Adult Viewpoints 2021

The Cybersecurity Skills Gap & Barriers To Entry

CHAMPLAIN
COLLEGE
ONLINE /

CONTENTS

SOURCE OF DATA

Champlain College Online commissioned Full Circle Research, INC. to field questions for its online survey from August 24-26, 2021 with a randomized, nationally representative sample of 1,011 U.S. adults ages 20-55.

The results are weighted to the U.S. Census data to be nationally representative with a confidence level of 95%.

1,011 ADULTS

PURPOSE OF SURVEY

The lucrative and fast-growing field of cybersecurity offers information security professionals a plethora of rewarding opportunities. From a competitive median annual salary of $103,590 to more than 460,000 job openings available across the United States, cybersecurity professionals experience an unemployment rate of 0% with endless directions to take their careers.

The purpose of this survey is to examine why an industry projected to grow 33% through 2030 with guaranteed job security is in the midst of a skills gap. Commissioned by Champlain College Online, this survey points to three distinct industry-wide barriers preventing professionals from entering the field of cybersecurity.

In this survey, the top barriers for exploring a career in cybersecurity include:

- High expectations of prior training
- Lack of diversity and inclusion
- Toxic work environment/culture

Additionally, the survey measures key behavioral dimensions including:

- Factors that would motivate individuals to pursue cybersecurity careers
- The positive outcomes and characteristics of cybersecurity careers
- Actions taken to protect and secure personal devices relative to the impact of recent cybersecurity breaches and events

DEMOGRAPHICS

AGE	Total N=1011	Gen Pop X-Cyber Workers N=661 A	Cybersecurity Hiring Managers N=324 B	Cybersecurity Professionals N=252 C
20 to 29 years old	24%	27% B	19%	22%
30 to 37 years old	27%	26%	28%	29%
38 to 45 years old	26%	22%	35% A	35% A
46 to 55 years old	22%	25% BC	18%	14%

GENDER	Total N=1011	Gen Pop X-Cyber Workers N=661 A	Cybersecurity Hiring Managers N=324 B	Cybersecurity Professionals N=252 C
Male-identifying	54%	44%	73% A	78% A
Female-identifying	46%	56% BC	27%	22%
Other	0%	0%	0%	0%

RACE/ ETHNICITY	Total N=1011	Gen Pop X-Cyber Workers N=661 A	Cybersecurity Hiring Managers N=324 B	Cybersecurity Professionals N=252 C
Asian or Pacific Islander	4%	3%	4%	4%
Black, non-Hispanic	7%	7%	6%	6%
Native American or Alaska Native	2%	1%	2%	3%
Caucasian, non-Hispanic	69%	71% C	66%	63%
Caucasian, Hispanic	15%	13%	19% A	21% A
Multi-Ethnic	2%	2%	1%	1%
Other	3%	3%	2%	2%

EDUCATION	Total N=1011	Gen Pop X-Cyber Workers N=661 A	Cybersecurity Hiring Managers N=324 B	Cybersecurity Professionals N=252 C
Less than high school degree or GED	3%	4% B	2%	3%
High school degree or GED	19%	22% BC	13%	11%
Some college, but no degree	17%	22% BC	8%	7%
Associate degree	11%	11%	10%	8%
Bachelor’s degree	28%	28%	26%	27%
Master’s degree	20%	11%	39% A	42% A
Doctoral degree/PhD	2%	1%	3%	3%

KEY SURVEY FINDINGS

BARRIER #1: HIGH EXPECTATIONS OF PRIOR TRAINING OR EXPERIENCE

54% of non-cyber respondents considering a career in cyber say high expectations for past training impede them from working in cybersecurity.

Of the respondents highly likely (25%), likely (21%), or maybe likely (27%) to pursue a career in cybersecurity, 54% of U.S. survey respondents not currently working in cybersecurity roles feel that high expectations for past training or experience impede them from pursuing cybersecurity as a career.

