OFFSEC WHITEPAPER

Building a Resilient Cyber Team

6 Essential Strategies for Enterprise Cybersecurity Workforce Development

OffSec
The Path to a Secure Future™

The Cybersecurity Talent Gap

Cybercrime is growing exponentially. From ransomware and phishing to supply chain and state-sponsored attacks, cybercriminals are rapidly becoming more prolific, sophisticated, creative, and destructive. Having a strong cybersecurity team in place has never been more critical than it is for today's businesses.

However, recruiting cybersecurity talent has become a daunting challenge. A staggering 60% of organizations are struggling to recruit qualified cybersecurity professionals, while 67% believe that the shortage creates significant risks to their company.[1] This talent shortage could quickly become a cybersecurity crisis, with Gartner predicting a lack of talent will be responsible for over half of all significant cyber incidents by 2025.[2] Even though over 93% of cybersecurity experts and 86% of business leaders believe a catastrophic cyber event is likely in the next two years, 34% say they lack the skills needed within their cybersecurity teams to prevent one.[3] How did we get into this precarious state?

Embracing the cloud and mobile and adopting IoT devices were already putting a strain on cybersecurity resources. Post-pandemic, companies are supporting an unprecedented number of remote workers, which has given cybercriminals a far greater field of attack due to more endpoints and corporate and personal devices, insecure Wi-Fi, remote access to sensitive corporate information, and more. Stress due to work overload, skill shortage, burnout, and low morale is another cause for today's cyber expert shortage. 64% of cyber security leaders have seen a rise in staff turnover, with 20% of cyber security professionals considering leaving their current role in the next six months.[4]

Developing a robust cybersecurity workforce is vital for enterprises to address the evolving cyber threat landscape effectively. So, how can you scale your team? Today, every CISO is hunting for their next cybersecurity unicorn — that perfect professional that has every skill, certification, and demonstrated experience needed to defend the modern enterprise. But realistically, there are very few unicorns in the wild. Instead, CISOs should focus on growing their own unicorns internally by nurturing the current talent they have, working on developing the specific skills needed for their organization, and helping them to grow their cyber security careers and leadership skills.

In this whitepaper, we will present six essential strategies organizations can use to strengthen their defense, enhance their cybersecurity posture, and have a resilient, well-prepared team. We will include valuable insights, practical recommendations, and actionable steps to empower decision-makers and cybersecurity leaders in building a skilled and resilient cybersecurity workforce through skills development.

STRATEGY 1:
Identify Skills and Knowledge Gaps

Knowing what you already have and what you need are critical requirements in this process. There are four key steps you can take to evaluate your team's readiness and prepare individual team members for skill development.

1 Conduct a skills inventory

Identify what certifications team members already have. Then, regardless of certifications, find out what skills individuals have developed and demonstrated. Finally, conduct a practical application and skills assessment during which you require individuals to show their skills on demand and in a testing situation.

2 Evaluate and determine job requirements

Knowing your attack surface is the main priority when it comes to understanding job requirements and identifying essential skills. Conducting a comprehensive assessment of all your assets and points of vulnerability is crucial to gaining insight into your current technological landscape and the overall environment that needs to be protected. Once you understand those elements, you can train and upskill your talent to ensure they have the expertise to protect and fortify your specific environment.

3 Identify performance gaps

You've conducted a skills inventory and performed an asset audit, now it's time to connect the dots. To truly understand the threat landscape and focus on what's important, leaders need to identify where there are existing performance gaps. Based on your current environment, where are you most vulnerable? What kinds of skills and talent are required to manage those vulnerabilities? Do your existing cyber professionals have the skills required, at what level, and do they have the appropriate certifications?

To find out, you need to conduct assessments that align to the skill sets required to protect the technology you have — certifications aren't everything, you need to know without a doubt that your people are competent and can demonstrate the skills required. An individual might intellectually know a process, but if they can't demonstrate it, they might be a liability. Conducting assessments within a lab environment is particularly valuable so individuals can prove they have the skill sets required to protect against a specific vulnerability class. Additionally, AI tools can be used to transform data into targeted, personalized, and improved learning journeys by factoring in an employee's job and experience history, certifications, skills, and qualifications required for different cybersecurity roles.

4 Train vs. recruit

You may hire that cybersecurity unicorn, but the reality of technology and cybercrime is that they are ever-evolving. The moment you stop training and developing your team's skills is the moment they become ineffective — even the unicorns. Having the ability to use an environment where you can conduct experiments and research-focused approaches to testing is critical to effectively managing skills for your team. Additionally, it is essential that you establish mechanisms for ongoing evaluation and determination of job requirements. Categorizing skills and aligning them with appropriate job requirements ensure that the right individuals are in the right roles, optimizing the effectiveness of the cybersecurity workforce.

