Goldgaber Research Group
Prepared for Signature Consultants
Third Quarter 2018

Cybersecurity Staffing Industry Report

Arthur Goldgaber | Market Analyst

signature® CONSULTANTS

The U.S. Bureau of Labor Statistics has predicted that the number of jobs in the cybersecurity space will increase 18% between 2014 and 2024.

Rise in Cyberattacks Drives Record Demand for Cybersecurity Professionals

Recruiter KPI Summary

To paraphrase Charles Dickens, the state of today's global technology may be described as the best of times, and the most challenging of times. For example, among consumers, the digital convergence has brought unprecedented lifestyle conveniences, improvements in healthcare and new, desirable features in homes and automobiles.

Unfortunately, these innovations have also created significant cybersecurity and privacy challenges as hackers continue to breach these systems at alarming rates. To defend themselves from cyber threats to computers, networks, mobile devices and Internet of Things (IoT), companies are acquiring the latest cyber intelligence tools to track and alert them about the newest vulnerabilities. Nevertheless, there is no substitute for qualified cyber professionals. As a result, corporations, organizations such as hospitals, and government agencies are struggling to hire people who know how to use the tools, understand the threats and their consequences, and, most importantly, have the know-how to respond to live attacks in real-world situations.

The high demand for cyber professionals is creating a shortage both in the United States and around the globe. It's a simple supply and demand problem. Cybersecurity data tool CyberSeek recently reported that the cybersecurity job market is tight, with more than 300,000 cybersecurity job openings on its site between April 2017 and March 2018. Every year in the U.S., 40,000 jobs for information security analysts go unfilled, according to CyberSeek. The total U.S. cybersecurity workforce was about 768,100 as of March 2018.[1]

An estimated 1.8 million cybersecurity jobs will go unfilled by 2022, according to research by (ISC)[2]. Companies will have to utilize creative techniques to find cyber professionals such as contracting with staffing companies with expertise in cyber defense, partnering with joint public-private ventures, and recruiting professionals while they are still in college.

[1] "Cyberseek Figures Show U.S. Still Struggles with Cybersecurity Skills Gap," by Burning Glass Technologies, June 7, 2018.
[2] (ISC)[2] blog,."Cybersecurity Hiring—An Issue for All," Feb. 6, 2018.

Technology's Benefits

On the positive side of the ledger, technology is playing an evermore important role in everyone's lives as people rely on several devices for communications, managing finances and organizing their lives. The digitization of the economy is revolutionizing the way day-to-day business is conducted on all levels of commerce, from Fortune 500 companies and financial institutions, to mom-and-pop retail stores. Just in the past few years, "advances in computer processing, cloud computing, and smart devices are making it faster, cheaper, and easier for firms to leverage data to improve nearly every aspect of their business," stated new U.S. Securities and Exchange Commission Commissioner (SEC) Robert J. Jackson Jr. in a recent speech.[3]

By 2020, Domo estimates that for every person on earth, 1.7 MB (megabytes) of data will be created every second. Today, Domo reports that every minute there are 3.8 million searches on Google, almost 13 million texts are sent, Americans use 3.1 gigabytes of internet data, and 1.25 bitcoin are created, just to name a few.

The new technology, including hardware, software and social media, is benefiting consumers' lives in ways previous generations could not imagine, even in the most prescient works of science fiction. In just the past decade, constantly improving cell phones, for example, have eliminated the need for separate cameras, watches, alarm clocks, radios, GPS, and many other devices. In addition, phone applications allow consumers to use their phones for thousands of activities, including paying for goods at retailers, hailing taxis, listening to any song they desire, navigating their car and staying in touch with people around the globe on sites like Facebook and Instagram. In short, modern life would come to a screeching halt without technology.

As part and parcel of the digital advances, computer systems and networks are becoming more and more interconnected with the fusing together of internet-enabled information, operational systems that control manufacturing, and consumer technologies; i.e., end-user products and services that include home automation and sensor-enabled automobiles. Interconnected systems include automated buildings and homes, utilities, manufacturing plants, automobiles, aircraft, oil and gas production, personal medical devices, and virtual assistants.

[3] "Corporate Governance: On the Front Lines of America's Cyber War," Robert J. Jackson Jr., March 15, 2018.

The Dark Side of Interconnected Computers and Devices

Unfortunately, technological advances and the world's interconnected computer systems continue to be threatened by global cyber threats. The critical infrastructure of the United States—including electrical power grids, financial systems, telecommunications, healthcare, transportation, water, defense, and the internet—is highly vulnerable to cyberattack. A cyberattack is defined as an attack launched from one computer or more against another computer, multiple computers or networks.