86% of survey respondents who identify as cybersecurity hiring managers indicate that the market expects entry-level cyber candidates to have vast industry experience.

Of the survey respondents who identify as hiring managers in the field of cybersecurity, 86% of them say there is an expectation in the cyber job market that candidates applying for entry-level cyber jobs have vast industry experience already.

72% of respondents estimate some type of university accreditation is required to enter the field of cybersecurity.

A majority of survey respondents (72%) estimate that in order to enter the field of cybersecurity, some level of university accreditation is necessary. More specifically, 28% of respondents believe a bachelor's degree is necessary, 16% believe a master's degree is necessary, and 28% believe any level of education from a college or university is necessary to work in cybersecurity.

77% of hiring managers estimate some type of university accreditation is required to enter the field of cybersecurity.

More than three-quarters of hiring managers working in the field of cybersecurity say some level of university accreditation is required to enter the field of cybersecurity. Similarly, 80% of cybersecurity professionals working in the industry estimate that university accreditation at some level is required to become a cybersecurity professional.

63% **of survey respondents believe more people need to become educated in cybersecurity.**

When asked which measures are needed to improve cybersecurity, 63% of survey respondents say more people need to become educated in cybersecurity.

69% **of cyber hiring managers believe organizations need to invest in cybersecurity internally.**

When asked how to address the current challenges facing the field of cybersecurity today, 69% of cyber hiring managers say they believe organizations need to invest in cybersecurity internally.

TAKEAWAYS

It is evident that individuals currently working in the field of cybersecurity, as well as individuals who are not, all agree some level of cyber training is required in order to become a cybersecurity professional.

A whopping 86% of survey respondents who identify as cyber hiring managers say there's an expectation in the cyber market that candidates applying for entry-level cyber jobs have vast industry experience already. Similarly, 54% of survey respondents who do not currently work in the cybersecurity industry say high expectations of past training hold them back from entering the cyber workforce. The vast industry experience expected of cyber professionals is a concern shared by Sérgio Tenreiro de Magalhães, Ph.D., co-chair of the cybersecurity programs at Champlain College Online. "I believe that organizations with larger IT departments have a social responsibility to contribute to solving this problem," says Dr. Tenreiro de Magalhaes, "[and could do so]...by establishing a hiring quota for qualified, non-experienced cybersecurity professionals." It is clear there is interest in - and demand for - organizations to make room for non-experienced individuals to work in cyber roles by learning on the job.

Even so, survey results indicate that an expectation of past training remains. Of the total population surveyed, 28% of respondents say a bachelor's degree is necessary to enter the field. Moreover, 29% of cyber hiring managers say a master's degree is required, with even more cybersecurity professionals identifying the master's level as the necessary qualification to enter the field (33%).

With 63% of overall survey respondents agreeing that more people need to become educated in cybersecurity, it is clear there is a need for individuals to invest in some level of education or training to become cyber professionals. An individual's best resource — as colleges and universities are well-equipped to provide the tech-focused education, industry-driven knowledge, and relevant expertise necessary for today's professionals to thrive in the cyber workforce — is to select a degree program that combines knowledge with hands-on learning experiences.

BARRIER #2: LACK OF DIVERSITY AND INCLUSION

90% of respondents believe it is important to increase diversity in the cyber workforce.

The percentage of people who believe it is "very important" or "somewhat important" to increase diversity in the cyber workforce is 90%. The percentage is higher among cybersecurity hiring managers and cybersecurity professionals currently working in the field of cybersecurity, with 94% of cyber professionals and 96% of cyber hiring managers ranking the importance of increasing diversity in cyber as "very important" or "somewhat important."

36% of all survey respondents say there needs to be more diversity of experience, race, and gender in cybersecurity.

When asked which actions are required to address current challenges in the field of cybersecurity, 36% of all survey respondents say there needs to be more diversity of experience, race, and gender.

59% of respondents say female-identifying individuals need more representation in cybersecurity.

