# Reverse Cybersecurity's Self-Inflicted Staffing Shortage

**Adopt More Realistic Expectations And More Effective Hiring Practices**

by Jeff Pollard, Chase Cunningham, and Joseph Blankenship

July 18, 2019

## Why Read This Report

Every day, we hear news stories, speeches, and vendor pitches that lament our acute cybersecurity talent shortage, one that will take years to address. However, the shortage is largely self-inflicted, which means CISOs can tackle it quickly by changing the ways they recruit, train, and retain people. This report dissects the myths, misconceptions, and half-truths within cybersecurity staffing and explains a more effective way for security and risk pros to build a complete, qualified security team.

## Key Takeaways

**Stop Looking For Perfection**

Job postings, recruiters, and firms are all seeking perfect candidates with all the right skills. Those candidates don't exist, and even if they did you could not afford them.

**Technology Will Ease Your Symptoms But Not Cure The Underlying Condition**

Your teams will adopt and use technology that enables them to scale more effectively through automation. Attackers will become easier to detect as machine learning and AI become commonplace in security products. Security analysts will improve with the exercises offered by cyber ranges. But the benefits of those technologies will vanish if you don't adjust the way you discover, hire, and retain security talent.

# Reverse Cybersecurity's Self-Inflicted Staffing Shortage

## Adopt More Realistic Expectations And More Effective Hiring Practices

by Jeff Pollard, Chase Cunningham, and Joseph Blankenship
with Laura Koetzle, Claire O'Malley, Elsa Pikulik, and Peggy Dostie

July 18, 2019

## Table Of Contents



## Related Research Documents

Best Practices: Recruiting And Retaining Women In Cybersecurity

CISO Career Paths: Plot Your Course For Advancement



FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

## The Cybersecurity Staffing Shortage Is Self-Inflicted

A cybersecurity staffing shortage is the industry's accepted truth. Vendor PowerPoints, conference sessions, and media coverage repeat this message over and over, describing it as a key barrier to fulfilling the security leader's agenda. But it's a fallacy. It's true that cybersecurity will continue to experience hiring growth that outpaces other industries.[1] Projections indicate a shortfall of at least 2.2 million candidates.[2] However, the perceived lack of qualified candidates is not a supply-and-demand problem — it's a problem of bias, expectation, compensation, and commitment. These issues present themselves in several ways:

- **Linking security compensation to IT compensation ignores supply and demand.** There is less demand for IT personnel than for security personnel: Cloud and software-as-a-service require less IT attention, while security needs are growing. The CISO of a major US manufacturing firm we interviewed mentioned most of his security employees needed compensation exceptions from HR. Obtaining exceptions slowed down the hiring process, costing them desirable candidates. Cybersecurity's long-standing ties to IT organizational structure, budgets, and payscales make hiring and retention more difficult for security leaders.
- **Cybersecurity leaders expect to hire MacGyver but pay like McDonalds.** Security hiring suffers from a rampant case of overqualification-itis, with role requirements over-scoped for compensation rates. This makes staffing more difficult in two ways: 1) fewer candidates apply for the role due to the restrictive set of qualifications and 2) candidates that do apply remove themselves from consideration due to lower-than-expected compensation (see Figure 1).[3] This results in seeking candidates with computer science degrees and multiple years of experience in incident response, penetration testing, malware analysis, and cryptography who are willing to work for the princely sum of $50,000 (39,500 GBP) per year. This unicorn candidate does not exist, given that any one of those skills alone can demand six figures in many geographies, with no shift work required.
- **Discovering security as a career worked when the field was a niche area.** Long-time information security pros often stumbled into the field. Whether it was discovering cybersecurity during military service, discovering hacking by circumventing copy protections in video games, or getting "volun-told" to help the security team with some enterprise initiative, many experienced security resources attained their present position through a combination of luck and accident. But to create a pipeline of viable candidates, security leaders can't depend on a candidate pool that stumbles into cybersecurity. People with those characteristics exist, but building around them leads to a lack of diversity and a shallow pool of available personnel.
- **Open positions remain vacant because security leaders fail to actively recruit.** In various interviews, most security leaders told us they felt like they needed to assess somewhere between 15 and 25 possible candidates to fill a single entry-level position. Interviewees also agreed that it's impossible to get this number of applications without marketing open positions on social media,

educational institutions, and job sites. If the security leader uses a set-it-and-forget-it approach, candidate flow dwindles, which then creates the perception of a shortage when it's a failure of creativity, networking, and marketing.