The convergence of everything digital brings many advancements and new services such as the IoT, but can present an immense security challenge. Operational technologies are becoming more interconnected with other technology domains and that, in turn, is increasing the risk of disruption and the integrity of products and services.

Cyberattacks are a growing global menace, with almost daily reports of costly threats, hacks, attacks, or major cyber events. The sources of all these attacks are evolving from rogue programmers to organized crime rings to state-sponsored actors such as Russia, China and North Korea. In 2017, there were over 1,579 data breaches, a jump of 44.7 percent from a year earlier, according to data gathered by the Identity Theft Resource Center.[4] The global average cost of a data breach is up 6.4 percent to $3.86 million in 2018, compared to a year earlier, according to the Ponemon Institute. In addition, the average cost for each lost or stolen record containing sensitive and confidential information also increased by 4.8 percent year over year to $148.[5]

A matter of when, not if

The Identity Theft Resource Center reported that hacking, an umbrella category that includes phishing and ransomware/malware, continued to rank highest in the type of attacks included in its annual survey. Because of these alarming statistics, many cyber professionals say that it's not a matter of if your organization's systems will be breached; it's when.

Companies and government agencies are more vulnerable to cyberattack now than in the 1970s, when 17 percent of S&P 500 firms' market value was tied to tangible assets; in 2015, that number was 87 percent, with firms like Sony particularly susceptible to theft of their intellectual capital that resides on company hard drives or in the cloud.

[4] Identity Theft Resource Center, 2017 Annual Data Breach Year-End Review.
[5] 2018 Cost of a Data Breach Study by Ponemon.

The High Cost of Cyberattacks

Global ransomware costs exceeded $5 billion in 2017, up 15 times from $325 million in 2015, according to research firm Cybersecurity Ventures. The estimate includes many, often overlooked costs: damage, destruction or even loss of data, downtime, lost productivity, post-attack disruption to normal business activity, along with restoration and deletion of hostage data and systems, and employee training in direct response to the ransomware attacks.[6]

Some of the major cyberattacks of 2017 and 2018 included the ransomware attack, WannaCry, that took over computers, encrypted the contents of their hard drives, and then demanded a payment in bitcoin to free the data. The major victim may have been the UK's National Health Services.[7]

In fact, the healthcare industry has long been a top target for cyberattacks. Eighty-nine percent of healthcare organizations polled by the Ponemon Institute had at least one data breach involving the loss or theft of patient data in the past two years, according to a 2016 study.

Unfortunately, hackers may have the upper hand right now due to several problems, such as phishing e-mails, attacks on firewalls, the misconfiguring of firewalls and many other weapons that are expanding the opportunities, said Kirsten Bay, president and CEO of Cyber and adAPT, in an Information Age report.[8] Bay stated that ransomware on mobile devices is one of the greatest vulnerabilities, and equally disturbing is the fact that "hackers can purchase government grade DDos-as-a-service kits on the Dark Web." [9]

Fear of corporate cyber threats on the rise

These threats are now a top concern for executives around the globe. One recent survey of 1,300 risk professional and other senior executives around the globe by Marsh and Microsoft found that nearly 75 percent of respondents identified cyber threats as a top-five risk to their company's future. That is about twice the percentage who rated cyber threats that high in a similar survey conducted in 2016.[10] Similarly, the World Economic Forum's The Global Risks Report 2018[11] placed cyberattacks and massive data fraud among the year's top-five risks—the first time two technological risks were among the top five.

With the barrage of cyberattacks, it should come as no surprise that people who can defend companies from these threats are in great demand. CyberSeek estimates that there are currently about 768,100 cyber defense workers in the United States, with 2.5 currently employed cybersecurity workers for every opening. By contrast, there are 6.5 current workers for every job opening overall, in what is already a tight labor market.

---

[6] Morgan, Steve, "Ransomware damages rise 15x in 2 years to hit $5 billion, CSO, May 23, 2017.
[7] "Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data," independently conducted by the Ponemon Institute LLC, May 2016.
[8] Ismail, Nick. "The Cybersecurity on the Front Line," Information Age, May 6, 2017.
[9] Ibid.
[10] Marsh, By the Numbers: Global Cyber Risk Perception Survey, February, 2018.
[11] World Economic Forum, The Global Risks Report 2018.