When survey respondents were asked which minority groups needs more representation in the field of cybersecurity, 59% of survey respondents agreed that female-identifying individuals require more representation.

57% of respondents say people of color need more representation in cybersecurity.

Coming in at a close second, 57% of survey respondents agreed that black, indigenous, and people of color (BIPOC) require more representation in the cyber workforce.

28% **of respondents believe minorities earning lower wages than similarly skilled/experienced colleagues is the main barrier impacting diversity in the cyber workforce.**

When it comes to barriers impacting diverse cyber professionals, 28% of overall survey respondents say that the main barrier is minorities are paid lower wages compared to similarly skilled/experienced colleagues. Twenty-seven percent of survey respondents say limited entry-level roles for minorities is another big barrier impacting diversity in the industry. 25% of overall respondents say that toxic work environments/culture impact diverse cyber professionals, with this barrier ranking higher among cyber hiring managers (33%) and other cyber professionals (34%). Finally, 20% of overall survey respondents say that fewer opportunities for career advancement compared to similarly skilled/experienced colleagues is another barrier impacting diversity in the cyber workforce.

80% **or more of respondents say it is "very important" or "somewhat important" to improve workplace trends to increase diversity in cyber.**

When asked to rate five different workplace culture trends in terms of how important it would be to improve them to increase diversity, 84% of survey respondents feel improving toxic work environments is the most important; 83% of individuals believe there is a lack of growth opportunities for minority groups; 82% say there is an expectation that entry-level candidates must have vast industry knowledge and experience; 82% believe there is a lack of diverse leadership in the industry at large; and 80% say the cyber workforce lacks diversity overall. It is worth noting that all of these figures were ranked even higher among survey respondents who identify as cyber hiring managers and cyber professionals.

44% **of respondents believe it will take five to 10 years before the cyber workforce becomes diverse.**

When it comes to estimating how long it will take to diversify the cybersecurity workforce, 44% of survey respondents believe it will take five to 10 years.

28% **of all survey respondents say that in order to improve cybersecurity, there needs to be more diversity.**

When it comes to identifying the measures needed to improve cybersecurity, 28% of all survey respondents say there needs to be more diversity in cyber.

TAKEAWAYS

Nearly all (90%) of survey respondents agree that it's important to diversify the cyber workforce. A whopping 80% of individuals believe more needs to be done to improve toxic workplaces to, in turn, increase diversity in cyber workforces. Nearly 60% of respondents say more should be done to encourage female-identifying individuals to enter the field of cybersecurity, as well as 57% of respondents say BIPOC (black, indigenous, people of color) require more representation. Moreover, 36% of survey respondents say, in addition to race and gender, there needs to be more diversity of experience in cyber.

To combat the systemic and disproportionate representations of female-identifying and BIPOC individuals in the cyber workforce, more efforts need to be made by cyber organizations to collaborate and partner with institutions that support women in cyber and BIPOC in cyber. A few organizations that support these efforts include:

- **Women in Cybersecurity (WiCyS):** This organization aims to bring women together from academia, research, and the private sector for knowledge sharing, networking, and mentoring in the field of cybersecurity in service of recruiting, retaining, and advancing the careers of women in cyber.

- **International Organization of Black Security Executives (IOBSE):** This leading organization for minority security professionals aims to impart professional resources on minorities in cyber by assisting them in their professional endeavors of networking, exchanging information and ideas, and gaining knowledge and experiences in cybersecurity.

- **Cyversity:** This organization aims to achieve consistent representation of women and underrepresented minorities in cyber through programs that diversify, educate, and empower professionals.

In addition to cyber organizations partnering and collaborating with institutions committed to diversifying the cyber workforce, more can be done at an elementary level to encourage young girls to explore their potential interests in science, technology, engineering, the arts, and mathematics (STEAM-based learning). Based on data collected by the U.S. Census Bureau in January 2021, women account for nearly half the U.S. workforce but only 27% of science, technology, engineering, and math (STEM) professionals are women. Too often women shy away from or are discouraged from exploring STEM careers and continue to be vastly underrepresented in the STEM workforce. If more young girls were encouraged to pursue STEM/STEAM-based learning from an early age, perhaps there would be more women in cyber and in the tech industry at large.

