How Views on Cybersecurity Professionals Are Changing and What Hiring Organizations Need to Know

The 2020 (ISC)^2 Cybersecurity Perception Study
INTRODUCTION
The age-old stereotype of cybersecurity professionals – working in isolated, darkly lit environments, utilizing suspicious hacking skills to root out cyberattacks – may be changing for the better. In a new research study of outsiders to the profession, a majority of 2,500 U.S. and U.K. respondents view these professionals as smart, technically skilled individuals and as “the good guys fighting cybercrime.” This is welcome news for a short-staffed profession that needs to attract more than 4 million more trained and dedicated colleagues globally.

These findings may come as a welcomed and overdue surprise to those in the field. The results indicate a marked change since a Thycotic study as recently as 2019 found that many security professionals believe they’ve got an image problem, with roughly two-thirds believing their teams are regarded as the company naysayers — either “doom mongers” or a “necessary evil.” On the contrary, a new level of respect and appreciation has developed for cybersecurity professionals.

However, while perceptions are improving, not enough job seekers are considering a career in cybersecurity. Even at a time of record unemployment, the strong job stability and career path that cybersecurity offers doesn’t seem to be enough to awaken interest in the profession for the public at large, even as 29% of respondents say they are looking for a career change during the COVID-19 pandemic. (ISC)²’s latest research reveals that most people highly value job stability and view cybersecurity as a good career path – just not for themselves.

So what’s going on? The answer may lie in the perception of the cybersecurity profession as a set of highly specialized technical roles, which appears to be a deterrent to joining the field. Even though roughly one in five respondents would consider a technology-related job, the study suggests that respondents see cybersecurity as requiring a particular set of skills that they lack and cannot – or are not willing to – acquire. They view cybersecurity jobs as aspirational and beyond their reach. While it’s true that many such technical positions do exist, the reality is that the field requires a broad array of skills and expertise to fill a range of roles, many of which favor nontechnical soft skills that many applicants may already possess.

This report discusses the perceptions uncovered by the study and provides conclusions that hiring organizations should consider as they work to locate and recruit additional staff to their cybersecurity teams.

STUDY PARTICIPANTS
The (ISC)² Cybersecurity Perception study was fielded in June 2020 and polled 2,500 people across the United States and the United Kingdom. The study sought out participants who do not currently work in cybersecurity roles to understand their perspectives on the field.

The median age of participants was 46, with a nearly even distribution of 51% women and 49% men. More than half of respondents (57%) hold a bachelor’s degree or higher, including 17% who have earned a master’s degree. A solid majority (70%) have full-time employment, and 54% hold positions of manager or higher, including 15% who have C-level positions. Only 11% of study participants consider themselves experts at using computers and mobile technology.

1(ISC)² Cybersecurity Workforce Study, 2019 https://www.isc2.org/Research/Workforce-Study
Unlike most cybersecurity research, the (ISC)² Cybersecurity Perception Study was designed to capture views of the industry from the outside looking in, having filtered out current and former cybersecurity professionals. According to the findings, the overall impression is positive: 71% of participants say they view cybersecurity professionals as smart, technically skilled individuals.

The second most popular choice regarding the image of cybersecurity professionals (51%) is one of “good guys fighting cybercrime.” About one third of respondents (35%) say cybersecurity professionals “keep us safe, like police and firefighters.” An additional 9% of respondents said they think of cybersecurity professionals as “heroes.”

The intimidation factor is more pronounced with women (37%) than men (17%). More than twice as many women find the profession intimidating. Women respondents (30%) also tend to view the field as composed of “mostly men” (22% of men agree). Another significant gender difference in perception has to do with diversity in the profession: A higher number of women are more discouraged than men by a perceived lack of diversity (13% to 7%).

Another factor that could be causing confusion about the profession is the sheer breadth and sprawl of cybersecurity as a far-reaching discipline, which pervades nearly every function of an organization. This makes it difficult for outsiders to easily grasp exactly what the professional does. Moreover, pop culture references and lack of exposure in educational curriculum also seem to play a role.

As for the profession itself, 69% of respondents admit it seems like a good career path, just not one that is right for them. Only 1% think it’s a bad career path. So why is there a lack of interest in pursuing it? Unfortunately, respondents view the profession as having a high cost of entry, with 61% saying they believe they would need more education or would need to earn a certification before getting a cybersecurity job. And even though 29% of respondents say they are considering a career change, several factors are holding people back from considering cybersecurity. For one, 32% of respondents believe it would require too much technical knowledge or training. Other factors include “don’t know how to code” (27%) and “the field is too intimidating” (26%).

