Developing cybersecurity talent and teams

Experts weigh in on closing skills gaps, building training programs and creating stronger teams.

INFOSEC™

How to better recruit, develop and retain cybersecurity talent

Building an effective cybersecurity team and keeping their skills sharp isn't easy, especially as the demand for seasoned cybersecurity professionals continues to grow. However, some organizations are overcoming these challenges, and in some cases, creating big wins around recruiting, developing and retaining their cybersecurity talent.

Those wins were one of the key topics at our Infosec Inspire Conference. We assembled an all-star team of experts — from Raytheon and Booz Allen Hamilton to JPMorgan Chase and the National Initiative for Cybersecurity Education (NICE) — to share their successful strategies with other team leaders.

This ebook contains key takeaways from each of their sessions at Infosec Inspire, as well as links to recordings of the full conversations and additional team training resources. We hope it helps you upskill and strengthen your own team, and we encourage you to share any successes you have with the community.

Learn from industry experts

Jessica Amato
Operations Manager, Raytheon Technologies

Romy Ricafort
Senior Director Sales Engineering, Comcast Business

Katie Boswell
Director, KPMG Cyber

Jason Jury
Lead Associate, Booz Allen Hamilton

Karl Sharman
Head of Cybersecurity Solutions & Consultancies, Stott and May

Danielle Santos
Program Manager, National Initiative for Cybersecurity Education (NICE)

Leo Van Duyn
Cybersecurity & Technology Workforce Development Strategy, JPMorgan Chase & Co

Contents

1 Fix the talent pipeline

2 Upskill employees

3 Build strong teams

4 Close your skills gap

5 Develop talent and teams

6 Resources

FLIP THE FUNNEL

Fixing the cybersecurity talent pipeline challenge

Organizations of all sizes are dealing with a critical challenge: the demand for cybersecurity talent continues to grossly outpace the supply of available and qualified cyber professionals. An Information Systems Security Association and ESG Research Report found that 71% of respondents feel the cybersecurity skills shortage has impacted their organization either “somewhat” or “significantly.” This has led to an abundance of unfilled roles, recruitment challenges, costly churn rates and burnout amongst security professionals.

While most agree that the skills gap is a significant challenge, a deeper look at the problem exposes a more fundamental issue. There is a lack of candidates who meet the experience and certification requirements often listed in job descriptions. Some believe that the problem is bolstered by employers in search of elusive “unicorn” candidates who meet seemingly unrealistic job requirements such as advanced certifications and extensive years of hands-on experience. These are rarities in such a strained market.

Opinions aside, what’s missing is actionable guidance to help fill vacant cybersecurity roles. Karl Sharman, Head of Cyber Solutions & Consultancies at Stott and May shares what successful security and IT leaders are doing to improve recruiting, hiring and retention.

Rethink how job descriptions are written and be open-minded about experience requirements

Seventy-six percent of cybersecurity roles take more than eight weeks to fill, according to Karl. In some cases, these positions remain unfilled for over six months, leading to wasted time, costs and prolonged security vulnerability within entities. This is a stark contrast to the increasing unemployment rates plaguing other industries during an ongoing pandemic.

A few companies have discovered a secret to overcoming this challenge: rethinking stringent candidate experience requirements. Fifty-eight percent of companies who successfully fill roles consider inexperienced candidates for open roles. Before writing a job description, it’s important to ask: “What are the three hard skills and soft skills we need in this role?” Focus on those. Everything else is not as relevant at this stage.

Have a plan for developing less-experienced workers

Companies often want to hire highly experienced cyber professionals to avoid risk. After all, the stakes are high. A simple mistake made by an inexperienced security employee can lead to breaches, financial consequences, brand damage and more.

While larger companies may be willing to take on this risk, this decision gets even harder for small and medium-sized businesses. No matter the size of the organization, take these steps to set yourself up for success.