BARRIER #3: TOXIC WORK ENVIRONMENT

81% of respondents feel toxic work environments would prevent them from exploring a career in cybersecurity.

For overall survey respondents, 81% say it is "very important" to improve toxic work environments in the field of cybersecurity in order to consider a career in the industry. The percentage is higher among individuals currently working in the field, with cyber hiring managers coming in at 88% and cyber professionals at 89%, noting that toxic work environment in the industry is "very likely" to prevent them from exploring cyber careers.

44% of respondents likely to pursue a career in cyber say that toxic work environments impede their decision to explore cybersecurity careers.

Of the respondents highly likely (25%), likely (21%), or maybe likely (27%) to pursue a career in cybersecurity, 44% of U.S. survey respondents said that the trend of toxic work environments/ cultures often found in cyber workforces impedes them from selecting cybersecurity as a career.

84% of all survey respondents rated toxic work environments as "very important" or "somewhat important" to improve to increase diversity.

When asked to rate cyber workplace trends on their importance in increasing diversity in cyber, 84% of all survey respondents rated toxic work environment/culture as "very important" or "somewhat important." Moreover, 90% of respondents who work as cyber professionals or cyber hiring managers agree.

TAKEAWAYS

An overwhelming majority of respondents (81%) feel the toxic work environments commonly associated with cyber workplaces would prevent them from exploring a career in cybersecurity. Moreover, of the survey respondents likely to consider a career in cyber, 44% say that the toxic work environments of cyber organizations impede their decisions to actually explore cyber careers. These figures are astounding when looking at the total population level for all survey respondents but they're even more concerning when the focus narrows to respondents who identify as cyber professionals or cyber hiring managers. These individuals, 90% to be precise, say that toxic work environments are "very important" or "somewhat important" to improve, especially when it comes to increasing diversity in cyber.

FACTORS THAT MOTIVATE INDIVIDUALS TO PURSUE CAREERS IN CYBERSECURITY

56%

Of the non-cyber respondents who showed interest in pursuing a career in cybersecurity, 56% said employer-sponsored training and education would motivate them to select a career in cyber.

46%

Nearly half of the non-cyber respondents interested in cyber careers mentioned tuition assistance from an employer would be a motivating factor to pursue a career in the field of cybersecurity.

54%

More than half of the non-cyber respondents who demonstrated an interest in working as a cybersecurity professional said they would consider a career in cyber if they were ever looking for a career change.

25%

A quarter of non-cyber individuals interested in cyber careers said a major cybersecurity event would motivate them to consider a career in cybersecurity.

TAKEAWAYS

Many non-cyber survey respondents would be motivated to pursue careers in cybersecurity if employer-sponsored training and education were available to them (56%) or their employer offered a tuition assistance program (46%). Moreover, more than half of non-cyber survey respondents (54%) said they would consider a career in cybersecurity if they were ever considering a career change, which suggests the industry is appealing to these individuals.

THE POSITIVES OF A CAREER IN CYBERSECURITY

69%

The majority of survey respondents ranked job security as the top positive trait about cyber careers.

61%

More than half of survey respondents said that protecting consumers from hackers is one of the top positives about working in cybersecurity roles.

58%

About 58% of survey respondents ranked career growth as one of the top positives about working in cyber.

52%

Roughly half of the overall survey pool said serving national security is a positive outcome of working in cybersecurity careers.

49%

About half of survey respondents deemed lucrative salaries as a positive of working in cybersecurity roles.

38%

More than one-third of survey respondents said that a broad application of skills across all industries is a positive outcome of working in the industry.

