CYBRARY

DECLASSIFIED

UNRAVELING THE CYBER SKILLS GAP & TALENT SHORTAGE

2018

IN COLLABORATION WITH:

CYENTIA® INSTITUTE

CYBRARY DECLASSIFIED

CYBRARY

This report was commissioned and partly conducted by Cybrary. Cybrary created and distributed the survey and then provided the response data to the Cyentia Institute for analysis and drafting of this report.

Cybrary is a crowdsourced cyber security and IT learning and certification preparation platform. Its ecosystem of people, companies, content, and technologies converge to create an ever-growing catalog of online courses and experiential tools that provide cyber security and IT learning opportunities to anyone, anywhere, anytime. Cybrary levels the playing field for those who want to advance in or start a cyber security or IT career by providing anyone with access to the tools they need to be competent and confident.

Find out more: www.cybrary.it

CYENTIA® INSTITUTE

Analysis for this report was provided by the Cyentia Institute. Cyentia seeks to advance cybersecurity knowledge and practice through data-driven research. We curate knowledge for the community, partner with vendors to create analytical reports like this one, and help enterprises gain insight from their data.

Find out more: www.cyentia.com.

Introduction

Searching the web for some variation of the "biggest risk 2018" is nearly certain to return numerous results containing the word "cyber." In fact, that exact query leads to an article by the World Economic Forum[1], which lists the "biggest risks to our world in 2018 ." Two of the top five risks fall squarely under the domain of cybersecurity.

The fact that cybersecurity is widely seen as a top risk is hardly surprising, especially to those of us in the industry. But what about the top cybersecurity challenges we will face in 2018? Go ahead, search that one too. We'll put on our Carnac the Magnificent turban and predict that those results will come back with several references to the cyber "skills gap" or "talent shortage."

In truth, it doesn't take a magic hat to know that our industry suffers from a critical shortage of skilled cybersecurity professionals. One source[2] measured the size of that gap and found that there were more than 285 thousand open and unfilled positions in the United States alone. That's one-third the size of the entire U.S. cybersecurity workforce!

Finding people to fill the gap is easy; finding people with the right skills is not. Thankfully, there are organizations out there working hard to address this issue, and Cybrary is one of them. Cybrary offers free and open source learning opportunities to 1.4 million security and IT professionals. They are dedicated to understanding and eliminating the cybersecurity skills gap, and this research report is one of the many ways in which they are doing that.

This report shares findings from a survey conducted of more than 3,100 IT, security and other non-technical professionals. It explores their learning habits, levels of personal and organizational preparedness, and factors that improve their confidence and defensive capabilities. If the key findings below resonate with challenges facing your organization, then you will definitely want to add this to the top of your reading list.

1. https://www.weforum.org/agenda/2018/01/the-biggest-risks-in-2018-will-be-environmental-and-technological/

2. http://cyberseek.org/heatmap.html

KEY FINDINGS

- Two out of three organizations admit that finding qualified cybersecurity professionals is a struggle.
- 80% of respondents do not feel adequately prepared to defend their organizations.
- 68% express doubts about their organization's readiness to thwart advanced threats.
- One-third say their organizations have experienced a security breach.
- 60% report using personal time for IT and security training. Only 13% conduct training during normal business hours.
- 35% of respondents spend at least $1,000 annually in training-related expenses.
- Half of respondents pay for their own training; only 15% say employers cover all training expenses.
- Respondents that receive anti-phishing and security awareness training show higher confidence in defensive capabilities.
- Organizations that invest in training show improved preparedness at both the employee and corporate level.
- Women and men receive equal training support from their employers, suggesting this is not a factor behind the gender gap in cybersecurity.
- Employer training support differs among ethnicities, but experience looks to be the underlying influencing factor.

The Respondents

This report primarily focuses on technical training habits and outcomes, but it will help to know a little bit about the backgrounds of the trainees before reviewing the findings that follow. The first thing to note is that respondents represent a fairly even split between IT and cybersecurity regarding their primary career focus. One in five claim something else as their profession, and their descriptions point to a wide range of occupations, including those currently unemployed.

The job titles in Figure 1 offer a different angle on the respondents participating in this study. Regardless of whether they focus on IT or cybersecurity, administrator, operator, analyst, and management roles are fairly well represented. Again, there's a large category for "Other" that encompasses everything from students to staff sergeants.

You might think that a forum like Cybrary would serve more junior-level members than seasoned professionals. But that would not be a correct assumption, according to Figure 2. In fact, respondents with five or more years of experience tied those with one to three years for the largest cohort. This may well point to a need for continual learning to stay relevant in a fast-moving field.

We asked quite a few additional questions about respondents and their organizations, but we are going to cut this section short and press forward into the main body of the report. Those interested in more details on the survey sample will find that information in the margins. Appendix A provides an overview of the sampling methodology.

FIGURE 1
Respondent job roles

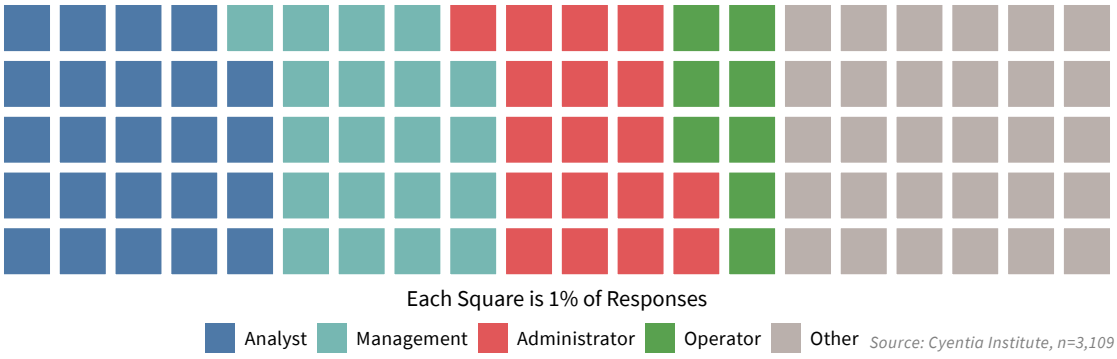
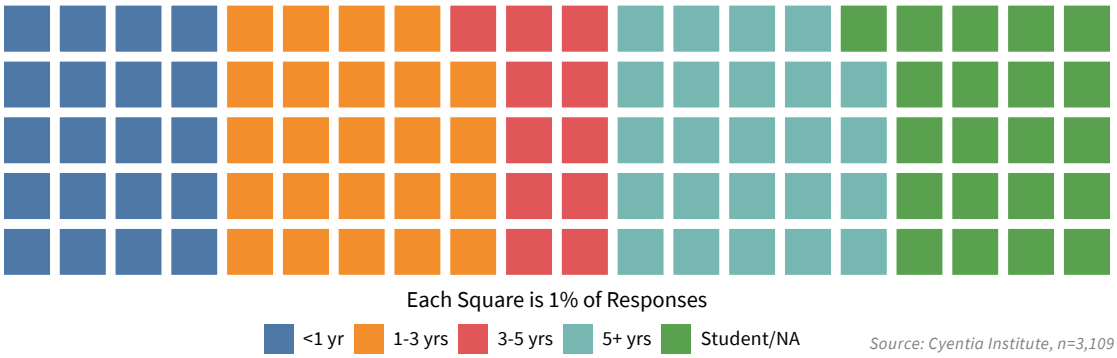