STRATEGY 2:
Instill Adversarial Thinking

When an adversary plans an attack, they spend more of their time researching the flaws in your landscape than actually executing the attack. By thinking like an adversary seeking to exploit your organization, cybersecurity professionals can adopt a proactive approach to identifying vulnerabilities and weaknesses in systems, networks, and applications. This method encourages cybersecurity professionals to anticipate and understand the strategies, motives, and techniques that malicious actors may employ. This mindset allows for a more comprehensive and effective approach to threat modeling, risk assessment, and vulnerability management.

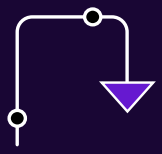
1 Employ the Cyber Kill Chain Model®

One way to instill adversarial thinking is by employing the Attacker Methodology or the Cyber Kill Chain Model,[5] a framework that describes the stages of a cyberattack, from the initial reconnaissance to the final objective. This is a methodology in which cybersecurity professionals can be trained and should be continuously used since your infrastructure is always evolving and adversaries are constantly using new methods of attack. Although different models may have variations, a typical 7-step process for the Cyber Kill Chain includes:

- **Reconnaissance:** Gathering information about the target system or organization such as potential vulnerabilities, network architecture, or employee information.
- **Weaponization:** Creating or obtaining the necessary tools, malware, or exploits to carry out the attack, which can include crafting malicious code or combining existing exploits.
- **Delivery:** Delivering the weaponized payload to the target system through various means such as email attachments, malicious websites, or compromised software.
- **Exploitation:** Exploiting vulnerabilities in the target system to gain unauthorized access or control, for example, by taking advantage of software flaws, weak passwords, or social engineering techniques.
- **Installation:** Installing backdoors, rootkits, or other forms of malware to establish persistence and maintain access.
- **Command and Control:** Establishing communication channels and control mechanisms to manage the compromised system and execute commands, extract data, or perform further malicious activities.
- **Actions on Objectives:** Carrying out the intended objectives, which could include data exfiltration, unauthorized access, system disruption, or any other malicious actions they aim to achieve.

2 Celebrate success and continuous improvement

It's important to keep your team motivated and inspired throughout this process. Gamification and competitions are excellent ways to engage individuals in the process of identifying exploitable findings within the environment. They give you the opportunity to continuously test your team's capabilities in a way that is fun, motivating, and non-threatening. The process is less about winners and losers, successes, and failures, and more about gaining the opportunity to learn. In fact, in this scenario both succeeding and failing ultimately lead to improvement for everyone involved.



STRATEGY 3:
Allow Your Team to Fail, Safely

Failure is a scary word in the security industry — but a breach is inevitable. The important thing is that we understand where we failed so we can better prepare teams for future events.

1 Fail forward

The irony of failure is that it's how we learn and get better. As Albert Einstein put it, "Failure is success in progress." That's why it is important to give your teams a safe place to try, fail and learn. Failing forward is an approach that encourages learning from mistakes and using them as opportunities for growth and improvement. It involves embracing failures as valuable experiences that contribute to enhancing the team's skills and effectiveness in defending against cyber threats.

Using a controlled lab environment, leaders can foster that fail forward motion and create an atmosphere of support and trust so that individuals are learning vs. being punished. They can simulate attacks and conduct offensive exercises to build experience and muscle memory without causing real damage to systems inside the environment. In this scenario, teams are given the ability to celebrate wins and try to understand losses without feeling denigrated or defensive.

2 Bridge gaps and remove boundaries

It's important to cultivate a secure mindset no matter what an individual's role is within the organization. For example, software developers can play a pivotal role in strengthening your cybersecurity. If you train the software development team on secure development and involve them in cybersecurity efforts, you will reinforce a secure foundation for all parts of your organization. By bridging this gap between software developers and cybersecurity teams, you can close static boundaries and siloed efforts. Rather than pointing fingers back and forth, the teams can collaborate to identify where there are deficiencies, learn from those deficiencies, and partner with the appropriate people to help them engage and get better.

STRATEGY 4:
Engage in Continuous Development

In today's rapidly evolving threat landscape, where new risks and vulnerabilities emerge every day, it's essential to develop training plans to cover gaps. This includes fostering long-term growth for the organization by nurturing a culture of learning within your company.