TAKEAWAYS

Surprisingly, cyber professions having lucrative salaries was not the top contender when it came to survey respondents ranking the positives of a career in cyber. About half of the respondents deemed high salaries as a positive outcome, but most respondents were more inclined to rank job security (69%), protecting consumers from hackers (61%), and career growth (58%) as more important positives associated with cybersecurity careers. With 52% of respondents saying serving national security is a positive outcome of a cyber career, individuals appear to be interested in roles that impact the greater good.

IMPACT OF RECENT CYBERSECURITY EVENTS ON SURVEY RESPONDENTS

55%

More than half of the total sample of survey respondents updated their passwords or activated two-factor authentication in response to recent cyber events.

49%

About half of the respondents actively read about cybersecurity to learn how to best protect themselves.

27%

Twenty-seven percent of survey respondents said they signed up for an identity protection service in response to recent cybersecurity breaches.

21%

Nearly one-quarter of respondents said they have taken no action in response to recent cyber events.

19%

About 19% of respondents said recent cyber attacks have prompted them to register for a cyber training program.

17%

Roughly 17% of survey respondents said recent cyber events have prompted them to consider a career in cybersecurity.

TAKEAWAYS

In response to recent cyber events, all survey respondents have taken some action. Perhaps unsurprisingly, the majority (55%) updated their passwords and/or activated two-factor authentication to protect their devices and accounts. This responsive action was higher among cyber hiring managers (63%) and cyber professionals (63%) who perhaps are more inclined to take action given that they work in the cyber industry and greater understand the need for strong password protection.

TAKEAWAYS CONTINUED

About half (49%) say they're actively reading about cybersecurity best practices to better protect themselves on their own. Again, this response is higher among individuals currently working in the field of cybersecurity, with 70% of cyber hiring managers and 73% of cyber professionals saying they read about how to best protect themselves from cyber attacks. The survey did not consider whether this reading was on their own or the byproduct of their careers and working in cybersecurity.

It is especially interesting that 21% of respondents say they have not taken any action to protect their accounts in response to recent cyber events, which suggests they either do not know how to best protect their accounts and devices or they are not concerned about their devices and accounts remaining unprotected. Unsurprisingly, this figure is lower among cyber professionals with only 6% of cyber hiring managers and a mere 4% of cyber professionals reporting that recent cyber events did not inspire them to take action. Perhaps the only surprise here is that these figures are not closer to 0% since cyber professionals understand the danger of cyber attacks. One might speculate these individuals did not take action because they have already used their knowledge of cyber hygiene and security best practices to protect themselves to the extent possible.

The remaining groups of survey respondents say that since recent cyber events have taken place, they have either signed up for an identity protection service (27%), registered for a cyber training program (19%), or are going so far as to consider a career in cybersecurity (17%).

CONCLUSION

Our findings paint a complex picture of the state of the cybersecurity industry today, especially as it relates to the cyber skills gap. Despite a lucrative median annual salary of $103,590 and more than 460,000 job openings available across the United States, only 11% of the general population say they are “highly likely” to consider a career in cybersecurity and 17% say they are “likely.” It is evident through our findings that high expectations of prior cyber experience, lack of diversity in cyber organizations, and toxic work environments are some of the most significant barriers preventing individuals from actively pursuing a career in cybersecurity.

However, our findings also reveal that there are ample opportunities to motivate individuals to pursue cyber careers. Survey respondents show great interest in the positives that come with a career in cyber, including job security (69%), protecting consumers from hackers (61%), career growth (58%), serving national security (52%), and lucrative salary (49%). It’s evident that there are characteristics of cyber professions that individuals are drawn to, and that might serve as motivators if other workforce factors were addressed and improved.

For example, survey respondents who do not currently work in cyber, but are interested in cyber, say that employer-sponsored training and education (56%) and employer tuition assistance (46%) would motivate them to actively pursue cybersecurity careers. Additionally, non-cyber survey respondents state that if current cyber workplace trends — including toxic work environments (82%), lack of growth opportunities for minority groups (81%), lack of diverse leadership in the industry (80%), and the expectation that entry-level candidates have vast industry experience already (80%) — were improved, they would be more likely to pursue cyber as a career, as these current workplace trends are deemed “very important” or “somewhat important” to address.