FIGURE 2
Respondent experience level



Learning Habits

Now that we know something about those who took part in this survey, we now seek to understand something about their level of preparedness to perform job duties. Keep in mind that all respondents are members of Cybrary, and therefore, interested in online cybersecurity training opportunities by default. How they compare to the broader population of IT and cybersecurity professionals is unknown, but we presume their inclination toward skill development and preparedness are above average, based on their joining Cybrary. Let's see what they had to say.

Where do you typically conduct training?

Given the caveat in the opening paragraph of this section, let's explore this first. Figure 3 verifies what we would expect to see; online training is the clear winner among Cybrary users. No surprise there.

The relative use of online to classroom to conference settings, however, is rather interesting—especially the latter. Many things might explain the lower involvement in conference-based training, but the added expense of travel, taking off work, and the need for ongoing training opportunities are probably three biggies. Additionally, those same issues could be extended, to a somewhat lesser degree, to the classroom. As you will see, each explanation finds support in the remaining questions under this section.

What types of training do you prefer?

So, respondents prefer online training venues, but what form or types of training do they view as most effective? This is an important question for trainees, trainers, and training developers, regardless of the venue.

By a healthy margin in Figure 4, practical hands-on exercises are the preferred way to conduct training. Perhaps quotes should be around "hands-on," as most of this is done in a virtual environment. Nonetheless, hands are kept on the keyboards. This active approach to learning is supported by years of research and practice from children to adults. The most popular courses among Cybrary users in December 2017 are good examples of the necessity of this form of training: 1) Penetration Testing and Ethical Hacking, and 2) CompTIA Security+. Though one is "Red Team" and one is "Blue Team," both require much more than passive learning to master.

Videos are also fairly popular among respondents, with just over one-in-five stating a preference for this option. It's worth noting that training videos are free for Cybrary members, which certainly contributes to their popularity. Things such as discussions and exams are much less preferred, which makes sense. These are great for supporting and verifying training activities, but not so much as a primary method of attaining knowledge and skills.

FIGURE 3

Training forum used most often

Source: Cyentia Institute, n=2,529

FIGURE 4

Preferred training format

Source: Cyentia Institute, n=2,575

Will you pursue training in the future?

We now know more about where and how IT and security professionals like to do their training, but do they see that as a once-and-done activity or something they will do on an ongoing basis? The answer to that is a definitive "yes"—nearly all respondents show a desire to continue their training in the future.

This perceived need for ongoing learning is not surprising. Technical disciplines like IT and cybersecurity are fast-moving and will quickly leave behind those who do not update their skills. As one participant said: *"I would like to be more effective in my field. To do that, I have to learn more and be more proactive in honing my skills."*

When do you typically conduct training?

Speaking of "being more proactive in honing skills," we asked the participants when they typically conducted their training sessions. Per Figure 5, the majority use their personal time for honing skills, rather than doing so while on the clock. Taking that down one notch, training after work in the evenings was most common, followed closely by weekends. Some go-getters took advantage of the wee hours of the morning to get in that extra learning, but they were in the minority.

A question may arise at this point as to whether this proclivity to an after-hours training session is by choice or by necessity. The short answer is "both," and we will elaborate on that next.

Who pays for your training?

Just because someone uses personal time for training doesn't necessarily mean their employers refuse to support those efforts. Many IT and security professionals enjoy learning new things, and tinkering with personal devices, analyzing home network traffic, and offering free penetration testing services to neighbors is all part of it[3]. So, who pays?

According to Figure 6, individuals rather than employers typically foot the bill for training. Only 28% of employers reach for the check, while another third splits expenses in some way. The breakdown is nearly identical for expenses related to certification. Before judging employers for not supporting their staff, let's consider some perfectly defensible reasons for this outcome.

The least accusatory explanation is that they do pay for the training, but employees decide on their own free will to pursue more. Maybe they want to learn something outside their current job scope. Maybe they want to prepare for a different job. Maybe they're just having fun. The bottom line is we shouldn't expect employers to pay for any and all training, especially if it's not work-related.

There is, however, a reasonable expectation that employers have an obligation to absorb the cost of preparing employees to perform duties their job requires of them. It's difficult to determine directly from these results whether that level of support is being met, but based on circumstantial evidence gathered through this survey, we have doubts that it is.

FIGURE 5
Time typically used for training

Source: Cyentia Institute, n=1,746

FIGURE 6
Source of funding for training

Source: Cyentia Institute, n=1,593

3. That's a joke. Neither the Cyentia Institute nor Cybrary recommend this. It's not a good way to make friends with your neighbors. It's also illegal, so there's that too.

How much is spent on training annually?

Who pays for training is one part of the picture; how much they pay is another. We asked respondents about that next.

The results in Figure 7 say that one-quarter pay nothing, and unfortunately, we have no further insight on that. We suspect many organizations have internal training capabilities, or that training was done in some way that the respondent never saw a bill. Just over 40% cap spending at $1,000, and another quarter of respondents estimate annual training costs between $1K and $5K. The remaining 10% say they or their organizations shell out over $5,000 annually for training. And when that much is spent, the employer-paid ratio doubles. Do these investments see a return? Sit tight; we're getting to that.

What about internal security training?

In addition to sponsoring external learning opportunities for their employees, many organizations conduct internal training of various forms. In many cases, this is a mandatory compliance requirement. About half of the respondents to this survey said their organizations conducted general security and awareness training and/or anti-phishing training. We thought it was rather "phishy" that about a quarter weren't sure if they received such training, which probably means they took the bait. That, or it was one of those circa 1997 slide decks laden with cheesy clip art that they had to click through to get off HR's naughty list. We've all tried to wipe those from our memory, so their forgetfulness is understandable.