- Work with your HR team to make sure you source the right budding talent, based on your needs.
- Incorporate skills demonstration projects into the hiring process. Companies seeing hiring success in filling cyber roles were 433% more likely to use projects in the hiring process.
- Ensure inexperienced hires are prepared to deliver on expectations through training and development programs. Partner with third-party

training providers to scale development efforts.

- Pair junior team members up with experienced mentors for reciprocal development benefits.
- Look at the talent you have within your company and consider upskilling internally.
- Assess employee skills and establish development pathways for employees within and outside of tech.

These steps provide a host of benefits, including cost savings associated with hiring less expensive labor, decreased turnover due to loyalty from employees who are appreciative of the investments made in their development and more.

Maintain a high-quality talent pool by looking beyond the resume

As companies widen selection criteria, there may be concerns around whether this reduces the quality of the talent coming into the company. Addressing this concern requires looking beyond the traditional resume to pinpoint the core hard and soft skills required to be considered a qualified candidate. Then, build consistent screening processes that encompass the following actions:

Conduct assessments: Require technical skills assessments to get a more accurate and consistent sense of candidate capabilities. Though often considered a larger time investment by all involved, this can also shed light on the true dedication of candidates and their interest in joining your team.

Examine culture fit: Hiring managers who consider culture fit important are more likely to be successful at filling roles than others. During interviews, consider whether the candidate is a good culture fit. Conduct video interviews as early in the process as possible to get a better feel of the personality and style of candidates.

Tackle bias: Be sure to proactively address potential biases in your hiring process. Create a consistent framework for evaluating candidates and get opinions from multiple people on trends in what a “good” candidate looks like from a skills and culture perspective. Also, be intentional about who you include in the interview process and ensure it’s a diverse slate. Train all involved in the process of recognizing and overcoming personal bias.

> “It’s so important to get the culture fit right. It’s also important to gain everyone’s opinion.” – Karl Sharman, Stott and May

As companies continue to hunt for highly experienced cybersecurity professionals, many question whether the industry is ready for an entry-level market. Though cyber enthusiasts are interested in breaking into the industry, it’s tough for candidates to get a job without experience. Companies are getting ahead of the talent challenge by embracing inexperienced workers with healthy caution and guardrails — and it’s working. These companies are seeing lower attrition rates, decreased cost associated with turnover, higher employee engagement and more satisfied and loyal employees.

The bottom line is that rethinking hiring processes and traditional job requirements are critical keys to filling the talent pipeline gap.

Upskilling to deepen employee engagement & retention

Having a highly-skilled, engaged and motivated workforce is in everyone's best interest, and it takes a combination of factors to support employees in becoming their best. Doing so requires that organizations engage their employees with learning opportunities, progression paths and strong mentorship. Employees also have a responsibility to be self-motivated in owning their career development journeys.

During Infosec Inspire, Jessica Amato, Operations Manager at Raytheon Technologies, and Romy Ricafort, Senior Director of Sales Engineering at Comcast Business, shared their strategies for developing strong, effective teams through empowerment and progressive development opportunities.

Engage, motivate and retain cybersecurity talent with an employee-focused talent development strategy

Building and retaining well-qualified and effective cybersecurity professionals to deliver on your cybersecurity needs requires three key steps:

1. Know how employees can get the foundational skills required for in-demand security roles.
2. It's not good enough to just focus on basic skills in the beginning. Aspire to upskill and be ready to continually grow skills to meet evolving demand.
3. Foster an environment that allows employees to be curious and learn about their interests.

There are a few key actions organizations can take to help make those steps a reality:

Outline career paths: Establish learning and growth paths to give employees a career line of sight. Employees with this insight tend to have greater confidence in their skills, longer retention rates and higher job satisfaction.

Train employees: Empower employees to achieve the necessary certifications to deliver on your needs through training. Leverage partners to build on the certification programs and provide training in specialized areas.