Given the state of the nation’s cybersecurity workforce today, systemic changes need to be implemented to motivate individuals to fill the hundreds of thousands of job openings in the cyber industry nationwide. Organizations across the country have work to do to make cyber professions more appealing by encouraging women and minorities to pursue cyber careers, addressing the toxic work environments cyber professionals face, and reviewing the entry-level knowledge requirements and expectations of cyber candidates. Reviewing minority representation, hiring qualifications, and employer-sponsored education and training programs are a few places organizations can start to have a positive impact on attracting and retaining cyber talent in the future.

SURVEY APPENDIX

Following is a complete list of the findings of the Champlain College Online survey.

SUMMARY FINDINGS

Survey population: n=1,011 US Adults
Fielded August 2021 for Champlain College Online

APPENDIX

Q.1) Do you feel companies are doing enough to protect your information?

	Total N=1011	Gen Pop X-Cyber Workers N=661 A	Cybersecurity Hiring Managers N=324 B	Cybersecurity Professionals N=252 C
Definitely	24%	13%	46% A	55% A
I think so	40%	45% BC	29%	25%
Not really	31%	37%	20%	16%
No, definitely not	5%	5%	5%	4%

Q.2) What measures should be taken to improve cybersecurity and protect our data? (Select all that apply)

	Total N=1011	Gen Pop X-Cyber Workers N=661 A	Cybersecurity Hiring Managers N=324 B	Cybersecurity Professionals N=252 C
Organizations need to invest in cybersecurity internally	67%	62%	76% A	78% A
More people need to become educated in cybersecurity	63%	63%	64%	63%
The government needs to play a bigger role in cybersecurity	47%	44%	53% A	55% A
We need more cybersecurity experts	41%	44% BC	35%	33%
There needs to be more diversity in cybersecurity	28%	25%	32% A	36% A

Note: Multiple response variable. Responses sum to more than 100%.

Q.3) How important do you think it is to increase diversity in the cyber workforce?

	Total N=1011	Gen Pop X-Cyber Workers N=661 A	Cybersecurity Hiring Managers N=324 B	Cybersecurity Professionals N=252 C
Very important	60%	52%	77% A	80% A
Somewhat important	30%	36% BC	17%	16%
Not very important	5%	7% BC	2%	2%
No importance to me	5%	6% BC	3%	2%

Q.4) What barriers do you expect more prominently impact diverse cyber workers? (Rank #1)

	Total N=1011	Gen Pop X-Cyber Workers N=661 A	Cybersecurity Hiring Managers N=324 B	Cybersecurity Professionals N=252 C
Lower wages than similarly skilled/experienced colleagues	28%	27%	29%	28%
Limited entry level roles	27%	30% BC	21%	20%
Toxic work environment/culture	25%	22%	33% A	34% A
Few opportunities for career advancement compared to similarly skilled/experienced colleagues	20%	22%	18%	18%

Q.5) Which workplace culture trends are most important to improve in order to increase diversity in cybersecurity?

%Very/Somewhat Important	Total N=1011	Gen Pop X-Cyber Workers N=661 A	Cybersecurity Hiring Managers N=324 B	Cybersecurity Professionals N=252 C
Toxic work environment/culture	84%	82%	90% A	90%A
Lack of growth opportunities for minority groups	83%	81%	87% A	87% A
Expectation that entry level candidates have vast industry experience already	82%	80%	86% A	87% A
Lack of diverse leadership in the industry	82%	80%	88% A	87% A
Lack of workforce diversity	80%	77%	87% A	88% A

Q.6) Would trends in _______ prevent you from exploring a career in cybersecurity?