How about options other than training?

Before ending this section on how respondents are using training to better prepare themselves, it bears mention that training isn't the only way to gain knowledge and skills. Joining professional associations, for instance, is something that just under 20% of respondents report doing. About a quarter say they receive free learning resources and opportunities through such organizations.

Certifications are also another popular method of leveling up skills and credentials in the tech world. A large proportion of respondents have active certifications, but nine out of ten say they don't have enough and plan to pursue more. We also asked the respondents about their preferences for micro-certifications vs. larger, more traditional certification programs. The feedback was split fairly evenly on that topic, with some form of "both" being the most common response.

We now know more about the training habits of IT and security professionals, but we still know very little about whether all this effort and expense is making a difference. Do respondents feel prepared to perform their duties and defend their organizations? We'll explore that question in this section.

FIGURE 7
Annual spending on training

Source: Cyentia Institute, n=1,746

Preparedness

Are you prepared to defend your organization?

The first outcome-based question we asked respondents was whether they felt personally prepared to do their part (whatever that was) in defending their organization. Only 16% answered in the affirmative. We find this statistic rather disappointing given all that we've learned about training habits. Can it really be that after working nights and weekends and paying out of pocket to improve their abilities, IT and security professionals still aren't sufficiently prepared?

If you suspect there's more to this than meets the eye, you would be correct. A lack of confidence does seem to haunt many tech professionals, but that doesn't necessarily equate to a defeatist mentality. Defending the organizations against the myriad of external and internal cyber threats that exist isn't easy, and nobody knows that better than those who practice it. Plus, we did find some things that tied to improved confidence, but let's stick with general preparedness before we go there.

Is your organization prepared to defend itself?

We then asked a modified form of the question to determine if this perceived lack of preparation was something personal or organizational. Interestingly, a greater proportion of respondents (about 1/4) felt their organization was ready to defend itself. And, for what it's worth, that view did not differ significantly between managers and individual contributor roles.

Again, we can only speculate about why this might be so. Could this be a symptom of Imposter Syndrome popping up, causing respondents to perceive "they've got it covered" in other groups? Perhaps it is a realistic understanding that "there's no 'I' in 'team,'" when it comes to a security program? While we're on the topic of "reality," let's check one other thing.

FIGURE 8

Personal security preparedness

Source: Cyentia Institute, n=1,667

FIGURE 9

Organizational security preparedness

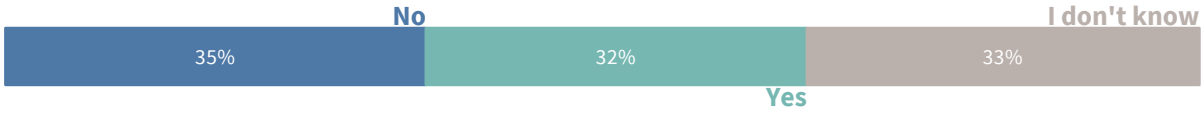
Source: Cyentia Institute, n=1,667

Has your organization been breached?

For many security programs, reality sets in hard and fast in the form of a breach. Everything goes along fine until it doesn't. Almost one-third of respondents to this survey report experiencing that reality in their organization. And another third isn't sure.

If that breach rate seems high to you, you're not alone. But keep in mind that a) there was no time frame given, and b) the term "breach" is broader than "data breach." The latter specifically refers to the disclosure of information, whereas the former generally refers to a wider array of security incidents. That caveat should not be interpreted as an attempt to minimize the weight of this finding; 32% represents quite a large number given the sample size for this survey.

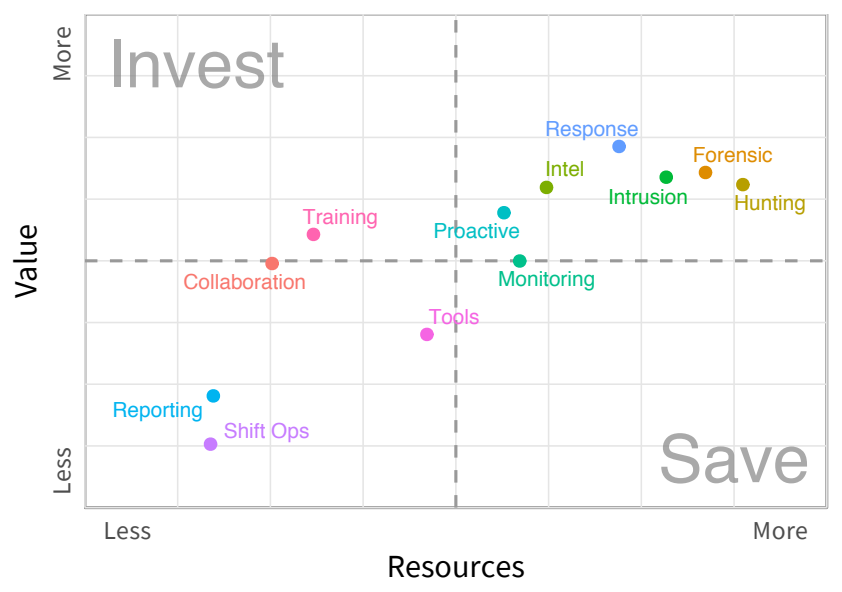
FIGURE 10
Organizations experiencing security breaches



Source: Cyentia Institute, n=1,667

TRAINING SHOWS STRONG ROI

The Cyentia Institute recently published the Voice of the Analyst Study. We asked Security Operations Center (SOC) and Incident Response (IR) staff about their perceptions, experiences, and activities relevant to defending their organizations. In one section, analysts rated activities they regularly performed along several dimensions. Two of those dimensions are show in the figure below—Resources and Value.



Source: Cyentia Institute

In theory, activities in the upper-left would offer good value at comparatively low cost. The only activity squarely in that quadrant? Training. It's good to know our members aren't the only ones who place value on leveling up skills.

Training Outcomes

This section essentially seeks to identify significant relationships amid everything discussed thus far. For instance, does training in their off time make respondents feel more prepared? How about online vs. classroom? Do organizations that pay for training reap the benefits of those investments? Does more spending lead to fewer breaches? These are important questions, and you'll have the answers by the end of this section.