Look ahead: Think about the future and the skills needed within 3-5 years and conduct a gap analysis against your current workforce. Create development plans, then incorporate those skills as early as possible.

Set expectations: Clearly articulate job expectations and success measures on an ongoing basis, so employees know what they need to do to not only perform well but also exceed expectations and get to the next level.

Prioritize listening to feedback from employees and address feedback promptly

Engaging and motivating employees with training and development programs requires continuous listening and application of feedback. Gain an understanding of what types of learners you are dealing with.

Not only do people learn in different ways, but there are also many different paths to growth in cybersecurity. For example, there are those who aspire to be penetration testers or incident responders and those who aspire to be managers and leaders. Each path requires different skills and unique learning approaches.

> "Dale Carnegie Training Foundation found that 60% of employees would leave their company if there was poor training."
> – Romy Ricafort, Comcast Business

To get a sense of the prevalent learning desires, styles and requirements in your organization, have your leadership team collect input from staff to learn of the gaps and opportunities for improvement. Create a safe space for employees to voice concerns. Also, remember that it's not good enough to collect data and do nothing. Listen and then do something to address the feedback, even if small. Make sure you check back in and follow up with employees to ensure you took the right actions. "Listen to the voice of your learners and take action," says Jessica. "A little bit of change is better than no change at all."

Think about professional development beyond cybersecurity skills

It's important to build an in-depth employee engagement program that spans beyond cybersecurity. After all, technical cybersecurity skills are but a portion of the important qualities that make a strong security professional. To establish a robust engagement program:

- Don't neglect the essential skills that round out talent. For example, presentation skills, executive presence and communication skills though not technical in nature, are arguably equally important.
- Provide opportunities for holistic on-the-job training and job shadowing.
- Help people connect with the bigger picture and understand how their contributions fit into the broader organizational mission.
- Provide organic opportunities to network and cross-collaborate across departments.
- Encourage employees to be self-motivated and dedicated to driving their own career growth.

Build partnerships with organizational units within the company and track key metrics to scale development and engagement programs

They say that two heads are better than one when it comes to tackling tough challenges, and the cybersecurity talent engagement is no exception. Strengthen your program by partnering with internal teams who have a vested interest in and ability to influence employee engagement. Groups such as HR, Talent Acquisition, Learning & Development and more can help.

You can also partner with these teams to get insight into blind spots and gaps in your employee skills inventory through employee satisfaction surveys and scores. Check-in on employees and make sure they feel fulfilled in their roles. Within this input, you can then work to address shortcomings. Where possible, leverage the data to intentionally bring diverse working styles and skills together within your teams as well.

> "Experiential learning means providing opportunities for people to use and develop the skills that they've learned."
> – Jessica Amato, Raytheon Technologies

It’s also important to track metrics that can highlight the value of your efforts.

- Track progress of employees’ training completion rates.
- Track employee retention and be sure to conduct exit interviews that provide insight on true reasons for employee departure. Listen to employees.
- Track how long it takes to onboard and hire employees.

All of these data points together can provide key insight into what’s working well and what requires improvement from an employee engagement and retention standpoint.

In conclusion, deepening employee engagement and retention is a long-term investment. Romy perfectly sums it up: “It’s not a destination. It’s a journey.” By creating an employee-focused talent development strategy, fostering talent beyond typical technical skill development and partnering with internal organizational units for greater impact, common engagement and retention challenges impacting the industry can be reduced.

3 tips to build a stronger cybersecurity team

While building stronger security teams isn't rocket science, there are some proven strategies to succeed.

In a discussion at the Infosec Inspire Conference, Katie Boswell from KPMG Cyber and Jason Jury from Booz Allen Hamilton discussed how to build stronger security teams using three key career path development strategies:

1. Well-structured onboarding experiences for new security hires
2. Mentorship opportunities for all employees
3. Ongoing skills development

"We want to make sure that they understand our mission, what we do and why we do it. In addition to that, we also walk them through things like the risk management framework, which is essential for anyone working in cybersecurity."
– Jason Jury, Booz Allen Hamilton

1. Onboarding experience

Jason, the corporate cybersecurity training and development manager at Booz Allen Hamilton, says that one of his roles is to create different learning experiences and development strategies to bridge the gap between the company, the market and the talent.