%Highly/Very Likely to prevent seeking a career	Total N=Varies	Gen Pop X-Cyber Workers N=Varies A	Cybersecurity Hiring Managers N=Varies B	Cybersecurity Professionals N=Varies C
Toxic work environment/culture	81%	77%	88% A	89% A
Expectation that entry level candidates have vast industry experience already	79%	75%	86% A	86% A
Lack of growth opportunities for minority groups	71%	64%	83% A	81% A
Lack of workforce diversity	68%	62%	80% A	80% A
Lack of diverse leadership in the industry	68%	60%	80% A	81% A

Q.6_B) Which minority group needs more representation in the cybersecurity workforce?

	Total N=1011	Gen Pop X-Cyber Workers N=661 A	Cybersecurity Hiring Managers N=324 B	Cybersecurity Professionals N=252 C
Female-identifying	59%	61%	58%	56%
Black, Indigenous, and People of Color (BIPOC)	57%	56%	58%	60%
Disabled-identifying	41%	45% BC	35%	31%
Lesbian, Gay, Bisexual, Transgender, Queer or Questioning (LGBTQ+)	41%	42%	39%	41%
Other	10%	10%	9%	10%

Note: Multiple response variable. Responses sum to more than 100%.

Q.7) How long do you foresee it taking for the cybersecurity industry to become diverse?

	Total N=1011	Gen Pop X-Cyber Workers N=661 A	Cybersecurity Hiring Managers N=324 B	Cybersecurity Professionals N=252 C
0-5 years	31%	35% BC	24%	21%
5-10 years	44%	41%	50% A	51% A
10-15 years	15%	14%	16%	19% A
15+ years	7%	7%	7%	7%
Other	4%	4%	2%	2%

Q.8) Have recent cybersecurity events led you to...

	Total N=1011	Gen Pop X-Cyber Workers N=661 A	Cybersecurity Hiring Managers N=324 B	Cybersecurity Professionals N=252 C
Update your password or use two-factor authentication?	55%	52%	63% A	63% A
Read about cybersecurity and how you can protect yourself?	49%	38%	70% A	73% A
Sign up for an identity protection service?	27%	21%	39% A	40% A
I have taken no action.	21%	30% BC	6%	4%
Register for a cyber training program?	19%	12%	31% A	35% A
Consider a career in cybersecurity?	17%	9%	33% A	37% A
Other	0%	<0.5%	1%	1%

Note: Multiple response variable. Responses sum to more than 100%.

Q.9) Would you currently consider pursuing a career in cybersecurity?

	Total N=1011	Gen Pop X-Cyber Workers N=661 A	Cybersecurity Hiring Managers N=324 B	Cybersecurity Professionals N=252 C
Highly likely	25%	11%	52% A	61% A
Likely	21%	17%	28% A	30% A
Maybe	27%	35% BC	13%	8%
Not likely	18%	25% BC	5%	<0.5%
Definitely not	9%	12% BC	2%	0%

Q.10) What would motivate you to pursue a cyber role?

Base: Highly likely, likely, maybe consider career in cybersecurity	Total N=741	Gen Pop X-Cyber Workers N=413 A	Cybersecurity Hiring Managers N=302 B	Cybersecurity Professionals N=251 C
Employer-sponsored training and education	59%	56%	62%	65% A
Employer tuition assistance	51%	46%	59% A	60% A
Looking for a career change	49%	54% BC	42%	38%
Reaction to major cyber event	32%	25%	42% A	41% A
In response to layoff / job loss	18%	22% A	13%	14%
Other	1%	1%	1%	0%

Q.11) Which of the following would impede your decision to pursue a cybersecurity career?

Base: Highly likely, likely, maybe consider career in cybersecurity	Total N=741	Gen Pop X-Cyber Workers N=413 A	Cybersecurity Hiring Managers N=302 B	Cybersecurity Professionals N=251 C
High expectations for past training or experience	58%	54%	63% A	67% A
Lack of work/life balance	46%	49%	42%	42%
Toxic work environment/culture	44%	46%	42%	41%
No employer support for tuition assistance or training	36%	39% B	32%	33%
Lack of diversity	28%	28%	27%	27%
Lack of growth opportunities for minority groups	23%	25%	22%	20%
Other	2%	2%	1%	1%

Q.12) What education do you think is needed to enter the cybersecurity field?