Growing Demand for Cybersecurity

With the dramatic spike in cyberattacks, changes in digital technology, and an array of new regulatory concerns, both the private and public sectors have plans to boost spending on cybersecurity, with investment in cyber defense professionals a major component of these investments. Several companies have announced that they are expanding their cybersecurity budgets, such as J.P. Morgan Chase, which doubled its budget to $500 million, and companies like Microsoft are investing over $1 billion annually on cybersecurity research and development now and are committed to maintaining that budget in the coming years.

In the public sector, the White House reported that the U.S. government will invest over $19 billion for cybersecurity in fiscal year 2017, up from $14 billion a year earlier.[12]

In fact, a study reported that investment in cybersecurity is now the fastest-growing priority for IT leaders, up 23 percent from 2017, according to the 2018 Harvey Nash/KPMG CIO survey.[13]

Big data/analytics remained the most in-demand skill for the fourth straight year, but "security and resilience," with 25 percent growth, was the skill with the largest year-over-year increase.

As a result, research firm Gartner estimated that worldwide enterprise security spending will total $96.3 billion in 2018, an increase of eight percent from a year earlier.[14] In its annual forecast, Gartner reported that the estimate is based on a rise in overall investment in antivirus, intrusion detection, monitoring, and other tools to safeguard data.

The driving force behind the security spending is a fear of data breaches. Cybersecurity Ventures forecasts that cybercrime will cost companies $6 trillion globally by 2021, up from $3 trillion in 2015. As a result, Cybersecurity Ventures predicts that global cybersecurity spending, driven by cybercrime, will exceed $1 trillion cumulatively from 2017 to 2021.[15]

Robust demand for cybersecurity experts

A major component of cybersecurity budget expansion is additional funds to hire more workers; no doubt businesses want and need help. Overall, 65 percent of IT leaders surveyed by the Harvey Nash/KPMG CIO survey said that a lack of talent is obstructing their cyber defense strategies, the highest recorded by the survey since 2008. Almost half of the participants, 47 percent, expect headcount to rise this year, three percentage points higher than a year earlier.

---

[12] Morgan, Steve, "2018 Cybersecurity Market Report."
[13] "CIOs report growing for cybersecurity talent, skills shortage: Harvey Nash," June 6, 2018.
[14] "Gartner Forecasts Worldwide Security Spending Will Reach $96 billion in 2018, Up 8 Percent from 2017," December 7, 2017.
[15] Morgan, Steven "Cybersecurity Jobs Report Vs Survey: Why industry forecasts are underestimating the cybersecurity workforce shortage...," Cybersecurityventures.com, June 8, 2018.

A study by Frost & Sullivan shows that hiring managers in the fields of healthcare, retail and manufacturing are particularly interested in hiring additional cyber defense professionals, with 40% in each sector desiring to expand their workforce by 15%.[16]

The public sector also needs more cyber professionals. The federal Office of Management and Budget reported that the federal government is struggling to improve its cyber defense systems.

The OMB found that there is little situational awareness, few standard processes for reporting or managing attacks, and almost no agencies adequately performing even basic encryption. As a result, the OMB concluded that "the current situation is untenable."[17] Of the 30,899 known successful compromises of federal computer systems in fiscal 2016, 11,802 of them never even had their threat vector identified.

However, qualified candidates for cybersecurity jobs are scarce and getting scarcer, which creates a challenge for companies to properly defend themselves against threats. Put simply, it's a classic supply-and-demand challenge, with too many vacancies for too few candidates. Statistics demonstrate that companies are struggling to hire cybersecurity workers.

Estimates for the growth of the cybersecurity workforce

Several organizations have provided robust estimates about the growth of the cybersecurity workforce. For example, the U.S. Bureau of Labor Statistics has predicted that the number of jobs in the cybersecurity space will increase 18% between 2014 and 2024.[18]

Other estimates include Cybersecurity Ventures' prediction of 3.5 million openings by 2021, the (ISC)^2 estimate of 1.8 million by 2022[19], and ISACA's estimation of 2 million openings by 2019. The disparity of the three surveys is that the (ISC)^2 and the ISACA surveys appear to focus on "information security" jobs, and not actually "cybersecurity" jobs, which helps explain their substantially smaller figures, according to Steve Morgan, editor-in-chief of Cybersecurity Ventures.[20]

In another study, CyberSeek recently reported that the cybersecurity job market remains tight, with more than 300,000 cybersecurity job openings on its site between April 2017 and March 2018, while the total U.S. cybersecurity workforce was 768,096 as of March 2018.[21]

