Building a Cybersecurity Workforce

MIKE GOFFIN, INTELLIGENCE LEADER, INFORMATION SECURITY

In This Paper

Introduction: Building a Cybersecurity Workforce

Invest in your future workforce by engaging with schools and colleges in innovative ways.

There is a substantial gap between what new workers expect from their employers and what their employers expect from those early in their career. This gap hurts both job seekers entering the workforce unprepared for the realities of work and corporate cybersecurity organizations who have unrealistic expectations of new graduates' capabilities.

Cybersecurity organizations are rich with nuanced and unique roles, yet students are graduating with broad, foundational cybersecurity knowledge that does not help them get those jobs nor does it help them to be effective to meet the rigors of the work once placed. With a threat landscape that continues to grow and evolve at breakneck speed, and a 4 million unfilled cybersecurity jobs to meet this need, corporations would be wise to take a more proactive approach to nurturing a future workforce.

Cisco is committed to helping people find opportunities in the growing disciplines of cybersecurity, AI, and more. We are expanding our cybersecurity and digital skills program across the EU to equip 1.5 million people with the skills they need to thrive in an AI-driven future. Learn more.

Get Them Early: Show High Schoolers the Possibilities

High-school students are expected to choose a college based on their intended majors and, by extension, their intended careers. Yet high-school students may not be aware of what a career in cybersecurity entails, if they even know these careers exist. Students are left to rely on their own personal research, requiring them to know what roles and functions encompass cybersecurity. But there are a lot of esoteric roles in cybersecurity. While most students may have heard of incident response, few are probably aware of detection engineering, threat hunting, threat intelligence, malware analysis, or other specialized roles in the field.

Without this information, high-school students can find themselves applying to colleges that may not prepare them for the cybersecurity work that best suit them or the needs of future employers. Conversely, students who might have a true affinity for cybersecurity and could be valuable assets to employers may never consider the career due to the mistaken belief that all cybersecurity roles involve requirements they may not prefer, such as coding or shift work, not realizing that many roles involve neither.

Seed the Future Workforce

To avoid these repercussions, corporations should partner more actively with high schools. Job fairs are already common, but they are usually limited to a company representative delivering presentations and answering questions. This provides only limited exposure to the true nature of the industry.

Instead, virtual job fairs with live sessions, Q&As, and videos explaining various cybersecurity roles would help students understand the opportunities available in cybersecurity. Meet the students where they are: Stand-up events on a Twitch stream; make reels on various social platforms; produce YouTube videos or memes of specialists explaining their work. Be innovative in how you communicate with students and do so in ways that will reach them.

Companies can also offer on-site tours that highlight the various departments and roles within the cybersecurity organization. A face-to-face experience can open the students' eyes to all the possibilities in cybersecurity and help them make the best decisions about choosing their college curriculums and direction.

The Disconnected Degree: Help Modernize College Programs

Cybersecurity degree programs tend to lag behind real-world needs. Threat actors evolve their tactics, techniques, and procedures faster than coursework can be created and delivered to teach how to counter them. For example, AI use is common in security tools yet uncommon in college programs. This lag leaves college students unprepared for the job market and often unhappy at their first jobs, or worse, disillusioned with their career choice.

Bundling all cybersecurity specialties into one general degree that only equips students with foundational skills is not an effective approach to preparing students properly for the workforce. Compare the technical expertise required of a reverse engineer to the knowledge and skills required of a threat intelligence analyst. An aspiring reverse engineer may be best served by taking specific technical classes early in their academic career, rather than devoting time and tuition to two years of general education classes. On the other hand, a prospective threat intelligence analyst benefits from those general education classes, which teach the history and political controversies necessary to contextualize and attribute malicious activity.