	Total N=1011	Gen Pop X-Cyber Workers N=661 A	Cybersecurity Hiring Managers N=324 B	Cybersecurity Professionals N=252 C
No education level required if they've had on-the-job training	9%	9%	6%	6%
High school diploma or equivalent	15%	17% BC	12%	10%
Bootcamp/non-credit training	4%	4%	4%	4%
Certification/Certificate from an accredited college or university	28%	32% BC	20%	19%
Bachelor's degree from an accredited college or university	28%	27%	28%	28%
Master's degree from an accredited college or university	16%	10%	29% A	33% A
Other	1%	1%	0%	0%

Q.13) What soft skills (or essential skills) do you think are required for cybersecurity professionals?

	Total N=1011	Gen Pop X-Cyber Workers N=661 A	Cybersecurity Hiring Managers N=324 B	Cybersecurity Professionals N=252 C
Problem-solving	81%	85% BC	72%	70%
Communication	72%	74% B	67%	68%
Adaptability	64%	70% BC	53%	52%
Collaboration	58%	61% B	53%	54%
Creativity	48%	53% BC	37%	36%
Leadership	47%	50% BC	42%	38%
Emotional Intelligence	46%	48% BC	41%	40%

Note: Multiple response variable. Responses sum to more than 100%.

Q.14) What do you perceive as the positives of a cybersecurity career?

	Total N=1011	Gen Pop X-Cyber Workers N=661 A	Cybersecurity Hiring Managers N=324 B	Cybersecurity Professionals N=252 C
Job security	69%	69%	69%	70%
Protecting consumers from hackers	61%	64% BC	55%	51%
Career growth	58%	56%	60%	61%
Serving national security	52%	53%	50%	47%
Lucrative salary	49%	51%	45%	48%
Broad application of skills across all industries	38%	43% BC	30%	27%
Other	1%	1%	1%	0%

Note: Multiple response variable. Responses sum to more than 100%.

Q.15) What actions need to be taken to address the cybersecurity challenges we face?

	Total N=1011	Gen Pop X-Cyber Workers N=661 A	Cybersecurity Hiring Managers N=324 B	Cybersecurity Professionals N=252 C
Organizations need to invest in cybersecurity internally	68%	67%	69%	70%
Everyone needs to become educated in how they can protect their data	62%	66% BC	55%	49%
The federal government needs to do a better job in setting and enforcing regulations that protect consumer data	54%	52%	56%	58%
The federal government needs to play a bigger role in setting cybersecurity policy for private sector companies	45%	42%	52% A	52% A
There needs to be harsher penalties for companies who not doing enough to protect consumer data	37%	42% BC	28%	25%
There needs to be more diversity of experience, race and gender in cybersecurity	36%	35%	38%	36%
Other	0%	0%	1%	0%

Note: Multiple response variable. Responses sum to more than 100%.

About Champlain College Online

Champlain College Online is at the forefront of adult education. Since 1993, we have carefully crafted online education to match the career aspirations of employees with the industry-driven needs of the organizations that employ them.

As one of the first online programs in the United States, we are proud to be part of the distinguished history of regionally accredited, not-for-profit Champlain College, founded in Burlington, Vermont in 1878.

Champlain College Online is consistently ranked by *U.S. News & World Report* as a leader in online higher education. Our nationally recognized programs address industry trends and critical skills gaps. We serve more than 3,000 students through 60 online undergraduate and graduate degrees, certificates, and stackable credentials in high-demand fields like cybersecurity, business, healthcare, and information technology.

Through our workforce development program called truED, we partner with some of the nation's leading businesses and organizations in a bold reimagining of workplace learning that enables employees to flourish and organizations to grow.

CHAMPLAIN COLLEGE ONLINE /

online.champlain.edu | 888.545.3859