There are two things his company is doing during the onboarding process. First, it uses skill assessments to help determine where new hires are at in terms of IT and cybersecurity aptitude. Secondly, it uses assessments to determine whether new hires are a good fit.

"Cyber Core is one program we offer at Booz Allen Hamilton helping individuals assimilate into a cybersecurity role," he says.
Katie, the director of cybersecurity for KPMG Cyber, says new employees often join their program straight out of college or technical school. Her organization, through its Cyber Academy program, takes a proactive approach to training staff on cyber issues. According to Katie, KPMG Cyber focuses on learning as much as possible — via internships and the job interview process — about the professionals coming on board. Her organization figures out what new recruits learned in school and what their interests in the industry are. It then offers baseline training for professionals in different verticals.

"We hope that when our professionals come in we've had an opportunity to get to know them — perhaps through an internship program and through the interviewing process," she stresses.

"We have a good idea of where, within our communities in cyber, they're going to fit. So then we have a baseline training for each one of those areas. For instance, if you come into a community where the majority of your work is going to be around identity and access management, then we have a course specifically built to enable you to get that foundational knowledge."

2. Mentorships

Both KPMG Cyber and Booz Allen Hamilton believe strongly in mentorship programs. It's especially important that mentor-mentee pairings exist at all levels of the company — and that those who participate do so voluntarily. "It's one thing to take a training," says Katie. "It's another thing to actually feel like you're able to apply it to your day-to-day job. That's where that mentorship is really important. If new workers come up against issues where they're not sure what to do, they have someone to call or email to seek advice."

Katie adds that the mentor-mentee relationship isn't just for newbies learning the ropes. It exists in different forms, up to the most senior professionals at KPMG Cyber. When done well, both mentors and mentees benefit. "Mentorship is definitely not just at a new-joiner level," she says. "It's something that exists up through our most senior professionals in different service areas. We have a really strong leadership team to support our senior professionals."

"Our mentorship program gives senior team members an opportunity to grow our professional talent and ready the next generation of technical specialists." – Katie Boswell, KPMG Cyber

Booz Allen Hamilton brings in seasoned practitioners to meet with the participants of its Cyber Core program as well. Previous program graduates return to share how they're using the skills that they learned through the program."Mentors literally just went through the same program, so they understand the process and the ecosystem we're using," Jason says. He adds that the hope is those who complete the program will return at some point to become mentors to new recruits.

3. Ongoing skill development

After a company hires an employee, the skill development process begins. And it never ends. In addition to onboarding, the company and the employee have to commit to ongoing training and skills development that will ultimately boost performance, increase workplace morale and heighten knowledge of policies and objectives.

"We've shifted gears and are focused on the top skills that are in demand versus prescriptive career paths," says Jason. "Our cyber learning website is structured to touch on the top categories. That can be offensive cyber, that can be defensive cyber, cyber engineering or risk management framework. Once you go into one of the sites, we introduce you to the overall definition of that space."

According to Katie, KPMG Cyber aims to give employees at all levels a variety of options — and on-demand content is especially useful since workers can access it when they want. "We also make it a part of our program to involve leaders at different levels," she says. "We're very oriented around the services we deliver. For instance, we know that building privacy professionals is going to be important to us. So to do that, we make sure we have some of our most senior privacy professionals involved in the building of our learning paths and the content of those ongoing skill development courses."

CLOSE YOUR SKILLS GAP

Putting the NICE Workforce Framework for Cybersecurity to work

If you're looking for a blueprint that classifies, manages and explains cybersecurity work, the National Initiative for Cybersecurity Education (NICE) has the answer you're looking for.