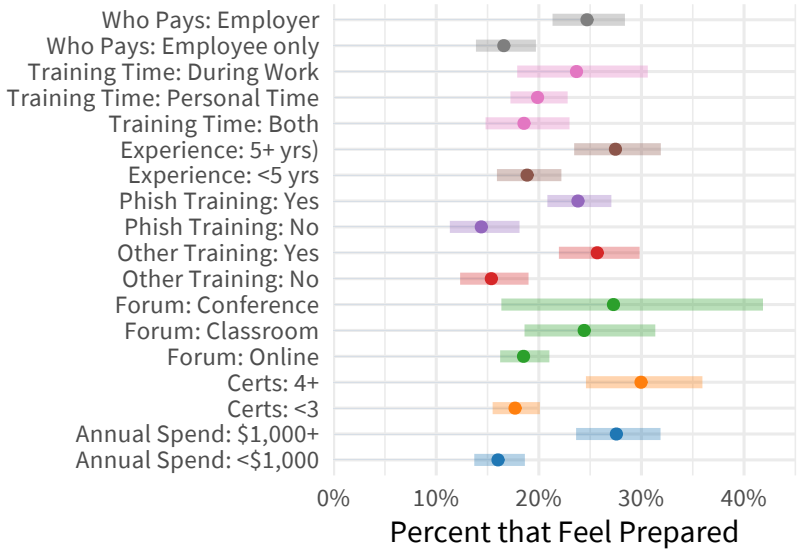
What factors influence personal preparedness?

Let's start with factors linked to respondents *feeling* personally prepared to perform their duties. Figure 11 lists the possible influencing factors on the left along with different variables for those factors. You're familiar with these from the preceding sections, so refer back for a reminder of what "Training Time: During Work" means, or how common it is relative to other variables for that factor. Factors and their associated variables are color-coded to make it easier to compare outcomes.

Those tired of the Pay-Your-Own-Way approach to training and certification should find Figure 11 a welcome sight. It suggests that employer-paid training results in higher levels of personal preparedness than employee-paid training. Racking up several certifications also improves confidence. Additionally, spending more on these activities helps as well, which will offer some comfort to those who have been footing their own training bill.

FIGURE 11

Factors influencing personal security preparedness



Source: Cyentia Institute, (n varies)

FIGURES 11-13

Once you crack the code, interpreting Figures 11, 12, and 13 should be a snap.

Find a factor of interest (e.g., who pays), then scan to the right to locate the dots for each factor (e.g., Employer vs. Employee only). The position of the dots on the x-axis at the bottom will, for instance, give the percentage of respondents who felt prepared when their employer paid vs. didn't pay.

The shaded bars form a confidence interval[4] around those point values to help determine whether the perceived differences are statistically significant. If the bars of the variables overlap, the effect is not significant—regardless of the distance between the dots. If they don't overlap, you can safely conclude a meaningful association exists.

4. To learn more about confidence intervals and why we use them, read this post from our blog: https://www.cyentia.com/2018/01/29/confidence-intervals/

Organizations that invest in anti-phishing and other security training should feel good about those investments based on Figure 11. They improve confidence in preparedness at the individual level. The answer to whether that benefits the entire organization will have to wait for the next section (spoiler alert: Yes!).

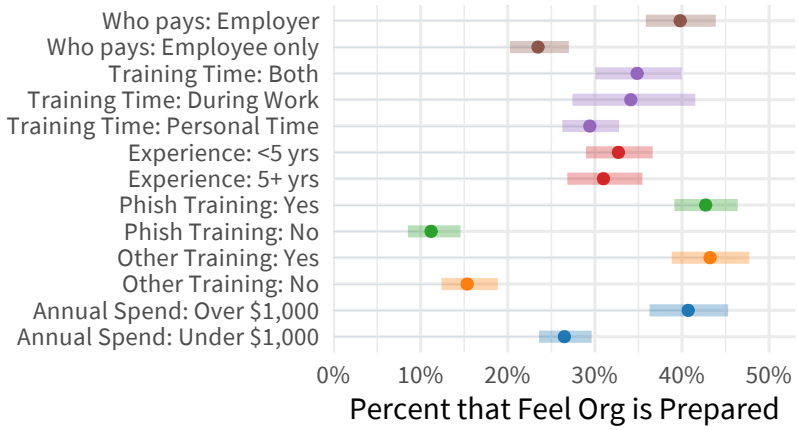
Factors that do not seem to matter are the timing of training or the venue in which it takes place. The results seem to promote a Nike-esque training slogan: "where and when isn't important; just do it." By extension, that implies if one training venue costs a lot more than another, the lower cost option is the way to go, all else being equal. That's enough about perceptions of individual preparedness; let's move on to factors that affect the entire organization.

What factors influence organizational preparedness?

In general, perceptions at the organizational level in Figure 12 mimic those at the personal level, except effect sizes, are more pronounced. Anti-phishing training, for instance, improves individual confidence by about 10% but catapults organizational preparedness by over 30% (11% > 43%). Other types of security and awareness training look to make a big difference as well. Such training is often mandatory for all employees and may give the impression that the organization is serious about security and actively doing something about it.

FIGURE 12

Factors influencing organizational security preparedness



Source: Cyentia Institute, (n varies)

In addition to these internal training initiatives, organizations that make external investments in preparing IT and security staff reap benefits as well. Respondents whose employers paid for their training (and spent higher amounts on that training) felt their organizations were significantly more capable of meeting the security challenges facing them. As we saw at the individual level, the timing and forum of that training do not influence perceptions of organizational preparedness. Thus, such decisions can be made based on other factors such as cost, convenience, and the preferences of staff without fear of sacrificing effectiveness.

FEELING VS. REALITY

The word "feeling" is important to keep in mind as you read this section. We cannot measure whether respondents or their organizations are actually prepared, just whether there is a perception of preparedness.

OTHER FACTORS?

If you are wondering whether factors about the organization, such as size, industry, region, etc. might influence its preparedness, you are not alone. We ask that exact question in the Miscellaneous Questions section later in this report.

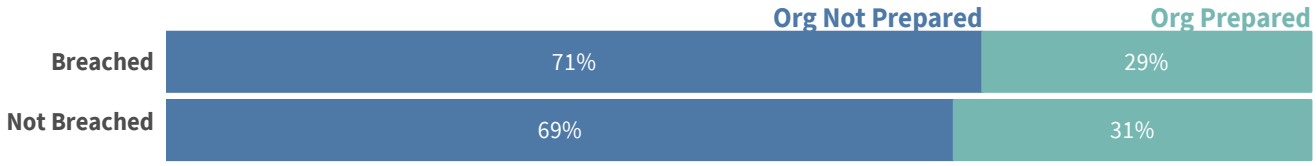
One area where the views expressed in Figure 12 (organizational) do differ from those in Figure 11 (individual) relates to experience. Having a longer tenure (5+ years) in the security industry improves confidence for individuals, but not at the organizational level. This may simply mean that respondents feel one person's expertise isn't enough to make or break the whole team. However, a team's experience (and preparedness) is based upon that of its members, and thus, this result prompts us to ask what matters more: experience or training? Given the choice of hiring expensive veterans or investing those extra dollars in training entry-level or intermediate staff, which will best prepare the organization to defend itself? While we can't answer that conclusively from the data provided here, it is compelling that company support for training displays a stronger effect than experience.

