Non-cyber IT roles reporting the highest level of degree attained. This data may explain the reason Cybersecurity professionals reported a higher response rate for university learning in the survey question regarding the resource used for learning.

# About the Author

Dr. Philip Kulp is a Cybrary Fellow and content creator on the Cybrary platform. He has been consulting in cybersecurity for over 20 years and performing other IT roles for over 25 years. In his current role as a cybersecurity architect and incident responder, he combines his passion for IT and cybersecurity to develop realistic approaches to secure the enterprise. He also serves as a secure code reviewer, independent assessor, and webapp tester. Dr. Kulp developed the NIST 800-53 and DevSecOps Fundamentals courses for Cybrary and is actively working on other classes to deliver content for the cyber community. Philip seeks opportunities to balance his cybersecurity skills between academic, technical, and compliance roles. He holds the CISSP certification and two Offensive Security certifications of OSCP and OSCE. In his educational capacity, Philip serves as a chair, committee member, and mentor for doctoral students in the Ph.D. and D.Sc. programs at Capitol Technology. He also serves as an adjunct professor at Drexel University. Dr. Kulp has authored research papers on security for medical drone security, graphing website relationships to predict website security, and the current topic of Hybrid Skills in the cybersecurity community.

## REFERENCES

[1] Bentley University. 2016. 2016 Year of the 'Hybrid Job'. http://www.bentley.edu/prepared/2016-jobskills.

[2] Joyce, L. 2020. Data Science: A 21st Century Job Skill for Every Discipline. https://blog.edx.org/data-science-a-21st-century-job-skill-for-every-discipline/.

[3] Bate, L. 2018. Cybersecurity Workforce Development: A Primer. https://www.newamerica.org/cybersecurity-initiative/reports/cybersecurity-workforce-development/.

[4] National Institute of Standards and Technology. National Initiative for Cybersecurity Education (NICE). https://www.nist.gov/itl/applied-cybersecurity/nice.

[5] The Economist. 2017. Lifelong Learning is Becoming an Economic Imperative. https://www.economist.com/special-report/2017/01/12/lifelong-learning-is-becoming-an-economic-imperative

[6] Elmore, T. 2018. The Seven Top Skills Google Now Looks for in Graduates. https://www.psychologytoday.com/us/blog/artificial-maturity/201807/the-seven-top-skills-google-now-looks-in-graduates.

[7] Ho, A.D., Reich, J., Nesterko, S.O., Seaton, D.T., Mullaney, T., Waldo, J., Chuang, I., 2014. HarvardX and MITx: The First Year of Open Online Courses, Fall 2012-Summer 2013. SSRN Journal. https://doi.org/10.2139/ssrn.2381263