As demand for skilled cybersecurity professionals continues growing, the ability to better identify, recruit, develop and retain your employees is a critical advantage. One way for your organization to accomplish this is through NICE's Workforce Framework for Cybersecurity.

Danielle Santos, program manager for NICE, and Leo Van Duyn, cybersecurity and technology workforce development strategist for JPMorgan Chase & Co., weighed in on the issue and explained how to provide role-based training and develop custom role profiles to match your company's needs.

NICE Framework goals

According to Danielle, one of the objectives of the NICE Framework is to assist organizations in hiring, training and holding onto their cybersecurity staff.

"Every day, there's a new threat vulnerability tool introduced, and so the framework really takes an agile approach and creates these building blocks that can be flexible enough to address that ever-changing ecosystem." – Danielle Santos, NICE

"But it also helps learners, and when we talk about learners, we're referring to anyone who's in that learning life cycle, whether it be students or job seekers or even current employees," says Danielle, who adds that the four attributes of a NICE Framework are agility, flexibility, interoperability and modularity.

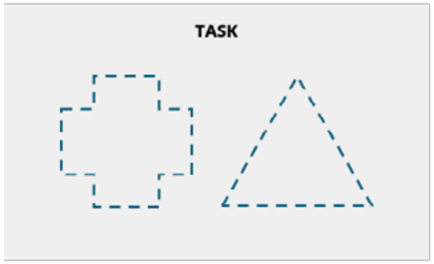
Leo acknowledges that the NICE Framework is relatively new. In fact, he says JPMorgan Chase & Co has been using it for, at most, a year and a half. He says one of the things his organization liked about the blueprint right away was that it provided a solid starting point for figuring out what was required as per specific cybersecurity roles.

"What that allowed us to do was then expand upon that and describe the different functions that we had within our organization and align them with the expectations for that particular role," he says. "By doing that, we were then able to collect the employee data to better understand where they fit within their current position."

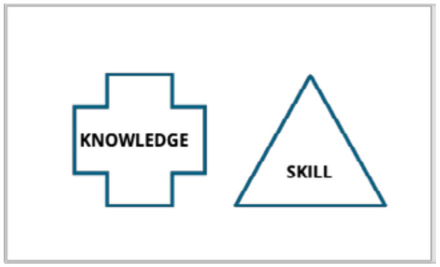
"Once we have that profile, it really then allows you to start doing a gap analysis as to where people are proficient within their current job function and where they need assistance or development efforts. It's a really unique way of looking at data, to start coming up with different learning plans and projecting your learning budget for your organization, whether it's a particular business unit, or an entire company. So, it really gives you a unique, data-driven perspective to understand your human capital."

Difference between tasks, knowledge and skills

Asked by the moderator to explain the relationship among task, knowledge and skills in the context of the NICE Framework, Danielle points to a graphic that was created by one of the co-authors of the NICE Framework.



Describes the work



Describes the learner

"On the right-hand side, we have knowledge and skills," she says. "And knowledge and skill statements are probably the lowest-level building blocks. They're the start. And this is what describes the learner. Describing the learner, we have knowledge, which we define as a retrievable set of concepts within memory. So think, for instance, knowledge of penetrating tools and techniques. In addition to knowledge, we have skills. And skills are the capacity to perform an observable action. So think, for instance, a skill in using social engineering techniques. Together these knowledge and skills make up tasks."

Tasks, she adds, describe the work being completed rather than the person doing the work. As well, tasks are activities designed to accomplish a specific objective or outcome.

"The strength of the framework is the ability to manipulate it until you see the use case that describes what you're trying to accomplish." – Leo Van Duyn, JPMorgan Chase

"This is what the workplace managers will build depending on their needs or the objectives for their organization ... So together knowledge and skills build tasks which then get into work roles and work roles describe the work being done. The work roles are not job titles but rather can be [used to] to create job roles, job functions."