---

[16] "2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk."
[17] Coldewey, Devin. "Government investigation finds federal agencies failing cybersecurity basics," Techcrunch.com, May 30, 2018.
[18] https://www.comptia.org/about-us/newsroom/blog/comptia-blog/2017/10/11/channeltrends-plugging-the-cybersecurity-talent-gap
[19] "Cybersecurity Hiring—An Issue for All," (ISC)2, Feb. 6, 2018.
[20] Morgan, Steven "Cybersecurity Jobs Report Vs Survey: Why industry forecasts are underestimating the cybersecurity workforce shortage..." Cybersecurityventures.com, June 8, 2018.
[21] "Cyberseek Figures Show U.S. Still Struggles with Cybersecurity Skills Gap," Burning Glass Technologies, June 7, 2018.

A growing, but still new, subset of the workforce

The cyber defense workforce estimate by CyberSeek may be low, according to Mark Aiello, vice president of Cybersecurity and Operations at Woburn, MA-based Signature Consultants. He estimated in Forbes that "there may be more cybersecurity people than we think; more than one million cyber-pros in the U.S. alone."[22]

However, it is difficult to quantify because it's such a new labor category and there may not be accurate records yet. There are no standard job titles and many cyber pros wear multiple hats. "They sometimes don't self-identify as cyber-pros," Aiello said.[23]

Various titles for cyber defense professionals

Of the "core" cybersecurity roles, the largest current demand is for cybersecurity engineers, with 37,580 openings. Four of the ten core cybersecurity roles have average advertised salaries over $100,000: these four are cybersecurity architects, cybersecurity managers, cybersecurity engineers, and cybersecurity consultants.

However, demand for security skills isn't limited to pure cybersecurity jobs. Many IT roles include cybersecurity as part of the job. In fact, the largest number of job openings, 194,224, are in the category of "operate and maintain," which includes work roles related to the support, administration, and maintenance of IT systems.

Other job titles for a cyber defense role may include systems administrator, network architect or engineer, forensics investigator, auditor, systems engineer, or integrator. Frost and Sullivan reports that globally the most sought-after jobs are in operations and security management, followed by incident management and forensics.[24]

Rising salaries

With the growing demand, salaries for key cybersecurity personnel have been rising dramatically. Cybersecurity jobs commanded a $6,500 premium over other IT jobs, according to a 2015 study by analytics firm Burning Glass.

As an example of these trends, an executive at a staffing agency stated recently in a media report that her candidates have been receiving competing offers from multiple companies with salary increases averaging over 30%. At the same time, current employers were trying to retain talent by making counteroffers with salary increases of 10% or more to retain information security team members.[25]

---

[22] Morgan, Steven. "Why Cybersecurity Companies Are 'Renting' Cyber Talent To Keep Up With Demand," Forbes, Sept. 28, 2015.
[23] Ibid.
[24] "2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk."
[25] Morgan, Steve. "Top Cybersecurity Salaries in U.S. Metros hit $380,000." Forbes, Jan. 9, 2016.

Security analyst is currently one of the most in-demand jobs, according to an executive at a recruiting firm. Security analysts work to prevent and mitigate breaches on the ground.[26]

In 2012, there were 72,670 security analyst jobs in the United States, with median salaries of $86,170. Three years later, 88,880 such analysts were earning a median yearly pay of $90,120. One of the top 10 technology jobs to watch in 2018 is network security administrator, with an average salary of $109,250, according to Robert Half Technology.

Another hot category is security manager. Security managers develop and implement overarching processes to keep information private.[27] Typically, professionals need certifications to be considered for such a role, like a CISM (Certified Information Security Manager) or CISSP (Certified Information Systems Security Professional).

At the top, the median salary for chief information security officers (CISO) was $224,000 in 2018, according to a survey, with salaries in San Francisco averaging $421,000 and in New York $406,000.[28] About 65 percent of large U.S. companies now have a CISO, up from 50 percent in 2016, according to ISACA.

Among major metropolitan areas, cybersecurity job openings are most heavily concentrated in Washington, D.C. (540% more openings per capita than the national average), Baltimore (190%), and San Jose, Calif. (180%), according to CyberSeek. In raw numbers, however, the top three cities were Washington, D.C., with 43,200 openings; New York, 19,993; and Chicago, 11,464.

Competition for cyber professionals

With the shortage of cyber professionals, more than half of organizations surveyed take at least three to six months to fill a cybersecurity vacancy, and 32 percent spend even more time to find qualified candidates, according to ISACA (a non-profit information security advocacy group previously known as the Information Systems Audit and Control Association).