› **Using certifications as a filtering mechanism is a senseless barrier.** In the words of Yanek Korff, COO and co-founder of Expel, who has over 20 years of experience hiring technical and managerial roles in security services and consulting, "If the role of a security leader is to evaluate the capabilities of a candidate, relying on certifications is an abdication of that responsibility." Other interviewees said that requiring certifications for candidates is too limiting: It selects for candidates who could afford the time, travel, and out-of-pocket expense necessary to attend training events and sit for certification exams. For a one-week course that requires travel, this can run in the $10,000 range when factoring in the cost of the course, course materials, exam, airfare, hotel, and meals. The importance of certification to get past the human resources filter has led to plenty of experts on paper who lack the practical experience security leaders need.

**FIGURE 1** Entry-Level Cybersecurity Job Requiring Master's Degree And Five To Seven Years Of Experience

| | |
|---|---|
| Title | Cybersecurity analyst |
| Salary | £39,500 |
| Level | Entry-level associate |
| Education | Bachelor of Science in computer science or network engineering (required); Master of Science in cybersecurity (preferred) |
| Experience | Minimum five to seven years' experience in cybersecurity |

## Cast A Wider Net To Find, Develop, And Retain Security Talent

Developing talent pipelines and training programs will reduce — or eliminate — the perception of scarcity in the market. Firms that build quality programs will find themselves with shortened hiring cycles, higher staff retention, and a better security program overall. Security leaders should consider the inability to obtain and develop good talent as a key risk; if they fail to staff a functional security team, their organization becomes an easier target for attackers. Rather than making the problem about a market shortage, place the emphasis on what your firm can control — finding talent and developing it.

### Change The Way You Find And Hire Security Talent

To overhaul the way you advertise, find, interview, and compensate security candidates, you must think differently than in the past:

- **Redefine what signals a good security candidate.** Emphasize behaviors and characteristics rather than experience with technologies and certifications when looking for early-career candidates for roles requiring five years of experience or less. Justin Baiko, co-founder of Expel, explains what signals a good security candidate for him: "I look for three things: intellect, motivation, and fit. If someone has those three, I can teach them anything and everything I need them to know (see Figure 2)." Baiko's argument for this approach is simple: Say it takes an average of 140 days to recruit someone with the right combination of skills; you can get those skills faster by recruiting in 30 days a person with intellect, motivation, and fit and then spending 90 days training him.
- **Develop unique compensation structures for security pros.** Security talent is in demand, so use compensation bands that make sense based on the market demand for the position. This is especially true for organizations that link security compensation bands with information technology bands. Doing so will cost you personnel in terms of hiring, but also lead to churn on the team as employees leave for higher-paying roles. Emphasize vacation time, learning, 20% time flexible hours, and flexible work arrangements for security pros. This lets your organization appeal to the more financially minded candidates out there as well as those interested in quality of life and those seeking roles that offer long-term growth.
- **Reduce the number of required skills on requisitions.** Most requisitions seek the best possible candidate in the required skills section and the dream candidate in the desired skills section. In the case of a role that the organization is backfilling, some of the required skills were likely learned on the job by the departing employee. Security leaders and hiring managers need to take a realistic look at the required skills section and pare it down to the three to five skills they can't live without, and then commit to finding candidates with the aptitude and desire to learn the other skills.
- **Broaden the backgrounds considered when recruiting veterans.** Pursuing cyberoperators from specialized military units is an extremely pricy and competitive method to find talent. It ignores the potential talent pool of military veterans who have demonstrated the ability to master technical and mission-critical roles. Broaden your search to include those with military backgrounds but not specific cybersecurity experience (see Figure 3). Though they lack direct cybersecurity skills, candidates with these backgrounds possess vast experience operating under extreme circumstances.
- **Establish or take advantage of apprenticeship programs.** Apprenticeship programs are still widely utilized in the traditional trades, which tend to see less use in more knowledge-work oriented professions. However, the need to identify and cultivate cybersecurity talent has them experiencing a resurgence in the information security field, especially in Europe.[4] Companies should take advantage of those programs as sources of talent, and in areas of the world where they are not present, consider establishing similar programs on their own, or through partnerships with post-secondary institutions, career training organizations, and other public-private partnerships.