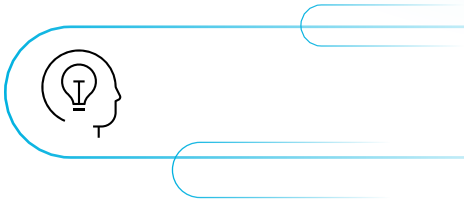
Historically, colleges have set the pace in training future workers. But colleges are not tightly aligned with the rapidly evolving needs of the cybersecurity industry. For instance, a corporation might need a malware analyst. The hiring manager expects a new graduate to show up with hands-on experience in assembly language, reverse-engineering tools, central processing unit (CPU) architecture, and general purposes programming languages such as Python, and perhaps Rust. But new hires that have graduated with only broad theoretical knowledge of these technologies are not sufficiently prepared to perform the job. And unlike in college, there are no study groups to help—coworkers are busy with their own jobs and the new graduate must figure out these complicated skills alone. This is how new grads become frustrated, resentful, and stalling out.

> "When students struggle to complete a degree, they have become disinterested in, they may feel like a cybersecurity career is a bad fit for them. The truth is that cybersecurity can be many things and there is a need for all types of minds."
>
> **Mike Goffin, Intelligence Leader, Information Security**

Contribute to College Curriculums

Colleges need a chance to collaborate with corporations to understand emerging trends, determine the requisite skills to meet these developments, and anticipate what the cybersecurity team of tomorrow looks like to start developing the workforce today. Conversely, corporations should be trying to work with college professors and deans to design curriculums packed with relevant skills and offer students chances to learn about and interact directly with modern and emerging technologies.

Corporations should also be thinking of innovative ways to work directly with students. Stand up security competitions that give participants access to, for example, Splunk Enterprise Security, so they can learn about risk-based alerting or provide threat-hunting opportunities for students to use Splunk's PEAK threat hunting framework. These same opportunities should be open to instructors as well, so they can understand these technologies, prepare lessons, and teach novel techniques to their classrooms.



These same ideas are relevant for college students. Deliver virtual job fairs with live sessions, Q&As, and videos explaining the distinct cybersecurity roles, and provide both virtual and on-site tours that can help students understand what life is like for cybersecurity professionals, as well as differences in corporate culture.

Limited Exposure: Internships

Internships are meant to provide students with real-world experience. But in cybersecurity, interns can only get a taste of the real-world, as there is too much at stake to allow interns free rein. The reasons for these limitations are well-founded, but the result is limited learning.

Some interns shine anyway, because they possess exceptional technical skills or are passionate about and dedicated to learning new skills. Technical skills are less critical, as current leaders can rather quickly teach someone the required skills and techniques to be, say, a detection engineer. We have documentation, e-learning, videos, and leaders on the team who know how to help people get started and progress through their careers. But a passion and dedication for learning cannot be taught. Team players who are excited to work, who are driven and thirsty for knowledge, skills, and experience are the ones a manager can trust to reliably give their best and excel at their trade.

Those Who Can't, Teach? Instructors Struggle to Stay Relevant

Instructors from leading colleges may participate in conferences and other learning events, though not all institutions will pay to send their instructors and even fewer will send adjunct instructors.

So how can an instructor keep his or her industry knowledge and skills up to date? Cybersecurity is not like science or math, where the foundation is evergreen. Consider tenured professors whose experience is entirely in networking. Can we expect them to research, train, and acquire enough mastery of a topic like Artificial Intelligence (AI) that they can then teach it to their students? That is an unrealistic expectation considering how much work they already must do to prepare their current syllabuses, course materials, and lectures. Researching new fields and innovation becomes a non-starter. Even if they can find the time and energy to acquire new understanding, their knowledge is generally all theoretical unless they have access to a corporate infrastructure on which to practice these new skills.

Teach the Teachers

Corporations need to think innovatively about how to help instructors stay current. For instance, companies could add a training track to their educational offerings that is only open to .edu emails and provides a sandbox to experiment with modern tools as part of the training. They could invite instructors to on-site tours exclusively for educators, develop vendor-agnostic webinars and training materials that could be incorporated into syllabuses, and sign-up instructors to receive collateral—such as annual trends and the hottest skills reports—that will help educators understand where the cybersecurity industry is heading.