1 Take advantage of resources

In this industry, if you're not continuing to train, educate yourself, and learn new aspects — hands on — then you're going to fall behind, and it's going to show. As part of continuous development, organizations should provide teams with access to resources, knowledge bases, experiences, and more where they can learn, develop, and practice on a continuous basis. Here are two examples of resources enterprises should consider.

- **Third-party training experts** can empower individuals and organizations to fight cyber threats with indispensable cybersecurity skills and resources. For example, OffSec trains cybersecurity teams using real-world network configurations and vulnerabilities. Our labs are updated regularly with the latest exploit vectors for offensive and defensive teams, and we conduct cybersecurity fire drills safely so teams can practice response.
- **Lunch and learn sessions** foster tribal knowledge, a sense of community, and informative discussions, giving cyber teams the opportunity to collaborate, share experiences, and ask questions.

2 Measure success

Continuous development is critical to growing and maintaining a robust cybersecurity team, but how can you measure success over time and why does it matter?

- Setting and tracking goals becomes important in identifying gaps and areas where teams need support.
- Tracking which individuals are upskilling is important as you continue to evolve your cybersecurity team, promote team members, and create new roles.
- If you can track and communicate continuous development, you can showcase business outcomes to executives, e.g., saving the organization money by upskilling and training within the organization or reducing risk because you're identifying more exploitable vulnerabilities and closing gaps.

STRATEGY 5:
Diversify Skill Sets through Collaboration

One approach to strengthening a security team is through cross-training, which involves training team members in multiple areas of expertise. This allows team members from different roles and departments to gain a deeper understanding of cybersecurity practices. Successful cross-training and collaboration can increase efficiency and strengthen the overall security posture of an organization.

Facilitate cross-training and collaboration

There are several ways to accomplish these goals within your organization.

- **Leverage real-world exercises** to cross-train your IT staff to take on security roles, especially for those who have already shown an aptitude for security. This approach can help the organization fill security gaps and build a more robust security team.
- **Organize regular knowledge-sharing sessions** or workshops where security team members and employees from other departments can exchange knowledge and best practices.
- **Involve representatives from other departments** in security training programs and exercises to provide them with a foundational understanding of cybersecurity principles.
- **Encourage rotational assignments or job shadowing** opportunities between security and other departments to foster mutual understanding and build relationships.
- **Establish cross-functional incident response teams** to ensure effective coordination during security incidents or breaches.
- **Promote open channels of communication,** such as regular meetings or forums, to encourage collaboration and the sharing of ideas and concerns.

Benefits of cross-training and collaboration

Diversifying skill sets can be hugely beneficial to employees, helping to broaden their experience and expertise and develop the skills and credentials that make them more valuable in the market and to their employer. It is important to note that skill development doesn't have to be complex or costly. Benefits of cross-training and collaboration include:

- **Creating better connections** between employees at different levels and departments can grow an understanding and respect for different roles, skills, and challenges.
- **Promoting communication** by working closely with other roles and departments can enable security professionals to better understand their needs, challenges, and priorities, which can help align security goals with business objectives and enhance teamwork.
- **Improving incident response** by cross-training team members in response procedures and involving representatives from different departments can significantly accelerate incident containment and resolution.
- **Identifying and mitigating risks** by allowing security professionals to gain insights into the specific risks and vulnerabilities associated with various business processes helps in identifying potential security gaps and implementing appropriate controls.
- **Fostering a culture of security awareness and responsibility** across the organization leads to better adherence to security policies, increased reporting of security incidents, and overall improved security posture.
- **Facilitating knowledge sharing** between security professionals and other roles can lead to innovative solutions, improved problem-solving, and a more well-rounded security team.
- **Leveraging diverse skill sets** of different roles and departments brings unique skill sets and perspectives to the table, enabling your security team to approach challenges from various angles and find creative solutions.
- **Creating a more robust and well-rounded security team** can effectively address the organization's security challenges while building stronger relationships with other departments.

STRATEGY 6:
Encourage Individualized Learning Experiences

Organizations should encourage, support, and even reimburse employees' efforts to further develop their own individual skills and pursue continuous learning and collaboration outside of the organization. Doing so benefits both the individual and the organization by expanding knowledge, fostering personal and professional growth, facilitating networking and collaboration, and promoting innovation and adaptability in addressing cybersecurity challenges.