Do breaches affect organizational preparedness?

One additional observation bears mention before we move from training outcomes to some additional questions of interest. Curiously, suffering a breach seems to have no impact on perceptions of organizational preparedness. Rather than chalking that up to delusions or bad data, it's more helpful to ponder why this might be. Having seen many programs rebound from a breach to become stronger and more capable than they were before, we're placing our bets on that explanation.

FIGURE 13

Effect of breaches on organizational preparedness



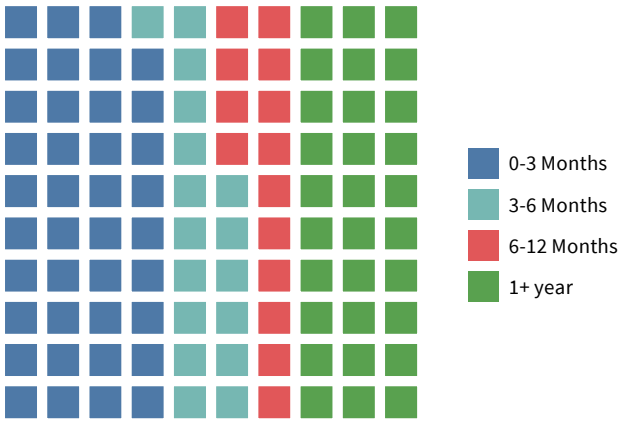
Source: Cyentia Institute, n=453 (breached) and 465

FINDING CYBER SECURITY JOBS

We mentioned the wide and growing cybersecurity talent gap in the beginning of this report. And given the large number of job openings, you'd think that landing the job of your dreams would be a snap. Not so, according to Cybrary members.

About 40% of respondents holding cybersecurity positions say they found their current gig in three months or less. But 30% worked the job market for a year or more, and the remaining 30% fell somewhere in between those extremes. All that to say, finding a job can still be a challenge, talent gap notwithstanding.

Of course, picking up cybersecurity skills and certifications to help reel in that dream job quicker is why many of our members joined Cybrary in the first place. We're proud to be a part of their career aspirations and growth!



Each Square is 1% of Responses

Source: Cyentia Institute, n=1,012

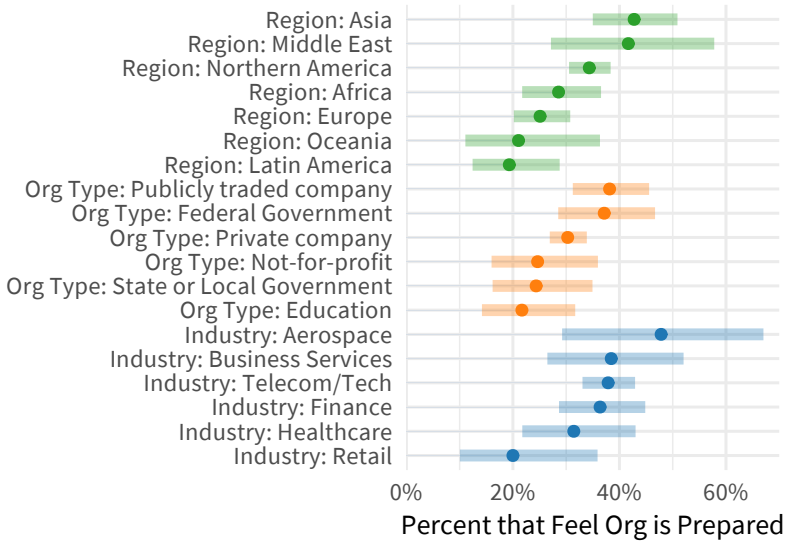
Miscellaneous Questions

Does preparedness differ by region?

We imagine some readers may be wondering whether organizational demographics make a difference in these results. To address that, we've included Figure 14, which shows how variables such as region, organization type, and industry affect perceptions of security preparedness.

FIGURE 14

Demographics influencing organizational security preparedness



Source: Cyentia Institute, (n varies)

While differences do exist, the mostly overlapping confidence intervals suggest either they aren't significant, or we don't have enough data to determine that. We also checked for demographic effects on breach prevalence and found a similar pattern. The most noteworthy exception is a significantly lower breach rate among private companies compared to public companies, educational institutions, and federal agencies.

What degrees do tech professionals have?

If you've been around long enough, you probably remember a time when computer science was about as close as you could get to an undergraduate degree in IT or cybersecurity. Many schools now offer programs in very specific sub-disciplines of those fields. As today's workforce is a blend of "old-timers" and "noobs," we thought it would be fun to identify the educational paths that led to where they are now.

Questions to this point have fallen logically into a few overarching categories. While answering them, additional questions arose that did fit so neatly. Rather than letting the structure of the report dictate the bounds of our curiosity, we tossed all those questions into this section.

Don't skip it...there's good stuff ahead!

DIVERSE DEGREES

Cybrary members have a wide range of educational background, and many are in the middle of that education now. Among respondents to this survey, the most widely-held degrees were:

- IT (28%)
- Computer Sci (18%)
- Engineering (11%)
- Info Science (6%)
- Business (5%)

Figure 15 traces the connections between the respondents' undergraduate degree and their current role. It's easy to see that although IT is the most commonly reported starting point, many backgrounds comprise today's IT and security workforce. So, don't sweat it if your educational qualifications don't match your ambition—just get training!

Will my company be breached if I have a music degree?

You may remember the consternation expressed by some[5] after Equifax's fall 2017 mega-breach; their Chief Security Officer (CSO) had a music composition degree. The assumption, of course, was that music has nothing to do with security, so anyone with that degree is unfit for such a role. Many in the industry voiced objection because, as we just learned, lots of security people have an educational background that doesn't match their current role.