Transition Challenges: New Hires are Frustrated and Worried

Generation Z (Gen Z) employees tend to change jobs at twice the rate of other demographics, so employers already face a challenge in retaining early-in-career workers. Add in the fact that a majority of first-time workers report feeling lost, anxious, and exhausted on the job, and it's clear that companies face difficulties in meeting the needs of new grads. While losing a seasoned worker has a greater financial and productivity impact on a team, turnover among new graduates can result in the loss of potential future leaders and encumber the department with a reputation for instability. The great majority of Gen Z job seekers will not apply to a company that has poor reviews on the job message boards, social media, and industry forums.

A primary challenge is to find the right graduate for the role. New job seekers complain about positions tagged as "entry level," yet require years of experience with a particular technology. This happens when the job description is based on the skills of the person who vacated the role. That person had two or three years on the job to grow his or her skill set, and an employer is not going to write a job description that rolls back the requirements by that timeframe—hiring managers do not want to lose ground. So, the job requirements seem rational based on the needs of the position yet are absurd to new graduates who could not possibly have that experience. This is why companies complain about not being able to find new graduates to fill junior roles, when the problem is inherent in the jobs' requirements and the hiring manager's expectations.

Proactively Aid in Curricula Development

If corporations partnered more closely with colleges to write educational curriculums, they would have accurate baseline standards and expectations of new graduates and could write more realistic job descriptions. That would set up new workers for success and facilitate smoother and happier introductions for first-time workers to the working world.

"That sounds great, how do I develop my career like that?"

Read job descriptions for the roles that interest you. Note the tools and skills in those descriptions and start doing them. Do them at your job if you can and do them in your personal time as well. You have a lot more power in a job interview if you can say, "I am already practicing these skills you require."

Career Progression or Career Oppression: Rethink Leveling

One out of five workers leave because they do not see opportunities for career advancement. In cybersecurity, that lack of clarity can be even greater for new graduates because the roles are so complicated.

Career growth is typically presented in a table with columns: for instance, the left column describes a junior analyst, the middle describes a senior analyst, and the right column describes a principal analyst. That predictable career progression can seem restrictive to a new graduate, who is still exploring his or her talents and preferences. We need to offer new graduates—and truly all employees—roadmaps of how their choices and the experiences, skills, and techniques they acquire can lead to opportunities that will catapult into a career.

Career Advancement as Career Adventure

A better way to help new workers understand the possibilities would be to present the progression as a "Choose Your Own Adventure," approach where if they develop X new skill, this new path will open for them, and if they add this Y skill, these other paths will also become available for them. If they learn to respond to alerts in their work as a junior analyst, and that sparks an interest in learning how alerts are created, then they can acquire the foundational skills required to become a junior detection engineer. Once they acquire that skill, they may become interested in figuring out the behaviors that trigger the creation of alerts and now are on track to work in threat hunting or threat intelligence. They have made themselves not only more valuable to their employer, but they are also more appealing to other potential employers.

3 Takeaways

1. Provide students—both high school and college—with the ability to engage with people in the industry so they can learn about the broad variety of cybersecurity careers. Help them understand how to progress from entry-level work to senior work and talk to them about how emerging trends might impact their choices.

2. Companies should sit down with college deans and department heads in relevant fields and share, “This is what we’re seeing today, and these are the skills we need. What questions can we answer for you? How can we make sure the degrees you’re offering are helping students to help us meet these challenges today and with emerging innovation in the future?”

3. Give students and professors opportunities to interact with the technologies we use today, such as Splunk Enterprise Security. Then, while being recruited, more candidates will be able to show they have an understanding and hands-on experience with the tools the company relies on. Rather than having to learn cybersecurity basics on the job, these new graduates will be able to contribute and be valuable team members of the team from Day One.

©2025 Cisco Systems, Inc.