It is a similar story with corporations' job-posting efforts. Employers typically have to repost or duplicate security job posts almost 35% more often than other IT jobs to find someone qualified, according to Burning Glass. Therefore, it may not come as a surprise that 27 percent of U.S. companies report that they cannot fill cybersecurity vacancies.

[26] Kauflin, Jeff. "The Fast-Growing Job with a Huge Skills Gap: Cybersecurity," Forbes, March, 16, 2017.
[27] Ibid.
[28] Morgan, Steve. "Top Cybersecurity Salaries in U.S. Metros hit $380,000." Forbes, Jan. 9, 2016.

In Forbes, Aiello stated that "competition [for cyber professionals] is fierce, but you can find the people. We invest all of our time in going where they (cyber pros) go and doing what they do. We attend industry events and conferences."[29]

Aiello explained that his agency is able to find people because they are experts in cybersecurity recruiting. They have a dedicated team whose only job is to speak with hundreds of cyber pros every week. His agency probably talks with more cyber professionals in a week than most companies do in a year. Aiello's recruiters are also expert networkers and have immersed themselves in the cybersecurity industry for the past decade. "It's still a small world in cyber so this experience has earned us excellent connections and a great network," he said.

Importance of cyber recruiters

Executives want to hire additional cyber defense professionals to cope with increased cyberattacks, but many are concerned that traditional hiring methods will not solve the issue of filling open positions.

The problem is simple. A typical in-house recruiter is well equipped to hire for standard jobs like accountant or auditor, but cybersecurity jobs are much more specialized. An in-house recruiter may struggle to look for candidates who have the skills required for a penetration tester, an application security engineer, an authentication and authorization specialist, a network security engineer, an intelligence analyst, or a security threat and countermeasures specialist. It may be asking too much.

Some companies try to assist recruiters by having them search for certain certification requirements, such as the CISSP or Security+. However, the problem with that strategy is that some of the most talented employees in the security field eschew certifications in favor of hands-on knowledge.

For that reason, many corporations are turning to niche recruiters to quickly obtain talented information security professionals for either full-time positions or a temporary role until the problem is fixed. At that point, their employees return to their normal routine, but that can take weeks, months or even years.

[29] Morgan, Steven. "Why Cybersecurity Companies Are 'Renting' Cyber Talent To Keep Up With Demand," Forbes, September 28, 2015.

The Rapid Growth of Staffing Agencies

IT employment growth has outpaced the overall economy for the last 15 years, and IT staffing has a relatively high temporary agency penetration rate in the United States, according to a recent study, "IT Staffing Growth Assessment: 2018 Update." About half of IT staffing revenue is generated in the United States, according to Staffing Industry Analysts (SIA).[30]

SIA forecasts that U.S. IT staffing revenue will stay on a 4 percent growth trajectory in 2018 to $30.9 billion, which would represent the eighth consecutive year of growth for the market and a new all-time high.[31] "Digital business transformation is driving investment in IT projects and workers, particularly those with specialized IT skills," according to Brian Wallins, a senior research analyst at SIA and author of the IT staffing report.

Overall, SIA estimates that temporary staffing will expand at a 3 percent rate in 2018 to $126.8 billion, and the overall staffing market is likely to grow 4 percent to reach $146.6 billion. Staffing companies placed about 3.2 million employees on average each week in 2017, up from 2.2 million in 2009, according to the American Staffing Association.

Demand is on an upswing for temporary IT staffing as buyers demand the flexibility to tap into these specialized skills, while managing costs. While a shortage of high-level IT talent creates greater demand for staffing services, it has also resulted in acute recruiting challenges, according to Wallins.

For the employer, contracting with a staffing agency also eliminates many of the costs and much of the work of vetting, hiring and keeping employees. Working with an agency also provides the company with more staffing flexibility to deal with market volatility. In turn, that helps the company avoid layoffs and the associated unemployment insurance costs.

When employers use a staffing agency they have the opportunity to ascertain if there is a good relationship with the employee before offering him or her a permanent position. Employees benefit by gaining new on-the-job skills and attaining quicker entry to the workforce.

In addition, temporary workers working with a staffing agency often receive offers of full-time work. In a media report, an executive with a major staffing company stated that 60 to 70 percent of temporary workers working with his staffing agency typically get offers of full-time employment at client firms in a robust economy.[32]

---

[30] "IT Staffing Growth Assessment: 2018 Update," February, 12, 2018.
[31] Ibid.
[32] Maziarz Christman, Samantha. "Permanent hiring of temporary works is picking up," Buffalo News, April 7, 2014.