I’m just thankful somebody’s doing it.

– said one study participant when asked their opinion of cybersecurity

71% of participants say they view cybersecurity professionals as smart, technically skilled individuals.
WHAT’S SHAPING PERCEPTIONS?

Two primary factors seem to shape perceptions of cybersecurity work: a lack of educational foundation about the career and how the media portrays cybersecurity professionals. Each is worth exploring by the cybersecurity industry in order to create a more realistic, accessible view of the profession.

Although two thirds (66%) of respondents have an associate’s degree or higher, 77% say cybersecurity was never offered as a part of their available curriculum. For the 9% who say cybersecurity was part of the curriculum, 39% were in high school and 69% in college. So even when cybersecurity education is available, it tends to come much later in the educational path when many students may have already determined another area of focus.

The lack of educational focus appears to have created a perception gap about the realities of the profession. There is no educational foundation to awaken interest in the field or even influence the public’s understanding of what it is and how those who participate in it perform their tasks. It appears that gap is being filled by media stereotypes.

Asked about their perception of the cybersecurity profession, most respondents (68%) say it is shaped by portrayals in TV shows and movies (37%) or by news coverage of security incidents (31%).

Other perception-shaping factors include:

- I know people who work in cybersecurity (24%)
- Job descriptions I have read (21%)
- Word of mouth from teachers, mentors and professionals (16%)
- Social media (14%)
WHY NOT CONSIDER CYBERSECURITY?

The study was conducted during a period of high unemployment created by the COVID-19 pandemic. In this context, job stability is understandably highly valued by respondents (61%), outpacing other desired job attributes such as a “flexible work environment” (57%), “earning potential” (56%) and “personal fulfillment” (55%). The good news is that many of the career attributes potential career changers say are important to them are available in the cybersecurity field.

Among all respondents, 29% are looking for a career change. And even though a solid majority of respondents view cybersecurity as a good career path, they are not drawn to it. Instead, respondents are interested in these industries:

- 24% EDUCATION
- 22% HEALTHCARE
- 22% TECHNOLOGY AND IT
- 21% FINANCE
- 18% HUMAN RESOURCES
- 18% SALES

It’s possible that working in cybersecurity doesn’t even occur to most people when considering a career path – most likely because they do not view themselves as having the required skills. The study reveals that only 8% of respondents have considered working in the field at some point. One of the study’s questions asked, “If you were interested in starting a career in cybersecurity, where would you begin?” The top four answers:

- 26% GO BACK TO SCHOOL
- 22% EARN A CERTIFICATION
- 14% INQUIRE WITH THE IT OR CYBERSECURITY TEAM AT MY EMPLOYER
- 13% TEACH MYSELF (I.E., ONLINE COURSES)

The perceived need to go back to school and earn certifications could be justified in some cases, since a level of training may be necessary. Nonetheless, the perception may be exaggerated and appears to be acting as a deterrent. Since only 11% of respondents rate themselves as having expert computer and mobile technology skills, it’s possible they may have a skewed expectation of how much training is actually required for a number of non-technical positions in the field. In reality, many cybersecurity teams are searching for a wider pool of skillsets to complement their technical staff, including those individuals who possess legal, risk, compliance or communications knowledge, among other areas. Yet when survey participants were simply asked about the first thing that came to mind when they thought of the term cybersecurity, their responses included sentiments like, “smart computer skills that I don’t have” and “I’m not qualified to apply for the jobs.”

Since only 11% of respondents rate themselves as having expert computer and mobile technology skills, it’s possible they may have a skewed expectation of how much training is actually required for a number of non-technical positions in the field.
ONE OF THE MOST UNEXPECTED FINDINGS IN THE STUDY IS THAT RESPONDENTS FROM THE YOUNGEST GENERATION OF WORKERS – GENERATION Z (ZOOMERS), WHICH CONSIST OF THOSE UP TO AGE 24 – HAVE A LESS POSITIVE PERCEPTION OF CYBERSECURITY PROFESSIONALS THAN ANY OTHER GENERATION SURVEYED. THIS ISSUE IN PARTICULAR MERITS CLOSE ATTENTION BY THE CYBERSECURITY INDUSTRY AT A TIME WHEN EMPLOYERS ARE STRUGGLING TO OVERCOME THE TALENT GAP.