**FIGURE 2** Choose Intellect, Motivation, And Fit Over Education, Certifications, And Experience

Candidates with these three characteristics shine:

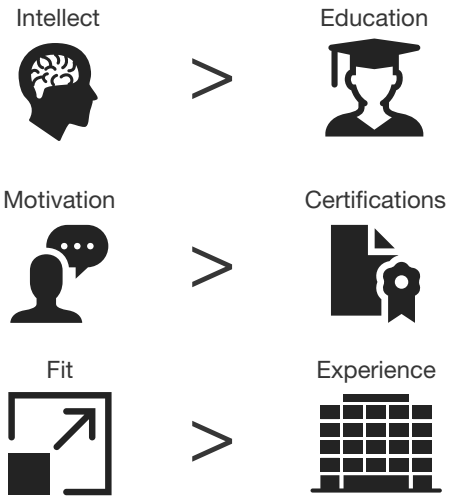


**FIGURE 3** Other Military Roles To Include When Seeking Cybersecurit y Pros

**Less common relevant roles**

| |
|---|
| Aircraft mechanics |
| Biological defense roles |
| Imagery and weather analysts |
| Counter intelligence |
| Air traffic controllers |
| Explosive ordinance disposal specialists |

## Keep Security Talent Motivated, Sharp, And Enthusiastic

Every security employee you retain — and every employee who sharpens her skills — is one less you need to recruit. To make sure that you keep the talent you find and grow:

- **Establish and publicize succession plans for security teams.** Your security team needs to know advancement is possible, and succession plans communicate that to them. One security leader we spoke with mentioned that all of his direct reports must maintain a succession plan for their own roles and discuss with the people in those plans that they are on a leadership track in the organization. This makes lateral moves less tempting because employees understand the list of priority candidates for open roles.
- **Let security staff members build and experiment.** Use open source tools and technologies that allow your team and your potential team members from other departments to play as a mechanism to retain and develop talent. These homegrown solutions can augment — or in some cases replace — commercial solutions from vendors. The trio of Elasticsearch, Logstash, and Kibana colloquially known as the ELK Stack springs to mind, but simply following install guides won't sate the more curious and capable security minds on your team. Encourage your SOC teams to build homegrown tools like custom decoders and packet analyzers that make repetitive SOC tasks easier, which are two examples we've seen. Contributions to the broader security can also take the form of threat intel community sharing, which allows your firm to help others facing the same incidents as you.
- **Use formal job sharing and rotation programs to broaden your team's skills.** These programs should allow security team members of various levels to jobshare across other departments. Send security personnel with scripting skills to ride along with application developers, and vice versa. Let S&R pros with skills in statistics sit beside data scientists, and send those with system administrator backgrounds to spend time with cloud administrators. These programs will introduce new roles to security team members, build culture through new perspectives, and identify potential new talent to the security team. This will help security team members who might otherwise get discouraged by the repetitive components to their jobs keep their advancement possibilities top of mind.

## Use AI, Automation, And Cyber Ranges To Elevate Security Pros

Technology also plays a pivotal role in security talent, and AI, automation, and cyber ranges offer substantial relief for overburdened, underskilled, or understaffed security teams. While security vendors have overblown the capabilities of AI and automation tools, these capabilities augment human security pros to increase capabilities and capacity. Many security pros wrongly believe that security requires human analysis and decision making at every step; thus, many SOC processes remain manual or employ minimal automation. To maximize efficiency and get the most out of limited staff automation becomes a necessity. In 2018, 51% of global network path security decision makers were implementing or expanding/upgrading implementation of security automation and orchestration, with an additional 20% planning to implement in the next 12 months.[5] Cyber ranges allow the team members you have today to sharpen their skills without the risk of failure. S&R pros should look for technology solutions that:

› **Use automation to reduce the grunt work done by security analysts.** Security automation and orchestration (SAO) solutions orchestrate security processes and automate activities, allowing teams to work faster and more accurately. SAO tools like those provided by vendors like FireEye, Palo Alto Networks, Splunk, and ThreatConnect deliver customizable playbooks that automate such SOC functions as event triage, context gathering, and response.[6]

› **Elevate less-experienced analysts with AI and machine learning tools.** Your more numerous entry-level analysts will naturally pass difficult investigations to more senior analysts, which creates investigation bottlenecks. Augmenting these less-experienced SOC operators with AI and machine learning tools gives them the information and guidance to continue investigations themselves so that they don't need to escalate as many incidents to their more-experienced colleagues. Solutions like IBM Watson, Jask, and Patternex augment human analysts with intelligence to provide needed intelligence and guide the investigation process.