Examples of external learning opportunities

- **Self-study and taking online courses** to learn new concepts and technologies.
- **Participating in Capture the Flag (CTF) competitions** to help develop practical skills in areas such as penetration testing, forensics, and exploit development.
- **Joining cybersecurity communities** to network, share knowledge, and learn from industry professionals.
- **Mentoring and coaching** for guidance and motivation on skill development, education, and career advancement.
- **Reading reputable cybersecurity blogs, articles, and books** to stay updated with the latest trends, news, and research in cybersecurity.
- **Setting up a home lab** to experiment with various tools, techniques, and technologies and simulate different network configurations and practice hands-on exercises.
- **Contributing to Open Source projects** to collaborate with other professionals, gain practical experience, and improve coding skills.
- **Attending conferences, forums, industry events, and meetups** to network with industry experts, learn about the latest trends, and participate in workshops.
- **Volunteering**, e.g., at nonprofit organizations to help assess and strengthen their security measures; for community outreach programs to educate local communities about cybersecurity best practices; at academic institutions as guest lecturers or mentors for students interested in pursuing a career in cybersecurity; and for government initiatives to support public safety and national security efforts.

Benefits for the cybersecurity professional

Supporting your team's professional development outside of the organization will create more engaged, creative, and motivated individuals. Benefits can include:

- **Enhanced expertise** in emerging cybersecurity technologies, trends, and best practices to stay updated with the latest developments in the field and become a subject matter expert.
- **Expanded skill set and competencies** that may not be readily available within the company to help the employee become more versatile, adaptable, and valuable in their role.
- **Career growth** by demonstrating their commitment to professional growth and development, helping them stay competitive in the job market, and opening up new opportunities for career advancement.
- **Networking and industry connections** with professionals from diverse backgrounds can be beneficial for future career prospects, provide access to job opportunities, knowledge sharing, and staying updated with industry trends.

Benefits for the employer

Encouraging individualized learning experiences beyond the enterprise can have a direct and positive impact on the organization, yielding benefits such as:

- **Enhanced cybersecurity** when employees apply their updated skills and knowledge to protect company systems, data, and infrastructure effectively.
- **Innovation and creativity** when the employee brings fresh ideas and perspectives to the company, which can lead to improved cybersecurity strategies, proactive risk mitigation, and the development of innovative solutions.
- **Knowledge sharing** with their peers fosters a culture of continuous learning within the organization.
- **Employee satisfaction, retention, and motivation** because the company demonstrates its commitment to their professional development.

Create Your Own Cybersecurity Unicorns

You can overcome the cybersecurity talent gap and build a skilled and resilient cybersecurity workforce. The key is investing in the valuable resources you already have by:

1. Identifying skills and knowledge gaps
2. Instilling adversarial thinking
3. Allowing your team to fail, safely
4. Engaging in continuous development
5. Diversifying skill sets
6. Encouraging individualized learning experiences

It takes an average of three to six months to fill a cybersecurity job, and likely far longer if you are pursuing a cybersecurity unicorn. It also takes around three months for a new cybersecurity team member to start demonstrating productivity. Within that same nine months it takes to hire and settle a new team member, your existing cybersecurity professionals could be trained on the specific skills you need for your unique environment. Leaders should think of internal cyber skill building and development as a business investment — something that will not only improve their security posture but also help reduce costs and contribute to employee retention, engagement, confidence, and job satisfaction.

OffSec can help you close the talent gap through training, content, and resources including:

- **OffSec Cyber Range:** The most realistic hands-on, in-depth labs on the market that emulate enterprise environments, allowing your team to hone their technical, mental, and tactical skills in recognizing and handling real-world incidents.
- **OffSec Learn Enterprise:** A learning platform and library that enables enterprise security teams to fight cyber threats better and improve their security posture with indispensable offensive and defensive skills training.

To learn more about how to improve your organization's security posture and drive long-term success through talent development, visit offsec.com.

REFERENCES

1. https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf
2. https://www.gartner.com/en/newsroom/press-releases/2023-02-22-gartner-predicts-nearly-half-of-cybersecurity-leaders-will-change-jobs-by-2025
3. https://www.weforum.org/press/2023/01/geopolitical-instability-raises-threat-of-catastrophic-cyberattack-in-next-two-years/
4. https://www.helpnetsecurity.com/2022/01/31/cybersecurity-teams-retention-issues/
5. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html#:~:text=Developed%20by%20Lockheed%20Martin%2C%20the,order%20to%20achieve%20their%20objective
6. https://www.statista.com/statistics/1322366/cybersecurity-staffing-time-to-fill-vacancy-worldwide/
7. https://www.zippia.com/cyber-security-analyst-jobs/how-to-hire-a-cyber-security-analyst/#

OffSec™
The Path to a Secure Future™