FEWER ZOOMERS (58%) VIEW CYBERSECURITY PROFESSIONALS AS SMART, TECHNICALLY SKILLED PEOPLE THAN MILLENIALS (67%), GENERATION X (73%) OR BABY BOOMERS (78%). THE SAME PATTERN WAS REVEALED WHEN RESPONDENTS WERE ASKED IF THEY SEE CYBERSECURITY WORKERS AS “GOOD GUYS, FIGHTING CYBERCRIME.” THE FOLLOWING PERCENTAGES AGREED WITH THAT STATEMENT:

<table>
<thead>
<tr>
<th>Generation</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baby boomers</td>
<td>60%</td>
</tr>
<tr>
<td>Generation X</td>
<td>52%</td>
</tr>
<tr>
<td>Millennials</td>
<td>45%</td>
</tr>
<tr>
<td>Generation Z</td>
<td>34%</td>
</tr>
</tbody>
</table>

The perception is problematic. If the cybersecurity talent gap of 4 million is ever to be filled, the industry needs to attract younger talent, which the study’s findings clearly identify as a challenge.

What’s causing the perception among the youngest respondents isn’t entirely clear. The study suggests factors such as media portrayals, industry acquaintances and social media exposure are shaping perceptions. Younger respondents are heavier users of social media. Unfortunately, these platforms tend to focus on the negative – arguments and venting – which could be influencing younger respondents’ views of the field.

It would stand to reason that if steady progress was being made on introducing more cybersecurity into formal educational curriculum, it would most likely influence Generation Z the most, given their proximity to such education. It appears though that their perception seems to be guided instead by other societal influences.

The study does reveal a silver lining when it comes to younger respondents’ attitudes toward cybersecurity. Of those who have actually considered cybersecurity as a career at some point, Generation Z respondents are five times more likely to do so than Boomers, pointing to a growing awareness of the field as a career option.
The overall perception of cybersecurity and the professionals working within it has evolved and become more positive, apparently even creating an aura of exclusivity. The study suggests there is an overriding expectation that cybersecurity is too technical and specialized, requiring education and certifications that participants are not willing to pursue. While some may view this as a good problem to have, it does pose a challenge in addressing the talent gap. It’s clear the industry would benefit by celebrating its most technically talented participants, while simultaneously taking measures to clarify and differentiate which roles are technical and which require other transferrable skills that do not necessitate more education or certification.

Here are three recommendations for hiring managers and organizations, as well as the industry at large, as they work to make cybersecurity more accessible to those considering a career change:

1. **Widen the appeal:**
   Increase the focus on the non-technical aspects of certain positions in job descriptions, such as the need for communication skills, problem-solving and creativity, in order to get a larger pool of candidates to consider. In a rapidly evolving field, the ability to handle ambiguities and apply creative approaches can be just as vital as technical credentials that show up on a resume or CV.

2. **Focus recruitment efforts:**
   Develop recruitment strategies that focus on outreach to individuals with complementary experience with areas such as communications, law enforcement, data flow, process development and controls, regulatory compliance, etc. These experiences develop and require skills that are transferrable to cybersecurity. Employers should also be training an eye internally on employees in different departments who may be looking for a new career (something 29% of survey respondents say they are considering). Retaining and repurposing strong employees who already know your organizational systems, personnel and culture may make the recruitment process much simpler and more cost-effective. Well balanced cybersecurity teams require a diversity of experience, and that can be pulled in from departments outside of IT.

3. **Address education:**
   Co-develop cybersecurity programs with school districts and higher learning institutions to awaken earlier interest in the field. Creating a stronger pipeline of candidates who understand the realities and the benefits of a cybersecurity career will help to reduce the global talent gap.

**Methodology**

Results presented in this report are from an online survey conducted by (ISC)² and Market Cube in June 2020. The total respondent base of 2,500 adults has never worked and does not currently work in the field of cybersecurity. 51% of respondents were women, and 49% were men. 1,500 respondents reside in the United States, while 1,000 reside in the United Kingdom.
(ISC)² is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)² offers a portfolio of credentials that are part of a holistic, pragmatic approach to security. Our membership, more than 150,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. For more information on (ISC)², visit www.isc2.org.

© 2020 (ISC)², Inc. All Rights Reserved