Reasons for Cyber Professional Shortage

Several factors are causing the shortage in cyber pros, according to (ISC)[2] [33] research. First, cybersecurity careers remain relatively novel. Almost 90 percent of cybersecurity professionals begin their careers in another line of work. Signature Consultants' Aiello stated in a broadcast that "employers are getting wise to sourcing their talent from social sciences, law, business, and the like, then bringing them in and teaching them the fundamentals of security."[34]

Students who are interested in a technology career are usually more interested in web or mobile app development, not protecting an organization from cyberattacks. However, this dynamic is changing rapidly as colleges expand their cybersecurity curricula, and the cybersecurity field matures.

Hiring practices are also problematic, according to (ISC)[2]. When demand far exceeds supply, even the best recruiters will struggle. However, drawn-out and protracted hiring processes may discourage jobseekers, who will find employment elsewhere. In a highly competitive market, hiring must be quick and efficient.

Another issue is that too often the people recruiting and hiring lack cybersecurity expertise, which can make it difficult to identify the right candidate.

Employers may also have unrealistic expectations. They need to make sure descriptions for cybersecurity positions accurately match the knowledge, skills and abilities the role requires. (ISC)[2] research indicates this is an area for improvement, and the same is true of employers' investment in training and certifications. Only about one-third of respondents said their company pays for all of their cybersecurity training.

Another major issue is that women are underrepresented in the ranks of cybersecurity. In North America, only 14 percent of the region's cybersecurity professionals are women. That compares with 10 percent in Asia-Pacific, 9 percent in Africa, 8 percent in Latin America, and 7 percent in Europe.

Also, surprisingly, millennials form only a small fraction of the cybersecurity job market despite their advanced digital and social media skills. Millennials are a diverse group with a strong interest in training, mentorship and apprenticeships, areas in which too many of today's budget-conscious employers could do a better job.

---

[33] "Cybersecurity Hiring—An Issue for All," (ISC)2, Feb. 6, 2018.
[34] "Dark Reading Radio: The Real Reason Security Jobs Remain Vacant," May 27, 2014.

Other Creative Ways to Find Cyber Professionals

To speed up the employment process for cyber professionals, the Cybersecurity Association of Maryland Inc. last year launched a new online jobs platform in partnership with SkillSmart.

The system, Maryland Cyber Jobs, was developed to address the shortage of qualified candidates to fill open cyber positions across all industry sectors.[35] Using a skills-based methodology that is tailored to each hiring company, the platform attempts to reduce the time, effort, and expense for Maryland employers to find qualified candidates for cyber-related positions.

The talent shortage is a particularly difficult issue for Maryland, which has more than 12,000 IT and cybersecurity companies. The state is also home to 17 higher-education institutions that have been designated National Academic Centers of Excellence in Cyber Defense.

Cybersecurity Association's executive director, Stacey Smith, said in a media report that numerous commercial businesses and cybersecurity companies have complained that using standard job boards is a difficult and time-consuming process. Recruiters often have to sift through too much information to find the few people they might actually want to hire. The new jobs platform represents an attempt to streamline the cyber-recruiting process.

In another example of creative methods to hire cyber professionals, an American Banker article described how banks are taking creative steps to find cyber professionals. U.S. financial institutions, in particular, may face a greater threat to cyberattacks due to the shortage of high-tech professionals, though many of these jobs offer six-figure salaries, signing bonuses and other perks. To remedy that, some banks are hosting coding events, which enable college interns to work remotely during the school year. Banks are also sending executives to attend ethical hacking competitions and global information events like Black Hat.[36]

Aiello, quoted in the article, said that banks might also consider hiring qualified cyber professionals without a bachelor's degree. As an example, he explained that a software-as-a-service company that needed a cyber pro to uncover its security weaknesses hired a 21-year-old without a bachelor's degree. The candidate received an offer of about $150,000, with a $40,000 bonus. "It's a seller's market, not a buyer's market," is how Aiello summed up the situation.

[35] "Eichensehr, Morgan. "Maryland cyber group aims to decrease number of unfilled industry jobs," Baltimore Business Journal, Aug. 22, 2017.
[35] Wisniewski, Mary. "Hackers Wanted (Must be Willing to Work at Bank)." American Banker, June 27, 2016.