› **Use cyber ranges to sharpen security skills without the danger.** Far too many security analysts learn on the job by making costly mistakes classifying or responding to an incident. Use cyber range technologies to reinforce operations-focused training. Also, thanks to virtualization technologies such as Hyperqube, your forensics and remediation team members can engage in virtual response operations to hone their skills. Try cyber range offerings from companies like SimSpace, or IBM's new Cybersecurity Training Operations Center (CTOC), which brings a mobile facility with training, simulation, and crisis management capability on wheels.

**Recommendations**

## Heal Your Self-Inflicted Wounds By Changing Your Hiring Processes

Alleviating the staffing pressure you may be experiencing requires not only that you invest in people, but that you also remove your explicit — and implicit — biases. Expand your search to include people and locations that you may have not previously considered. This approach also guarantees a more diverse workforce with new perspectives. To overcome "the cyber security talent shortage":

› **Network with local talent at regional security association events.** Recruiting is like marketing: Lead generation matters. Contributing to, sponsoring, attending, and meeting security practitioners through cybersecurity organizations like the ISSA, and at B-Sides and other local security meetups, is a great way to network, develop name recognition, and increase your potential candidate pool. Some of the people attending these events may be looking for a job. And you can build relationships with people who are investing time to improve their security skills who may be candidates in the future.

› **Commit to inclusive hiring practices.** Make sure that your hiring managers are recruiting from diverse populations. For example, many recruiters today limit their searches to colleges with strong computer science programs or hackathon events. Despite the candidates possessing

much talent and promise, these pools are often almost entirely men; they also don't showcase the full scope of skills necessary to excel in the cybersecurity industry. Expand your job descriptions and job qualifications to search for skills that go beyond technical certifications and technical abilities. Unteachable qualities like communication and creative thinking can be equally crucial for cybersecurity success and will expand your potential candidate pool.

- **Expand your horizons and consider remote options.** Affordable security talent may not be located near your corporate headquarters or technology hubs. If you're only looking for talent in very competitive markets like Dublin, San Francisco, or Singapore, the talent pool will be scarcer and salary demands will be higher. If the position for which you are recruiting can be done remotely, look for experienced talent who may not be willing to move but who can do the job from home. This approach may not work for every job or every person, but it will give you more options to consider as you build your team.
- **Drop default requirements for college degrees.** There are many highly skilled, experienced cybersecurity pros who don't have university degrees. Companies like Apple, Google, and IBM recently dropped their requirements for university degrees because they recognize that the top tech talent may not have them.[7] Technical schools, community colleges, and specialized bootcamps offer cybersecurity and computer science programs that teach hands-on skills.[8] You may have to convince HR and senior leadership, since the bias toward university qualifications may come from the top.

## Supplemental Material

### Companies Interviewed For This Report

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

Expel

## Endnotes

[1] Source: "Information Security Analysts," Bureau of Labor Statistics, June 14, 2019 (https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm).

[2] Source: "Cybersecurity Workforce Shortage Projected At 1.8 Million By 2022," (ISC)² Blog, February 15, 2017 (https://blog.isc2.org/isc2_blog/2017/02/cybersecurity-workforce-gap.html).

[3] Source: Michael Hiltzik, "Employers will do almost anything to find workers to fill jobs — except pay them more," Los Angeles Times, July 10, 2018 (http://www.latimes.com/business/hiltzik/la-fi-hiltzik-employment-20180710-story.html).

[4] Source: "Apprenticeships," BAE Systems (https://www.baesystems.com/en/careers/careers-in-the-uk/apprenticeships).

[5] Source: Forrester Analytics Global Business Technographics® Security Survey, 2018.

[6] For more information about SAO vendors and their capabilities, see the Forrester report "Now Tech: Security Automation And Orchestration (SAO), Q3 2018."

[7] Source: Courtney Connley, "Google, Apple and 12 other companies that no longer require employees to have a college degree," CNBC, October 8, 2018 (https://www.cnbc.com/2018/08/16/15-companies-that-no-longer-require-employees-to-have-a-college-degree.html).

[8] Source: "The 20 Best Associates In Cybersecurity Online 2019," Best College Reviews, August 2018 (https://www.bestcollegereviews.org/top/online-associates-cybersecurity/).

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

## We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

## Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

**Marketing & Strategy Professionals**

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

**Technology Management Professionals**

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

**Technology Industry Professionals**

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.



150055