JPMorgan Chase first adopted the NICE Framework prior to the rollout of the blueprint's 52 identified work roles. So the company worked with competencies allowing them to focus on logical modular parts that made sense for a position.

"The competencies are great pivot points," says Leo. "They're a good anchor point into learning systems, into certifications, into your work role. So they allow you a good way to pivot from one resource to another, while still maintaining interconnectivity between systems."

Creating custom role profiles

So how can businesses actually use this resource to, for example, structure their own cybersecurity rules and teams?

Leo has actually constructed a pivot table tool that he uses to build out custom roles. And he also has some advice for organizations that are pondering whether to use one of the existing work roles within the NICE Framework or to start from scratch and build their own.

“At the end of the day, if you create roles that use a common taxonomy approach, and you establish your baselines for proficiency expectations, you can begin gathering your employee input,” he says. “And that allows for a lot of creative and interesting ways to deal with that data. The first thing is how do you create learning plans based on that date, and the second thing is can you use it to express mobility options to your employees based on their profile.

“Those two things right there are extremely interesting to companies as they try and keep employees around and have them have second, third, and fourth careers within the company, so that they can continue to develop and continue educating themselves. Then, once you have those profiles established, you can use that to start informing your learning strategy goals for a particular role, or even an organization, if you need to.”

DEVELOPING SECURITY TALENT AND TEAMS

Perspectives from NICE, Stott and May, and JPMorgan Chase

During a Q&A session at the Infosec Inspire Conference, we had the chance to gain valuable insights on developing talent from a panel of leading cybersecurity professionals, including Danielle Santos of NICE, Karl Sharman of Stott and May and Leo Van Duyn of JPMorgan Chase & Co.

We've gathered some of the highlights from an illuminating round of questions and answers.

Recruiting strategies are only part of workforce management. Employee retention and churn are big factors as well. From a practical point of view, how long does it take and how much does it cost to get someone hired and onboarded?

Karl: The average tenure within cybersecurity is about 18 months leading to increased costs associated with more frequent hiring efforts, training and onboarding. Sometimes, this turnover is uncontrollable. To proactively reduce the impact, have a succession plan and pipeline of resources lined up for replacement if needed.

Leo: Reduce churn and associated costs by assessing the skills you have in-house and where your employee strengths reside. Then, analyze how their existing skills fit into roles across the entire company, even beyond cybersecurity. Empower employees to craft their career paths to growth internally before they even think about leaving.

Through the process of identifying what human skill asset you have internally, you can also gain insight into where the gaps are. Then establish processes for hiring to fill the gap. As you hire to fill these gaps, conduct skills assessments and culture assessments to ensure you have a constant way to assess and bring in the right talent. Be sure to work with your HR talent acquisition group to identify candidates who are good fits and keep them on the radar whether they're a good candidate for a current role or future opportunities.

What kind of mentorship programs do organizations offer to help upskill junior or inexperienced members of staff?

Karl: Solving the talent shortage is all about the upskilling and development of talent. Focusing on this leads to increased productivity and better performance from employees. Seasoned employees can connect with those early in their careers to foster a collaborative environment where employees can learn from each other. There is also value in having teammates at the same level partner to share ideas and bring diverse perspectives to initiatives.

Danielle: Create opportunities for organic mentorship. For example, by creating general communities and groups focused on specific demographics, such as women's or LGBTQ groups, mentoring relationships inherently grow out of them. In terms of upskilling, leverage workforce management groups and apprenticeship programs to help people who are not in cybersecurity re-skill and transition into the industry. Mentoring is a critical part of this journey and it's helpful to partner with nonprofits who are already creating these mentorship programs.

One of the biggest problems in cybersecurity employment is the concern that the industry is siloed. The NICE Framework addresses this and aims to standardize roles across the industry. Is this being taken up and are we seeing any progress within the industry?