FIGURE 15

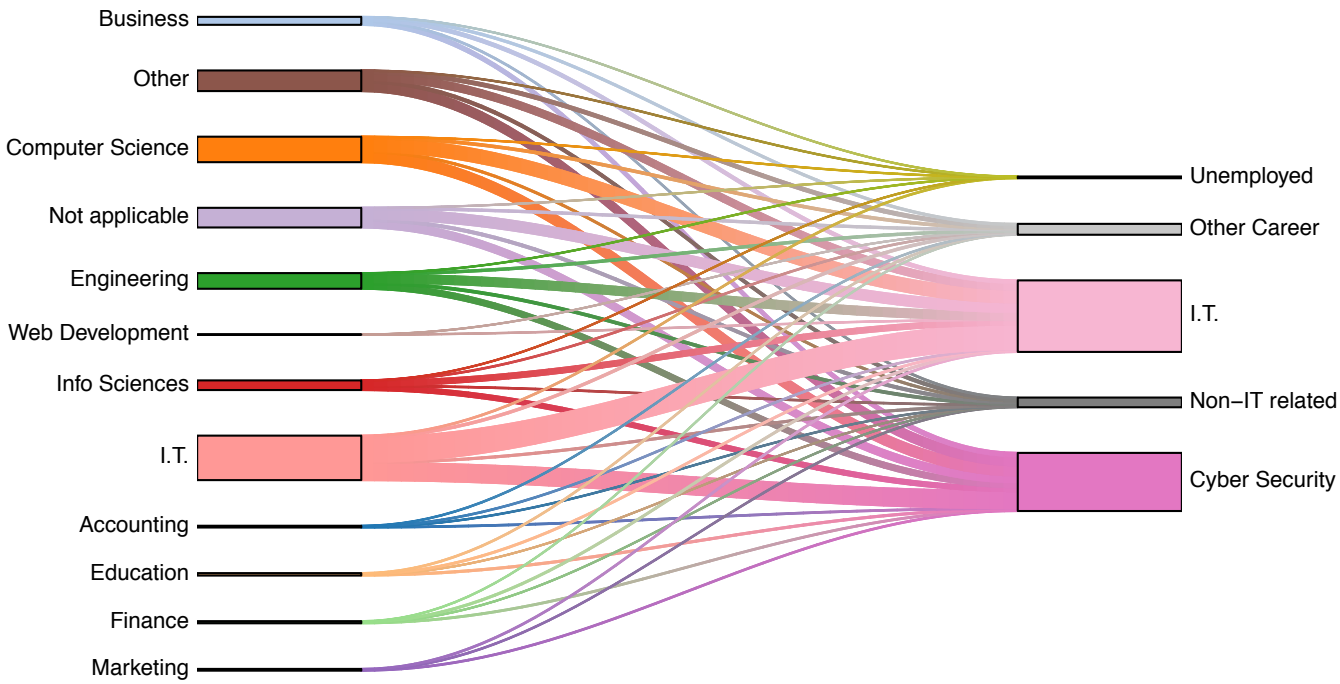
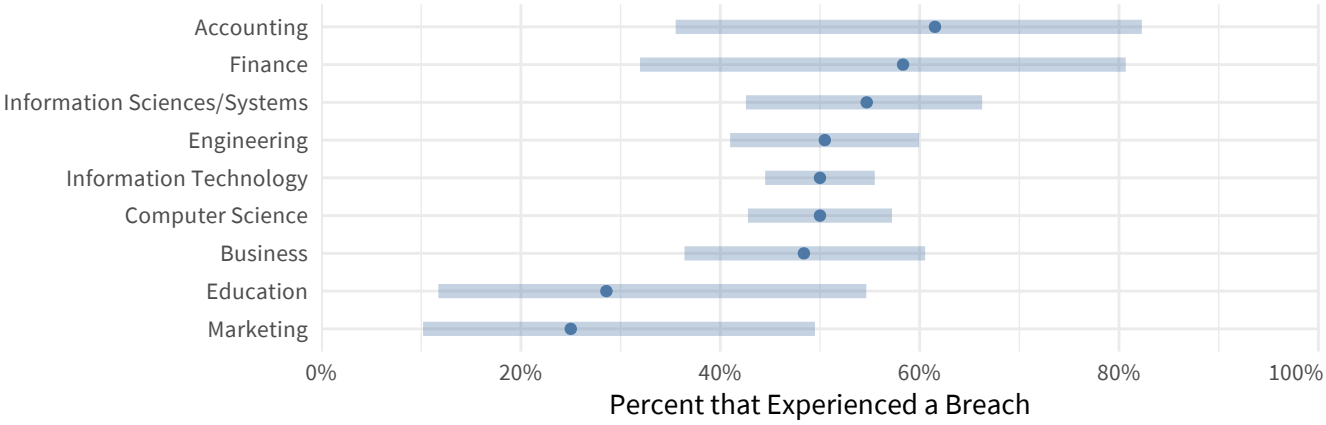


FIGURE 16

Educational background of respondents experiencing security breaches



Source: Cyentia Institute, (n varies)

The fervor around that event has died down, but we'd still like to lend some data to that discussion. And the data's stance on this subject is pretty clear: there is no correlation between degree and the likelihood of a breach. In fact, the lowest breach rates were reported by people with education and marketing degrees![6] Don't fire your security leadership over this, folks.

Are genders given equal training support?

Sticking with the Equifax incident for a moment, some were of the opinion[7] that it wasn't so much the CSO's degree that was the issue, but rather her gender. Indeed, there is an increasing concern (from both women and men) about the gender gap that exists within the security industry. And one has to look no further than this report to see that a gap exists, as only 13% of respondents were female. Though this survey was not designed to diagnose the causes of that gap, we can search for evidence of unequal organizational support for training between genders that may contribute to it.

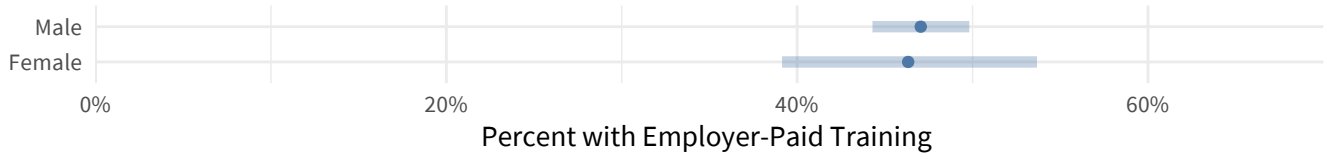
Figure 17 shows the percentage of respondents who say their employer covers at least a part of their training costs. We didn't show it, but we also examined the proportion of training budgets that exceed $1,000 annually. Neither reveals significant differences between males and females. Thus, we find no evidence that discrimination in training support offered by employers contributes to the gender gap in the security industry. So, what *is* causing it? We don't find an answer to that question in this dataset, but we all have a duty to continue searching for one.

Are ethnicities given equal training support?