Danielle: Growing and sustaining global cybersecurity talent requires standardization. The NICE Framework provides a unified way to view and discuss the cybersecurity workforce, create career pathways and develop talent. At least 30 large corporations have endorsed the movement, and the NIST group continues to enhance the program to meet growing needs in niche areas, such as operations technology.

Leo: NICE is a great resource for understanding how someone's background and life experience translates into cybersecurity roles. This is especially helpful for people who have non-traditional experiences, such as being self-taught. In addition, though NICE was built for application in cybersecurity, it can apply to other domains beyond cybersecurity. As you adopt the Framework, think about how it can be leveraged broadly across other areas of the organization, (such as technology) and even internationally.

Karl: Many industries are struggling with talent challenges, and the NICE Framework helps break down barriers. An aspiration we should look to as we adopt the framework is whether we can standardize things enough to effectively hire without job descriptions or a resume. A resume is not enough to judge talent, and people can be biased. The NICE Framework can help us overcome that challenge.

What can organizations do to make sure bias isn't injected into job descriptions and hiring processes?

Karl: The language included in job descriptions is important. Different groups have different interpretations of job requirements and qualifications, and it's important to ensure bias does not impact this process. When you have nine different interviewers involved, for example, everyone has different preferences in personalities, skills and more. To control this, make job description language crystal clear, establish standard grading systems for evaluating candidates and train interviewers on the process to reduce bias. Establishing this level of consistency requires a solid framework, and NICE is a good place to start.

Danielle: Bias can come in many different forms, and the Framework is continually improved to remove this as much as possible. For example, NICE doesn't list specific software or technologies, and region-specific regulations are avoided. This is intentionally done to reduce bias.

For organizations planning to use the NICE framework for the first time and map out job descriptions, what do you recommend?

Leo: NICE gives you a good starting point, but HR and management teams must be on board. The real benefit is in engaging subject matter experts (SMEs) in the process to help you map your jobs out. The challenge is that the Framework can be very overwhelming, especially to those who aren't cyber experts. Set a very focused scope on how you want to apply the Framework to your organization before looping in SMEs.

Given the human resources challenges in cybersecurity, are there any free resources for training and certification?

Danielle: The NICE website has a useful page for people looking for resources. It includes links to low-cost or free cybersecurity learning content, as well as a Frequently Asked Questions page with advice on free scholarships and low-cost programs.

Addressing the challenges impacting cybersecurity talent pipelines can seem like a near impossible feat to solve. However, standardized frameworks, like NICE, are making it easier for organizations to speak a consistent language when it comes to cybersecurity talent efforts. This inherently fosters consistent hiring processes, reduces bias and leads to more streamlined hiring, engagement and retention of employees.

DEVELOPING SECURITY TALENT AND TEAMS

Perspectives from Raytheon, KPMG Cyber, Booz Allen Hamilton and Comcast Business

Organizations of all sizes continually struggle to address modern-day cybersecurity talent supply and demand disparities. Thankfully, there are experts out there who have faced these challenges head-on and have come out on top.

During a Q&A session at Infosec Inspire, we were fortunate to gain expert insight from professionals who have made notable strides in this space, including Jessica Amato of Raythen Technologies, Katie Boswell of KPMG Cyber, Jason Jury of Booz Allen Hamilton and Romy Ricafort of Comcast Business.

Here are just a few highlights from the discussion.

What advice do you have for people looking to transition into a new cybersecurity role?

Romy: Don't wait for someone to push you to do it. If you want a position, learn what it takes to do the job and start preparing for it. It's up to individual enthusiasts to own their path. It's also important to learn from others. Ask questions around how established professionals got where they are and what paths worked for them.

Jessica: You are in the driver's seat of your career. Networking is key. Taking the initiative to make your first connections into the industry is critical. If you see something you are interested in or like in the industry, be curious and talk to those people in your network to learn more. Talk to your mentors to see if the path you have in mind makes sense.

Jason: Explore the various domains of cybersecurity and get a sense of what it means to work in the industry. Narrow your focus and find as many answers as possible on your own, then start reaching out to experts for additional insight.

Jessica: Be vocal about your interests, passions and goals. Companies should also create an environment where people can express that interest. It's beneficial to the organization to listen and help employees transition into these roles within the company instead of seeking external roles.

How do you recruit the right pool of cybersecurity talent?

Katie: Early efforts should start at the campus level. Plan to engage strategically with the right schools that can fill the skill sets you need. If possible, rely on a team of recruiters who can also help you look for niche skills.

Jessica: Leverage partnerships with academic institutions. Also, work with your talent acquisition resources to ensure they understand what skills you are seeking and can help. On a more advanced level, host invitation-only events to bring in qualified candidates and get to know them better. Lastly, work to understand skill sets and levels of expertise needed across the organization from interns and college hires to advanced professional hires. Then, host virtual events to bring pipelines of those pools into your organization in a larger scale fashion.

How can organizations partner with colleges to hire for internships and entry-level opportunities?

Katie: Create a rich pipeline of talent through internships and start the process early. Post internship openings at the beginning of the year so that you have talent lined up and confirmed before the summer season arrives. Also, expand your talent pool to include foreign nationals and students from different backgrounds when possible. Have students begin working on certifications during internships so that by graduation, they are already qualified professionals with both credentials and experience.

Romy: Work with academic institutions across a variety of cybersecurity domains to bring talent in early. Don't neglect to focus on the culture fit of talent as well. Also, note that the strongest candidates will have multiple offers and choices. It's important to get in early, teach them about company and culture, and ensure it's something they want to be a part of.

Has remote work changed the supply and demand within the cybersecurity workforce?

Katie: As more companies embrace remote work, there has been an increased demand for resources to help keep those remote workers secure. From a training perspective, organizations also need to be agile with learning and development in order to continue training efforts in remote settings.

Jason: The shift to remote work has forced organizations to consider how as many programs as possible can be converted and scaled virtually. Prepare for the inherent trials that come with this setup, such as the need for additional production staff and the missed face-to-face experiences that are often necessary to host training labs or teach more hands-on lessons.

Romy: In the past, many employees had two-to-three-hour commutes. In today's environment, where most are working remotely, more people are reallocating that time to engage in development programming. Organizations have a greater opportunity to focus on upskilling now.

In conclusion

When it comes to developing cybersecurity talent and teams, the early bird gets the worm. A common theme throughout the session has been highlighting the need to partner with academic institutions to start building talent pipelines for your organization as early as possible. Establish these programs with diversity and inclusion in mind and be ready to take the agile approach warranted by the dynamic nature of the industry. Keeping these key recommendations in mind will put you one step closer to developing, engaging and retaining the team you need to secure your organization.

Additional resources

- » Infosec Resource Center
- » Infosec webcasts and events
- » Cyber Work Podcast
- » Infosec YouTube channel

Get your team certified

How, when and where they learn best

INFOSEC Boot Camps
CERTIFICATION TRAINING

Live boot camps get your team certified fast — and include an Exam Pass Guarantee.

INFOSEC Boot Camps
SELF-PACED CERTIFICATION

Self-paced boot camps provide high-quality learning that fits your teams' busy schedule.

INFOSEC Boot Camps
CAREER IMMERSIVE

Immersive boot camps help reskill your workforce and build a pipeline of entry-level talent.

Book a meeting

About Infosec

Infosec's mission is to put people at the center of cybersecurity. Through role-guided security training, our platforms — Infosec IQ, Infosec Skills and Infosec Boot Camps — help individuals and organizations protect their data, mitigate risk and empower employees. From security awareness for your accounting team to secure coding training for your developers, we'll help you deliver the right security education to protect your employees and organization.

Learn more at infosecinstitute.com.