So, there is no evidence of gender discrimination in training support; that's good. But can the same be said for different ethnic backgrounds? We applied the same process from above to compare employer support for knowledge and skill development among the five most common ethnicities among respondents. We see some immediate warning signs.

FIGURE 17

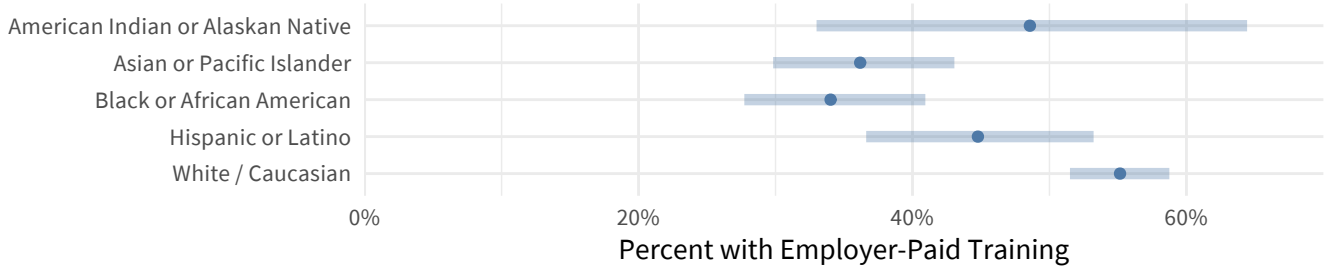
Comparison of employer training support by gender



Source: Cyentia Institute, (n varies)

FIGURE 18

Comparison of employer training support by ethnicity



Source: Cyentia Institute, (n varies)

5. https://www.marketwatch.com/story/equifax-ceo-hired-a-music-major-as-the-companys-chief-security-officer-2017-09-15

6. Before changing your degree or hiring plans, please note the very small sample size with a very large sample error that is indistinguishable from other degrees.

7. https://securityledger.com/2017/09/opinion-when-they-say-your-major-is-a-problem-what-they-mean-is-your-gender-is-a-problem/

In particular, Figure 18 reveals that a significantly higher percentage of White / Caucasian respondents benefit from employer-paid training compared to Black or African American and Asian or Pacific Islander ethnic groups. While it's dangerous to jump to conclusions, the results in Figure V are cause for concern and warrant further investigation.

The first order of business when confronted with a finding like this is to test for confounding or mediating variables—additional factors that may influence those we're trying to establish a causal relationship between. Particular to this outcome, perhaps it is not ethnicity that determines whether employers pay for training, but something else entirely. Maybe job role or experience level is the actual influencing factor, and ethnicity correlates with that. Thankfully, we don't have to guess; we can isolate and study these interactions. Let's do that now.

Figure 19 shows the breakdown of individual contributor vs. management roles for the most common ethnicities.

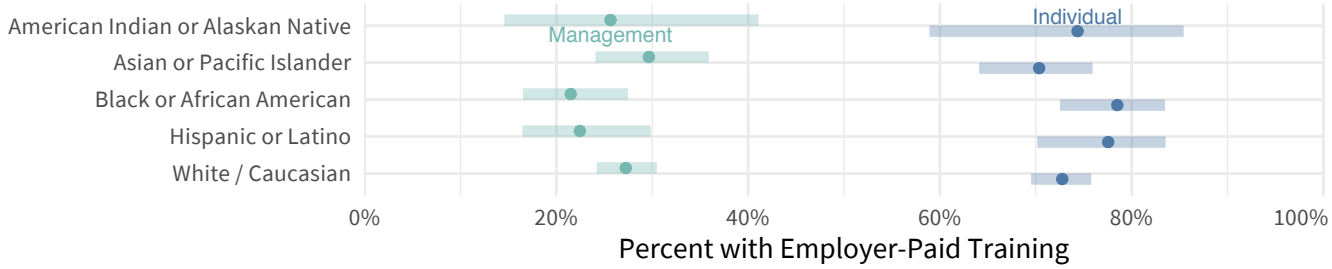
Though we see some variation among means, the overlapping confidence intervals suggest those differences fall within the sampling error. We see no evidence here that job role explains the apparent inequalities from Figure 18. We'll try something else; perhaps experience level will yield some insight.

From Figure 20, it is clear that the likelihood of employer-paid training increases with the respondent's level of experience. Whether that's a good thing or not is another question. Logic suggests that the learning needs of junior employees were at least equal to that of those with more experience—and quite possibly more. This in itself might be a contributor to the overall talent gap in IT or cybersecurity, regardless of gender or ethnicity. For now, let's bring this back to the question at hand—could this explain the ethnic discrepencies from Figure 18?

If so, we would expect to see a higher proportion of minorities in lesser-experienced position and the opposite for White / Caucasion respondents. We test that hypothesis in Figure 21.

FIGURE 19

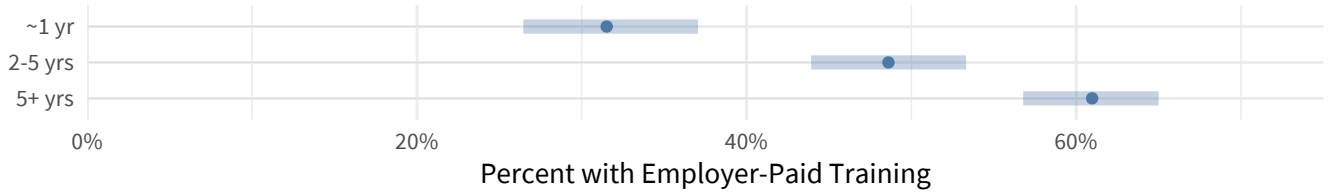
Individual vs. managerial roles by ethnicity



Source: Cyentia Institute, (n varies)

FIGURE 20

Comparison of employer training support by level of experience



Source: Cyentia Institute, (n varies)

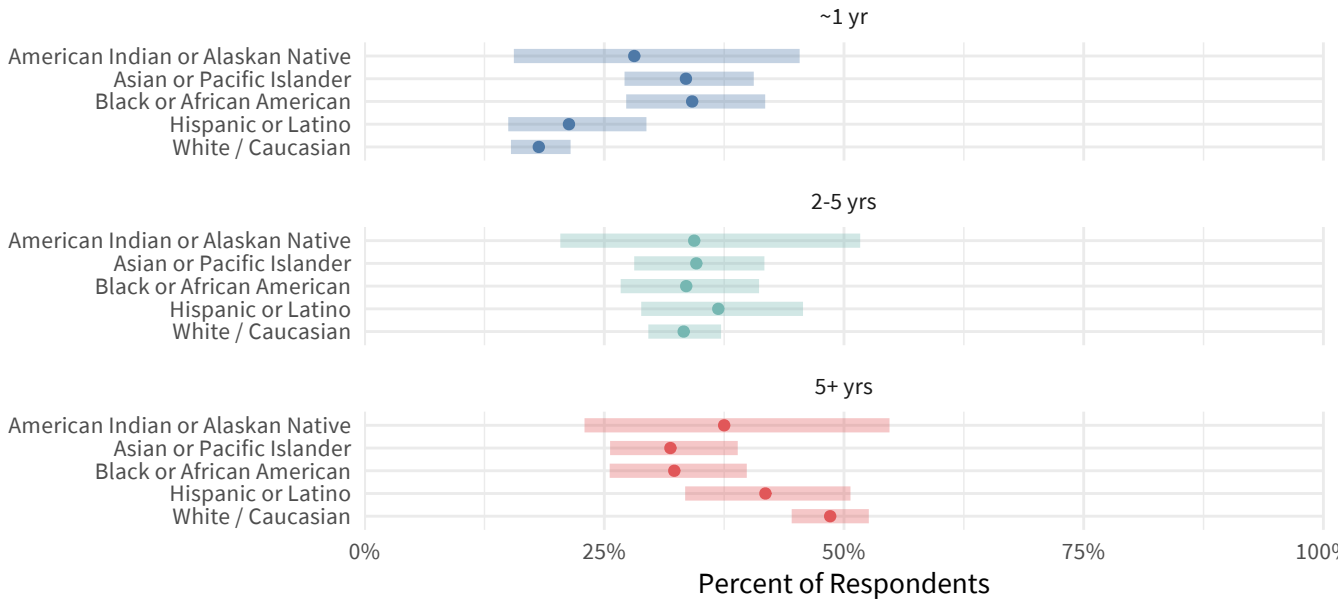
Looking at Figure 21, it is apparent that a larger share of Black or African American and Asian or Pacific Islander groups have less than one year of experience. Those same groups, on the other hand, exhibit a significantly smaller proportion of professionals with at least five years in the field (compared to the White/Caucasian group). Respondents falling in the middle of these two experience ranges exhibit very little difference across the ethnicities.

There are two ways we can interpret results in Figure 21, one optimistic and the other pessimistic. The optimistic interpretation is that we're seeing the emergence of a more diverse crop of new/young professionals in the IT and cybersecurity field. This would be good news indeed for the aforementioned talent gap that plagues the industry.

The pessimistic interpretation is that Figure 21 doesn't show an emergence at all, but rather an exodus. Minorities enter the field at high rates, but then leave after a few years of experience. Why they might be leaving is unclear from the data (as is whether they are, in fact, leaving at all).

Based on a straightforward interpretation of the results seen here, we lean toward the more optimistic view that ethnic diversity is growing. Equally important, employers are not necessarily doling out dollars based on ethnicity; they're exhibiting a preference for supporting experienced staff. As already stated, this may not be the best workforce development strategy, but it is more palatable than the discrimnatory alternative. Obviously, all of these possibilities and interpretations are worthy of further study and we look forward to doing just that in the future.

FIGURE 21
Individual vs. managerial roles by ethnicity



Source: Cyentia Institute, (n varies)

Conclusions & Recommendations

Thank you for your interest in this important topic and for taking the time to read this report. We believe strongly that knowledge and skill development is a critical pillar in bridging the wide talent gap that currently exists in IT and cybersecurity. If you're interested in integrating an organizational training approach, here are a few points to keep in mind:

- Get employee feedback on the types of training they're interested in pursuing
- Use annual performance reviews as a means of implementing structured, consistent training
- Align training material to both company objectives and individual employee objectives
- Identify which skill-based training is required by all employees
- Provide incentives for participating in training

In the end, the goal is not just to make your organization more secure, but to make employees feel valued and motivated. Employees who understand the benefit of continuous learning will regularly invest in their career development.

A COO PERSPECTIVE

KATHIE MILEY

"It is the job of company leaders to define the mission, vision, and values of their organization and communicate them regularly to employees. Teaching an understanding of how the company can and will benefit from every employee's contributions helps professionals to feel more responsible for their career development. This can only be done in an organization where training is integrated into the work culture already, but presents a unique opportunity for companies where it is not. Leaders must prioritize creating a dynamic learning environment where experience is not only rewarded, but less-experienced employees receive the support they need to improve their skills. The future of modern business is dependent on Human Intelligence, e.g. human beings."

JOIN CYBRARY

Did you know joining Cybrary costs nothing? Did you know that joining gives you access to hundreds of training modules that can be taken from the comfort of your home any time you choose?

What are you waiting for - Register Today!

HAVE IDEAS?

Readers like you are the key to our ability to conduct and share research like this. If you have interest in comissioning or participating in future Cyentia Institute studies, drop us a line at research@cyentia.com.

APPENDIX A

GENERAL PURPOSE

To examine the knowledge and skill development preferences, habits, and outcomes of IT and cybersecurity professionals.

TARGET POPULATION

IT and cybersecurity professionals participating in online training exercises to develop job-related knowledge and skills

SAMPLING METHOD

Cybrary invited members to participate in an online survey in Fall 2017. The survey was live for 10 days and one reminder was sent. No incentives were offered.

SAMPLE SIZE

3,109 respondents of varying roles, tenures, and specialties in technical and non-technical disciplines.

The following sample demographics are given to assist readers in assessing the relevance of this survey and its results to themselves and to their organizations.

RESPONDENT DEMOGRAPHICS

Employment status

Full time	62%
Part time	8%
Student	19%
Unemployed	11%

Primary career focus

Information Technology	42%
Cybersecurity	39%
Other	19%

Region of residency

Americas	47%
Asia	19%
Europe	17%
Africa	14%
Oceania	3%

ORGANIZATION DEMOGRAPHICS

Type of organization

Federal Government:	6.2%
State or Local Government	5%
Education	10.6%
Private company	46.2%
Publicly traded company	11%
Not-for-profit	5.7%
NA/Unknown	15.5%

Number of employees

Under 500	35%
500 to 2500	13.3%
2,500 to 5,000	6.2%
5,000 to 10,000	6.2%
10,000 to 150,000	10.2%
Over 150,000	5.8%
NA/Unknown	10.7%

CYENTIA INSTITUTE

CYBRARY DECLASSIFIED

"I would like to be more effective in my field. To do that, I have to learn more and be more proactive in honing my skills."